RAND
CORPORATION

Lessons from Others for Future U.S. Army Operations in and Through the Information Environment

CASE STUDIES

Christopher Paul, Colin P. Clarke, Michael Schwille, Jakub P. Hlávka, Michael A. Brown, Steven S. Davenport, Isaac R. Porche III, Joel Harding

For more information on this publication, visit www.rand.org/t/RR1925z2

Library of Congress Cataloging-in-Publication Data is available for this publication.
ISBN: 978-0-8330-9997-6

Published by the RAND Corporation, Santa Monica, Calif.

*Cover photos (clockwise from top left): Giorgio Montersino via Flickr (CC BY-SA 2.0);
U.S. Air Force photo by Airman 1st Class Adawn Kelsey;
U.S. Air Force photo by Tech Sgt John Gordinier;
U.S. Air National Guard photo by Master Sgt Andrew J. Moseley;
Russian Ministry of Defence (CC BY 4.0);
North Korean national media*

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Preface

The information environment (IE) has become more complicated, more extensive, more ubiquitous, and more important to the outcomes of military operations than ever before. Because the U.S. Army does not have the same level of overmatch in the IE that it maintains in the land domain, there is room for improvement and there are opportunities to learn from others. This project sought to draw lessons from the efforts of others (both nation-state and nonstate actors) in and through the IE for future U.S. Army force planning and investment. It was supported by case studies of other forces, presented in this report, that can help the Army (1) identify capabilities and practices that it should consider adopting and (2) identify adversary capabilities and practices that it must be prepared to counter in future operations in and through the IE. The study drew lessons from the practices and principles for operating in the IE in 12 cases: four allies, four state actors of concern, and four nonstate actors of concern. Eight practices and principles are worth emulating:

- generous resourcing of information power and information-related capabilities (IRCs)
- giving prominence to information effects in operational planning and execution
- increasing the prestige and regard of IRC personnel
- integrating physical and information power
- extensive use of information power in operations below the threshold of conflict
- employing the concept of getting the target to unwittingly choose one's own preferred course of action
- carefully recording and documenting one's own operations
- high production values.

There appear to be three reasons for gaps between U.S. Army capabilities and the best-in-breed capabilities of others: capacity gaps, conceptual gaps (where effective concepts have not been adopted), and gaps stemming from authority or ethical constraints.

The study makes the following recommendations to the Army:

- Give effects in and through the IE greater emphasis and priority.
- Promote a view of information power as part of combined arms.

- Routinize and standardize the processes associated with operations in and through the IE to be consistent with and part of other routine staff processes.
- Tie political, physical, and cognitive objectives together coherently in plans, and communicate those compound objectives clearly to maneuver forces.
- In coordination with the U.S. Department of Defense and the U.S. government more broadly, seek expanded authorities to operate in the IE short of declared hostilities.
- Bring more information opertions (IO), military information support operations, and other IRCs out of the reserves.
- Tear down or move the firewall between public affairs and other IRCs.
- Increase the volume and efficacy of education and training in operations in and through the IE and information power to reflect the increasing importance of these capabilities for the U.S. military and the nation, as well as the greater role they will play in future conflicts.
- Take steps to close capacity gaps in key capability areas—including cyber, influence, operations security, and military deception—by making IO and IRC career fields and military occupation specialties larger, more attractive, and more prestigious.

This report should be of interest to Headquarters, U.S. Department of the Army, personnel who are responsible for force planning and capability investment for cyber operations, information operations, and IRCs, as well as information operations officers and members of both planning and operations staffs who might be called to operate alongside or against any of the forces studied. A companion report, *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment*, provides an overview of the research approach and summarizes key findings and insights from the case studies presented here.[1]

This research was reviewed and approved by RAND's Institutional Review Board (the Human Subjects Protection Committee). RAND operates under a "Federal-Wide Assurance" (FWA00003425) and complies with the Code of Federal Regulations for the Protection of Human Subjects Under United States Law (45 CFR 46), also known as "the Common Rule," as well as with the implementation guidance set forth in DoD Instruction 3216.02.

This research was sponsored by Deputy Chief of Staff, G-3/5/7, and conducted within the RAND Arroyo Center's Strategy, Doctrine, and Resources Program. RAND Arroyo Center, part of the RAND Corporation, is a federally funded research and development center sponsored by the United States Army.

The Project Unique Identification Code (PUIC) for the project that produced this document is RAN167283.

[1] Christopher Paul, Colin P. Clarke, Michael Schwille, Jakub Hlávka, Michael A. Brown, Steven Davenport, Isaac R. Porche III, and Joel Harding, *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment*, Santa Monica, Calif.: RAND Corporation, RR-1925/1-A, 2018.

Contents

CHAPTER FOUR

CHAPTER FIVE

CHAPTER SIX

CHAPTER SEVEN

Figures and Tables

Figures

Tables

Acknowledgments

We would like to express our gratitude to our various points of contact and interlocutors in the sponsoring office, originally Headquarters, U.S. Department of the Army, Department of the Army Military Operations, Cyberspace and Information Operations Division, including COL Carmine Cicalese, COL Jeffery Church, LTC Joel Humphries, Patrick Scribner, and LTC John Zollinger. We also thank the RAND publications team, especially editor Lauren Skrabala, for the hard work of standardizing and harmonizing these case studies written by different authors. Our thanks, too, to our quality assurance reviewers, Edward Fisher at the IO Center for Research at the Naval Postgraduate School and Arturo Munoz at RAND, whose valuable comments improved the final version of this report.

Abbreviations

AJP	allied joint publication
AQAP	al-Qaeda in the Arabian Peninsula
AQI	al-Qaeda in Iraq
AQIM	al-Qaeda in the Islamic Maghreb
C2	command and control
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CAF	Canadian Armed Forces
CIA	Central Intelligence Agency
CIMIC	civil-military cooperation
CJOC	Canadian Joint Operations Command
DND	Canadian Department of National Defence
DTO	drug trafficking organizations
EMS	electromagnetic spectrum
EW	electronic warfare
FSB	Russian Federal Security Service
FVEY	Five Eyes (Australia, Canada, New Zealand, United Kingdom, and United States)
IA	influence activity
IATF	Influence Activities Task Force (Canadian Armed Forces)
IDF	Israel Defense Forces

IE	information environment
IO	information operations
IRC	information-related capability
IRGC	Iranian Revolutionary Guard Corps
ISAF	International Security Assistance Force
ISIL	Islamic State in Iraq and the Levant
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
KFOR	Kosovo Force
KGB	Soviet Committee for State Security
KPA	Korean People's Army
MILDEC	military deception
MOS	military occupational specialty
NATO	North Atlantic Treaty Organization
OPSEC	operations security
PA	public affairs
PLA	People's Liberation Army
PSYOP	psychological operations
SACEUR	Supreme Allied Commander Europe
SHAPE	Supreme Headquarters Allied Powers Europe
SLA	South Lebanon Army
StratCom	strategic communication
TTPs	tactics, techniques, and procedures
UN	United Nations

CHAPTER ONE

Israel

Case Summary

Israel and the Israel Defense Forces (IDF) face a near-constant threat from both nation-states and violent nonstate actors in the Middle East. As such, they are compelled to test new ideas and rigorously assess both successes and failures, as well as adapt and evolve appropriately, in the information environment (IE). Israel's military has faced a sharp learning curve when operating in and through the IE. This is partly due to the distinctive emphasis placed on the main audience for its information efforts: its domestic population. This narrow focus has contributed to some critical errors and missed opportunities over time, but like any advanced force, Israel has sought to learn from its mistakes, and, since the Winograd Commission in 2008, there is a much greater focus on coordinating communication and information efforts across the entire government to avoid information fratricide. Furthermore, Israel has worked diligently to both document and explain operations to domestic audiences, and it compellingly refutes false claims that might undermine domestic support. As such, embedded press, combat camera or equivalent, independent journalists, and other sources of transparent reporting and verification have played a vital role in insulating against falsehoods and propaganda.

Background and Overview

Since its founding in 1948, Israel has been a country on the defensive. The IDF, comprising an army, navy, and air force, have fought numerous wars, including the Sinai War (or Suez Crisis) in 1956, the Six-Day War (1967), and the Yom Kippur War (1973). The IDF occupied southern Lebanon for nearly two decades, from 1982 to 2000, when Israel unilaterally withdrew its military forces. And since 1987, Israel has engaged in on-again, off-again battles (including two intifadas) with myriad militant groups—from Hamas to Hezbollah—and launched campaigns against terrorists, including the Second Lebanon War (July 2006), Operation Cast Lead (2008–2009), Operation Pillar of Defense (2012), and Operation Protective Edge (2014).

As a Jewish State in a sea of Arab and Islamic countries, Israel is often portrayed as a pariah by its neighbors in their respective media outlets, although its prowess as a military power is beyond reproach. Interestingly, Israel's more recent setbacks while operating in and through the IE could be related to the country's enduring characterization of itself as an underdog, or David in the "David-versus-Goliath" narrative. Israel is now clearly the Goliath to the Palestinians' David, even if Tel Aviv has struggled to accept this reality and adapt accordingly. Nevertheless, Israel has retained its image as a "nation in arms" defended by its "people's army," a three-tiered system of long-service professionals, conscripts (both male and female), and reservists.[1] With a conscript force, Israeli society remains closely connected to the military and, especially, the institutional army through the *miluim*, or reserve forces.

Concepts and Principles for Operations in and Through the IE

In Israel, "[c]ommunication policies have long been regarded as secondary both by military commanders and political leaders."[2] To be sure, part of Israel's recalcitrance is related to how it perceives its own image in the international arena as decidedly negative, especially among certain elites and intelligentsia in the West. This has reinforced the notion that the domestic audience is the only audience that matters, because no matter what Israel does or how it behaves, it is going to be vilified and critiqued for its behavior vis-à-vis the Palestinians. Israel's focus on securing domestic legitimacy has, at times, consumed the resources and energy of its information efforts. Accordingly, this overt focus on domestic stakeholders has inhibited Tel Aviv's messaging in the international community, thus reinforcing the notion that the domestic audience matters while the international arena is of secondary importance.

Strategic Goals/Vision

Israel considers its military among the most elite in the world, and, as such, the IDF seeks to remain on the cutting edge of military innovation—adapting, responding to, and improving on past performances. As discussed later in this chapter, the IDF is a learning organization and scrutinizes mistakes in an effort to better the force. Lessons learned and best practices are continuously integrated into doctrine, and commissions to investigate occasional failings are launched when necessary. Israel stresses its right to defend itself and is working to improve its global image. A major part of this effort is closer integration and an improved relationship between the government and military.

[1] Stuart A. Cohen, "The Israel Defense Forces (IDF): From a 'People's Army' to a 'Professional Military'—Causes and Implications," *Armed Forces and Society*, Vol. 21, No. 2, Winter 1995.

[2] Thomas Rid and Marc Hecker, *War 2.0: Irregular Warfare in the Information Age*, Westport, Conn.: Praeger Security International, 2009, p. 104.

How Operations in and Through the IE Fit With Israel's Overall Strategic Goals

IDF strategic doctrine is based on the following principles, among others:

- cannot afford to lose a single war
- should seek to fight short wars where possible
- should use political means to avoid war and maintain a credible deterrent posture
- must determine the outcome of war quickly and decisively
- must combat terrorism
- should suffer a very low casualty ratio where this can be achieved.[3]

Operations in and through the IE are at the core of many of these principles, including avoiding war by political means and maintaining a credible deterrent posture, as well as working to determine the outcome of war in a quick and decisive manner. Indeed, at various times throughout Israel's recent history, it seems that elevating the importance of the IE was more of a distraction from the pursuit of more kinetically based military objectives. This has changed over the past decade, however, with the IDF placing a greater emphasis on messaging while recognizing that its adversaries rely on "lawfare"—a strategy of using or misusing law as a substitute for traditional military means to achieve an operational objective.[4]

Targets and Audiences

IDF communication strategies distinguish among three major audiences: national, international, and adversarial.[5] As a nation under siege, Israel must continuously respond to its citizens and explain why the military is undertaking specific operations—for example, to keep the country safe or to defend against rocket attacks and incursions from adversaries. Its international messaging attempts to portray Israel as the victim of continued aggression, although illegal settlements in the West Bank and complaints about proportionality in warfare have made it something of a pariah. Another controversial policy that has affected the country's international reputation is house demolitions, in which the IDF completely destroys the homes of any families linked to terrorists. According to the IDF, as related by Daniel Byman, house demolitions are "a message to terrorists and their accomplices in terrorism, that their acts come at a price that will be paid by everyone taking part in hostile terrorist activity."[6] The Israeli government considers these demolitions a form of messaging in their own right, and, like other IDF messaging efforts, these acts are controversial and punitive

[3] Jane's World Armies, "Israel," May 16, 2016.

[4] Charles J. Dunlap, Jr., "Will 'Lawfare' Define Palestinian-Israeli Conflict?" *Al-Monitor*, July 30, 2014.

[5] Rid and Hecker, 2009, p. 103.

[6] Daniel Byman, *A High Price: The Triumphs and Failures of Israeli Counterterrorism*, New York: Oxford University Press, 2011, p. 166.

in nature. To be sure, these forms of collective punishment have opened Israel up to accusations that it has violated the law of armed conflict and subsequently contributed to high levels of unpopularity elsewhere in the world, including in Western Europe.

Israel's external messaging is focused primarily on deterring Israel's neighbors, including Hamas and Hezbollah but also Iran, from conducting offensive actions that would force Tel Aviv to respond in kind. To be sure, credibility, even among Israelis themselves, has been a recurring challenge. While 82 percent of Israelis trust the IDF, a much lower proportion trust the government and political parties, according to the country's Central Bureau of Statistics. However, trust in the IDF was far from uniform in the most recent polling: The 82-percent average obscures a confidence level of 93 percent among Jewish Israelis and a mere 32 percent among the country's Arab population.[7]

Foundational Principles

Israel has long struggled to differentiate the roles of media spokespeople and its soldiers, and this ambiguity has negatively affected the credibility of certain messages. During the 1991 Gulf War, the editor of *Maariv*, one of the largest Hebrew newspapers, demurred, "I am first of all an Israeli and an IDF soldier, only then a newspaper editor."[8] With respect to "winning hearts and minds," Thomas Rid and Marc Hecker have observed that "Israel has given up on appealing to the benevolent emotions of its opponents." Under this model, international outreach is judged to be futile, since many Israelis feel that world opinion is decidedly set against them and is unlikely to change.[9]

History and Evolution

After a brief history of treating communication and information as secondary, Israel gained a greater appreciation for the importance of operating in and through the IE in the mid-2000s—namely, after the 2006 war with Hezbollah. There is no doubt that the Israeli military has suffered from a disregard for official policy in its own press, with journalists from well-regarded newspapers, such as Haaretz, lamenting the lack of public affairs (PA) policy within the Israeli army. At times, it has seemed more art than science, as captured in a quote attributed to Shimon Peres, the former Israeli prime minister who would go on to become the country's president: "Good policies are good P.R.; they speak for themselves."[10] Unfortunately, there is no clear mandate on what makes "good policies" in the first place or how to measure the information-related effects of policy with respect to public relations mishaps or successes.

[7] "Israelis Trust the IDF, Are Skeptical of Politicians—Survey," *Times of Israel*, July 10, 2016.

[8] Rid and Hecker, 2009, p. 103.

[9] Rid and Hecker, 2009, p. 103.

[10] Rid and Hecker, 2009, p. 104.

The relationship between the Israeli press and the defense establishment can be divided into four distinct periods:

- Independence in 1948 to the 1973 Yom Kippur War: Soldiers are suspicious of the media, and military censorship is common and accepted.
- Yom Kippur War to the 1982 Lebanon War (Operation Peace for Galilee): The military slowly opens up, but some topics (e.g., nuclear weapons) are still off-limits.
- Post–Lebanon War to the Oslo Accords (1993): Censorship declines precipitously, and the IDF begins cooperating more consistently with the press.
- Post–Oslo Accords to 2000 (the same year Israel withdraws from Lebanon): The Israeli press is critical of the army and its harsh tactics in Palestinian territories.[11]

Despite boasting one of the world's most advanced military forces, "the IDF has long underperformed in its public communication activities."[12] The evolution of Israel's valuing of information operations (IO) has been slow and, at times, reluctant. For the first several decades of the country's existence, Israel was in a fight for survival and relied almost exclusively on its military to fight and win wars using purely kinetic means. Over time, the country came to recognize the importance of IO and began devoting more resources to influence operations and psychological operations (PSYOP). However, even today, there is a critical gap between the government and the military, hindering the IDF's performance in the IE.

Second Lebanon War (2006)

The 33-day war that broke out in July 2006, sometimes referred to as the Second Lebanon War, exposed a wide array of shortcomings in how Israel operated within the IE. From the start, statements about the objectives of the operation differed from day to day and from spokesperson to spokesperson. Many were left wondering what the actual objectives were—to prevent rocket fire, to secure the release of abducted soldiers, or to destroy Hezbollah once and for all? Some suggested that Israel's hubris led the IDF to take Hezbollah's military capabilities for granted and underplay the militant group's ability to manipulate social media and the IE writ large. According to Pahlavi, Israel forfeited the psychological upper hand on all fronts: domestic, regional, and international.[13] Other Hezbollah actions in and through the IE included using signals intelligence to monitor IDF communications and then using the information gleaned

[11] Rid and Hecker, 2009, pp. 104–105. For more on the relationship between the media and the military in Israel, see Yoram Peri, "Intractable Conflict and the Media," *Israel Studies*, Vol. 12, No. 1, Spring 2007.

[12] Rid and Hecker, 2009, p. 101.

[13] Pierre Cyril Pahlavi, "The 33-Day War: An Example of Psychological Warfare in the Information Age," *Canadian Army Journal*, Vol. 10, No. 2, 2007.

to ambush Israeli commando units.[14] According to Russell W. Glenn, "Too great a reliance on force perhaps helps explain the limited extent to which Israel sought to employ information to shape Lebanese and international public opinion." Glenn does note that information-related capabilities (IRCs) were not completely neglected.[15] The IDF employed a phone and text message campaign, in addition to dropping more than 17.3 million flyers warning the Lebanese that "Hezbollah is your enemy."[16] Still, the destruction wrought throughout Beirut and its environs negated any goodwill Israel had earned through a relatively basic attempt to influence Lebanese civilians.

Operation Cast Lead (2008–2009)

In the words of Rid and Hecker, "The 2008/2009 war in Gaza illustrated how far the IDF had come, and that the organization had made an effort to implement the lessons learned from the war in 2006 both with respect to its public affairs and the way public affairs can be harnessed to deter."[17] Still, the short-lived conflict was not without its failures. One important Israeli gaffe during Cast Lead was limiting international media access to the battlefield in an effort to control the message. Some argue that this decision backfired, as no independent media were available to refute Palestinian claims of atrocities and civilian targeting. Another major negative outcome of Operation Cast Lead was the 2009 *Human Rights in Palestine and Other Occupied Arab Territories: A Report of the United Nations Fact-Finding Mission on the Gaza Conflict*, otherwise known as the Goldstone Report after the South African judge Richard Goldstone, who headed the analysis. The report was highly critical of Israel for wanton disregard of civilian casualties and collateral damage inflicted in Gaza, further damaging Israel's reputation and fueling the Boycott Divestment Sanctions movement, which seeks to isolate and delegitimize Israel.[18]

Operation Pillar of Defense (2012)

Operation Pillar of Defense was a one-week incursion into the Gaza Strip in response to rockets launched by Palestinian militants based in Gaza in late 2012. Throughout the brief tit-for-tat fighting, Hamas and the IDF exchanged barbs over several social media

[14] David E. Johnson, *Hard Fighting: Israel in Lebanon and Gaza*, Santa Monica, Calif.: RAND Corporation, MG-1085-A/AF, 2011, pp. 51–52.

[15] Russell W. Glenn, *All Glory Is Fleeting: Insights from the Second Lebanon War*, Santa Monica, Calif.: RAND Corporation, MG-708-1-JFCOM, 2012, p. 49.

[16] Itai Brun, "The Second Lebanon War, 2006," in John Andreas Olsen, ed., *A History of Air Warfare*, Washington D.C.: Potomac Books, 2010.

[17] Rid and Hecker, 2009, p. 123.

[18] United Nations General Assembly, *Human Rights in Palestine and Other Occupied Territories: A Report on the United Nations Fact Finding Mission on the Gaza Conflict*, A/HRC/12/48, September 25, 2009.

platforms.[19] Perhaps in an effort to compensate for its relatively poor performance in the IE in previous battles, Israel waged an aggressive social media campaign against Hamas, even offering visitors to the IDF blog incentives (in the form of points, a gamification feature used on other sites, such as Foursquare and Facebook) for repeat visits and retweets of its articles.[20] Posts on the IDF blog taunted Hamas members and featured posters of militants killed in the conflict. Israel's social media campaign was criticized for failing to learn lessons from Operation Cast Lead—namely, for appearing callous to the loss of Palestinian life and overly designing its messages to resonate with its own base.[21]

Operation Protective Edge (2014)

In early July 2014, the IDF began a seven-week offensive against Hamas militants operating in Gaza. The stated aim of Israel's ground invasion was to destroy the group's tunnel system. And while Israel was judged to have succeeded at both the tactical and operational levels of warfare, once again, international opinion focused largely on Israel's disproportionate use of force, and this became the defining narrative of the entire conflict. Hamas deliberately amplified even minimal accomplishments for strategic effect, thus capitalizing on the asymmetry between its organization and the much larger, better-trained, and better-equipped IDF.[22]

Organization for Operations in and Through the IE

After the Second Lebanon War, Israel established the Winograd Commission to investigate shortcomings in its military's performance, including the IDF's poor showing in the IE. A significant portion of the report focused on the disconnect between the political and military establishments in Israel, noting, "The overall image of the war was a result of flawed conduct of the political and the military echelons and the interface between them."[23]

[19] Anshel Pfeffer, "Psychological Warfare on the Digital Battlefield," *Haaretz*, November 19, 2012; see also Noah Shachtman and Robert Beckhusen, "Hamas Shoots Rockets at Tel Aviv, Tweeting Every Barrage," *Wired*, November 15, 2012.

[20] Sam Gustin, "The War Will Be Gamified: Israel, Hamas in Social Media Struggle," *Time*, November 16, 2012.

[21] Michael Koplow, "How Not to Wage War on the Internet," *Foreign Policy*, November 16, 2012. See also Allison Kaplan Sommer, "Israel's Online PR Offensive Sees Blowback," *Haaretz*, November 18, 2012.

[22] Alon Paz and Naday Pollak, "Operational Wisdom and Strategic Distress," Washington, D.C.: Washington Institute for Near East Policy, PolicyWatch 2289, July 22, 2014.

[23] Council on Foreign Relations, *Winograd Commission Final Report*, Washington, D.C., January 30, 2008.

Structure

During periods of intense conflict, the IDF's PA command can be staffed by as many as 300 soldiers, primarily conscripts.[24] According to Rid and Hecker,

> The Israeli government's communication architecture was complicated and the lines of authority unclear. Several agencies were involved at different levels: the press office of the Prime Minister, [the Government Press Office]; the department in charge of *hasbara* [advocacy or public diplomacy] within the foreign office; the office of the spokesperson of the defense minister, Dover Tsahal; and the press operations of the various commands. The responsibilities and the actual power of these administrative bodies often were not clearly defined, and hugely depended on the persons in charge.[25]

Cyber defense capabilities are housed in the command, control, communication, and computers branch of the IDF, while offensive cyber capabilities are under the direction of Unit 8200, the equivalent of the U.S. National Security Agency and the single largest military unit in the IDF. These capabilities can be found in other communities associated with military intelligence.[26]

Funding

Although no hard data are available, the IDF is known to have invested heavily in cyber capabilities in recent years, and it will continue to do so with the goal of consolidating cyber-related investment, training, and planning for both offensive and defensive operations under a unified cyber command.[27]

Functional/Organizational Divisions

The Winograd Commission recommended that Israel organize an information and propaganda unit to coordinate public relations across a wide spectrum of activities, including traditional media, new media, and diplomacy. The result was the creation of the National Information Directorate, tasked with managing *hasbara* and housed in the prime minister's office. The directorate also liaises with a host of nongovernmental entities to coordinate messages online (e.g., friendship leagues, bloggers, Jewish communities). Its role is to direct and coordinate the information sphere to present a unified, clear, and consistent message and maintain a single voice.[28] The directorate works across ministries and shapes key messages to be delivered to a range of audiences. This

[24] Rid and Hecker, 2009, p. 111.

[25] Rid and Hecker, 2009, p. 116.

[26] John Reed, "Unit 8200: Israel's Cyber Spy Agency," *Financial Times*, July 10, 2015.

[27] Barbara Opall-Rome, "Israel to Consolidate Cyber Spending, Ops," *Defense News*, June 18, 2015.

[28] William B. Caldwell IV, Dennis M. Murphy, and Anton Menning, "Learning to Leverage New Media: The Israeli Defense Forces in Recent Conflicts," *Military Review*, May–June 2009, pp. 6–7.

government body helped formulate Israel's public relations strategy and even developed plans, including role-playing activities, to help ensure that Israeli officials presented a clear and unified message to the press.[29]

IRCs Employed/Available

As Israel's use of IO continues to evolve, the IDF relies on a range of methods to operate in the IE, from psychological warfare to cyber operations. Israel has been forced to learn "the hard way" as its adversaries, especially Hezbollah, have elevated information to a veritable warfighting function.[30] The IDF has more recently adopted newer and more popular forms of social networking, including Instagram, where the photos posted to its feed tend to target Israel's domestic audience and "aim at promoting an integrated system of values."[31]

Coordination/Integration Efforts/Challenges

The story of the *Karine A* is another example of poor coordination between the Israeli military and the government. In early 2002—coinciding with a high-level meeting between U.S. special envoy Gen. Anthony Zinni and Palestinian National Authority President Yasser Arafat to promote peace talks—the Israeli Navy intercepted a Palestinian freighter (the *Karine A*) loaded with rockets, mortars, and other weapons. The IDF announced the seizure without alerting the Israeli government, which learned of it from a radio broadcast. The Palestinian leadership subsequently denied any involvement and blamed the Israelis for attempting to sabotage the proposed peace talks. In the end, according to Rid and Hecker, "the communication was so clumsy that some international observers began to doubt Israel's official version."[32]

Information Operations in Practice

During the 2006 33-day war against Hezbollah, Israel relied on the traditional use of information to support its PSYOP and electronic warfare (EW) efforts. The IDF dropped leaflets, jammed broadcasts on Lebanese satellite television station al-Manar, and pushed text messages to Hezbollah combatants and Lebanese noncombatants alike. In 2000, a photo of several Israeli soldiers posing with dead Hezbollah fighters appeared on a website unofficially maintained by IDF personnel. After an Israeli cameraman

[29] Rachel Shabi, "Special Spin Body Gets Media on Message, Says Israel," *The Guardian*, January 1, 2009.

[30] Caldwell, Murphy, and Menning, 2009, p. 4.

[31] Ayelet Kohn, "Instagram as a Naturalized Propaganda Tool: The Israel Defense Forces Web Site and the Phenomenon of Shared Values," *Convergence: The International Journal of Research into New Media Technologies*, Vol. 23, No. 2, 2015, p. 198.

[32] Rid and Hecker, 2009, p. 108.

was shot dead by a sniper in the Gaza Strip in April 2003, an IDF general publicly questioned the wisdom of sending photographers and videographers into combat, asking, "What price are we willing to pay for an image?"[33] After this incident, the IDF began equipping elite commandos with mounted mini-cameras to film their missions and took the further step of working to improve the training and the protection of soldiers specializing in communications.

Other controversies included the "stretcher incident," in which the IDF reported that it had captured drone footage of Palestinian fighters loading a rocket into a United Nations (UN) ambulance, while the UN argued that the object was merely a stretcher; ongoing leaks within the IDF ("each defense correspondent had his generals"); the *hitnatkut*, or unilateral disengagement plan from the Gaza Strip in 2005; the IDF's Operation Summer Rains in Gaza, an offensive launched in summer of 2006 that killed 200 or more Palestinian civilians; and an incident on a Gaza beach in which seven members of a Palestinian family, including several children, were killed in an explosion that was never investigated by an impartial commission.[34]

Examples of Interesting Operations in the IE

Over time, Israel has dedicated more attention to social media, moving out of a defensive crouch on this front and onto the offensive. During 2012's Operation Pillar of Defense against Hamas, the IDF circulated a graphic on Facebook that showed missiles raining down on iconic landmarks in the West—specifically, the Statue of Liberty, the Eiffel Tower, Big Ben, and the Sydney Opera House—with the phrase, "What Would You Do?" in bold red letters across the top. The post included the prompt: "Share this if you agree Israel has the right to self defense" and the IDF logo on the bottom.[35]

Noteworthy Capability Demonstrations or Practices

Israel sought to learn from its experience against Hezbollah in 2006 when it launched Operation Cast Lead in late December 2008 against Hamas militants in Gaza. Beginning with Operation Cast Lead, the IDF displayed a more nuanced understanding of strategic communication and a greater appreciation for unity of message and integration of IRCs. Two days after airstrikes commenced in Cast Lead, the IDF launched its own YouTube channel, "IDF Spokesperson's Unit," which attracted the site's second most subscribed-to channel and ninth most watched worldwide. The videos featured precision airstrikes on Hamas rocket-launching facilities, scenes of humanitarian assis-

[33] Rid and Hecker, 2009, p. 111.

[34] See Rid and Hecker, 2009, pp. 111–118.

[35] Luke Justin Heemsbergen and Simon Lindgren, "The Power of Precision Airstrikes and Social Media Feeds in the 2012 Israel-Hamas Conflict: 'Targeting Transparency,'" *Australian Journal of International Affairs*, Vol. 68, No. 5, 2014, p. 582.

tance, and video logs by IDF spokespeople. Furthermore, as discussed in more detail later, Israel's use of combat camera has, on several occasions, helped it dispute false claims made by Palestinian militants alleging IDF misconduct.

Anticipated Developments

It seems likely that Israel will continue to make strides in developing more-effective IO as part of its already comprehensive military capabilities. To this end, cyber capabilities—both offensive and defensive—are a logical avenue to pursue, given Israel's tech-savvy population.

Efforts of Others to Counter Israel's Efforts in the IE

In terms of operations security, Hezbollah exploited Israeli soldiers' willingness to use cell phones and social media during the 2006 conflict. Indeed, almost every IDF unit maintains a group and a following on Facebook. Perhaps the most telling incident during the conflagration with Hezbollah was the INS *Hanit* incident in mid-July 2006. Hezbollah militants fired an Iranian-made C-802 missile at the Israeli *Hanit* Sa'ar 5–class missile corvette, killing four sailors and rendering the vessel unable to further engage in combat operations. Before the IDF could respond, Hezbollah Secretary General Hassan Nasrallah announced the strike on al-Manar with accompanying footage for distribution by regional media and YouTube, leaving Israel seeming flat-footed and caught off guard.

After the war against Hezbollah, *The Economist* featured a cover with the phrase, "Nasrallah Wins the War," further cementing the impression that the IDF was defeated. This perception soon became reality throughout the region, with Nasrallah hailed as a hero for standing up to the "little Satan" (with the United States being the "great Satan") and emboldening other violent nonstate actors throughout the region. This outcome exposed Israel's vulnerabilities and sullied the IDF's image as an elite fighting force bordering on invincible. Palestinian militants, including Hamas, have also sought to counter Israel's IO and overall effectiveness by releasing photos showing injured and dead civilians, including children. These photos are released without context and are clearly intended to portray Israel as a callous force determined to unleash wanton violence with little concern for collateral damage or civilian casualties.

Lessons from Israel's Operations in and Through the IE

One important gaffe committed by Israel during Cast Lead was to limit access to the battlefield by international media in an effort to control the message. When independent media are barred from reporting a story, it opens up space for the adversary to be "the only voice in the room." There is no doubt that Israel has learned lessons the hard way.

The incident involving Muhammad al-Durrah is instructive. In the early stages of the Second Intifada, in September 2000, a 12-year-old boy named Muhammad al-Durrah was shot and killed in Gaza. The image that made front-page news around the globe, captured by a Palestinian journalist and first broadcast through France 2, was that of al-Durrah dying in his father's arms. Israel claimed that the boy was caught in the crossfire between the IDF and Palestinian militants, and an investigation by the IDF concluded that it was not bullets fired by its soldiers that ultimately killed al-Durrah. Nevertheless, the image portrayed to the world was one of innocent Palestinian children being gunned down by an aggressive occupying force.

From this incident, Israel reached two conclusions: Palestinian journalists will attempt to manipulate images for sympathy, and having only Palestinian journalists in a conflict zone is worse than having no journalists at all or equal access for all Israeli and foreign journalists.[36] Because Israeli and IDF leadership believe they have been mistreated by the press, they have vacillated from a policy of openness to a policy of restriction, with the latter often backfiring as rumors spread about numbers of civilian fatalities that were unable to be immediately disproven.

Effectiveness of Israel's Efforts in the IE

Of all the countries in the Middle East, Israel retains the most advanced cyber capabilities, including offensive cyber capabilities and the ability to stoutly defend its own networks and critical infrastructure.[37] Israel leverages its advantage in the high-tech sector and has moved to streamline various IRCs in the cyber domain over the past several years. In 2013, the IDF integrated cyber situational awareness, intelligence, and command activities into a new cyber headquarters, which is itself connected to the government's Internet infrastructure as well as the nascent National Cyber Bureau.[38]

Vulnerabilities of Israel's Operations in the IE

A significant vulnerability for Israel is its security posture. Israel is in a near-constant state of heightened alert and uses its military to maintain a robust security presence within the country and in parts of the West Bank. Not-so-subtle signals of the IDF's presence are the ubiquitous checkpoints scattered throughout the West Bank and Gaza Strip, constant reminders of what many Palestinians view as an occupying force. There have been numerous incidents of bad behavior by Israeli soldiers mistreating Palestinians at these checkpoints, further contributing to feelings of helplessness and humilia-

[36] Rid and Hecker, 2009, p. 106.

[37] Rhea Siers, "Israel's Cyber Capabilities," *Cipher Brief*, December 28, 2015.

[38] Michael Raska, *Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy*, Singapore: Nanyang Technological University, January 2015, p. 5.

tion that feed back into support for militant groups, such as Hamas and the Palestinian Islamic Jihad movement.[39]

Benjamin Runkle and William Caldwell identified several institutional and external challenges that limited the effectiveness of Israel's IO campaign during the 2014 Operation Protective Edge in Gaza:

- The IDF suffered from a role and capability mismatch.
- The IDF saw its primary audience as the military and the Israeli public, while the Ministry of Foreign Affairs, lacking access to the same real-time information as the IDF, was tasked with influencing international opinion.
- The IDF's public affairs branch was stymied by classification restrictions and procedural impediments.
- Israeli IO was limited by an inability to release certain full-motion videos and other forms of sensitive intelligence that could help disprove Hamas accusations.
- The campaign faced international media bias.
- The IDF lost "the war of narratives." According to Runkle and Caldwell, "Hamas understood it could not defeat the IDF on the battlefield, and hence pursued a strategy of undermining Israel's legitimacy by exploiting an asymmetric advantage in information operations." This was true even though Israel went to "extraordinary lengths" to limit civilian casualties and collateral damage, while Hamas violated the law of armed conflict through its reliance on indiscriminate attacks aimed at terrorizing a civilian population.[40]

Key Takeaways

A major takeaway from Israeli IO is that one seemingly minor incident can counteract the effectiveness of an entire operation. Take the example of an incident at the UN-administered al-Aida refugee camp, in which raw footage of an Israeli incursion into a civilian home made its way to Israel's most popular television channel, Channel 2. The footage showed Israeli soldiers breaking into the Palestinian family's home by detonating explosives, mortally wounding the mother. In the aftermath, an Israeli soldier is sitting in the living room and looks into the camera, proclaiming, "I don't know what we're doing here. Purification? Apparently it's dirty here. It's not clear to me what a Hebrew soldier is doing so far from home."[41]

[39] Ron Schleifer, *Perspectives of Psychological Operations (PSYOP) in Contemporary Conflicts*, Eastbourne, UK: Sussex University Press, 2011, pp. 25–26.

[40] Benjamin Runkle and William Caldwell, "The War of Narratives in Operation Protective Edge," *Jerusalem Post*, March 29, 2015.

[41] Rid and Hecker, 2009, p. 107.

Capabilities or Practices That the U.S. Army Might Want to Replicate (or Access Through Joint, Interagency, International, or Multinational Efforts)

The major practice that the U.S. Army might want to replicate is the constant scrutiny of prior operations and a relentless effort to dissect missions and operations to find what worked, what failed, and how the IDF could improve during its next operation in the IE. The IDF, like the U.S. Army, prides itself on innovation and adaptation and thus must work to adapt, based on lessons learned in real time, to the proliferation of new technologies and social media.

Distinctive Features

Israel faces a near-constant threat from its neighbors and, as such, has the opportunity to frequently test out new ideas and assess successes and failures, as well as the ability to adapt and evolve appropriately. The IDF faces a breakneck operational tempo due to constant skirmishes with an array of nonstate actors, including Hezbollah, Hamas, the Palestinian Islamic Jihad movement, and various other offshoots. The accelerated pace has been accompanied by a rapid change in the media and IE, further complicating the IDF's operational environment.

Takeaways for the U.S. Army

One of the major takeaways for the U.S. Army is the importance of elevating, combining, and coordinating efforts to inform and influence. The Israeli Winograd Commission, established after the Second Lebanon War in 2006, recommended that Israel organize an information and propaganda unit to coordinate public relations across a wide spectrum of activities, including traditional media, new media, and diplomacy. It also emphasized the importance of moving closely related but functionally separate capabilities under a single umbrella and ensuring that they operate across the whole of government. Two other conclusions from the commission's report were that there was an absence of clear messaging among political and military leaders and an utter lack of coordination between the myriad agencies and departments tasked with presenting a unified, coherent message.[42] The longer-term success or failure of these reforms is critical because efforts to communicate and inform must be coordinated across the entire government to avoid information fratricide, to both document and explain operations to domestic constituencies, and to compellingly refute false claims that might undermine the support of the domestic constituency.

Another major takeaway is the importance of an embedded press, combat camera, and other sources of reporting and verification. Some argue that Israel's decision to limit access by journalists backfired, as no independent media were available to refute Palestinian claims of atrocities and civilian targeting. Operation Cast Lead reemphasized the importance of combat camera and the issue of transparency: When independent media are barred from reporting a story, it opens up space for the adversary

[42] Council on Foreign Relations, 2008.

to be "the only voice in the room." Photographic and video capabilities ensured that the IDF captured evidence that Hamas was using mosques to hide anti-aircraft weaponry. Embedded press, combat camera or equivalent, independent journalists, and other sources of transparent reporting and verification are absolutely critical to insulate against falsehoods and propaganda.

Even for elite fighting forces like the IDF, failing to integrate information-related activities can squander gains on the battlefield. Operations must be planned with their consequences in and through the IE in mind.

CHAPTER TWO

NATO

Case Summary

The North Atlantic Treaty Organization's (NATO's) focus in the IE has been on developing a strong strategic communication (StratCom) capability, given that all operations are staffed by personnel from individual member states rather than from NATO headquarters. Strategic communication in NATO consists of multiple key areas: public diplomacy, PA, military PA, IO, and PSYOP. Doctrine has been actively updated with the emergence of digital technology and social media. Like most of its European member states, NATO refrains from using anything other than "white" information (completely true and fully and accurately attributed) in its communications targeting internal and external audiences.

The threat adversaries pose in the information space has been most recently highlighted by the discussion of IO and PSYOP in the wake of Russia's invasion of Ukraine and the effective information campaign Russia has waged against the United States and its allies.[1] However, coordination in responding to these new threats has been hampered by NATO's decentralized governance and a lack of IO capability in many NATO member states. Among the NATO's leading actors in IO are the United States, the United Kingdom, Germany, Estonia, and Italy. In these countries, IO is typically seen as an embedded function rather than an autonomous capability.

NATO member states distinctly separate communications with the public at home from engagement with foreign populations, drawing on significant operational experience in Afghanistan, Bosnia, and Kosovo. Members regularly discuss new ways of addressing contemporary military threats in both the physical and information spaces. Other initiatives have included strengthening of NATO's collective cyber defense capability, setting up new offices to fight foreign propaganda, and supporting better intelligence sharing after terrorist attacks in Paris, Brussels, and London.

[1] See Chapter Eight for a discussion of Russian information warfare approaches and capabilities.

Background and Overview

NATO has closely integrated its IO efforts with those of its member states, even though these efforts were founded on distinct doctrine. Responding to changes in the threat environment, NATO's activities in the IE prior to 1990 focused on deterring the Soviet Union and its influence, while the emphasis moved to the Balkans in the 1990s, the Middle East in the 2000s, and back to the European periphery after the recent conflicts in Ukraine and Syria erupted. NATO's most significant efforts to improve its information-related capabilities resulted from the challenges experienced by the International Security Assistance Force (ISAF) in Afghanistan. Since then, NATO has adopted a number of key documents, including the NATO StratCom concept in August 2010, and has been pursuing better cooperation between its international military staff and member states' national armed forces. In 2016, a new Assistant Secretary General for Intelligence post was proposed in a clear attempt to address the threat emerging powers pose in the information space. Although NATO manages with limited resources and depends on individual member contributions and unanimity-based decisionmaking, its integrative function has never been in greater demand as threats emanate from state and nonstate actors alike.

The end of the Cold War was a turning point for NATO. Four decades after the alliance's founding, the rivalry between the Soviet Union and the West came to a sudden end, and NATO faced the challenge of redefining its purpose. Yet, the world of the 1990s was not without security threats to NATO partners: In 1990–1991, many of them joined coalition forces against Saddam Hussein's Iraq in the Gulf War, and NATO first participated in combat as an alliance in the Bosnian War (1992–1995) and the Kosovo War (1998–1999).[2] These highly controversial interventions were later overshadowed by NATO's involvement in other lethal conflicts based on the principle of collective defense—for example, in Afghanistan (2001–2014) in response to the September 11, 2001, terrorist attacks, and in Libya (March–October 2011).[3] NATO has conducted other operations in Pakistan (a relief effort after the 2005 Kashmir earthquake), in the Gulf of Aden (a counterpiracy operation under way since 1999), and in Turkey (contributing to missile defense since December 2012, though that relationship has been strained since Turkey announced a decision to purchase missile batteries from Russia in 2017). NATO has also maintained some presence in Afghanistan as part of the Resolute Support Mission (starting in 2015) that focuses on training, advising, and counterterrorism assistance. All these operations have posed IE-related challenges of varying intensity and nature—some in building strong relations with local populations

[2] In Bosnia, NATO conducted air strikes after the Markale and Srebrenica massacres in 1994 and 1995, respectively. It engaged in an air campaign in Kosovo in the spring of 1999 and has maintained a peacekeeping force on the ground ever since.

[3] On collective defense, see North Atlantic Treaty Organization, "Collective Defence—Article 5," web page, last updated March 22, 2016a.

(Kosovo, Afghanistan), others in gaining a broad international support for rapid action against a dictator (Bosnia, Libya), and still others in building political support to provide the operation with sustainable funding (Somalia, Pakistan).

As a security alliance defending the interests of more than 900 million people, NATO has one of the largest domestic constituencies and a plethora of state and nonstate adversaries, and it continues to face significant interoperability and cohesion challenges in multinational operations. The alliance's characteristics also pose unique challenges and opportunities for its leadership. NATO's leadership and individual member states have been increasingly more attentive to gaps in their collective IO capability, and, as we show in this chapter, they have undertaken significant modernization efforts at both the national and supranational (NATO) level.

Concepts and Principles for Operations in and Through the IE

There was no explicit governance for NATO information activities until the mid-2000s, when challenges to ISAF operations led NATO leadership to set up its first formal role to coordinate relevant efforts at the strategic level. What began as a three-person cell for StratCom at Supreme Headquarters Allied Powers Europe (SHAPE) is now a complex governance infrastructure at both NATO's headquarters in Brussels and in other cities (most notably in Riga, Latvia). NATO now uses *strategic communication* as the umbrella term for all information activities. NATO issued Allied Joint Publication (AJP) 3.10, *Allied Joint Doctrine for Information Operations*, in 2009 and drafted other documents in subsequent years to harmonize understanding of IO across the alliance. Still, individual member states resort to national doctrine first before using NATO language, sometimes leading to frictions in communication and execution.[4] For NATO, IO are not a static concept but have been continually redefined as allied forces engage in multinational exercises, information exchanges, and consultations. Despite these advances, NATO continues to be challenged by its adversaries on many information fronts, including social media.

Strategic Goals/Vision

By engaging in information and psychological operations, NATO aims to promote its own objectives and achievements, counter propaganda, support PA, and convey situation and cultural awareness to its own troops.[5] This means reducing the risk of kinetic action while bolstering the positive impact of its engagement with local populations by

[4] Lothar Buyny, "Implementing STRATCOM," *Three Swords Magazine*, No. 28, May 2015.

[5] Ulrich M. Janssen, *Psychological Operations: NATO Psychological Operations Within the Context of Strategic Communications*, Oberammergau, Germany: NATO School Oberammergau, Intelligence, Surveillance, Target Acquisition, and Reconnaissance Department, 2012.

developing an understanding of both the adversary's military capabilities as well as the broader "human terrain." However, as mentioned, NATO's terminology and doctrine do not always align with those used by its individual member states.[6]

Between 2007 and 2009, NATO began formalizing its IO capabilities by creating a cell for StratCom at SHAPE and, in 2011, implementing the StratCom Capability Implementation Plan.[7] Throughout its recent history, NATO has aimed to develop a new capability that could address existing gaps in communication with both domestic and foreign audiences by differentiating among public diplomacy, PA, military PA, IO, and PSYOP. The joint strategic goal consists of achieving nine "essential capabilities":

> 1. The ability to *coordinate* NATO and coalition force information and communications activities with other military actions and to *shape the battlespace* and *maximize desired effects* on selected audiences;
> 2. The ability to *coordinate NATO and coalition information and communications activities* with the efforts of other agencies and partners within the context of a broader NATO strategy, and in accordance with the Comprehensive Approach Action Plan;
> 3. The ability to access, *produce and maintain information and knowledge of the perceptions, attitudes, behaviours and beliefs of potential audiences*;
> 4. The ability to access, *produce and maintain updated information and knowledge of complex social communication systems*, taking into consideration the characteristics of various media agencies;
> 5. The ability to *detect, monitor, translate and assess the effects of the StratCom efforts on stakeholders*—whether friendly, neutral or adversarial;
> 6. The ability to estimate how direct and indirect actions and signals potentially could affect the perceptions, attitudes, behaviours, beliefs and actions of certain audiences;
> 7. The ability to *develop and disseminate timely and culturally-attuned messages* based on narratives (including spokesmanship);
> 8. The ability to *quickly develop and disseminate information* designed to change the attitude of, or influence, certain audiences;
> 9. The ability to *document NATO and coalition force operations and exercises*, and to *disseminate this information* in real or near-real time.[8]

The key relevant processes have been captured in a StratCom handbook (published in spring 2015), the Narrative Development Tool, the StratCom Strategic Training Plan, and other documents cited later in this chapter. New capabilities have been

[6] Alternative terms include *local communication*, *operative information*, *military information support operations*, *influence activities*, and *influence operations*. See Janssen, 2012.

[7] Buyny, 2015.

[8] Buyny, 2015, p. 41. Emphasis added.

piloted in several multinational initiatives, including the Multinational Information Operations Experiment, which enables cooperation with NATO partners, such as Australia, Austria, Sweden, Finland, Japan, the European Union, academia, and think tanks; the Multinational Capability Development Campaign; and various conferences, workshops, and meetings with experts.[9]

These initiatives have been supported by the NATO school in Oberammergau, Germany, which has developed a StratCom familiarization course for NATO senior officials, and by multinational exercises in which StratCom plays an important role (including the Steadfast Jazz and Viking exercises in 2013 and Trident Juncture 2015 and 2016). Finally, the newly founded NATO Strategic Communications Centre of Excellence, based in, Riga, Latvia, is tasked with integrating and coordinating the alliance's various IO-related efforts.[10] Its value added has yet to be fully demonstrated, but initial indications have been positive, and it has begun to document StratCom case studies and lessons learned for future application.[11]

How IO/IW Fits Within NATO's Overall Strategic Goals

As a defense alliance, NATO has historically aimed to avoid military engagement if possible and favor diplomatic resolution of conflicts.[12] When it has engaged, its engagement has tended to be comprehensive and include an active outreach to local populations, relying heavily on the capability of its member states to effectively carry out IO. According to General Petr Pavel, chairman of the NATO Military Committee, key challenges faced by NATO today include a "revanchist Russia, cyber attacks, and hybrid warfare" in the East and conflicts in Syria and Yemen in the South, prompting the alliance to establish a "responsive deterrent."[13] This concept of a responsive deterrent, is, in turn, "underpinned by effective Strategic Communication."[14] In other words, as components of StratCom, NATO public diplomacy, PA, military PA, IO, and PSYOP all collectively contribute to the defense of the alliance against the most imminent threats it faces.[15]

At its 2014 summit in Wales, the North Atlantic Council reaffirmed the importance of information in modern warfare and committed to enhancing NATO StratCom and strengthening cooperation with other organizations:

[9] Buyny, 2015.

[10] Buyny, 2015.

[11] For an overview, see NATO Strategic Communications Centre of Excellence, "Publications," web page, undated(d).

[12] North Atlantic Treaty Organization, "What Is NATO?" web page, undated.

[13] Petr Pavel, Chairman of the NATO Military Committee, "The Road to Warsaw and Beyond," speech to the NATO Parliamentary Assembly, Defence and Security Committee, last updated October 14, 2015.

[14] Pavel, 2015.

[15] These functions existed separately in NATO prior to StratCom's introduction as an integrative concept.

> We will ensure that NATO is able to effectively address the specific challenges posed by hybrid warfare threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design. It is essential that the Alliance possesses the necessary tools and procedures required to deter and respond effectively to hybrid warfare threats, and the capabilities to reinforce national forces. This will also include enhancing strategic communications, developing exercise scenarios in light of hybrid threats, and strengthening coordination between NATO and other organisations, in line with relevant decisions taken, with a view to improving information sharing, political consultations, and staff-to-staff coordination. We welcome the establishment of the NATO-accredited Strategic Communications Centre of Excellence in Latvia as a meaningful contribution to NATO's efforts in this area. We have tasked the work on hybrid warfare to be reviewed alongside the implementation of the Readiness Action Plan.[16]

Targets and Audiences

In 2010, RAND found that NATO StratCom efforts reach various audiences, not all of which are intended: both national populations of member states and foreign populations, including those of allies and adversaries.[17] The four general audiences for NATO efforts in the IE—NATO's own troops, member states' own populations, enemy conflict parties, and enemy populations—may appropriately be reached through various types of engagement, including diplomatic, economic, social and cultural, and media activities, as well as by conventional, covert, or special operations forces. This includes *command information* targeted to NATO troops, *PA* information targeted to member states' populations, and *PSYOP* targeting enemy fighters and leadership and the populations that support them.

Cohesive messaging across such a wide range of targets presents an immense challenge, no less for an alliance of more than two dozen member states. NATO has recognized this challenge and has indicated the need to inform its own personnel what other target audiences are being told before these personnel engage in IO themselves. However, NATO's messaging across audiences lacks strategic and sometimes even operational and tactical agreement (with respect to content or specific audiences), leading George Dimitriu of the Dutch Ministry of Defence to argue with respect to Afghanistan in 2012,

> NATO still lacks a central Stratcom strategy including a common narrative and there still seems to be no national Stratcom policy within the different participant ISAF countries. Only recently, in August 2010, did the NATO's highest political

[16] North Atlantic Treaty Organization, "Wales Summit Declaration," press release, last updated September 26, 2016e.

[17] Anais Reding, Kristin Weed, and Jeremy J. Ghez, *NATO's Strategic Communications Concept and Its Relevance for France*, Santa Monica, Calif.: RAND Corporation, TR-855/2-MOD/FR, 2010.

> organ, the North Atlantic Council agree on a first formal document over Stratcom: the "Military Concept for NATO Strategic Communications." In this document, however, one finds no univocal working definition: that is, even at the highest level, Stratcom still stands in need of further explication and agreement.[18]

Foundational Principles of NATO IO

By its very nature, NATO's foundational purpose has been to effectively integrate the capabilities of diverse partners to build a strong deterrent capability—and, if needed, to defend its territory through collective action. In StratCom, however, NATO did not pursue a common approach until the mid-2000s, when its first working group was formed to consider the gap between the existing and desired states of NATO's joint capabilities in the information domain. While still residing exclusively at the national level and spearheaded by a handful of NATO countries, IO capabilities have been increasingly more critical to NATO's senior leadership and supported by a number of initiatives. As a result, IO have become a key component of NATO's deterrent. The major development, as we discuss next, has included the agreement on joint NATO doctrine on IO.

Doctrinal Principles

NATO's doctrine is a patchwork of documents developed with sufficient rigor but implemented only selectively. As a result of national caveats, NATO's doctrine is rarely ever completely identical to the doctrine of individual member states, leading to discrepancies in both definitions and substantive content. However, NATO has spearheaded a joint effort to coordinate and harmonize its approach to IO with the use of a new phrase to describe its focus: StratCom.

This broad term is now used as a general descriptor of NATO IO activities and has several elements: public diplomacy, PA, military PA, IO, and PSYOP.

We describe these elements in detail later in this chapter. As a whole, NATO StratCom emphasizes both foreign and domestic audiences:

> - Contribute positively and directly in achieving the successful implementation of NATO operations, missions, and activities by incorporating strategic communications planning into all operational and policy planning;
> - Build, in close and lasting coordination with NATO nations, public awareness, understanding, and support for specific NATO policies, operations, and other activities in all relevant audiences; and

[18] G. R. Dimitriu, "Winning the Story War: Strategic Communication and the Conflict in Afghanistan," *Public Relations Review*, Vol. 38, No. 2, June 2012, p. 204.

- Contribute to general public awareness and understanding of NATO as part of a broader and on-going public diplomacy effort.[19]

To achieve these objectives, however, the alliance has had to walk a difficult road in which virtually all responsibility for engaging domestic and foreign audiences remains at the national level.

History and Evolution

The 1980s were not an era of coordinated public diplomacy but, rather, a one-off approach to handling large protests while sticking to policies developed earlier. Yet, there were examples of some early synchronization success. In crafting the "NATO brand," officials recognized the value of tightly coordinating actions with words. During the U.S campaign to persuade Europe to accept the deployment of Pershing II ballistic missiles there, NATO integrated its physical actions with public diplomacy. By convincing European policymakers that Russia would not see the act as belligerent, no *say-do gap* was created. Instead, as then–U.S. Secretary of State George Shultz stated, public diplomacy was critical for the success of this decision: "'I don't think we could have pulled it [missile deployment] off if it hadn't been for a very active program of public diplomacy.'"[20]

In the years to follow, however, NATO maintained only a limited capability to communicate with the broader public and other stakeholders. This led to an inadequate capacity to handle immense public interest in its role in the wake of interventions in Bosnia and Kosovo, partly due to the emergence of numerous pressing challenges for NATO, including the resurgence of terrorism.

In general, NATO officials engaged in IO work were PA personnel or from the lower ranks, distanced from PSYOP personnel. This distance and failure to integrate capabilities may have reflected a conscious decision to limit the influential role that information can have and restrictions on doing more than informing. The need for a more robust IO strategy became more evident as communication technology advanced and gave voice to millions of people. The new popularity of social media platforms further reinforced the need to coordinate the engagement of external audiences. Moreover, the alliance suddenly recognized gaps as its adversaries started to develop robust strategies in the information domain. The need for integration driven by highly qualified personnel quickly surfaced as a pressing need, and StratCom emerged as a priority area.[21]

[19] NATO Strategic Communications Centre of Excellence, "About Strategic Communications," web page, undated(a).

[20] Andrew T. Wolff, "Crafting a NATO Brand: Bolstering Internal Support for the Alliance Through Image Management," *Contemporary Security Policy*, Vol. 35, No. 1, March 20, 2014, p. 77.

[21] Personal conversation with the author in Ontario, Canada, in November 2015.

NATO's history is thus one of putting less emphasis on IO while investing heavily in building interoperability and cohesion in other domains, particularly in low-intensity conflicts and postconflict stabilization operations. Only later did NATO's leadership start investing in building a coherent and unified approach to StratCom, and, much later, in leveraging emerging communication technologies.

Systematizing StratCom

Following multinational efforts led by Germany to evaluate NATO's interoperability gaps as part of the Multinational Information Operations Experiment from 2003 on, the alliance has adopted several key doctrinal documents.[22] These have included analysis supporting the development of a multinational information strategy in October 2008 and the Multinational Experiment 6 analytical concept *Enhanced Systemic Understanding of the Information Environment in Complex Crisis Management in August 2010* and framework concept *Integrated Communication in Multinational Coalition Operations Within a Comprehensive Approach* in October 2010.[23]

NATO first formally acknowledged the importance of strategic communications in 2007 when the first StratCom cell was created at SHAPE. The cell consisted of just two staff officers and was led by Mark Laity, a former NATO spokesperson in Kabul.[24] While the formal recognition of strategic communication does not connote success or failure, its acknowledgment at the time provides a good reference point. Soon thereafter, the first StratCom conference was held in 2008, allowing the member states to agree on the key principles of a new StratCom policy.[25] Laity himself has concluded that NATO StratCom has "always been, in part, a response to failure." While NATO's operation in Kosovo presented several hurdles to NATO's media operations, Laity concluded that ISAF was a "much larger" challenge, primarily because of the complexity associated with linking civilian and military efforts at both the strategic and tactical levels. (He also noted that no NATO personnel were lost in combat in Kosovo, while the operation in Afghanistan produced thousands of casualties on both sides.)[26]

Led by Laity, the Supreme Allied Commander Europe's (SACEUR's) first directive on StratCom, Allied Command Operations Directive 95-2, was published in 2008. (It has been updated twice since then.) NATO's StratCom policy followed soon

[22] Multinational Information Operations Experiment, *Narrative Development in Coalition Operations*, draft, version 0.96, January 10, 2014, p. 3.

[23] Multinational Information Operations Experiment, 2014, p. 3.

[24] Mark Laity, "NATO and the Power of Narrative," *Information at War: From China's Three Warfares to NATO's Narratives*, London: Legatum Institute, September 2015b, p. 22; see also Mark Laity, "Rising to the Challenge as Information Takes Centre Stage," *Three Swords Magazine*, No. 28, May 2015a.

[25] The first time that staff representing all three key functions (PA, PSYOP, and IO) held concurrent annual conferences was in 2014. See Laity, 2015a.

[26] Laity, 2015a.

thereafter in 2009. As a result of this guidance, all IO-related disciplines were subordinated to StratCom, which was defined as

> coordinated and appropriate use of NATO communications activities and capabilities . . . in support of Alliance policies, operations and activities, and in order to advance NATO's aims.[27]

The creation of a unified NATO IO authority was not without its opposition: Some NATO staff were reluctant to let PA and PSYOP even share the same room, while others did not immediately accept the need for StratCom-level coordination of all IO.[28]

NATO adopted AJP-3.10 on allied IO in 2009, arguing that "military information activities may include a wide range of actions . . . and will be achieved by lethal and/or non-lethal means."[29] According to AJP-3.10, NATO information activities may play any of the following roles:

- Compel: To force someone to undertake a desired course of action.
- Diminish: To make less or cause less to appear to reduce the effectiveness of an activity.
- Disrupt: To break or interrupt the flow of information. To use force or other non-lethal means to shatter the cohesion of a (target) audience and prevent them from functioning effectively.[30]

Emergence of PSYOP in NATO

AJP-3.10 was expanded in 2014 with the adoption of AJP-3.10.1, *Allied Joint Doctrine for Psychological Operations*, with the purpose of outlining NATO PSYOP, "focusing on its planning and execution when supporting NATO activities."[31] AJP-3.10.1 is based on MC 402/2, which defines NATO military policy for PSYOP and its applications and is complemented by the NATO PSYOP handbook, which provides details on tactics, techniques, and procedures (TTPs).[32] MC 402/2 (updated in 2012) defined PSYOP as follows:

[27] Laity, 2015a.

[28] Laity, 2015a.

[29] North Atlantic Treaty Organization, *Allied Joint Doctrine for Information Operations*, Allied Joint Publication 3.10, November 2009.

[30] North Atlantic Treaty Organization, 2009, pp. 1–6.

[31] North Atlantic Treaty Organization, *Allied Joint Doctrine for Psychological Operations*, Allied Joint Publication 3.10.1, September 2014a, p. 16.

[32] North Atlantic Treaty Organization, 2009.

> Planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives.[33]

In 2012, Lieutenant Colonel Ulrich Janssen from the NATO School in Oberammergau, Germany, argued that the alliance's mission was 20-percent kinetic operations and 80-percent influence operations, emphasizing the key role of IO in NATO's toolbox.[34] He added that "presenting a positive image at all times and in all context[s] is mission critical" and suggested that the main aims of NATO PSYOP activities were as follows:[35]

- Weaken the will of the adversary or potential adversary target audiences.
- Reinforce the commitment of friendly target audiences.
- Gain support and cooperation of uncommitted or undecided audiences.

According to Janssen, key principles that NATO adheres to in executing PSYOP include

- a focus on mission rather than products
- research and evaluation
- understanding
- early integration and coordination
- timeliness
- truthfulness
- acknowledgment of the intelligence source (white, gray, or black).

NATO IO Reference Handbook

The *Information Operations Reference Book*, first published in 2010, outlines operation-specific principles, procedures, and decisionmaking processes. IO are described in light of their operational phases—planning, execution, campaign assessment, and plan review—and the handbook describes the role of various entities at both the strategic and operational levels, as shown in Table 2.1.

The handbook indicates that the key players in NATO IO are subject-matter experts within the NATO International Military Staff headquarters and SHAPE, who "are responsible for 'translating' the decisions made by the [North Atlantic Council]/

[33] North Atlantic Treaty Organization, *NATO Military Policy on Psychological Operations*, MC 402/2, June 22, 2012a, p. 3.

[34] Janssen, 2012.

[35] Janssen, 2012.

Table 2.1
NATO Entities Involved with IO Execution

Strategic Level	Operational Level
Information Strategy Working Group	Joint Operations Planning Group
Headquarters, NATO Crisis Management Task Force	Information strategy meeting
StratCom Working Group	StratCom/engagement working groups
SHAPE Strategic Operations Planning Group	IO Coordination Board
	IO contributions to the Joint Operations Centre
	Campaign Assessment Working Group
	Command Assessment Board

SACEUR in terms of 'military information activities' and for integrating the operational-level military information concerns in the SHAPE StratCom Working Group."[36]

EU Concept for Civil-Military Cooperation for EU-Led Military Operations

Parallel to NATO, the European Union developed its own IO concept, which is "compatible and consistent with NATO CIMIC [civil-military cooperation] policies, concepts and doctrine."[37] Published in 2008, this concept defines CIMIC as "co-operation and coordination, as appropriate, between the EU military force and independent external civil organisations and actors (International Organisations, Non-Governmental Organisations, local authorities and populations)."[38] Thus, it focuses on external audiences, typically in countries of deployment. It refers to several key activities that would fall under the umbrella of CIMIC:

- civil emergency planning
- EU military IO (defined as "activities that can directly contribute to establish[ing] and build[ing] confidence in the EU-led military operations [and] gaining the trust and support of the local population")
- host-nation support
- contracting
- medical support
- management of civil resources.[39]

These activities predominantly include efforts aimed at supporting the capability of the host nation to build its own security forces and to increase domestic stability (and secondarily, affinity toward EU objectives). By explicitly listing IO as one compo-

[36] North Atlantic Treaty Organization, *NATO Bi-SC Information Operations Reference Book*, version 1, March 5, 2010, pp. 35–36.

[37] Council of the European Union Military Staff, *EU Concept for Civil-Military Co-Operation (CIMIC) for EU-Led Military Operations*, Brussels, July 11, 2008, p. 6.

[38] Council of the European Union Military Staff, 2008, p. 5.

[39] Council of the European Union Military Staff, 2008, pp. 11–13.

nent of CIMIC, the European Union makes a clear statement about the importance of other efforts in aligning its own interests with those of a third country.

NATO MC 422/3 (Final), July 8, 2008

While the full text of MC 422/3 is not available, public sources cite the definition of IO this document provides:

> a military function to provide advice and co-ordination of military information activities in order to create desired effects on will, understanding and capabilities of adversaries, potential adversaries and other [North Atlantic Council] approved parties in support of Alliance mission objectives.

NATO StratCom Concept, August 10, 2010

NATO developed its new strategic concept in response to its relative inability to "gain the support of the Afghan populations to the extent hoped and within the timetable set" in the course of its leadership of ISAF beginning in 2003.[40] Its key objectives were to ensure that local audiences received clear, fair, and timely information while reinforcing the strategic impact of its communications.[41] The new documents addressed the following elements of the NATO StratCom portfolio: public diplomacy, PA, military PA, IO, and PSYOP.[42]

The new strategy reflects the changing environment for information sharing and distribution, in which control of information dissemination is partly outside of NATO's capabilities—especially in hostile environments where local populations do not have easy access to uncensored information. NATO's use of the term *strategic communications* follows the U.S. example, and its execution, similar to that of the United States, is shared by multiple offices.[43]

As documented in another RAND study, the subordination of various StratCom capabilities differed under different ISAF commanders.[44] A reorganization by General McChrystal, for instance, introduced the role of the Deputy Chief of Staff for Communications, who was responsible for IO, PSYOP, and military PA, while the operation's spokesperson reported to both the force commander and the Deputy Chief of Staff for Communications.[45]

[40] Reding, Weed, and Ghez, 2010.

[41] Reding, Weed, and Ghez, 2010.

[42] Reding, Weed, and Ghez, 2010.

[43] Reding, Weed, and Ghez, 2010.

[44] Reding, Weed, and Ghez, 2010.

[45] Reding, Weed, and Ghez, 2010, p. 21.

To oversee the execution of StratCom, NATO established the Strategic Communications Working Group, which meets monthly.[46] This group includes NATO force commanders, representatives of the Public Diplomacy Division and the Media Operations Center, the International Military Staff PA adviser, and IO staff.[47]

NATO Military Public Affairs Policy (MC 0457/2)

In December 2010, all NATO Chiefs of Defense agreed on the language of MC 0457/2, *NATO Military Public Affairs Policy*. The document was endorsed by the North Atlantic Council in February 2011, superseding 2001's MC 0457/1, which was largely a response to the "overwhelming media and public demand for information regarding NATO's military role, mission, forces and operations stemming from the Kosovo air campaign."[48] In addition to providing definitions and descriptions of NATO's military PA, it situates this activity within NATO StratCom.

MC 0457/2 introduces military PA as part of the wider NATO StratCom portfolio. It states that PA should

> support commanders by communicating accurate information in a timely manner to audiences to improve public awareness and understanding of the military aspects of the Alliance's role, aims, operations, missions, activities and issues, thereby enhancing organisational credibility.[49]

In characterizing PA audiences, it describes the whole range of "allied, international, regional, local or internal [audiences], depending on the issue or activity." NATO's PA work is based on direct reports to commanders and can thus be "subordinated to other staff functions."[50]

NATO military PA personnel have a tripartite functional responsibility:

- external communication (media relations and outreach activities)
- internal communication ("with and among NATO military and civilian personnel and their families")
- community relations ("interaction between NATO military installations in NATO member states and their surrounding civilian communities").[51]

[46] Reding, Weed, and Ghez, 2010.

[47] Reding, Weed, and Ghez, 2010.

[48] North Atlantic Treaty Organization, *NATO Military Public Affairs Policy*, MC 0457/2, February 2011a, p. 3.

[49] North Atlantic Treaty Organization, 2011a, p. 10.

[50] North Atlantic Treaty Organization, 2011a, pp. 10–11.

[51] North Atlantic Treaty Organization, 2011a, pp. 11–12.

NATO's military PA strategy is "a command responsibility at all levels," carried out at the political level by the North Atlantic Council (which provides "overall guidance and direction for Strategic Communications"), the Assistant Secretary General for Public Diplomacy (who coordinates all StratCom activities), and the NATO StratCom Policy Board and its StratCom Standing Working Group. In the military realm, responsibility falls to NATO's Military Committee (which "establishes overall policy" and whose chair is NATO's spokesperson on all military issues) and the strategic commands (SACEUR is the spokesperson for NATO operations).[52]

Organization

Since its founding, NATO's workforce has been separated into a military and a civilian staff, yet NATO does not possess military forces of its own.[53] As a result, while NATO bodies may coordinate allied activities in the information domain, respective member states remain responsible for the vast majority of IO. Within NATO, the United States, Germany, and the United Kingdom have the most significant IO capability and operational experience.

While the best-resourced IO capabilities in NATO reside with individual member states, the alliance plays a key role in allowing information sharing and coordination, and it provides other supportive functions. In addition, it strengthened intelligence sharing after terrorist attacks in Brussels (2016) and Paris (2015), and it continues to invest in this capability.[54]

Additionally, it is likely that the U.S.-funded Intelligence Fusion Center (now focused on Afghanistan) will be given a broader mandate in the fight against terrorism.[55] General Pavel, chair of the NATO Military Committee, has said that NATO's intelligence structure would be revamped to pull "military and civilian intelligence together into one product, combined from these two branches," although some observers have been skeptical that intelligence sharing would shift from a bilateral to a multilateral model within the alliance.[56]

Given NATO's limited experience executing IO, its organizational structure for these operations is chiefly political, as Figure 2.1 indicates.

Virtually all NATO offices and commands have some role to play in NATO StratCom—be they the International Staff led by the Secretary General, NATO Military Staff led by the Military Committee (with its chair reporting directly to the North

[52] North Atlantic Treaty Organization, 2011a, pp. 13–14.

[53] North Atlantic Treaty Organization, "Troop Contributions," web page, last updated June 27, 2016c.

[54] Julian E. Barnes, "NATO Moving to Create New Intelligence Chief Post," *Wall Street Journal*, June 3, 2016.

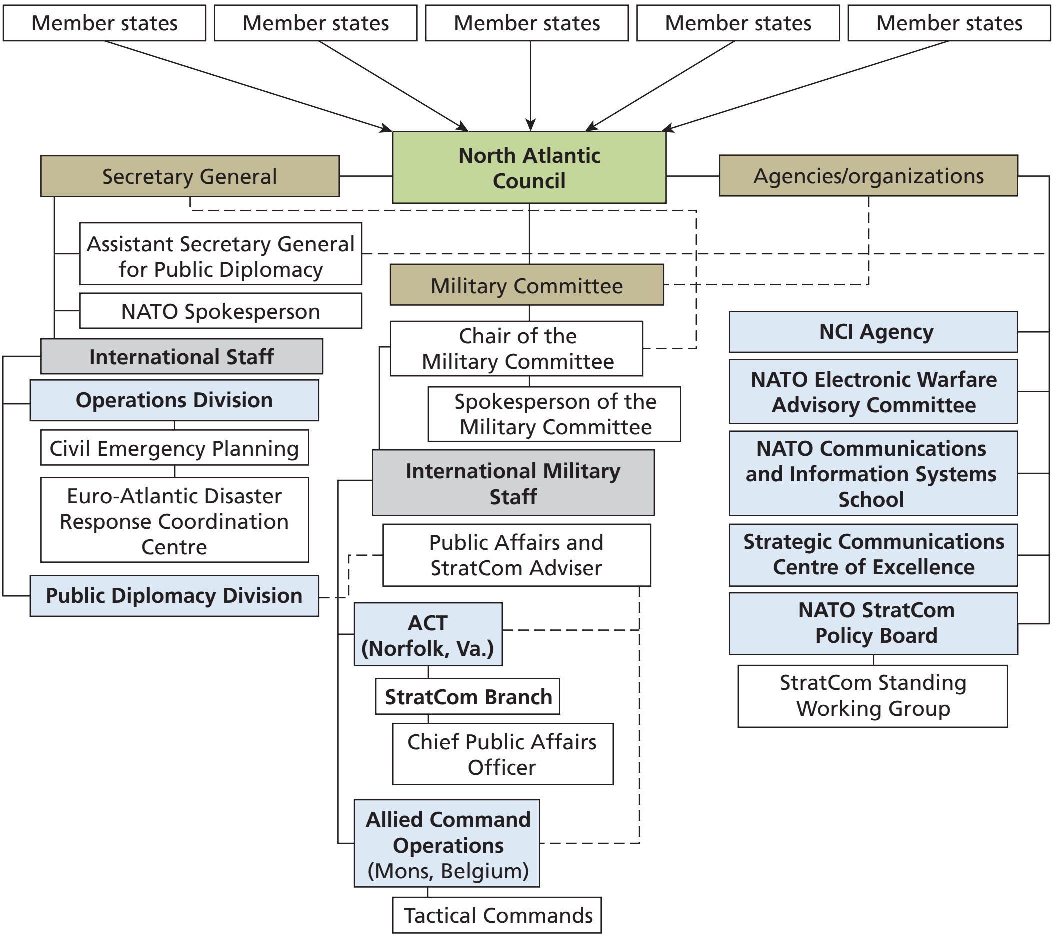
[55] Barnes, 2016.

[56] Barnes, 2016.

Atlantic Council and working closely with the Secretary General), or the individual agencies and organizations that support NATO's work across borders.

The five components of StratCom—public diplomacy, PA, military PA, IO, and PSYOP—incorporate different principals, making coordination challenging and relatively cumbersome but allowing inclusivity in determining an overall communication strategy. Consider PA: Its execution is delegated to individual NATO offices and orga-

Figure 2.1
NATO's Key Organizations for IO-Related Activities


Member states
Member states
Member states
Member states
Member states
North Atlantic Council
Secretary General
Agencies/organizations
Assistant Secretary General for Public Diplomacy
NATO Spokesperson
Military Committee
Chair of the Military Committee
Spokesperson of the Military Committee
International Staff
Operations Division
Civil Emergency Planning
Euro-Atlantic Disaster Response Coordination Centre
Public Diplomacy Division
International Military Staff
Public Affairs and StratCom Adviser
ACT (Norfolk, Va.)
StratCom Branch
Chief Public Affairs Officer
Allied Command Operations (Mons, Belgium)
Tactical Commands
NCI Agency
NATO Electronic Warfare Advisory Committee
NATO Communications and Information Systems School
Strategic Communications Centre of Excellence
NATO StratCom Policy Board
StratCom Standing Working Group

SOURCE: RAND Analysis based on NATO, 2011a, and other NATO documents.
RAND *RR1925z2-2.1*

nizations, and the complete list of PA contacts in the alliance is more than 30 pages long.[57] Some of these points of contact include

- Public Diplomacy Division (Brussels, Belgium)
- NATO Information Office (Moscow, Russian Federation)
- PA and StratCom adviser (Brussels, Belgium)
- PA office at SHAPE (Mons, Belgium)
- PA office at headquarters, Allied Joint Force Command Brunssum (Brunssum, Netherlands)
- PA office at headquarters, Allied Joint Force Command Naples (Naples, Italy)
- PA office at headquarters, Allied Air Command (Ramstein-Miesenbach, Germany)
- PA office in Norfolk, Virginia
- PA office at the Joint Warfare Centre (Stavanger, Norway)
- PA office at the NATO Communications and Information Agency (Brussels, Belgium).

Coordinating the network of PA officials at more than 30 NATO postings, 28 national defense ministries, and many other specialized postings in NATO member states (such as the French Rapid Reaction Corps, British Forces Germany, and Headquarters, U.S. Army Europe) poses a formidable challenge to the consistency and quality of NATO's engagement with the public and the media.

The IO Working Group was established to advise NATO on the execution of IO, as well as doctrinal matters. Its function of reviewing existing operations, doctrine, coordinating joint IO efforts, and applying lessons learned to doctrine documents provides NATO's senior leadership with relevant input as it adapts its IO efforts to new realities.[58]

Communications and Information

NATO's emphasis on bolstering its IO capabilities culminated in the creation of several offices dedicated to IO and cyber-related efforts. Its key arm for communication, the NATO Communications and Information Agency plays an important integrative role for IO within the alliance.

NATO Communications and Information Agency

The NATO Communications and Information Agency was stood up in July 2012 to coordinate the alliance's information technology (IT) and command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) activities

[57] North Atlantic Treaty Organization, *NATO's Directory of Public Information and Public Affairs Officers*, November 2012b.

[58] Multinational Information Operations Experiment, 2014.

(including cyber and missile defense) per the Lisbon Summit of 2010.[59] The agency is an executive arm of the NATO Communication and Information Organisation and is headquartered in Brussels, with a significant presence in The Hague, Netherlands, and Mons, Belgium. It reports to the Agency Supervisory Board, which consists of national representatives from all NATO member states. (The board reports to NATO's executive body, the North Atlantic Council.)

The NATO Communications and Information Agency is the successor organization to the NATO C3 Organisation, the NATO Communication and Information Systems Services Agency; NATO Consultation, Command and Control Agency; NATO Air Command and Control System Management Agency, and NATO Headquarters Information and Communication Technology Service.[60] It consists of several components, including units dedicated to communication and information system support, network operations, cyber defense operations, operational analysis, command and control (C2), joint ISR, ballistic missile defense, and cyber security.[61] The agency's full organizational structure is shown in Figure 2.2.

The importance of cyber defense was highlighted at the 2016 NATO summit in Warsaw: Two paragraphs of the final communiqué were devoted to highlighting the challenge cyberattacks pose to the allies and reiterating NATO's commitment to the cyber domain, which it made at the 2014 NATO summit in Wales.[62] The language used ("[We] recognise cyberspace as a domain of operations") signals intensified attention. In the "Cyber Defence Pledge" adopted at the Warsaw summit, NATO is described as having a role in "facilitating co-operation on cyber defence including through multinational projects, education, training, and exercises and information exchange, in support of national cyber defence efforts."[63] NATO has also engaged nongovernmental stakeholders through the NATO Industry Cyber Partnership, launched in 2014.[64]

[59] North Atlantic Treaty Organization, "NATO Communications and Information Agency (NCI Agency)," web page, last updated April 7, 2016b.

[60] North Atlantic Treaty Organization, 2016b.

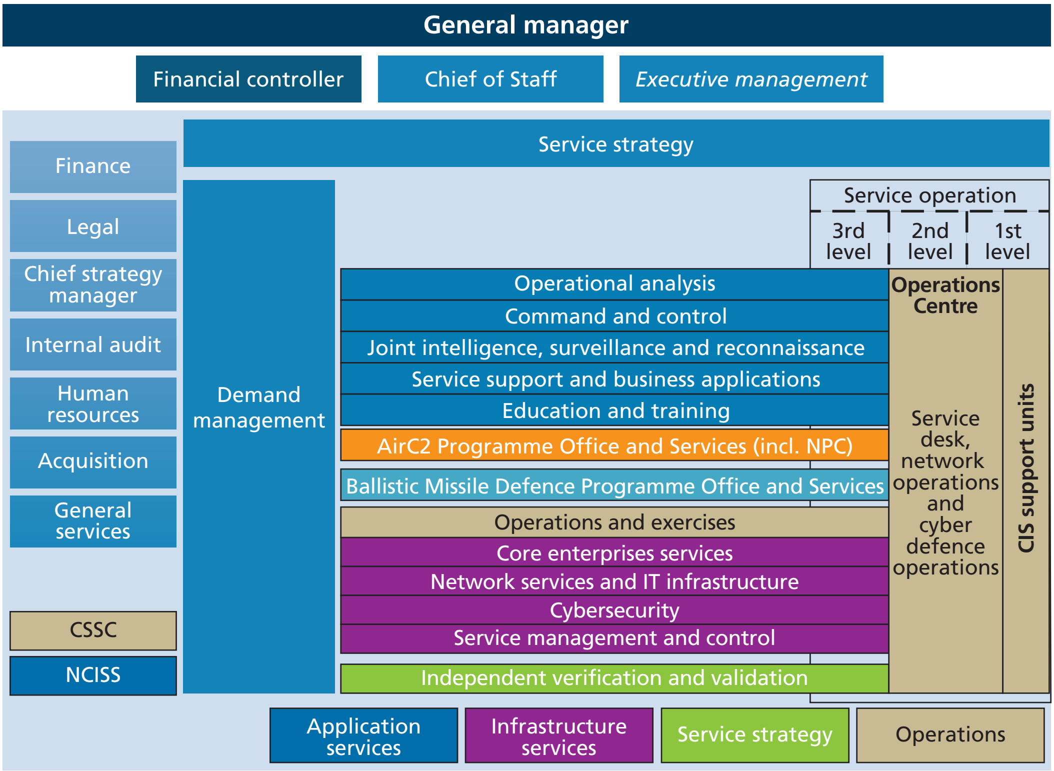
[61] NATO Communications and Information Agency, "NCI Agency Organisational Overview," web page, undated.

[62] North Atlantic Treaty Organization, "Warsaw Summit Communiqué," press release, last updated March 29, 2017b.

[63] North Atlantic Treaty Organization, "Cyber Defence Pledge," press release, July 8, 2016d.

[64] North Atlantic Treaty Organization, "NATO Launches Industry Cyber Partnership," web page, last updated September 18, 2014b.

Figure 2.2
Organizational Overview of the NATO Communications and Information Agency



SOURCE: NATO Communications and Information Agency, undated.
NOTES: NPC = NATO Programming Centre. CSSC = Communication and Information Systems Sustainment Support Centre. NCISS = NATO Communications and Information Systems School.
RAND *RR1925z2-2.2*

Civil Emergency Planning

Euro-Atlantic Disaster Response Coordination Centre

The Euro-Atlantic Disaster Response Coordination Centre oversees NATO's civil emergency response efforts and operates 24/7.[65] Although it focuses mainly on responding to natural and man-made disasters, it also conducts exercises and engages other international institutions and national stakeholders. It serves as a clearinghouse for requests and offers of assistance in the aftermath of disasters—and it has an important role in engaging vulnerable populations around the world.[66] It was established in 1998 and was first actively engaged in coordinating the humanitarian assistance effort following

[65] North Atlantic Treaty Organization, "Euro-Atlantic Disaster Response Coordination Centre," web page, last updated April 28, 2017d.

[66] North Atlantic Treaty Organization, 2017d.

the Kosovo war.[67] NATO member states, geographic combatant commands, and other partner countries (especially Afghanistan, Australia, Iraq, Japan, Mongolia, New Zealand, Pakistan, and South Korea) are involved with the center.[68]

Electronic Warfare

While EW is strictly under member-nation control, NATO established a coordinating body for this capability in 1966, the NATO Electronic Warfare Advisory Committee. The committee is responsible for policy oversight, doctrine, and C2 concepts, and it monitors EW support to NATO operations.[69] It consists of national representatives, and its chair and secretary are permanently based at NATO headquarters in Brussels. Subordinate groups deal with EW database support, training, and doctrine. NATO Electronic Warfare Advisory Committee meetings have traditionally been annual or semiannual.[70] NATO's EW policy is outlined by MC 0064, *NATO Policy for Electronic Warfare*, which is regularly amended to reflect technological and procedural changes, as well as emerging threats. It serves as a starting point for common doctrine and interoperability standards.[71]

In addition, NATO draws on the technical expertise of the NATO Joint EW Core Staff. Eleven NATO member states have made a significant commitment to this effort: the Czech Republic, France, Germany, Greece, Italy, Netherlands, Norway, Poland, Romania, the United Kingdom, and the United States.[72] The NATO Joint EW Core Staff provides EW expertise to allied command operations, Allied Command Transformation, and SACEUR and is part of SHAPE's military chain of command.[73] Its mission includes the development of NATO EW policy, doctrine, and concepts, as well as experimentation.[74]

NATO-Accredited Centers of Excellence

Strategic Communications Centre of Excellence

In 2013, coordination of NATO StratCom was bolstered by a request from the Supreme Allied Commander Transformation to launch the NATO Strategic Communications Centre of Excellence, which was accredited and activated in September 2014 in Riga,

[67] North Atlantic Treaty Organization, 2017d.

[68] North Atlantic Treaty Organization, 2017d.

[69] North Atlantic Treaty Organization, "Electronic Warfare," November 16, 2011b.

[70] North Atlantic Treaty Organization, 2011b.

[71] North Atlantic Treaty Organization, 2011b.

[72] NATO Joint Electronic Warfare Core Staff, "NATO Joint Electronic Warfare Core Staff (JEWCS): A History of Transformation," briefing slides, undated.

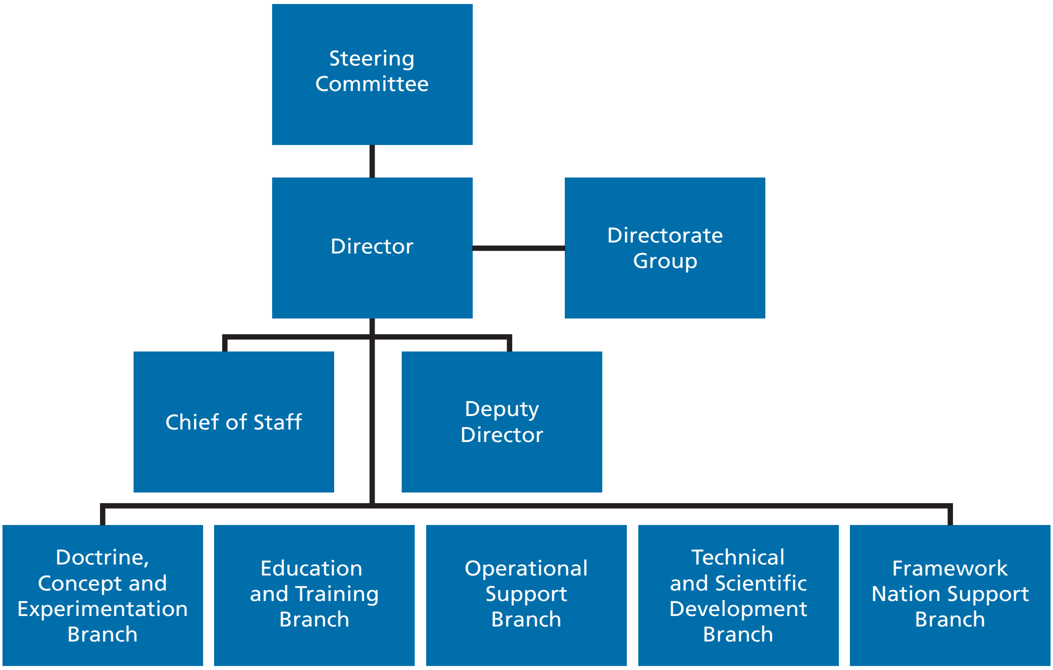
[73] NATO Joint Electronic Warfare Core Staff, undated.

[74] NATO Joint Electronic Warfare Core Staff, undated.

Latvia.[75] The center was inaugurated in August 2015, in conjunction with a conference on the importance of perceptions in international security.[76] Figure 2.3 shows the center's structure.

The center was founded under the auspices of Latvia with sponsorship from Estonia, Italy, Poland, Germany, Lithuania, and the United Kingdom. Additional contributions have been made by the United States, Finland, and the Netherlands.[77] Aside from supporting NATO's efforts to coordinate and properly execute StratCom efforts, it also serves as a "hub for research as well as testing ideas and approaches," and it contributes to education and training in the field.[78]

Figure 2.3
Structure of the NATO Strategic Communications Centre of Excellence in Riga, Latvia


Steering Committee
Director
Directorate Group
Chief of Staff
Deputy Director
Doctrine, Concept and Experimentation Branch
Education and Training Branch
Operational Support Branch
Technical and Scientific Development Branch
Framework Nation Support Branch

SOURCE: NATO Strategic Communications Centre of Excellence, "Structure," web page, undated(e).
RAND *RR1925z2-2.3*

[75] NATO Strategic Communications Centre of Excellence, "History," web page, undated(b).

[76] NATO Strategic Communications Centre of Excellence, undated(b).

[77] NATO Strategic Communications Centre of Excellence, "Participating Countries," web page, undated(c).

[78] NATO Strategic Communications Centre of Excellence, *NATO Strategic Communications Centre of Excellence: Report for the Period from 1 October 2014 to 31 December 2014*, Riga, Latvia, March 2015d.

Funding

Member countries make direct and indirect contributions to the costs of running NATO, implementing its policies, and undertaking its activities. Members contribute according to an agreed cost-share formula, based on gross national income, representing a percentage of each member's defense budget. Common funding arrangements are used to finance NATO's principal budgets: the civil budget (the costs of running NATO headquarters), the military budget (costs of the integrated command structure), and the NATO Security Investment Programme (military capabilities).[79]

Combined, NATO's annual budget is about $2.3 billion.[80] Of that, the United States is responsible for around one-fifth, or $514 million. The 2016 U.S. defense budget was $585 billion, meaning that its NATO expenditure is only 0.09 percent of its total defense spending.[81] While NATO spending on IO has not been made public, a 2011 review shows that the core budget consisted of a military budget pool of $1.2 billion (including pensions), a civilian budget pool of $0.2 billion (including pensions), and a security investment budget of $0.7 billion.[82] It is likely that IE-related capabilities, including StratCom, receive an amount in the lower tens of millions of dollars annually.

Functional/Organizational Divisions

IRCs Employed/Available

In NATO, *StratCom* is an umbrella term for the following concepts:

- Public Diplomacy: NATO civilian communications and outreach efforts responsible for promoting awareness of and building understanding and support for NATO's policies, operations and activities, in complement to the national efforts of Allies
- Public Affairs: NATO civilian engagement through the media to inform the public of NATO policies, operations and activities in a timely, accurate, responsive, and proactive manner
- Military Public Affairs: promoting NATO's military aims and objectives to audiences in order to enhance awareness and understanding of military aspects of the Alliance
- Information Operations: NATO military advice and co-ordination of military information activities in order to create desired effects on the will,

[79] North Atlantic Treaty Organization, "Funding NATO," web page, last updated January 19, 2017a.

[80] North Atlantic Treaty Organization, 2017a.

[81] Philip Bump, "Donald Trump Is Just About Over This Whole NATO Thing," *Washington Post*, March 21, 2016.

[82] Michael Liska, Budget Chief, Supreme Headquarters Allied Powers Europe, "NATO Resources: An Overview," briefing sides, undated.

understanding, and capabilities of adversaries and other [national assembly]–approved parties in support of Alliance operations, missions and objectives

- Psychological Operations: planned psychological activities using methods of communications and other means directed to approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives.[83]

Public Affairs

NATO public diplomacy has faced considerable challenges throughout the institution's history. Even the organization's foundation was controversial in Europe, culminating in France's decision to leave the alliance's military command structure altogether in 1966.[84] In the 1980s, large protests in Germany against a proposal to host nuclear-capable Pershing II missiles in Europe, along with missions in Kosovo, Bosnia, and Afghanistan (ISAF), have stirred mixed reactions among the citizens of NATO member states, as well as among the populations of other affected states.[85] Since the conclusion of NATO-led combat operations in Afghanistan in 2014, public support for the alliance has increased in some member states, most directly as a result of Russian actions in Ukraine. Figure 2.4 tracks historical support for NATO among its largest member states.

Coordination/Integration Efforts/Challenges

Several coordination challenges have plagued NATO operations in the past. In Afghanistan, for instance, initiatives that aimed to solidify NATO's StratCom had only limited reach and were implemented "only fitfully" on the ground.[86] As a result, coordination between NATO PA personnel and military staff tasked with PSYOP was limited at best, and there were concerns about integrity and credibility arising from the strict separation between the information shared with domestic and foreign audiences. Moreover, NATO forces often faced the challenge of aligning the interests of different political constituencies—both within individual member states and across the alliance.[87]

Another integration challenge has stemmed from differing interpretations of StratCom principles among NATO members. For example, George Dimitriu of the

[83] NATO Strategic Communications Centre of Excellence, undated(a).

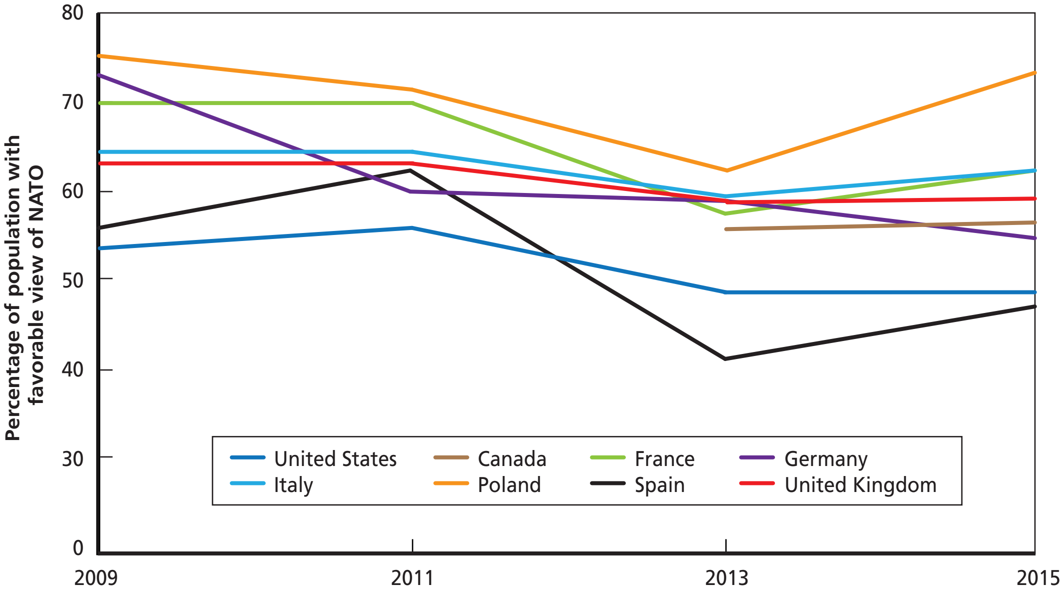
[84] Wolff, 2014.

[85] The total number of demonstrators against the Pershing II missile arrangement was estimated at 300,000 as of April 8, 1985. See Times Wire Services, "Hundreds of Thousands Protest Missiles in Europe: Urge U.S. to Match Soviet Halt," *Los Angeles Times*, April 8, 1985. For more on member-state popular support for NATO, see Wolff, 2014.

[86] Dimitriu, 2012.

[87] Dimitriu, 2012.

Figure 2.4
Support for NATO in Its Largest Member States, 2009–2015



SOURCE: Data from Katie Simmons, Bruce Stokes, and Jacob Poushter, "NATO Public Opinion: Wary of Russia, Leery of Action on Ukraine," Washington, D.C.: Pew Research Center, June 10, 2015.
RAND *RR1925z2-2.4*

Dutch Ministry of Defence claims that "the United States and NATO encourage soldiers to blog (within set guidelines), to [use] twitter and . . . other social media to talk about their mission, but in other countries such as Germany the law forbids this."[88] Without a social media strategy with broad consensus, the alliance could put itself at risk, exposing gaps in the social media environment that could be further exploited in the physical environment.

Information Operations in Practice

Examples of Interesting Operations in the IE

Kosovo Air Campaign

Before the 1999 Kosovo air campaign, NATO lacked a coordinated PA policy, let alone an overarching StratCom strategy.[89] Entrenched in Cold War thinking—which was anything but conducive to transparency and regular engagement of the public on

[88] Dimitriu, 2012, p. 204.

[89] Massimo Panizzi, "The Development of NATO Strategic Communications: From Public Affairs to a Broader Communications Policy," *Three Swords Magazine*, No. 21, Autumn–Winter 2011.

military affairs—the alliance was inadequately equipped for the war that opened the 21st century and was among the first conflicts essentially streamed live on cable TV. NATO's most visible presence in the media was its Office of Information and Press, a rather archaic and rigidly employed entity. After NATO's initial strikes on Yugoslav forces, its headquarters in Brussels was overwhelmed by journalists from around the world demanding information. The Office of Information and Press was not equipped for a crisis response, however. It had "one NATO Spokesperson, no Media Operation Centre and one Military Spokesman." As a result, coordination of messaging on the strikes was "was cumbersome, and even erratic," and the processes supporting it were rather slow.[90]

Afghanistan

After making difficult adjustments in the wake of the Kosovo campaign, the alliance entered a new conflict demanding significant communication efforts in 2003, this time in Afghanistan. As in Kosovo, the war in Afghanistan resulted in both military and civilian casualties on both sides, requiring robust communication efforts vis-à-vis the public in NATO member states, civilians in Afghanistan, and regional partners, as well as the adversary (chiefly the Taliban and its affiliates). However, the complexity of the challenge was much greater than in Kosovo because the IE underwent a radical change at the end of that conflict.

In its initial months, Operation Enduring Freedom lacked a communication strategy, and IO activities focused primarily on supporting offensive operations. The U.S.-led operation initially conducted leaflet drops and developed radio broadcasts (deploying the specially modified EC 130J Commando Solo aircraft) that aimed to discourage locals from supporting the Taliban. However, some have argued that these activities were largely ineffective because perceptions of indiscriminate bombing "terrorized the local population." Others criticized the coalition for having "little knowledge" of IO and a lack of consistency in carrying out these operations.[91] During the early years of the war, PSYOP efforts focused on avoiding civilian casualties by informing locals about upcoming engagements; only later did the allies start to directly engage Afghan civilians to win their trust and support. The deployment of Provincial Reconstruction Teams—albeit not with the primary goal of influencing their attitudes—made meaningful contributions to building better relationships between NATO forces and the Afghan public.[92]

[90] Panizzi, 2011, p. 10.

[91] See Wolff, 2014.

[92] Wolff, 2014.

The 2008 ISAF Theatre Strategic Communications Strategy emphasized a need to coordinate PA, PSYOP, IO, and key leader engagement to gain the local population's support and build confidence within the Afghan government.[93]

GEN Stanley McChrystal noted the importance of StratCom in his Commander's Initial Assessment from August 2009:

> Strategic Communication (StratCom) makes a vital contribution to the overall effort, and more specifically, to the operational center of gravity: the continued support of the Afghan population. In order to achieve success we must make better use of existing assets and bolster these with new capabilities to meet the challenges ahead. To date, the Insurgents have undermined the credibility of ISAF, the International Community (IC), and Government of the Islamic Republic of Afghanistan (GIRoA) through effective use of the information environment, albeit without a commensurate increase in their own credibility. Whilst this is a critical problem for ISAF, the consequences for GIRoA are even starker. GIRoA and the IC need to wrest the information initiative from the [insurgents].[94]

McChrystal further acknowledged the importance of nonmilitary players in the conflict, "especially in areas outside security such as the governance, reconstruction, and development arenas" and suggested several operational priorities for ISAF IO:

- Diminish the credibility of insurgents and their extremist allies.
- Partner with the Afghan government and civilian population to foster a sense of ownership and responsibility for countering violent extremism and to promote security, stability, and development.
- Increase the effectiveness of international and Afghan government communications locally and internationally.
- Increase political and popular will to counter violent extremism and protect the operational center of gravity—specifically, the support of the Afghan people.
- Enhance StratCom coordination with higher headquarters and troop-contributing nations to maintain the alliance's cohesion.
- Promote Afghan National Security Forces capability and credibility.
- Increase international and public support for ISAF's goals and policies.[95]

Most critical was McChrystal's emphasis on integrating StratCom activities in preparing for and executing operations, rather than treating them as a "separate Line

[93] Wolff, 2014.

[94] Stanley A. McChrystal, *U.S. Forces–Afghanistan/International Security Assistance Force, Afghanistan: Commander's Initial Assessment*, August 30, 2009, p. D-1.

[95] McChrystal, 2009, p. D-2.

of Operation."[96] In addition, McChrystal advocated for the strong protection of civilians and for bolstering ISAF's ability to engage regional political leadership through its Government Media and Information Centre.[97]

Finally, while favoring strong relationship building with the locals, McChrystal also advocated for an offensive use of IO against insurgents:

> A more forceful and offensive StratCom approach must be devised whereby [insurgents] are exposed continually for their cultural and religious violations, anti-Islamic and indiscriminate use of violence and terror, and by concentrating on their vulnerabilities. . . . These vulnerabilities must be expressed in a manner that exploits the cultural and ideological separation of the [insurgents] from the vast majority of the Afghan population.[98]

Despite NATO's intentions, the results of ISAF operations were mixed at best. Many Afghans did not receive information through traditional channels (newspapers, radio) but, rather, directly from insurgents—sometimes under duress—and the majority of the population (77 percent of Afghans) reported that they feared the international forces.[99] Such failures in communication were never completely alleviated, and the current government in Kabul faces continual pressure from insurgents.[100] The Taliban continued to hold considerable influence in the country even after the withdrawal of most NATO troops in 2014, and it now holds more territory than at any time between 2001 and 2014.[101]

Yet, the capabilities of respective NATO member states and their integration across the alliance have progressed. Within a few months of the campaign's start, the alliance strengthened its engagement with local stakeholders by attempting to make patrols as personable as possible and holding events with local senior leaders to communicate its own intentions. As a result, it was able to better manage perceptions and adjust its own policies, such as its rules of engagement and the content of its operational plans.[102] However, criticism of NATO's efforts has been directed at its effectiveness in gaining the support of Afghan citizens, particularly when they are faced with a choice between cooperating with the Taliban and resisting.[103]

[96] McChrystal, 2009, p. D-2.

[97] McChrystal, 2009, p. D-3.

[98] McChrystal, 2009, p. D-4.

[99] Wolff, 2014.

[100] Associated Press, "Official Suicide Bomb Attack Kills 30 Afghan Trainee Police," NBC 26 (Green Bay, Wisc.), June 30, 2016.

[101] "Taliban Chief: U.S. Forces Must Leave Afghanistan," *Deutsche Welle*, February 7, 2016.

[102] Laity, 2015b, p. 22.

[103] Wolff, 2014.

Anticipated Developments

Russia

In Russia, NATO faces a highly potent adversary with well-resourced information warfare capabilities backed by rigorous training and long-term experience in the field. Russia's sustained and well-integrated information campaign is part of a broader military strategy; it builds on robust narratives and an understanding of culture and psychology, as well as target audience analysis.[104] Russia has also developed strong information warfare doctrine and policy and adapted well to the information age.[105] For these reasons, it presents challenges to the defensive-natured alliance. A key obstacle is that actions may not be consistent across NATO member states, given the lack of coordination to conduct defensive operations against state-sanctioned propaganda from Russia and other potential sources of psychological influence.

ISIL/Daesh

The Islamic State in Iraq and the Levant (ISIL), also known as Daesh, has emerged as a potent adversary. It uses multiple communication systems and methods and has leveraged digital media to spread its message to millions of people around the world. NATO has identified several lessons learned from its recent review of its engagement with the group:

- "A unified linguistic and strategic approach is needed to disrupt the networking Daesh does through various social media platforms."
- "From the psychological point of view, intimidation or ridicule will not be effective counter narrative strategies." A potentially effective alternative is to illustrate how its propaganda works to the broader public.
- The effectiveness of the coalition fighting the group, as well as ISIL losses, should be communicated coherently to the public.
- The study of influence activities and the vulnerability of domestic audiences is key to developing a robust strategy to protect them from the group's information strategy, recruitment, and radicalization. "Each country, society, and audience needs to have its own specialised and comprehensive approach based on local demographics and psychographics."[106]

Alliance Partners

Recent Russian aggression has generated strategic questions about the framework best suited for prevention and response efforts. Although not much has been done with it

[104] Laity, 2015a.

[105] Laity, 2015a.

[106] NATO Strategic Communications Centre of Excellence, *Daesh Information Campaign and Its Influence: Results of the Study*, Riga, Latvia, 2015b, p. 8.

historically, NATO's concept of *psychological defense* serves as a framework for member states' use. The correlation between investment in psychological defense and proximity to Russia is likely significant, but its use in most of Central, Western, and Southern Europe is unknown.

For example, Sweden's defense command announced in 2016 that it was amending the doctrine under which the Swedish military deals with threats to the country's sovereignty. One of the four legs of Swedish defense is psychological defense (the other three are military, civil defense, economic defense). In this context, psychological defense includes intensive civic training. More than 1 million Swedes engage in volunteer work supporting the armed forces, such as the Red Cross, women's auxiliaries that staff air and sea control centers with communication specialists, and transport corps personnel, who volunteer to drive all types of vehicles, including heavy cross-country vehicles, for the military. Swedish telephone books traditionally have a section telling the population exactly what to do in case of an attack and warning them not to pay attention to disinformation broadcasts, such as those stating that "the mobilization has been cancelled."[107]

Finland, too, has emerged as a particularly active front in the information wars. As "a country at the center of Russia's concerns about NATO's expansion toward its borders . . . unnerved by Russian military actions in Ukraine and its saber-rattling in the Baltic Sea, [Finland] has expanded cooperation with NATO and debated whether to apply for full membership."[108] Actual or perceived hostile action could accelerate and facilitate cohesion between Finland and NATO.

Impact of Social Media

The applicability of NATO's Article 5 will be challenged as cyber and social media capabilities increase.[109] Officials have already begun to question the extent to which NATO's legal framework is ready to deal with modern warfare, since attack has a different meaning than it did even just a decade ago. In 2016, NATO agreed that cyberattacks could trigger an Article 5 response on a "case-by-case" basis and in line with international law. However, member states must individually decide what constitutes a cyberattack that rises to the level of an armed attack.[110]

[107] GlobalSecurity.org, "Sweden: Defense Policy," web page, last updated July 5, 2016.

[108] Andrew Higgins, "Effort to Expose Russia's 'Troll Army' Draws Vicious Retaliation," *New York Times*, May 30, 2016.

[109] Article 5 of the Washington Treaty states that "parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all" (North Atlantic Treaty Organization, 2016a).

[110] Patrik Maldre and Jarno Limnell, "Key Cyber Issues for NATO's Warsaw Summit," *Breaking Defense*, July 5, 2016.

Effectiveness of NATO Information Operations

In recent conflicts, NATO's efforts have yielded mixed results: Although it has been militarily superior to its adversaries in areas of deployment, the alliance has been unable to attain the trust of local populations in either Afghanistan or Libya; it was able to achieve some success in stabilizing Kosovo only due to significant contributions by the German contingent. (We analyze this case in detail in Chapter Four.) In addition, the fragmented and highly bureaucratic nature of the alliance has prevented it from developing a strong IO capability in the majority of the dimensions examined here:[111]

- NATO StratCom has often lagged behind the narrative offered by adversaries.[112]
- It has had a limited ability to influence public opinion (domestic or foreign) and limited success in developing a single narrative in most conflicts (largely due to differing levels of engagement by partners and occasional internal disagreements on military strategy).[113]
- It has played a secondary role in cyberwarfare, which falls under Article 4 as consultation, not collective defense.[114] (The alliance has developed limited tools to deter and counter cyberattacks against its members but has not pursued a joint offensive capability.)
- It has not succeeded in achieving universally high levels of operations security and denial capability in highly kinetic conflicts (particularly involving less well-resourced armed forces), and it has used social media in a relatively conservative way.[115]

Moreover, NATO's doctrine prevents it from engaging in deception and manipulation (a common tactic of its adversaries), puts limitations on the use of IO in fire/maneuver (IO units are typically embedded within national forces and have a relatively narrow mandate), and lacks specifics on collaborating with proxies. NATO's relative strength vis-à-vis other large forces is in EW and other technological IO means, for which it relies on the capabilities of its most advanced militaries.[116]

[111] On NATO's bureaucratic structure, see Elizabeth Oren, "A Dilemma of Principles: The Challenges of Hybrid Warfare from a NATO Perspective," *Special Operations Journal*, Vol. 2, No. 1, 2016.

[112] Consider the unsuccessful U.S.-led "reset" of relations with the Russian Federation.

[113] In some NATO countries, such as Germany, France, and Italy, populations have expressed opposition to upholding Article 5 of the Washington Treaty if another member state were attacked by Russia. See, for instance, Simmons, Stokes, and Poushter, 2015.

[114] Myriam Dunn Cavelty, "Cyber-Allies: Strengths and Weaknesses of NATO's Cyberdefense Posture," *IP Global Edition*, Vol. 12, No. 3, 2011.

[115] NATO's social media information channels include Facebook, Twitter, Flickr, LinkedIn, and YouTube.

[116] Consider NATO's common deployment of its Airborne Warning and Control System and the establishment of NATO Joint EW Core Staff.

NATO IO efforts, in short, face several challenges to their effectiveness: (1) a lack of unity among allies, most obvious in the form of national caveats when capabilities are deployed jointly; (2) a limited toolbox to engage local populations while conducting combat operations (NATO depends fully on national contributions, often leading to problems integrating IO activities in its operations); and (3) high turnover at both its headquarters and at the tactical level, leading to difficulties in developing a coherent IO strategy and building interpersonal trust with local populations.

If effectiveness is measured in terms of sustainability, NATO may face a series of new challenges in the future if it cannot show flexibility in the rapidly evolving IE. Narrative development and delivery are a useful entry point for engagement, but shifting conditions require sustainability. For example, the NATO-crafted narrative on Libya disintegrated in 2011 when it did not align with reality, despite intentions to convey how a competent rebel army would win the universal support of the Libyan public, defeating Gadhafi and taking Tripoli with little resistance.[117]

Efforts of Others to Counter NATO IO and Their Effectiveness

One of the most direct confrontations NATO has faced has been with the Russian Federation, primarily over strategic interests in the Middle East and Eastern Europe. Moscow's military strategy has included "a range of tools including psychological operations, information warfare and intimidation with massing of conventional forces."[118] (We describe these dynamics in detail in Chapter Eight.)

Despite profound and persistent disagreements, NATO has reiterated that it does not seek a confrontation with Russia.[119] Yet, efforts by the United States to engage the Russian Federation have been seen as failures, and Russia's actions in Ukraine, Syria, and other parts of the world have demonstrated that it is prepared to use novel tools—including sophisticated propaganda and cyberattacks—to gain a strategic advantage over NATO. A study of three Russian television stations and an analysis of tweets revealed Russia's effective use of audience analysis and deception tactics, but they also showed that some audiences have been alienated.[120] While NATO's ability to reach audiences within Russia is very limited (the media landscape is largely controlled by state-sponsored TV and radio stations, and local actors are censored or intimidated), NATO has the capacity to defend its own populations and undermine Russian actions

[117] Kjell Engelbrekt, Marcus Mohlin, and Charlotte Wagnsson, eds., *The NATO Intervention in Libya: Lessons Learned from the Campaign*, New York: Routledge, 2013.

[118] UK House of Commons Defence Committee, *Towards the Next Defense and Security Review, Part 2: NATO*, London, July 31, 2014.

[119] North Atlantic Treaty Organization, "Relations with Russia," web page, last updated April 6, 2017c.

[120] NATO Strategic Communications Centre of Excellence, *Analysis of Russia's Information Campaign Against Ukraine*, Riga, Latvia, 2015a.

in the information domain if it adopts a coherent and unified approach to this emerging threat.

Vulnerabilities in NATO IO

As Mark Laity noted in 2015, "The cadre of experienced StratCom professionals [in NATO] is still dismayingly small, as new staff arrive, do one tour, and move on never to return."[121] The fact that key personnel are constantly rotated in and out of NATO headquarters hinders the building of an institutional memory and strong interdepartmental relations; it also limits the ability of NATO's StratCom staff to develop and execute and effective long-term strategy. As the NATO Wales Summit Declaration affirmed, the effort to build a stronger StratCom capability is high on the agenda of NATO's leadership, yet the pace at which NATO's adversaries execute their information strategies and keep surprising NATO planners reflects the alliance's limited agility in the IE.

A 2015 review of StratCom practices in NATO countries indicated that the greatest capacity across these militaries is currently devoted to public diplomacy and military PA, with the relatively smallest number of personnel working on IO, PSYOP, and PA.[122] Interestingly, the most common training across NATO is in military PA, IO, and PSYOP, and no training is offered in public diplomacy or PA.[123] That review identified two weaknesses in NATO's approach to IO:

- Lack of formalised "top down" StratCom mindset, awareness, guidance and coordination.
- Incoherent information and resource silos within [government] departments.[124]

Lessons from NATO Operations in and Through the IE

NATO IO in Contrast with U.S. IO

NATO's role as a multilateral coordinator puts it in a unique position—namely because it is not in charge of many of its own resources and because of its dependency on its members. Its size and complexity are comparable to the U.S. Department of Defense. (NATO has 1,000 civilians and 500 military staff permanently based at its headquarters in Brussels, but its strategic and tactical commands host thousands of person-

[121] Laity, 2015a, p. 62.

[122] NATO Strategic Communications Centre of Excellence, *Mapping of StratCom Practices in NATO Countries*, Riga, Latvia, February 2015–June 2015c.

[123] NATO Strategic Communications Centre of Excellence, 2015c.

[124] NATO Strategic Communications Centre of Excellence, 2015c.

nel and national staff at NATO headquarters, and other offices add another several thousand.)

However, decisionmaking in NATO is not as centralized as in the U.S. Department of Defense, in which the Secretary of Defense has a near-complete authority over the department. With a consensus-based decisionmaking process, NATO's North Atlantic Council is the political body solely responsible for setting the political and geostrategic agenda of the alliance. Both the civilian and military staffs' representatives report to the council but have some autonomy in defining the specific approaches they take to implement the council's directives. The professionalism and continuity of decisionmaking are ensured by the cadre of permanent international staff, but member states exercise significant influence at both the tactical and operational levels.

This patchwork of multiple lines of oversight—each member state, in theory, has veto power, and national caveats have been commonplace in previous NATO operations, leading to internal fragmentation—leads to considerable difficulties in defining a unified StratCom policy. Given these constraints, NATO has attempted to build more-flexible capabilities, especially in responding to cyber and hybrid warfare threats, but it is not generally seen as a leader in any of these domains. Most of its expertise and capability resides within individual member states' armed forces.

Key Takeaways

Given the nature of the transatlantic alliance, NATO has yet to build an IO capability that is robust enough to deter an adversary. With the recently stood up NATO Strategic Communications Centre of Excellence and other NATO agencies tasked with a broader IO agenda, it is clear that the alliance is aware of the new challenges it faces in the information domain.

NATO's IO function is largely a coordinating one; it has no forces of its own and depends on national contributions to its missions, leaving the decisionmaking to member states.

The following are among the chief IO challenges that NATO faces today:

- a resurgent Russia with highly potent and aggressive IO capabilities (including a robust and sophisticated social media presence and an ability to influence public opinion in many NATO member states)
- a high turnover of NATO IO experts at the headquarters level, as well as in strategic and tactical commands, which limits the alliance's ability to retain institutional memory in the constantly changing information domain
- a possible lack of unity that a cyber or other form of nonlethal attack may elicit among NATO member states, crippling the allied response to the attack (though it faces this challenge in traditional warfare as well)

- a limited toolbox to engage domestic populations, particularly in times of crisis[125]
- slow response times, given NATO's institutional and decisionmaking complexity, particularly compared with the pace of the modern news cycle, the use of nontraditional media to distribute content (videos, blog posts, and promoted digital content, often tailored to specific population segments), and the pollution of the information domain by discordant messages from multiple sources.

[125] NATO does not have the capability to communicate with the citizens of its member states should their national governments become incapacitated and lines of communication interrupted.

CHAPTER THREE

Canada

Case Summary

Canada positions itself to its home audience as a global partner—specifically, featuring itself in a stabilization operations role. The focus is mainly on interoperability with partners, and it is not overly focused on constructing an individual narrative of force domination. The Canadian Armed Forces (CAF) have a series of IRCs, or "enablers," in their arsenal, though synchronization of IO remains a work in progress.

Once personnel are funneled into a state of high readiness, the functional model of the Canadian military requires individual operators to execute requirements in support of specific commanders' operations in a specific mission. There is no standing command dedicated to IO, so enablers tend to be integrated on a situational basis, in many cases by the military's reserve personnel, who are trained but do not hold a specific military occupational specialty (MOS). Pockets of excellence do exist; for example, elements within the CAF, such as the Influence Activities Task Force (IATF), are standardizing training, planning, and doctrine.

Canada has made progress in synchronizing PSYOP and CIMIC into colocated "influence activity" (IA) companies, but full strategic coordination with counter-command activities and information-protection activities has yet to occur, leaving the importance and fit of IO within Canadian national missions undefined. Beyond the military's commitment to high-readiness training, the IA structure at the company level has not deployed in more than five years, so it is unknown whether the current operating model adequately aligns with the execution of strategic IO goals. Cyber is beginning to receive increased attention and could provide an opportunity for the Canadian Department of National Defence (DND) to reassess its organizational priorities. There is some evidence that the integration of IO enablers may be on the horizon, but without a high-level champion to advocate for synchronization, questions remain about whether such changes will meet the demands of a quickly evolving IE.

Background and Overview

Canada is a U.S. ally and is aligned with its continental and NATO partners on bilateral and multilateral issues. The CAF's three roles are (1) protecting Canadians, (2) defending North America in cooperation with the United States, and (3) contributing to international peace and security.[1]

Canada positions itself to its home audience as interoperable with other partners' forces and specifically portrays itself playing a stabilization operations role, albeit without emphasizing IO as a critical enabler. It associates U.S. forces with leading the counterterrorism effort, the United Kingdom with a counterfinancing role, other partners with leading counterinsurgency efforts. While these generalizations are perhaps simplistic, they nonetheless position Canada as a participatory ally in multilateral campaigns.

The CAF structure has moved away from the U.S. inform/influence construct to focus on interoperability with the tactical and operational influence activities of the NATO and FVEY (Australia, Canada, New Zealand, United Kingdom, and United States) communities. The nation's strategic communication efforts tend to focus more on its domestic audience.

Canadians have filled hefty roles in Iraq and Qatar and may be looking to serve in an expanded role in FVEY and NATO operations.[2] Canada's most recent land operations doctrine (2008) highlighted its alliance with NATO, with a section on IO outlining "the broad Info Ops doctrine generally accepted across the NATO alliance in order to place it in the perspective of coalition operations."[3] These alliances have continued, with CAF involvement in various NATO IO panels and CAF personnel filling positions at multinational headquarters and on NATO missions.

Justin Trudeau's administration has indicated that it plans to play up this compatibility narrative. In a March 2016 visit to the White House, the new prime minister amplified this point by playing *down* the size of Canada's military:

> One of the things that we highlight is the fact that we have different scales. . . . [This] is actually a benefit in that we can complement each other in our engagement with the world and our approach to important issues.[4]

[1] Canadian Department of National Defence and Canadian Armed Forces, *A Role of Pride and Influence in the World: Canada's International Policy Statement*, Ottawa, Ont., April 2005, p. 1.

[2] John Paul Tasker, "Top Ranks of Canadian Forces Get Shake-Up with New Army, Navy Commanders," CBC News, January 19, 2016.

[3] Canadian Armed Forces, *Land Operations*, Ottawa, Ont., B-GL-300-001/FP-00, January 1, 2008.

[4] Obama White House, "President Obama and Prime Minister Trudeau Hold a Joint Press Conference," video, March 10, 2016.

Trudeau's intention may have been to manage the expectations of global partners, some of which have questioned whether Canada carries its weight. However, Canadian researchers assessed the country's development assistance and defense spending, reporting that

> Liberal and Conservative governments both made similar higher commitments to global engagement between 1975–1995 and similar lower commitments between 1995–2014. . . . [T]he difference in commitment to global engagement between these two eras is 10 times greater than the difference between parties within each era.[5]

This drawdown is clearly depicted in the realm of Canadian IO. After personnel are funneled into a state of high readiness, the functional model of the Canadian military requires individual operators to execute requirements in support of specific commanders' operations on a specific mission. There is no standing command or high-level champion dedicated to IO, so IRCs tend to be integrated on a situational basis. There has been progress in synchronizing PSYOP and CIMIC into colocated IA companies, but full strategic coordination with counter-command activities and information-protection activities has yet to occur, leaving the importance and fit of IO within Canadian national missions undefined. This may be changing, however: The DND has noted that "Canada is facing a range of new challenges, from the rise of terrorism in ungoverned spaces, to the expanded use of hybrid tactics in conflict, to new opportunities and vulnerabilities associated with the space and cyber domains."[6]

IO could serve as an enabler as the CAF reposition for the future. Canada is exploring a new peacebuilding agenda, and the administration is considering proposals to deploy troops, likely to Africa, as part of its pledge that Canada is back on the world stage. A 2016 statement by Defence Minister Harjit Sajjan's emphasized the importance of consistency between the nation's message and action: "We will be moving ahead on this because it's very important to send a message to our multilateral partners that Canada will play a responsible role in the world."[7] Performance will reflect whether the say-do gap is filled.

[5] Robert Greenhill and Megan McQuillan, *Assessing Canada's Global Engagement Gap*, OpenCanada, October 6, 2015.

[6] Canadian Department of National Defence and Canadian Armed Forces, "Defence Policy Review," web page, last updated November 16, 2016d.

[7] Bruce Campion-Smith, "Liberals Consider Peacekeeping Mission to Africa," *Toronto Star*, July 14, 2016.

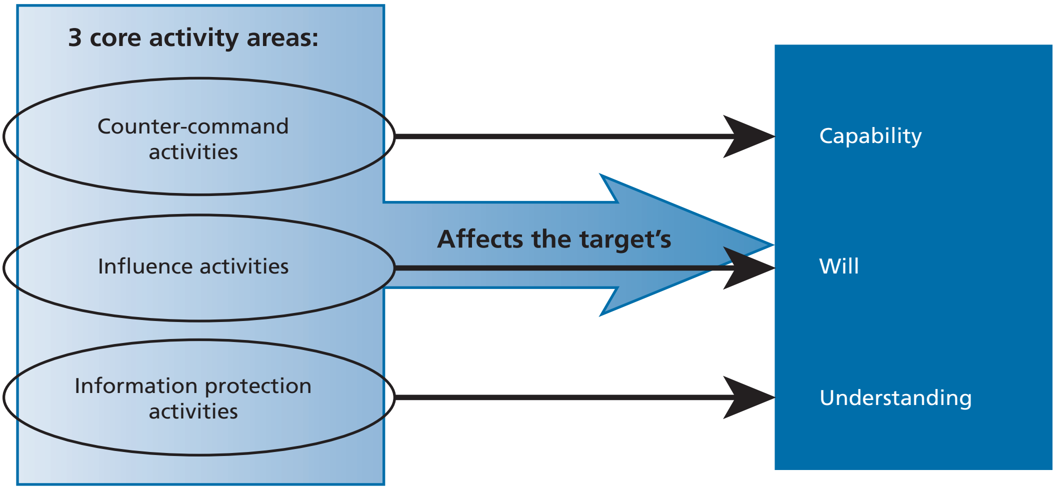
Concepts and Principles for Operations in and Through the IE

Strategic Goals/Vision

In Canada, IO "are not operations per se; rather, they are a doctrinal construct that includes a 'collection of capabilities related to maximizing the use of information while at the same time denying it to the adversary.'"[8] The Canadian IO enterprise is a larger umbrella of *influence activities*, *counter-command activities*, and *information protection activities*, designed to affect the target's capability, will, and understanding (see Figure 3.1).[9]

While Canadian doctrine highlights this focus on IO, formal policy declarations reveal limited references to the direct role of IO within Canada's strategic goals, and overall documentation is somewhat scarce. Until mid-2017, Canada's most recent strategic vision was delineated in its *First Defence Strategy*, published in 2008 to inform a 20-year plan to strengthen key military capabilities.[10] The current government issued an updated review of Canada's defense policy in June 2017 specifying plans to increase

Figure 3.1
Construct of Canadian Information Operations



SOURCE: NATO model from Canadian Armed Forces, 2008, p. 5-46, Figure 5-13.
RAND *RR1925z2-3.1*

[8] Matthew A. Lauder, "The Janus Matrix: Lessons Learned and Building an Integrated Influence Activities Capability for the Future Security Environment," *Canadian Army Journal*, Autumn 2013, quoting Canadian Armed Forces, 2008, p. 5-44.

[9] Canadian Armed Forces, 2008.

[10] Canadian Department of National Defence, *Canada First Defence Strategy*, Ottawa, Ont., June 2008.

investment in IO and cyber capabilities (including cyber threat detection and response), as well as intelligence support to operations and joint ISR.

Among the primary goals of the new policy are to "defend Canada, work with the United States in the shared defence of North America, and be a credible and engaged international actor."[11] The policy also specifies the following CAF core missions, among others, as well as deployment capabilities in support of the policy's goals:

> - Lead and/or contribute forces to NATO and coalition efforts to deter and defeat adversaries, including terrorists, to support global stability;
> - Lead and/or contribute to international peace operations and stabilization missions with the United Nations, NATO and other multilateral partners;
> - Engage in capacity building to support the security of other nations and their ability to contribute to security abroad; . . .
> - Provide assistance to civil authorities and non-governmental partners in responding to international and domestic disasters or major emergencies.[12]

The government's 111 military investment goals include plans to increase the cyber force and to create a new MOS for cyber operators.[13] Also notable in terms of Canada's capabilities in the IE is a focus on "the development of military-specific information operations and offensive cyber operations capabilities able to target, exploit, influence, and attack in support of military operations."[14]

The administration's plans for the Canadian Army focus on modernization and agility, along with increased investment in C2 and communication capabilities. These goals align neatly with the vision statement of the Canadian Army: to "produce combat-effective, multipurpose forces that deliver focused and integrated land effects across the full spectrum of operations."[15]

How IO Fits Within Canada's Overall Strategic Goals

Despite plans to invest in IO capabilities, the new policy does not feature the IE as a focal point, and as of today, there is no standing command or unit structure at the strategic or operational levels for IO. Because IO does not have a high-level champion within the CAF, the importance and "fit" of IO within Canadian national missions appear to be determined on a situational basis.

[11] Canadian Department of National Defence, 2017, p. 16.

[12] Canadian Department of National Defence, 2017, p. 17.

[13] Canadian Department of National Defence, 2017, pp. 106–113.

[14] Canadian Department of National Defence, 2017, p. 41.

[15] Canadian Department of National Defence and Canadian Armed Forces, "Canadian Army," web page, last updated August 3, 2016b.

Targets and Audiences

CAF IO doctrine generally parallels U.S. models, stating,

> IO targets are determined by the Commander's global objectives and are influenced largely by in-depth intelligence analysis. Intelligence support to the Commander should include the development of databases and templates to determine the vulnerabilities of an adversary's information, information-based processes, and information systems. Conversely, the [IO Coordination Cell] should identify the vulnerabilities of friendly information, information-based processes, and information systems that an adversary is likely to target.[16]

The following are examples of CAF IO targets:

- leadership: key personnel, StratCom, organizational power base
- military infrastructure: commanders, C2 communication links, C2 nodes, troops, intelligence collectors
- civil infrastructure: communication links and nodes, industry, financial sector, population
- weapon systems: planes, ships, artillery, precision-guided munitions, air defense systems.[17]

Canada's land operations doctrine, updated in 2008, notes that targets and audiences vary with the operational mission, depending on the perception, will, or behavior to be affected. For example,

> Activities on the psychological plane and their resulting effects may seek to: undermine an *adversary's* cohesion and will (e.g., PSYOPS); influence a *commander's* perception of a situation (e.g., deception); affect the perceptions and understanding of a *populace and their leaders* (e.g., the profile of forces and CIMIC projects to gain campaign legitimacy); and, inform a *general public* (public affairs).[18]

Doctrinal Principles

Canadian doctrine and policy can be classified under one of four general categories: strategic directive or policy; joint doctrine, which cross-cuts organizations involved in a single mission set (such as IO doctrine); environmental doctrine, which is service-specific (such as land operations doctrine); and TTPs and doctrinal notes, which are written into systems and procedures to guide operations and activities.

[16] Canadian Armed Forces, *CF Information Operations*, B-GG-005-004/AF-010, April 15, 1998, pp. 1-11–1-12.

[17] Canadian Armed Forces, 1998.

[18] Canadian Armed Forces, 2008, p. 5-3. Emphasis added.

Formal doctrine for IO and related IRCs (or, "enablers," as the Canadians call them) at the tactical and joint levels remain "woefully out of date."[19] Moreover, the cornerstones and pillars of capabilities have largely not yet been sorted. (The few cases when they have—as in the 1998 military deception (MILDEC) doctrine—it was through the lens of a different IE.) Table 3.1 provides examples of the age of relevant Canadian doctrine.

Ideally, all doctrine and policy would be harmonized across all tiers, but this rarely happens in reality. By the time doctrine or policy is written, it is often outdated because it takes so long to prepare and affirm.

Consequently, doctrinal notes offer the most tactical and practical use. However, relying on doctrinal notes creates a clear concern for IO: These methods fail to institutionalize IO as an integrated construct. This increases the likelihood that best practices and new techniques will not become institutionalized across the CAF, contributing to capability excellence gaps. It may also produce expectations that diverge from actual practice.

Further, since some doctrine is limited to individual services, there is a potential gap in coordination within capabilities. For example, while there is Army MILDEC

Table 3.1
Published Canadian Armed Forces Doctrine

Doctrine/Policy	Last Published
Policy guiding application of IO	2004
Joint IO doctrine	1998
Joint PSYOP doctrine	2004
CIMIC doctrine	1999
Land operations doctrine	2008
MILDEC doctrine	1998
EW doctrine	2011
CIMIC doctrine	2006
PSYOP doctrine	2010
Key leader engagement doctrine	Not published
Media operations doctrine	Not published
Operations security (OPSEC)	Not published
Presence, posture, and profile	Not published
Cyber	Not published

[19] Lauder, 2013.

doctrine, there is none in the Navy or Air Force. Likewise, there are nontraditional environments that will call for the Canadian Army to conduct PSYOP; the Canadian Air Force provides a platform to drop leaflets, and the Navy provides a platform that may be used for broadcasting. While these capabilities may reside in one service, in actuality, they are joint capabilities. The absence of standardized or joint-level coordination doctrine for these capabilities may create a risk, since multiple elements within the CAF have a role to play.

Current land operations doctrine, issued in 2008, describes the standing IO doctrine as "motivated by rapid technological advances in information processes, but lack[ing] a fathering and guiding holistic philosophy and set of principles."[20] Generally speaking, the 2008 doctrine states that "activities and their effects exist on two planes, the physical and the psychological, and activities fall into two categories, physical activities and influence activities."[21] It highlights the relationships between these operating planes and the functions within each. There is a conceptual recognition that physical activities should be planned and conducted so that they also have second-order effects on the psychological plane.[22]

Offensive (physical) IO

> are conducted to physically destroy, attrite, disrupt, or deny the use of the electromagnetic spectrum and its supporting infrastructure. These may stem from a physical attack . . . (e.g., raid, attack) against a C2 system, or from an attack via the electromagnetic spectrum. The aim is to contribute to the defeat of opposing forces by rendering them unable to accurately perceive situations, make decisions, or direct actions in a timely manner to carry out their intentions.[23]

Aerospace doctrine from 2010 notes that understanding the IO process will help commanders consider the possible effects of their actions and how they can use these effects to shape the information domain to maintain or gain an operational advantage.[24] It also highlights "coordination across the informational domain, including the seamless integration of Air Force info ops capabilities and activities into the overall campaign plan," including PSYOP, computer network operations, and electronic warfare.[25]

[20] Canadian Armed Forces, 2008, pp. 5-44–5-45.

[21] Canadian Armed Forces, 2008, p. 5-2.

[22] Canadian Armed Forces, 2008, p. 5-4.

[23] Canadian Armed Forces, 2008, p. 7-24.

[24] Royal Canadian Air Force, "Chapter 5: The Functions of Canada's Air Force," *Canadian Forces Aerospace Doctrine*, last updated June 20, 2016.

[25] Royal Canadian Air Force, 2016.

Aerospace EW doctrine from 2011, one of the more recently updated CAF doctrine documents, also recognizes the need for integration:

> As the Air Force develops and becomes reliant upon a network-centric warfare approach, the usage and reliance on a broader range of the EMS [electromagnetic spectrum] will emerge. Therefore, EW elements, electronic warfare support, electronic protection, and electronic attack, across the broader EMS will become essential [network-centric warfare] considerations. And as such, those agencies external to DND who control and regulate the usage of the broader EMS will need to be included in the collaborative effort to implement Air Force EW activities.[26]

It continues,

> The Air Force rarely acts alone, and as such, it is necessary to develop the means for integrating EW activities into joint and combined plans. EW activities have the potential to impact external agencies as well. It is essential that EW activities are effective and do not interfere with friendly forces or those other agencies that require unfettered access to the EMS.[27]

Generally speaking, current service and joint doctrine have not been fully updated to account for changes in the IE, including

> changes to the operating environment, in particular the inclusion and pervasiveness of the Internet and social media as a means of communicating to target audiences, establishing and maintaining human terrain situational awareness, or facilitating cooperation with non-government and international organizations.[28]

Thus, key emerging principles in new doctrine will drive IO's applications broadly across the spectrum of force—OPSEC in defensive efforts, as well as offensively through counter-command efforts and campaigns to exploit low morale among adversary fighters and supporters. New doctrine is not expected to be available until around 2018, rewritten to reflect the evolution of IO coordinating functions since 1998. The Strategic Joint Staff commissioned an IO policy review in 2015, and the draft policy document was awaiting ratification at the time of this research.

[26] Royal Canadian Air Force, *Aerospace Electronic Warfare Doctrine*, Ottawa, Ont., B-GA-403-002/FP-001, March 2011, p. iv.

[27] Royal Canadian Air Force, 2011, p. 23.

[28] Lauder, 2013, p. 40.

Canadian IO/Information Warfare Organization

Structure

The Minister of National Defence is a Cabinet member who leads the CAF, DND, Defence Research and Development Canada, and other organizations. CAF components include the Canadian Army, Canadian Navy, Royal Canadian Air Force, Canadian Joint Operations Command (CJOC), and Canadian Special Operations Forces Command, along with support organizations.[29]

Canada does not have a system like the National Guard in the United States because its provinces do not control any armories, equipment, or reserve personnel. The DND has federal ownership of the country's regular and reserve force footprints and can operate within Canadian borders, unlike the U.S. Department of Defense. Each divisional headquarters has at its disposal one mechanized brigade group, an Arctic response company, a search-and-rescue team, and an immediate response unit to address domestic crises and provide aid to civil power.

The Canadian Army is the CAF's land component. The Army reported a force strength of around 50,500 as of mid-2016:

- 21,600 members serve as full-time soldiers in the Regular Force
- 24,000 are part-time, volunteer soldiers in the Reserve Force
  – including 5,000 Rangers who serve in sparsely settled northern, coastal and isolated areas of Canada)
- 4,900 civilian employees who support the Army.[30]

The Canadian Army has 13 brigades, including three symmetrically designed, equipped, self-sufficient, field-ready Regular Force mechanized brigade groups and ten Reserve Force brigade groups. Units are spread across four geographic regions: 2nd Canadian Division (Quebec), 3rd Canadian Division (western Canada), 4th Canadian Division (Ontario), and 5th Canadian Division (Atlantic region).

Unlike the deployable headquarters construct of U.S. divisions, CAF divisions largely provide force generation to prepare for operational deployments. The 2nd, 3rd, 4th, and 5th Canadian Divisions do not pick up and go. They are static and provide support for the geographic regions they cover. These divisions recruit, train, equip, and funnel personnel into high-readiness units. (There is always one group in reconstitution, one retooling, and one in high readiness.) When the balloon goes up, the group in high readiness will strike up a headquarters and push out the door.

Under this structure, a division has never gotten to the point that it could force-generate enablers (i.e., IRCs), even though there was a period when institutional support

[29] See Canadian Department of National Defence and Canadian Armed Forces, "Organizational Structure," web page, last updated May 1, 2017a.

[30] Canadian Department of National Defence and Canadian Armed Forces, 2016b.

was building for CIMIC and PSYOP career paths. As the CAF experienced greater force reductions over time, they eliminated numerous occupational specialties that became too small to support. Since the return of peace following World War II, the size of the Regular Force declined from as high as 110,000 personnel to today's level of 68,000, which is slightly lower than the total number of active-duty U.S. Special Operations Command personnel, National Guard personnel, and reserve personnel from the four U.S. service component commands and eight sub-unified commands.[31] Consequently, Canada removed tactical enablers from its structured Regular Force mechanized brigade groups and order of battle, and they became secondary support functions as part of the Reserve Force brigade groups.

IO enablers are found in both the Reserve Force and the Regular Force. PSYOP and CIMIC are Canadian Army Reserve capabilities, while EW and cyber are joint functions primarily owned by the Regular Force (though there is a Reserve Force unit as well). Reserve Force personnel augment Regular Force components by serving as the CAF's primary operators for IA. There are ten such companies—one assigned to each brigade group.

Canada's equivalent to the U.S. Army's Training and Doctrine Command—the Canadian Army Doctrine and Training Centre—plans and manages the intellectual development and training of the Canadian Army, including all personnel deployed as part of a task force or joint task force.[32] In 2014, a subordinate unit within the Canadian Army Doctrine and Training Centre was created as a first step to organize nonkinetic enablers (including those related to IO) under one support battalion.

That unit, the Canadian Army Enablers Group, includes multiple organizations, such as the Peace Support Training Centre (also known as the IA/IO schoolhouse), which serves as the Canadian Army's center of excellence for the development of IA capabilities (PSYOP and CIMIC).[33] It also includes the Canadian Army Intelligence Regiment and the IATF. The role of the Canadian Army Enablers Group is in transition; as of this writing, the Canadian Army was assessing how it should look and function. It was expected to reach full operational capability around 2018 and be responsible for providing force development, force generation, and operations support for its assigned enablers.

The IATF was established in 2009 to manage and coordinate the institutionalization and professionalization of IA in the Canadian Army and, by extension, the CAF.[34]

[31] Canadian Department of National Defence and Canadian Armed Forces, "Frequently Asked Questions," web page, last updated October 27, 2017; Andrew Feickert, *U.S. Special Operations Forces (SOF): Background and Issues for Congress*, Washington, D.C.: Congressional Research Service, April 8, 2016.

[32] Canadian Department of National Defence and Canadian Armed Forces, 2016b.

[33] Canadian Department of National Defence and Canadian Armed Forces, "Peace Support Training Centre (PSTC), web page, last updated August 22, 2016c.

[34] Lauder, 2013.

It is the most clearly recognizable organization within the IO enterprise, acting as a chief proponent for IA in the CAF and representing the CAF on NATO and FVEY working groups. Even while it stands out as a leading initiative, the task force's reputation has taken a while to develop; in 2013, it was previously described as "little known [within the CAF] and even less studied."[35] The IATF is the broader organization for force development/employment and force generation for IA as a capability. It is largely a tactical-level entity, as are IA capabilities, but it is often asked to fill a high-tactical/low-operational–level headquarters role. The IATF has three functional sections:

- operations officers for headquarters support
- the Field Force Support Group, which supports collective IA training, including the IA portion of the CAF's annual Road to High Readiness Plan that specifies which division is responsible for which brigade and which training gaps need to be filled to meet staffing requirements[36]
- the Plans and Capabilities Development Group, responsible for the IA implementation planning and directives, force development, doctrinal notes, policy, and TTPs.

The IATF is led by a commanding officer at the lieutenant colonel level and is based in the 1st Canadian Division. It consists of 35–50 people, depending on the year. Members in full-time billets serve in a three-year secondment and are responsible for training their own replacements during each six- to eight-month transition period. Those serving in IATF positions are able to develop their cognitive skills and receive extensive training through self-directed IA training courses offered by the United States, the Netherlands, Germany, and NATO.

Each division maintains its respective ownership for IA. These units have a "dotted-line" reporting relationship with the IATF. As part of the restructuring of the Canadian Army Enablers Group, proposals have called for the IATF to operate as a permanent regiment rather than a task force.

PA is a fully joint capability, listed with its own trade classification. The Army, Navy, and Air Force PA branches report into the Assistant Deputy Minister for PA, whose mission is to "deliver excellence in communications advice, guidance, services and products in support of Government of Canada and its defence priorities."[37] This office reports to the Chief of Defense and the Deputy Minister of Defence under a

[35] Rita LePage, "Understanding Influence Activities," *Vanguard*, February 19, 2013.

[36] The Field Force Support Group is available (when necessary) to deploy personnel to support operations with the 1st Canadian Division

[37] Canadian Department of National Defence and Canadian Armed Forces, "Assistant Deputy Prime Minister (Public Affairs)," web page, last updated December 8, 2016e.

general agreement within each service branch that PA resides under IO and needs to be coordinated with other IO enablers.

To ensure that a strategic narrative is coherent before it is delivered, coordination is required among the Privy Council Office, which serves in an integration role similar to the U.S. National Security Council staff; government ministers (the Cabinet); deputy ministers (who represent the civil service); and the Office of the Prime Minister. The Office of the Prime Minister holds ultimate decisionmaking authority for PA on a broad level.

Counter-command and information protection activities are dispersed across entities at the tactical and operational levels. Canadian Army doctrine highlights this distinction: "While this [IO] section will embrace the Counter Command Activity and Information Protection Activity components of Info Ops Doctrine, the main focus of land Info Ops is Influence Activity."[38]

Counter-command activities are joint functions spread throughout regular and reserve force squadrons and regiments, covering exploitation, penetration, defense, and other activities. EW and cyberwarfare are joint IO capabilities, with elements and varying skill sets spread across different platforms and equipment in the Canadian Army, Air Force, and Navy. The CAF Communications and Electronics Branch, which has more than 7,100 members, serves as a unifying personnel branch providing cohesive professional groups for those in related occupations.[39]

One of those groups is the 21st EW Regiment, which provides trained Army EW operators and support personnel to the CAF. It is the only reserve EW squadron that is a part of the Regular Force. This allows the unit and its members to train, exercise, and deploy with both regular and reserve units throughout the country and (voluntarily) deploy overseas. Personnel deploy both in their EW specialties and in positions related to their initial military trade training.[40] The 21st EW Regiment has three Regular Force units and one Reserve Force unit, but none are permanently in the mechanized brigade groups. The mechanized brigade groups assign personnel and assets to units that are fielded operationally and in support of major exercises, and they also establish EW coordination centers.

The Assistant Deputy Minister for Information Management, like the Assistant Deputy Minister for PA, reports to both the Chief of Defense and the Deputy Minister of Defence. But while the CAF IO Group and EW Centre in Shirley's Bay, Ottawa, are subsidiaries of the Assistant Deputy Minister for Information Management, the focus is less on IO and more on network operations, with computer network defense and C2 serving as these organizations' core functions. There is an ongoing effort to better

[38] Canadian Armed Forces, 2008, p. 5-45.

[39] Canadian Department of National Defence and Canadian Armed Forces, "Organization—Communications and Electronic Branch," web page, last updated July 28, 2015b.

[40] Canadian Army, "21 Electronic Warfare Regiment," web page, last updated June 23, 2016.

define C2 activities because strategic and operational lanes have crossed as the IE has evolved. This is an important area for future attention, since cybersecurity is emerging as a higher priority for the government and among the public.

There are no permanent CAF regiments dedicated to information protection activities; such activities are overseen by the operational command of the deployed force.

When a high-readiness group pushes out the door, planners within the G9 (captains/majors or senior noncommissioned officers) create a planning cell, or IA coordination center, to facilitate integration at the tactical level. The commander decides what composition of assets should be taken. This deployable headquarters is not a standing, permanent body; there have been varying structures used for this purpose, and understanding of what a coordinating center should look like is still developing. (The IATF has three centers: one that supports the 1st Canadian Division, one to support the division/brigade on the road to high readiness, and one to support the division/brigade at high readiness.)

One exception is the 1st Canadian Division, whose command authority transferred from the Canadian Army to CJOC in 2015. As a subordinate command of CJOC, it is not a typical division of symmetrically designed mechanized brigade groups. It uniquely functions as a deployable headquarters staff that forms as a multinational joint interagency task force when deploying, similar to the U.S. construct. If the 1st Canadian Division needs to deploy, it draws on the IATF to staff its IA coordination center and make up the vast majority of its J9 staff, because of its joint structure.

The role of IO within joint commands is also developing. The joint operational structure is a relatively new construct in the CAF. Combatant commands were created in 2004–2005 and later transformed in 2011–2012, when an amalgamation of commands and further restructuring of the CAF found greater efficiencies. In October 2012, CJOC was stood up to replace three of four joint formations to conduct domestic and continental operations, expeditionary operations, and operational support. (Canadian Special Operations Force Command remained intact as the home of the special forces community.)[41]

CJOC develops, generates, and integrates joint force capabilities in seven operational domains, including IO, IA, cyber support, and operational support. CJOC's component commanders contribute to the understanding of the operating environment, inform and support engagement, and participate in contingency planning and readiness activities.[42] However, the efficacy of CJOC's broad planning ability for IO and IA coordination functions is unknown.

[41] Canadian Department of National Defence and Canadian Armed Forces, "Canadian Joint Operations Command," web page, last updated December 8, 2016f.

[42] Canadian Department of National Defence and Canadian Armed Forces, 2016f.

Fortunately, the 1st Canadian Division and the IATF are in close proximity to each other. During mission planning, an IATF liaison officer is embedded within the division.

Upon deployment as an expeditionary or domestic task force, the 1st Canadian Division creates a task force headquarters element under the command of CJOC. To address its current IO capacity gap, the division has added a strategic communication adviser to its headquarters staff, as well as an IO officer to lead a small IO cell. This coordinates efforts, through CJOC, with the Strategic Joint Staff's cyber and IO desk (a three-person team serving the four-star Chief of Defense in an advisory role). The cyber and IO desk coordinates tasks at the strategic level to ensure that suitable IO rules of engagement are in place and to facilitate the task force's efforts. The offices of the assistant deputy ministers for PA and policy are involved in crafting messaging, and there is significant effort to coordinate all stakeholders through a joint operational planning group. CJOC serves as the key facilitator of these meetings and helps ensure that the requirements of the 1st Canadian Division's task force are met.

While not nearly the size of the U.S. Joint IO Warfare Center in San Antonio, Texas, such staffing initially institutionalizes command-level activities by ensuring that IO efforts can deliver input to achieve desired effects and by coordinating non-munitions enablers in conjunction with the 1st Canadian Division.

Prior to adopting this structure, IO coordination with joint fires and effects was essentially executed through ad hoc agreements in support of a J9 equivalent; in between were a joint EMS coordination center and Reserve Force personnel engaged in IA. This was managed below the operational command level for expeditionary efforts.

In summary, Canadian organization for IO remains a mixed bag. There are IO capabilities, but there is no hard-and-fast command structure for IO force generation at the strategic or operational level, nor does there appear to be much appetite for force employment of IO at the tactical and operational levels. While there is some evidence of IO deployment (notably for EW), there is typically no one responsible for coordinating all IO enablers, particularly at the tactical and operational levels.

Funding and Legal Authorities

Budgetary resources for the DND in 2015–2016 were estimated at $18.9 billion. This, and the department's total planned human resources (68,000 Regular Force personnel, 24,000 civilians, and 27,000 Reserve Force personnel), were projected to hold relatively steady for the following three years.[43] However, funding amounts for IO and its respective enablers were not specifically available at the time of this research, leaving the scalability of this structure in comparison to U.S. forces unknown.

Like the United States, Canada can influence foreign populations. Unlike the U.S. Department of Defense, however, the CAF are not constrained from fielding IA

[43] Canadian Department of the National Defence and Canadian Armed Forces, *2015–16 Report on Plans and Priorities*, Ottawa, Ont., 2015a, p. 19.

(PSYOP and CIMIC capabilities) domestically. If there is a national defense matter, the government can enact the Emergencies Act, which provides it with broad powers to deploy the military.[44] In such cases, PSYOP teams generally provide support through aid to civil power or domestic response operations. For example, CAF PSYOP personnel have assisted with product dissemination (e.g., posters, leaflets) during floods, ice storms, power outages, and other disasters.

To target the domestic audience with PSYOP teams, the Minister of National Defence is required to go before Parliament to secure additional authority from the Prime Minister. But there are no legal constraints on such a request, according to PSYOP doctrine:

> PSYOPS can be used throughout the entire spectrum of CF operations. CF commanders are permitted when authorized, to execute Offensive IO such as PSYOPS that negate, alter, impair or destroy information or the information infrastructure of Canada's opponent in an international military crisis or war emergency. However, CF PSYOPS Policy underline that CF will not engage PSYOPS in domestic operations except at the direct request/approval of Cabinet. Use of PSYOPS domestically must be in accordance with applicable Canadian law and Canadian doctrine. *This limitation will still provide the [government of Canada] options in a time of crisis.*[45]

Thus, the CAF could, with Cabinet approval, conduct PSYOP in support of law enforcement efforts to diminish the radicalization efforts of terrorist organizations or to address other exigent needs. This is a notable difference from the authority granted to the U.S. military, which is bound to restrictions associated with *posse comitatus*.

Canada's cyber capabilities and related authorities and constraints were unclear in a review of government records. Its military is prohibited from conducting offensive cyber operations and, according to press reporting, may even lack an effective defensive capability in this domain. Canada's electronic spy service, the Communications Security Establishment—which operates independently from the DND—is devoted to protecting civilian infrastructure and working with utilities and major corporations to help them protect their networks, but it is possible that it could develop an offensive posture if that were deemed necessary.[46]

[44] John Lindsay, "The Power to React: Review and Discussion of Canada's Emergency Measures Legislation," *International Journal of Human Rights*, Vol. 18, No. 2, 2014.

[45] Canadian Armed Forces, *Psychological Operations*, Ottawa, Ont., B-GJ-005-313/FP-001, January 15, 2004, p. 1-1.

[46] Murray Brewster, "Former CSIS Head Says Canada Should Have Its Own Cyber-Warriors," CBC News, June 22, 2016.

Enablers Employed/Available

Information Operations

Because there is limited strategic coordination of CAF IO elements, the exact size of Canada's "IO forces" is unclear. It may be deduced by the number of people in the CAF who have been "qualified IO," defined by completing the staff officer's training course at the Peace Support Training Centre or by the number of those people who have served on a mission or deployment in an IO position. Since these capabilities tend to be modularized, IO needs are defined based on the requirements for particular task forces. If there is a requirement for an IO capability (essentially, enabler integration), the enabler will be built into a specific table of organization instead of remaining available as a standing unit.

Under this structure, there is one IO billet staffed for the deployable headquarters, and the IO chief is synched with the commanding officer. Whether such a position is established is subject to evaluation. At the tactical level, there should be an IO chief designated for integrating the nonmunition enablers to deliver input to the commander on what effects will be generated. This coordination should occur at the division level through a joint IO coordination cell and IA coordination center, at the brigade level through an IA coordination center, or through an ad hoc agreement with a joint EMS coordination center.

There is no IO officer designation (like a U.S. FA30 equivalent) in the CAF. There is no formal skill identifier indicating an IO specialty, and the IO course is open to all trades for those who meet specific rank requirements. Once personnel complete the IO course at the Peace Support Training Centre, it is unclear whether they are expected to deploy in an IO capacity. It is reasonable to believe that they would serve in a coordination function, albeit without operational control (unless the commander deems otherwise, based on input from advisers and planners). However, no specific designation is issued, and "qualified" personnel are scattered throughout the CAF. Since there are no IO units to draw on, the CAF must rely on a list of trained personnel who have taken the IO course.

Those who serve in an IO role are expected to be officers who are also qualified to conduct planning. As the role of IO becomes better defined, officers selected for joint planning roles (J5) will be well positioned if they have successfully completed the IO course.

The IO course and IO doctrine cannot be read in isolation. Integrating IO enablers requires an intimate understanding of the various ways to achieve effects, which includes an understanding of CIMIC, MILDEC, and EW. Failure to do so places an operator at a disadvantage.

Influence Activities

IA is defined as

> any activity for which the primary purpose is to influence the understanding, perception and will of the target audience, be it friendly or hostile and designed to have a first-order effect that is psychological and a second-order effect that is behavioural.[47]

Land operations doctrine lists the following as IA capabilities:

- PSYOP
- CIMIC
- presence, posture, and profile
- MILDEC
- PA (sometimes referred to as *media operations*). [48]

Key leader engagement is not identified as a central IA capability in land operations doctrine. However, in practice, the deployed IA unit is responsible for coordinating and managing these engagements.[49]

Each of the ten Reserve Force brigade group regional commanders is required to satisfy an interim implementation directive by staffing an IA company of 52 personnel, or 89 with drivers and gunners, for a total of 520 personnel. Canadian brigade groups include full- and part-time reservists and can be called upon for domestic service or short-term contracts. The commanders have the ability to force-generate their IA capability to support CAF operations in different ways, depending on threat levels, geographic limitations, permissiveness in the area of operations, and available platforms. (For example, Edmonton-based reserve units range from northern Ontario all the way to British Columbia.) The Regular Force has no IA companies, but its personnel can and do serve in a variety of IA staff positions. However, the Canadian Army is in the process of standardizing the implementation of IA companies to reduce the possibility of short-staffing or overstaffing.

Each IA company generally consists of six tactical teams, with three tactical PSYOP teams in each PSYOP platoon (five operators each, supported by three to four drivers and gunners) and three tactical CIMIC teams in a CIMIC platoon (three operators each, also with three to four support personnel). This IA company structure supports the 2nd, 3rd, and 4th Canadian Divisions as specified in the Managed Readiness Plan and the Road to High Readiness Plan; one of the mechanized brigade groups is tasked with supporting expeditionary operations for one year in high readiness on

[47] Lauder, 2013, p. 34.

[48] Canadian Armed Forces, 2008.

[49] Lauder, 2013.

a rotating basis. The lead division on the road to high readiness is responsible for the force generation of the IA company, which is then attached to the mechanized brigade group during training and confirmatory exercises.

There has been discussion about whether a lieutenant colonel or major should serve as the chief IA officer dedicated to the J9, but resolution has been delayed by concerns about staff wearing too many hats. This may not position the forces for success, as it suggests that all positions cannot be filled for an exercise or operation. The current construct of the IA company was designed to support one battle group in a coalition setting, supporting CAF interoperability with NATO and FVEY partners.

This differs from the U.S. approach because the U.S. civil affairs structure is much larger (i.e., battalion size). CIMIC is managed as a tactical function, with tactical teams of operators conducting civil-military liaison in support of an operational commander. Looking ahead, there is a proposal in Canada to increase the size of IA companies beyond the current footprint to support three maneuver elements within a brigade, not one battle group. If approved, this would triple the number of tactical PSYOP and CIMIC team personnel.

While IA at the tactical level—PSYOPS and CIMIC—are principally owned by the Army and led by senior noncommissioned officers, the Navy and Air Force do have staff in the IA community, particularly as part of the IATF. PSYOP and CIMIC are fielded capabilities, with tactical teams and an organizational structure to support activities once training is completed. PSYOP personnel are trained as disseminators and generally hold the rank of master corporal or above. PSYOP roles include tactical operators, target audience analysts, production specialists, and planners.[50] CIMIC operators are restricted from holding a training rank, so they hold the rank of captain or, at least, sergeant. They need to meet a planning requirement in addition to engaging tactically in liaison activities.

There are no MOS identifications for IA specializations in the CAF; such roles are picked up as additional specialties. There are also not many full-time IA personnel because IA work is generally a Reserve Force capability. For example, an IA operator in uniform may carry an MOS identification as an infantry officer. To be promoted in rank, personnel must return to their original unit (e.g., infantry) to become a captain or major. Understandably, the actual line unit may not be particularly enthused about losing staff to IA work, as the shortage creates organizational strains, pulls, and frustration.

For example, someone who is interested in becoming a PSYOP operator and joining an IA company first submits an application to the brigade that owns the unit. Upon acceptance, the applicant is registered for a three- to four-week course at the Peace Support Training Centre, which is the schoolhouse for IA and IO individual training, as well as other courses. After completing the course, the individual is quali-

[50] Canadian Army, "Psychological Operations," web page, last updated May 6, 2017.

fied as a tactical fire operator in the IA company and positioned for future tasking as a tactical PSYOP operator. The individual is deemed "IA-ready," and the brigade is put into a state of managed readiness upon completing collective training and a series of exercises with the division and the IATF.[51]

Individuals do not change career paths by doing IA work, and there is no designated career path that leads to a highly professionalized field. To cultivate the skill sets required for a professionalized cadre of IA operators, there has been some discussion of packaging coursework, rather than assigning one-off training based on short-term needs. As of 2016, courses were available for IO officers, CIMIC operators, CIMIC staff officers, peace support operators, PSYOP tactical operators, PSYOP analysts, and PSYOP officers, among others.[52]

Part-time IA personnel are challenged to get comparable formal training, so those with an interest in such roles often hone their skills through nontraditional means. They may do so through civilian courses or practical application in their civilian roles, for reservists who work, for example, as marketing directors, psychology professors, or even graphic designers.

At the tactical level, IA personnel are sent into exercises and operations with various specialized gear. This includes tablets and various mobile devices, high-definition portable video cameras to film interactions with people, and speaker sets for broader messaging efforts.

To enable IA interoperability, MILDEC, key leader engagement, and presence, posture, and profile activities are conducted in a coordination role. There are no individual courses for these enablers. The IATF streamlines IA company training packages to prepare units on the road to high readiness. PSYOP personnel are qualified to review the MILDEC and presence, posture, and profile packages; CIMIC personnel are qualified to review the key leader engagement package; and commanders are responsible for evaluating their respective presence, posture, and profile. It is up to the commander to decide how much of each plan will be used.

Despite general agreement within each branch of the CAF that PA resides under IO—and even though doctrine recognizes PA as an influence activity—the fact that PA is identified as a "separate but related IO capability" does not indicate support for coordination. There has been no objective evaluation of the impact of linking PA and IO, but better coordination could help achieve desired effects. While certain enablers (e.g., MILDEC and PSYOPS) should keep a greater distance from PA, there is an opportunity for the CAF to connect PA to CIMIC objectives.

[51] According to our discussions with CAF officers, there is institutional pressure on the Peace Support Training Centre to move personnel through training at an aggressive pace. Whereas IA companies were previously recognized by the IATF as fully qualified when 90 percent of their billets met all requirements, the standard has been lowered to 70 percent. This could introduce some risk and future shortfalls in capacity.

[52] Canadian Department of National Defence and Canadian Armed Forces, "Courses at the Peace Support Training Centre," web page, last updated February 24, 2016a.

Land operations doctrine, published in 2008, uses the phrase *media operations*, though this capability is not defined. It is a risky term to use without detailed clarification, since both PA and PSYOP may use media, but as a means to varying ends. While the intention may have been to address emerging communication channels (notably, the Internet), its misuse could inadvertently partition the capability and limit its applicability.

Counter-Command Activities

Counter-command activities include the following:

- physical destruction or exploitation of C2, communication, and information management networks
- offensive actions that span the EMS (i.e., electronic and cyberwarfare).[53]

Canadian land operations doctrine is similar to U.S. doctrine, stating that offensive (physical) IO

> are conducted to physically destroy, attrite, disrupt or deny the use of the electromagnetic spectrum and its supporting infrastructure. These [operations] may stem from a physical attack . . . against a C2 system, or from an attack via the electromagnetic spectrum. The aim is to contribute to the defeat of opposing forces by rendering them unable to accurately perceive situations, make decisions, or direct actions in a timely manner to carry out their intentions.[54]

There are clear MOS identifications for Communications and Electronics Branch members. Occupational specialties include Officer—Communications and Electronics Engineering (Air); Officer—Signals; Communicator Research Operator; Aerospace Telecommunication and Information Systems Technician; and Army Communications Information Systems Specialist.[55]

Service members can specialize in counter-command activities after completing basic training. There is one EW regiment of 400 people in the CAF, consisting of both regular and reserve force members. Communicator research operators, intelligence operators, Army communications and information systems specialists (signals operators), and support trades receive combined training to fulfill the EW mission, which involves intercepting, locating, analyzing, and jamming a potential enemy's communications on the battlefield.

[53] Lauder, 2013.

[54] Canadian Armed Forces, 2008, p. 7-24.

[55] Canadian Department of National Defence and Canadian Armed Forces, "Communications and Electronic Branch: About Us," web page, last updated July 29, 2015c.

A CAF recruitment video portrays communicator research operators as using the world's most sophisticated electronic equipment to intercept and analyze electronic transmissions and computer data, including foreign communications. To work in the highly classified world of communications and signals intelligence, these personnel are required to complete 45 weeks at the Canadian Forces School of Communications and Electronics in Kingston, Ontario. They serve in every branch of the CAF. EW work includes low-level voice intercept with mobile EW technology, monitoring spectrums for activity that could be conspicuous, or executing actions against opposing forces. This capability allows the CAF to intercept, develop situational awareness, and intervene.[56]

The communications and information systems specialist designs, installs, and maintains satellite, wireless, and cable networks to support the entire range of Canadian Army missions, whether they involve pursuing the enemy, providing humanitarian relief after a natural disaster, or enabling the normal flow of information to and from headquarters or on bases at home. The specialist receives 18 weeks of classroom and lab training at the Canadian Forces School of Communications and Electronics on sophisticated communication equipment, from radiation detection devices to circuit boards and cryptographic gear. Courses offer a basic overview of all three branches of the specialty: communication systems, information systems, and hardwired line and cable systems. Upon completion, most specialists are assigned to a signals squadron or joint signals regiment, where on-the-job training will continue. After about a year, specialists branch out into one of the three core specialties of the trade and become attached to the artillery, the infantry, an armoured regiment, or the combat engineers.[57]

The communications and information systems specialist trade includes signallers, who operate all the equipment at hand (e.g., computers, radios, networks), and linemen, who are in charge of laying fiber-optic, Category 5, and coaxial cables. In the role of information systems technologist, the communications and information systems specialist also administers, maintains, and repairs the computer networks at bases and headquarters.[58]

Both communicator research operators and intelligence operators take a series of additional courses directly relating to EW equipment and processes. Many of these personnel have chosen to serve in various UN and NATO peacekeeping missions around the world.[59]

Communications and Electronics Branch members interact with theater-level capabilities in the Regular Force, serving the mechanized brigade groups in joint roles in signals squadrons, telecommunication and information services squadrons,

[56] Philip Kitchen and Jeff Newell, "Communicator Research Operator," video transcript, undated.

[57] Chris Tidd and Amanda Collins, "Army Communication and Information Systems Specialist," video transcript, undated.

[58] Tidd and Collins, undated.

[59] Canadian Army, 2016.

and communication regiments. They interact with Reserve Force units as members of signals regiments aligned with each of the ten brigade groups under four geographic divisions. There are no concerns that a deployed command may not have control over its capabilities, as the brigade commander ensures that the asset is available to the battle group and incorporated into the functional chain of command in the theater.

Information Protection Activities

The purpose of information protection activities is to prevent access to, or mitigate the impact of, an adversary's penetration and exploitation of CAF C2, communication, and information management activities and networks.[60] These activities can be understood as defensive actions that include

- OPSEC
- counterintelligence
- information security
- Counter–intelligence, surveillance, targeting, and reconnaissance activities
- computer network defense.

These capabilities are interdependent and interconnected, so all have a part to play during preparation for operations in the IE. For example, CJOC has published a doctrinal note on OPSEC across the CAF that focused on the protection of unclassified information from adversary exploitation. Further, Canadian Forces Intelligence Command has more formalized counterintelligence, information security, and counter–intelligence, surveillance, targeting, and reconnaissance measures in place to protect classified information.

There is no permanent group dedicated to information protection activities. Like counter-command activities, these activities and the staff who conduct them are overseen by the operational command of the deployed source. The brigade commander incorporates the activities into the functional chain of command and maintains control over the capability.

Coordination/Integration Efforts/Challenges

First, even though commanders have stood up cells and centers to support the coordination of IO enablers, integrated doctrine has yet to be issued on capability integration and synchronization. Absent a defined unit similar to the U.S. Army Civil Affairs and Psychological Operations Command, integration among capabilities remains a challenge.[61] For example, a *Canadian Army Journal* article described the state of affairs for IA integration as follows:

[60] Lauder, 2013.

[61] For more on the U.S. structure, see U.S. Army Reserve, "U.S. Army Civil Affairs and Psychological Operations Command (Airborne)," web page, undated.

> As a unified and integrated capability residing in a single force structure, IA is both a relatively new construct and, within NATO, somewhat unusual (most NATO partners do not co-locate and integrate PSYOPS and CIMIC). As a result, some capabilities within IA are nascent in terms of development or are not well established (e.g., military deception, especially as it relates to IA, and media operations), whereas other capabilities are extremely robust, such as PSYOPS and CIMIC.[62]

In addition, reliance on the Reserve Force for IA fulfillment across four divisions and 13 brigades creates the potential for misemployment. The Reserve Force does not have a training academy, so basic training is conducted locally at the company level, and it is unlikely that an infantry unit will send staff offsite for training outside their MOS. Consequently, different trainers' perspectives may yield disparate expectations for the role of IO enablers, depending on the level of training administered. For instance, a division- or brigade-level perspective is very different from that of a tactical CIMIC team that travels each day. (This underscores the importance of the IATF's training role.)

Further, there is a mingling of enablers, forced by social media, which needs to be singled out. Currently, there are no TTPs for who should own or operate in the social media space. Personnel responsible for PA, PSYOP, and cyber enablers are challenged to sort out tactical interventions online, before information fratricide occurs. It would be inaccurate to assert that the IE is limited to one capability, as social media activities, texting, and future applications present cross-cutting questions for governments, especially as target audiences achieve greater interconnectedness.

Information Operations in Practice

Examples of Interesting IO Efforts

Since the end of their combat mission in Kandahar, Afghanistan, in July 2011, the CAF have memorialized the war effort as a notable high point, largely attributed to a "whole-of-government" concept, which

> remained primarily concerned with integrating all instruments of policy, regardless of department or agency, in order to produce a desired effect linked to national strategy. The growth of the integrated approach to this conflict can be demonstrated by examining the work done in 2010–2011.[63]

[62] Lauder, 2013, p. 35.

[63] Howard G. Coombs, "Afghanistan 2010–2011: Counterinsurgency Through Whole of Government," *Canadian Military Journal*, Vol. 13, No. 3, Summer 2013, p. 17.

Beyond engaging in high-readiness training, the current IA structure at the company level has not deployed since then, so these lessons learned offer the most recent insight into Canadian IO efforts in practice. Joint Task Force Kandahar recognized IA as critical, and no operation was planned or conducted without representation from the IA group in operational planning groups and the joint targeting process. To achieve the desired security, governance, and development outcomes, Joint Task Force Kandahar saw the need to reinforce the coalition tactical operations by both military and other means:

> This gap was closed by the CAF, under the rubric of Influence Activities, (IA), where information operations, psychological operations, and civil-military cooperation (CIMIC) teams contributed to connecting the immediate effects needed by security operations within governance and development with the longer-terms programs, processes, and policies established with the assistance of agencies. . . . [T]he non-sustainable effects of the type attained by military quick action projects were connected to the longer-term sustainable activities required by sub-national and national processes through the work of IA. These small teams were attached to field forces, and they worked hand-in-hand with district stabilization teams, combined military civilian teams, which were located at district centres.[64]

The series of activities contributed to success in securing local police support; finding caches of improvised explosive devices, suicide vests, and mines; and leveraging a joint targeting process that guided lethal and nonlethal operations. There was a persistent focus on integration across all lines of operations, and strong relationships and a common vision were key. Moreover, the task force implemented cross-cutting IO with numerous PSYOP and CIMIC enablers. For example, the CAF set up a military-run radio station (RANA-FM), based out of Kingston, Ontario, to influence 15- to 25-year-olds by mixing music with a pro-NATO, anti-Taliban message.[65] Other examples included the following:

- "Local hero" campaigns portrayed Afghans in uniform on billboards alongside positive messages.
- District newsletters were well received by local populations.
- Women's affairs were legitimized by linking the Ministry of Women's Affairs with the Afghan Department of Veterans' Affairs.
- Radio literacy programming improved education levels while also introducing nonprejudicial types of literature.

[64] Coombs, 2013, p. 21.

[65] Muzaffar Iqbal, *Definitive Encounters: Islam, Muslims, and the West*, Dehli, India: Al-Qalam Publishing, 2008, p. 204.

- Schools were staffed and connected to the Ministry of Education.[66]

The impact of the enablers on the efforts of the fires and effects brigades demonstrated the value of IA and justified the addition of 60 personnel by December 2010. The increased capacity ended up supporting U.S. brigades, which required additional staffing.

Noteworthy Capability Demonstrations or Practices

Canada's most significant efforts to demonstrate its IO-related capabilities were in Afghanistan. "Route Hyena" is a noteworthy example of IO synchronization that specifically demonstrated how to link strategic objectives with tactical effects. At the strategic level, IA personnel engaged in discussions about governance, specifically seeking ways to connect people in the western Panjwai district of Kandahar. The CAF helped the agrarian society flourish by building a road to transport products to market and connect locals to government services, such as clinics and hospitals.[67] The information effects were as great—if not greater than—the physical effects of CIMIC.

IA teams have also participated in disaster assistance response teams, which deploy on short notice anywhere in the world in response to situations ranging from natural disasters to complex humanitarian emergencies. Deployment decisions are made on the advice of Canada's Department of Foreign Affairs, Trade and Development in close partnership with core departments and agencies, including the DND and the Privy Council Office. In April and May 2015, the IATF sent an IA team to assist with earthquake recovery in Nepal.[68] There, the disaster assistance response team distributed water filtration units, treated Nepalese patients, provided maps and imagery products, removed rubble and cleared roads, facilitated the dissemination of public safety announcements, and distributed crank radios to connect remote communities with relief efforts.[69]

Key IO Initiatives or Programs

In seeking to expand their nonmunition capabilities, the CAF have begun to examine the role of information and its applicability in joint targeting efforts. Because IO is recognized in Canada as a joint coordinating function, there is an opportunity to incorporate its related enablers into the six-step joint targeting cycle (commander guidance and end state, target development, capability analysis, commander decision and force

[66] Howard G. Coombs, "North Atlantic Treaty Organization System Analysis and Studies 117," Human Behaviour Representation, Research Task Group Symposium, Kingston, Ont., November 17–19, 2015.

[67] Matthew Fisher, "Route Hyena a Canadian-Built 'Dagger Through the Heart of the Taliban,'" Postmedia News, April 13, 2011.

[68] Canadian Department of National Defence and Canadian Armed Forces, "The Disaster Assistance Response Team," web page, last updated May 19, 2017b.

[69] Canadian Department of National Defence and Canadian Armed Forces, 2017b.

apportionment, mission planning and execution, and assessment). This approach and recognition of the roles of influence in the physical, information, and psychological domains offers the potential to reduce the footprint of downrange deployments in the future.[70] As nonkinetic missions are brought into the targeting process, IO can garner greater visibility of the area of operation for commanders.

Anticipated Developments

Bilateral/Multilateral Compatibility

There are ongoing discussions about integrating Canadian and U.S. forces for joint deployments under a unified command. Additional engagements are being explored with NATO and the UK-led Joint Expeditionary Force, with which the disaster assistance response team could align in noncombatant evacuation operations. According to the Canadian media, "The so-called Canada-U.S. Integrated Forces would be the result of an agreement between the two countries under which air, sea, land and special operations forces would be jointly deployed under unified command, outside Canada." While this effort would improve relationships and promote familiarity between U.S. and Canadian forces, it introduces questions about whether the CAF may continue to explore shared service agreements with other partners conducting IO.[71]

Future IO Positions

CAF IO coordination roles continue to develop. A recent U.S.-led course ("Information Environment Advanced Analysis") hosted by Australia included one Canadian political adviser and one Canadian member of the J5 staff. Within their respective sections, they served in an IO role. This is notable because should Canada's joint staff seek to further institutionalize IO, it is possible that an IO qualification will be added to the position description for future billets (such as J5 planner). This, or creating a cell within CJOC, is more likely than formalizing a standing organization within the headquarters.

Effectiveness of Canadian Information Operations

The effectiveness of IO integration in today's IE is dubious, mainly because the performance baseline has not been updated in five years. It is unknown whether Canada's current operating model adequately aligns with the execution of strategic IO goals.

IA companies were not deployed to Afghanistan until after the CAF left Kabul for Kandahar, so there is no comparative baseline to assess efforts conducted through 2011. Because the IA company structure has not been deployed since, there is still no available baseline. It is difficult to empirically evaluate what effect the changes to the

[70] Discussion with John M. Roach, Joint Targeting and Effects, CJOC.

[71] James Cudmore, "Canadian Military Ponders Integrated Force with U.S. to Respond to Hotspots," CBC News, September 28, 2015.

IA company structure will have (i.e., colocating PSYOP and CIMIC), because variables are different in each historical case.

Moreover, synchronization between IA and counter-command activities has yet to occur, despite the acceleration of connectivity between enablers due to the advancement of social media.

Information protection activities and other OPSEC efforts are likely effective, insofar as the absence of identified incidents may demonstrate that adversaries are merely failing to exploit any gaps Canada has left in this space.

Efforts of Others to Counter Canadian IO and Their Effectiveness

To date, examples of efforts to specifically counter Canadian IO are limited, though attempts could be on the rise. Recent news has revealed that the propaganda wing of ISIL has recruited "several Canadians." And when the group claimed responsibility for a series of coordinated suicide bombings and mass shootings in Paris in November 2015, the statement was delivered by a spokesman with a distinctly Canadian accent. Canadian recruits could provide insider knowledge and present long-term challenges to Canadian (and Western) IO.[72]

Vulnerabilities in Canadian IO

Many of the vulnerabilities to Canadian IO come from within. If it is not addressed consistently, the lack of an IO command structure presents the potential for information fratricide. The IO coordination board serving the 1st Canadian Division is not a standing organization at headquarters. Leadership remains critical at every level—division, brigade, tactical, and strategic—to coordinate enablers and manage the operational formations deployed.

In addition, Canadian officials still seem to maintain a narrow interpretation optimal functionality, limiting the utility of IO to individual capabilities. Coordination remains a challenge, especially during operations that focus primarily on first-order fires and effects. Education from within the CAF remains an uphill climb, especially without a high-level champion, as commanders will recognize the value of IO only when they understand the broader impact on their respective missions. This could be addressed by institutionalizing the IO role and creating a dedicated MOS.

Furthermore, the CAF have yet to document IO lessons learned, and there is no known formal movement to institutionalize knowledge in the specialty. Absent ongoing deployments, it remains to be seen whether lessons have indeed been learned and whether solutions are being put back into the CAF. This uncertainty means that the CAF may need to relearn the lessons acquired in Afghanistan in 2011, possibly in the context of preparing for another deployment. Unlike regiments that have museums

[72] Stewart Bell, "The Propaganda Wing of ISIL Has Recruited Several Canadians, Former CSIS Official Says," *National Post*, April 27, 2016.

and records of historical legacy, the temporary nature of IO and enabler roles limits investment in further institutionalizing the discipline. A CAF "statement of capability deficiency" is required to initiate a review of raw data and the development of capabilities, but no such statement has been recorded for IO. Although the Canadian Army Lessons Learned Centre is mandated to collect observations and actionable lessons from operations at the tactical level, it has not released a record of IO successes (or failures).[73] Even though enablers, like PSYOP and CIMIC, are mature, there is limited evidence pointing to practical progress in their use, leaving officials to rely on individuals who have followed the specialty for years.

Lessons from Canadian Operations in and Through the IE

Canadian IO in Contrast with U.S. IO

As discussed earlier, unlike the deployable headquarters construct adopted by U.S. divisions, CAF divisions largely provide force generation to prepare for operational deployments. They do not, themselves, deploy; they are static and provide support for the geographic regions they cover. These divisions recruit, train, equip, and funnel personnel into a state of high readiness. (There is always one group in reconstitution, one retooling, and one in high readiness.) When the balloon goes up, the group in high readiness will strike up a headquarters and push out the door. This *modus operandi* may be a reason that IO has yet to emerge as a key priority within the CAF. Despite successful efforts in Kandahar in 2011, force generation has continued to occur on a part-time basis, and there is little evidence of political will to establish a stand-alone IO force.

In contrast to U.S. forces, the smaller size of the CAF can be used to Canada's benefit because it can adapt its force to changing conditions. While Canada looks to the United States and NATO for lessons learned, it recognizes that it can readily cover joint capabilities when its forces deploy, similar to the U.S. Marine Corps.

Key Takeaways

Given the nature of Canadian IO, the CAF are moving toward synchronizing enablers, albeit more on the side of IA than counter-command activities or information protection activities. It remains to be seen whether Canada can address emerging challenges in the information domain. The key takeaways for Canadian IO are as follows:

- There is no high-level champion for IO within the CAF; the lack of a standing command reduces the strategic recognition of IO as a key priority.

[73] Canadian Army, "Army Lessons Learned Centre (ALLC)," web page, undated.

- The IA structure at the company level has not deployed since 2011; without an updated performance baseline, it is unknown whether the current operating model adequately aligns with the execution of strategic IO goals.
- The CAF are starting to organize nonkinetic enablers, including the IATF. Housing all such enablers under one unit could cultivate synchronization in the IE.
- The CAF are not constrained from undertaking IA (PSYOP and CIMIC) domestically. The government can enact the Emergencies Act, which provides it with broad powers to deploy the military, including PSYOP team support to aid civil power or domestic response operations.
- IRCs are to be included as part of the joint targeting enterprise by 2020, along with updated doctrine.
- CJOC objectives include a focus on message integration with desired effects (i.e., disruption), as opposed achieving an objective (i.e., destroy C2 capabilities).
- IO is a joint function and requires coordination across multiple service platforms; the joint targeting process may serve as a useful mechanism to achieve strategic and operational objectives.

CHAPTER FOUR

Germany

Case Summary

Since Germany's reunification in 1990, its military (Bundeswehr) has developed a unique and well-resourced capacity to engage local populations in areas of deployment and to communicate information to its troops. These two activities have been the key focus of the Center for Operational Communication of the Bundeswehr, founded in 2015, and the several battalions designated for psychological warfare before that. Given its complex history, however, Germany has a relatively narrow definition of military information: It has completely refrained from using misleading or selective information and employs strict controls to ensure that information disseminated both to its troops and to local populations is as accurate and complete as possible. The Bundeswehr's ability to counter foreign propaganda is underdeveloped, particularly in light of how the security environment has evolved in Europe since Russia's invasion of Georgia in 2008. However, the German military is constantly evaluating the effectiveness of IO and its Center for Operational Communication. Electronic and cyberwarfare capabilities are not part of German operational communication but are housed under joint staff elements. Germany has one of the three best-resourced IO (or PSYOP) capabilities among NATO member states, alongside the United Kingdom and the United States, and it regularly engages in training allied forces. In their foreign deployments, German IO personnel are typically embedded in combat and other units and rely heavily on local stakeholders to disseminate information and win public support for German strategic objectives on the ground. Similar to other European countries, Germany has effectively blurred IO and PA work, although some important distinctions remain.

Background and Overview

As initial German reluctance to support the 2011 Operation Unified Protector in Libya has illustrated, the country places a strong emphasis on using nonlethal tools to achieve geostrategic goals.[1] Yet, over the course of its modern history (since the end of communism in 1989 and reunification in 1990), Germany has developed one of the strongest PSYOP capabilities in NATO. These capabilities are intended to support the primary mission of German and allied combat troops, and Germany is actively involved, with the United States and United Kingdom, in training other allied forces in this area. With the long-standing deployment of German troops in Kosovo (deployed since 1999) and other recent experiences in Somalia (1993–1994), Bosnia and Herzegovina (1997), Afghanistan (since 2001), Croatia (1995–1996), and Macedonia (2001, 2003), German troops have contributed significantly to allied engagement of local populations in crisis-stricken regions in Europe and beyond. On the NATO Kosovo Force (KFOR), Germany has taken a leadership position in the information domain and provided key support for the mission's engagement with local populations through newspapers and radio.

Concepts and Principles for Operations in and Through the IE

Strategic Goals/Vision

With post–Cold War deployments of German troops to peacekeeping and, later, combat missions beginning in the early 1990s, a new approach to engaging civilian populations became necessary. While doctrinal and strategic documents are not publicly available, we learned from interviews and publicly available documents that the role of IO-trained officers in the Bundeswehr is to serve as a communication link among German troops as well as between the Bundeswehr and local populations. With new challenges on the European periphery, German IO officers contribute to the collection of information about local perceptions of German military activities, forge situational awareness among German troops, and communicate critical findings to senior decisionmakers. With limited engagement in other types of IO-related activities,[2] the key characteristic of German IO is a strong emphasis on sharing accurate and evidence-based information—particularly vis-à-vis local populations—to avoid this risk of being seen as disseminating manipulative or even propagandistic materials. This is largely driven by the German memory of Nazi and communist manipulation of public opinion, but it is also grounded in the principle of strong civil-military relations.

The most direct recent reference to IRCs can be found in 2011's Defence Policy Guidelines, which broadly state,

[1] Eve Bower, "Germany's Libya Policy Reveals a Nation in Transition," *Deutsche Welle*, December 9, 2011.

[2] For example, there is no mandate for IO officers to engage in or coordinate cyberwarfare or EW; these capabilities reside with the Bundeswehr IT Center.

> The growth of global interconnectedness encourages the rapid distribution and use of advanced technologies, in particular information technology. For every great opportunity there is an equally great risk. These technologies also help to mobilise pro-democracy movements. The risk of political, economic and criminal abuse by state and non-state actors is increasing. At the same time irreversible developments in the field of telecommunications and information technology have led to the almost instant, worldwide propagation of often unverified information. This gives extremists, too, numerous opportunities for disinformation and facilitates radicalisation and destabilisation.
>
> Today, information infrastructure is considered to be critical infrastructure without which public and private life would come to a halt. Due to its complexity, attacks on such infrastructure can also destabilise our state with serious repercussions for our national security. Given this threat from the information environment, governments will need to adapt the way they see and resolve conflicts. The quick and unpredictable nature of these attacks makes it almost impossible to consider the origin of enemies and their motives in our own preparatory action. The possibility of denying cyber attacks after the fact has already become a strategic element in a new type of computer-based conflict even between states and is developing into an asymmetric threat with serious consequences.[3]

Information Operations and German Strategic Goals

The current focus of German IO units is twofold: (1) serving as a communication link for German troops and fostering an internal force identity, and (2) engaging local populations in countries where German troops are deployed or could be deployed in the future.[4] To achieve these goals, Germany has built effective IO infrastructure, led by a single command (the Bundeswehr's Center for Operational Communication [Zentrum Operative Kommunikation], founded in 2014), and has gained significant operational experience since 1989. The organizational character of German institutions engaging in PSYOP and IO has changed gradually over time, however, with the most recent reform completed in December 2013. German preference for diplomatic and civilian engagement has been a key driver of the country's continual investment in its IO capability.

[3] Bundeswehr Planning Office, *Defense Policy Guidelines*, Berlin, May 27, 2011, p. 2.

[4] It broadcasts for them through Radio Andernach, founded in 1974. See Stefan Pauly, "Vier Jahrzehnte 'Radio Andernach'" ["Four Decades of 'Radio Andernach'"], *WochenSpiegel*, September 14, 2016; Bundeswehr Joint Support Service, "Operative Kommunikation—Die Medienmacher" ["Operational Communication: The Media Managers"], web page, last updated July 1, 2016d.

Targets and Audiences

Throughout its history, the targets and audiences of German IO have changed as the military has adapted to external circumstances. As we discuss later in this chapter, the original targets were primarily the political and military institutions of the adversary—both actively engaging with and countering foreign propaganda and passively studying its capabilities and vulnerabilities. After the fall of the Iron Curtain in 1989 and a shift toward peacekeeping operations around the world, German IO has predominantly turned its focus to two types of audiences: deployed German troops and the local populations with which those troops engage. Secondarily, German IO activities have expanded to benefit the troops of other allied nations (through training events and other types of collaboration). These activities also provide a source of information about German deployments for the German public (albeit without a direct intent to influence its opinions).

Doctrinal and Foundational Principles

The Bundeswehr's 2006 "white book" on defense policy described the Center for Operational Information as having a supportive role in the Bundeswehr's foreign deployments by targeting "audiences in the areas of operation."[5] While German doctrine is not publicly available, available evidence suggests that the core foundation of German IO can be summarized as follows:

- exclusive focus on disseminating verified, accurate information
- efficiently providing support and information to deployed troops and their families
- relying on positive relations with local populations to collect information and intelligence that can be used for strategic purposes.

This is distinct from the IO and information warfare concepts of the United States and others. Most other countries emphasize specific effects on adversaries' or populations' decisionmaking, perceptions, or behaviors and include at least the possibility of manipulation or deception.

High Regard for Data Privacy

According to Netzpolitik.org, a German blog on digital rights and culture, the Bundeswehr's Center for Operational Communication (the command tasked with implementing German IO in military operations) evaluates the IE to better understand public opinion and sentiment in areas of current and possible future Bundeswehr deployment. It does so using chiefly open sources, including social media, and analyti-

[5] German Federal Ministry of Defence, *White Paper 2006 on German Security Policy and the Future of the Bundeswehr*, Berlin, 2006, p. 99.

cal tools, such as Textrapic and Brandwatch, but it refrains from collecting individually identifying information (in contrast to intelligence services, in some cases).[6] As Ole Schröder, State Secretary at the Federal Ministry of the Interior, has noted, the collection of personally identifiable data is not allowed on German soil and does not occur unless as part of a formal criminal investigation.[7] Although it is unable to store any personal data, the Bundeswehr's Center for Operational Communication has used publicly marketed software to evaluate the effectiveness of its own communications, including Textrapic (an algorithm developed at the University of Rostock to analyze and graphically visualize large amounts of text) and Brandwatch (originally a British tool that assesses open-source data, which the Bundeswehr has used to inform its social media engagement).[8] Similar efforts have been undertaken by the German Foreign Intelligence Service [Bundesnachrichtendienst], which expected to invest €300 million (about $340 million) in efforts to collect information from blogs, forums, and social media in real time between 2014 and 2020.[9] It is yet to be seen if these new capabilities make the agency more effective in dealing with foreign propaganda and influence shaping. In 2014, only €6 million of the total planned funding was disbursed—a result of strong political opposition.[10]

In 2008, Germany's highest court decided that, in general, open-source collection by state authorities was allowed (including, for instance, accessing a publicly available website). However, the court specified that special permission and a mandate were needed to deliberately compile, store, and evaluate data acquired from the public domain.[11]

History and Evolution

Germany's use of media in war dates back at least to the Thirty Years' War (1618–1648), when German factions used leaflets to denounce opponents and justify their

[6] Andre Meister, "Wissenserschließung aus offenen Quellen: Wie Bundeswehr und BND die Überwachung sozialer Netzwerke rechtfertigen" ["Knowledge Discovery from Open Sources: How the Bundeswehr and BND Justify Social Network Monitoring"], Neztpolitik.org, June 25, 2014.

[7] Meister, 2014.

[8] Meister, 2014.

[9] Christian Fuchs, "Bundeswehr will soziale Netzwerke überwachen" ["Bundeswehr Wants to Monitor Social Networks"], *Zeit Online*, June 2, 2014.

[10] René Heilig, "BND ausgebremst? Irrtum!" ["German Federal Intelligence Service Blocked? Error!"], *Neues Deutschland*, June 11, 2014.

[11] German Federal Constitutional Court, *Judgment of the First Senate of 27 February 2008*, Berlin, February 27, 2008, Section 309.

own political and war claims.[12] Since then, German PSYOP methods have continually improved, peaking during the World War II era: The Nazi regime used psychological profiling to select military personnel, to rigorously indoctrinate soldiers, to advise political leaders on the management of public opinion, and to analyze the vulnerabilities of its adversaries.[13] Interestingly, Nazi officers also devoted special resources to studying the "homesickness of troops."[14] Military staff at one of the dozens of psychological testing stations and psychological laboratories in Nazi Germany were required to hold doctorates in psychology and have deep knowledge of military history and specific personality traits.[15] Moreover, the Nazi Central Psychological Laboratory for the High Command had 20 departments, all motivated by the notion that "masses of technical weapons are not themselves sufficient to win war."[16] Outside the military, the secret service consisted of an estimated 36 divisions with close to half a million personnel working in domestic intelligence and propaganda.[17] Coordination between the secret service and intelligence divisions of the armed forces was facilitated by the Cabinet Council for the Inner Defense of the Reich.[18]

Military officers working in PSYOP received three years of training, but their very first interaction with the system happened much earlier—when psychological profiling of children from as early as age 6 (those serving in the Hitler Youth corps and Storm Detachment) informed the decisions to recruit them into the German military.[19]

The operations of the psychological departments followed scientific protocols in shaping public opinion about the war and enhancing the morale of the population: "German leaders have proven that economic, political and psychological attacks can be sufficient by themselves to win a war."[20] Psychology experts were also used to profile the leaders of foreign countries and to conduct "comparative national psychology" studies. Yet, these operations were targeting emotions first:

[12] Olaf Mörke, "Pamphlet und Propaganda, Politische Kommunikation und technische Innovation in Westeuropa in der frühen Neuzeit" ["Pamphlet and Propaganda: Political Communication and Technical Innovation in Western Europe in the Early Modern Period"], in Michael North, ed., *Kommunikationsrevolutionen: die neuen Medien des 16. und 19. Jahrhunderts* [*Communication Revolutions: The New Media in the 16th and 19th Centuries*], Köln, Germany: Böhlau, 1995.

[13] R. D. Gillespie, "German Psychological Warfare," *British Medical Journal*, Vol. 1, No. 4239, April 4, 1942.

[14] Gillespie, 1942, pp. 445.

[15] Gillespie, 1942.

[16] Gillespie, 1942, p. 446.

[17] "What Makes Hitler Tick? Brain in the Machine," *Journal of Electrical Workers and Operators*, Vol. 40, No. 8, August 1941, p. 396.

[18] "What Makes Hitler Tick?," 1941, p. 396.

[19] Gillespie, 1942.

[20] Gillespie, 1942, p. 447.

> The essential principles of propaganda in the German view are that the emotions rather than the intellect must be appealed to; it must be simple, it must be repetitive, and it must have a reckless pugnacity.[21]

Post–World War II Era

After Nazi Germany's defeat by allied forces, its military and heavy industries were almost completely disbanded.[22] Yet, existing military infrastructure and highly trained military officers were used to quickly rebuild new armed forces in both parts of the newly divided country. In the East, Soviet principles of governance were applied, and a large-scale domestic security apparatus was set up; in the West, new democratic institutions were founded alongside a separation of powers.[23] Given the new tensions between the East and West, however, new tools for IO were required, leading to the development of several concepts—from psychological warfare to psychological defense—emphasizing both civic education (mainly in the West) and extensive surveillance and domestic intelligence capabilities (led by the Ministry for State Security, or Stasi) in the East.[24] Other security forces in East Germany included the National People's Army (established in 1956), Border Guard, Barracked People's Police, Transport Police, and General People's Police.[25] In addition, outreach efforts were expanded to include students, teachers, and youth groups in the 1980s—and the study of propaganda was introduced in school curricula and documentaries emphasizing civic engagement.[26]

New Institutional Structure for Psychological Defense

Drawing on interviews with former officers of the West German military who were involved in PSYOP, Dirk Drews observes that the Bundeswehr's focus on IO-related activities solidified in 1957, when dedicated officers for psychological warfare and defense of the Bundeswehr were asked to develop an understanding of IO tools.[27] Very

[21] Gillespie, 1942, p. 447.

[22] David Clay Large, *Germans to the Front: West German Rearmament in the Adenauer Era*, Chapel Hill, N.C.: University of North Carolina Press, 1996, pp. 17, 25.

[23] Large, 1996.

[24] Ingo Pfeiffer, *Gegner wider Willen: Konfrontation von Volksmarine und Bundesmarine auf* [*Opponents Against Their Will: Confrontation Between the East German Volksmarine and the West German Bundesmarine at Sea*], Norderstedt, Germany: Books on Demand, August 2012, p. 300.

[25] Dirk Drews, Die Psychologische Kampfführung/Psychologische Verteidigung der Bundeswehr—eine erziehungswissenschaftliche und publizistikwissenschaftliche Untersuchung [The Psychological Battlespace/Psychological Defense of the Bundeswehr—An Educational and Journalistic Examination], dissertation, Mainz, Germany: Johannes Gutenberg-Universität Mainz, 2006, p. 245.

[26] Martin Kirsch, *Die Psychologische Verteidigung der Bundeswehr bis 1990* [*The Psychological Operations of the Bundeswehr to 1990*], Tübington, Germany: Informationsstelle Militarisierung, December 3, 2014, p. 7.

[27] Drews, 2006.

early after dedicated units for PSYOP were founded in 1957–1958, the government established a divide between defensive and offensive operations.[28]

In 1961, the Bundeswehr formally launched a study group for psychological warfare, which was defined as follows:[29]

> A fight in the political-military sphere using ideological tools and mass media to change the opinion, attitudes, and actions of the opponent to favor one's interests. In peacetime, psychological warfare is limited, but it is allowed in a time of war to influence populations, their leaders, and their soldiers and undermine their willingness to attack and fight.[30]

With a new institution in place, the psychological training began with up to 1,000 soldiers per year participating in 40 sessions lasting four to 40 days each. The main audiences for such training included senior and junior officers of the Bundeswehr, as well as those of allied nations' militaries.[31]

In 1970, the Bundeswehr adopted the term *psychological defense* (instead of psychological warfare), and, in 1971, it founded a battalion for psychological defense (Battalion 800) in Clausthal-Zellerfeld. Following the reorganization of 1981, Battalions 800, 850 (Andernach), and 851 (Adenau) were assigned to the Signal Corps. These battalions provided the foundation for modern IO activities but focused predominantly on psychological defense on domestic soil (rather than operations security) and collecting information about the adversary. They shared this information with senior decisionmakers, provided culture-specific training to domestic troops, and built a capacity to engage civilian populations in areas of foreign deployment. With the exception of Battalion 950—a successor of Battalion 850 in Andernach—units dedicated to psychological defense did not survive German reunification.

Post-1989 Developments

With the end of the Cold War, public skepticism about the military's role in the information domain did not subside; rather, it reached its highest point due to the secrecy associated with the Bundeswehr's activities and with ambitions to build strong democratic institutions for a unified Germany.[32] The psychological defense battalion in Clausthal-Zellerfeld was dissolved in September 1989, and the one in Andernach was dissolved in April 1990.[33] Battalion 850's classification changed to Battalion 950 in

[28] Drews, 2006, p. 106.

[29] Kirsch, 2014, p. 3.

[30] Drews, 2006, p. 107.

[31] Kirsch, 2014.

[32] Kirsch, 2014, p. 8.

[33] Kirsch, 2014, p. 8.

March 1990.[34] According to some sources, by October 1990, public pressure resulted in the complete elimination of PSYOP from the Bundeswehr's activities.[35]

Yet, the very same year saw the launch of the Bundeswehr's Academy for Information and Communication, focusing on operational aspects of psychological warfare and training German and allied units for missions around the world.[36] The academy took over the role played by psychological warfare battalions internally and engaged in communication with the civilian population and shaping Bundeswehr StratCom. After a restructuring effort in 2014, the academy became part of the newly established Center for Information Work, which was tasked with three functions: concept development, training, and information production. Its two main components are an academy and the press office of the Bundeswehr (based in Strausberg, with a second location in Berlin).[37]

Figure 4.1 shows the current structure of the Center for Information Work, which works closely with the Center for Operational Communication. As Figure 4.1 indicates, today's center has five main offices:

1. a joint command for IO, which is tasked with leading operational communication and consists of a joint staff command and staff barracks
2. the Department for Bundeswehr and Society (based in Strausberg), which is tasked with organizing the military's public engagement events
3. the Department for Further Development (also in Strausberg), which analyzes trends in information work and assesses the Bundeswehr's efforts in this domain, directly reporting to the Press and Information Staff of the Ministry of Defense
4. the academy, which focuses on providing training to personnel in "information work," career advice to members of the Bundeswehr, and media training to German military officers
5. the Press Office of the Bundeswehr, which consists of a publishing house and staff to manage the German military's online presence, including social media.[38]

Finally, the center houses a library with more than 1.2 million books, maps, and other documents, along with subscriptions to more than 300 magazines and journals.[39] The center hosts around 270 events each year, organized both by the military and other

[34] Drews, 2006, p. 341.

[35] Kirsch, 2014, p. 8.

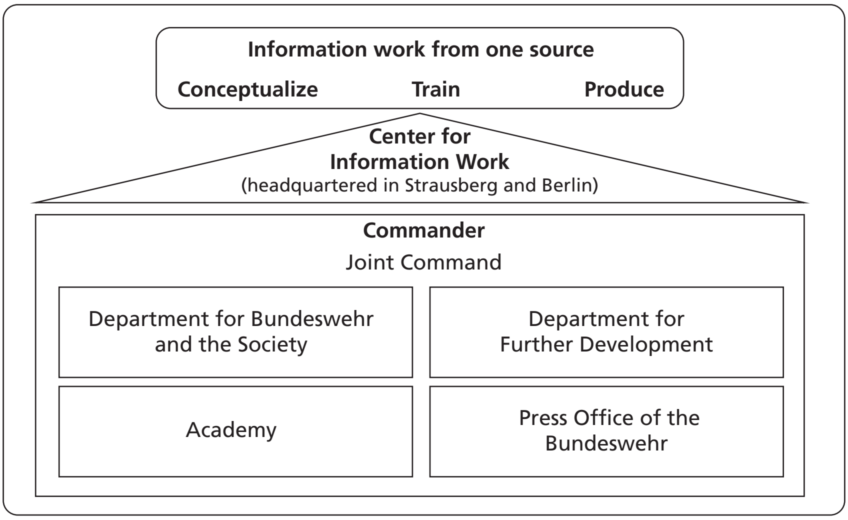
[36] Kirsch, 2014, p. 8; Christoph Schäfer, "Propaganda: Die Psychokrieger der Bundeswehr" ["Propaganda: The Psychological Warrior of the Bundeswehr"], *Der Spiegel*, October 24, 2001.

[37] Bundeswehr Joint Support Service, "Zentrum Informationsarbeit Bundeswehr: Über uns" ["Center for Information Work of the Bundeswehr: About Us"], web page, last updated May 11, 2017b.

[38] Bundeswehr Joint Support Service, 2017b.

[39] Bundeswehr Joint Support Service, 2017b.

Figure 4.1
Logical Structuring of IO in the Bundeswehr


Information work from one source
Conceptualize
Train
Produce
Center for Information Work
(headquartered in Strausberg and Berlin)
Commander
Joint Command
Department for Bundeswehr and the Society
Department for Further Development
Academy
Press Office of the Bundeswehr

SOURCE: Bundeswehr Joint Support Service, 2017b. RAND translation.
RAND *RR1925z2-4.1*

institutions, and has a large conference hall with more than 600 seats and 190 beds at its disposal.[40]

Social Context

Nazi and communist propaganda remains among the most studied topics in the social sciences, and several institutions are devoted to analyzing, storing, and contexualizing and publicly presenting materials from that era.[41] German study of dictatorial history has been a significant focus of academic research as part of a field of study commonly described as *Vergangenheitsbewältigung* ("coming to terms with the past"). A widespread awareness of the methods used to influence public opinion during the Nazi period and the communist era in East Germany is largely a product of the subject's inclusion in elementary and secondary education in West Germany prior to 1989 and across the unified country after that. This largely explains the current German opposition to mass collection of intelligence and the dissemination of untrue information.[42]

[40] Bundeswehr Joint Support Service, 2017b.

[41] These institutions include most universities and research institutes, such as the Federal Agency for Civic Education [Bundeszentrale für politische Bildung], the Federal Foundation for the Reappraisal of the East German Socialist Party Dictatorship [Bundesstiftung zur Aufarbeitung der SED-Diktatur], and the Museum in the "Round Corner" [Museum in der "Runden Ecke"] in Leipzig.

[42] Malte Spitz, "Germans Loved Obama. Now We Don't Trust Him," *New York Times*, June 29, 2013.

In addition, Germany has a much shorter history of protecting privacy. Youth rebellions in the 1960s were partly fueled by concerns that new emergency laws limiting personal freedoms could be passed, and resistance to other, similar proposals manifested in West Germany throughout the 1970s and 1980s.[43]

We address the rise of new threats, including Islamic terrorist groups and a resurgent Russia, later in this report.

German IO Organization

Structure

As noted earlier, in December 2013, the long-standing 720-strong Operational Information Battalion 950 was transformed into the Bundeswehr's Center for Operational Communication, also based in Mayen. The original Center for Operational Information (previously subordinate to Battalion 950) was dissolved and most of its staff transferred to the new center.[44]

This change was largely motivated by the need to create a central coordinating hub for IO and to create a new core competency within the Bundeswehr after the end of the Cold War. (Other psychological warfare battalions were dissolved in early 1990s, as we discussed earlier.) Given its sole purpose to collect and disseminate verifiable and objective information, the Center for Operational Communication became a natural home to IO and has worked closely with the Bundeswehr's Center for Information Work to coordinate PA activities. The Center for Operational Communication has specifically been tasked with information work, focusing mainly on providing audio-visual services for foreign deployments, deployment documentation, and media products, among other tasks.[45]

The center consists of 900 soldiers, some of whom have an education in political science, ethnology, or psychology.[46] Colonel Christian Bader, former commander of PSYOP Battalion 950, was named commander of the Center for Operational Communication and currently serves as the key coordinator of Bundeswehr IO. In a 2015 interview, he noted, "What we are doing here is far from propaganda. We see ourselves as a unit that informs, not misinforms."[47]

Bader added that the shift in terms for IO—from *psychological warfare* to *psychological defense* and from *operational information* to *operational communications*—

[43] Jannis Brühl, "Why NSA Snooping Is Bigger Deal in Germany," ProPublica, August 23, 2013.

[44] Bundeswehr Joint Support Service, "Zentrum für Operative Kommunikation der Bundeswehr" ["Center for Operational Communication of the Bundeswehr"], web page, last updated January 10, 2014.

[45] Bundeswehr Joint Support Service, 2014.

[46] Peter Dausend, "Ethnologen in Flecktarn" ["Ethnologists in Flecktarn"], *Zeit Online*, August 6, 2015.

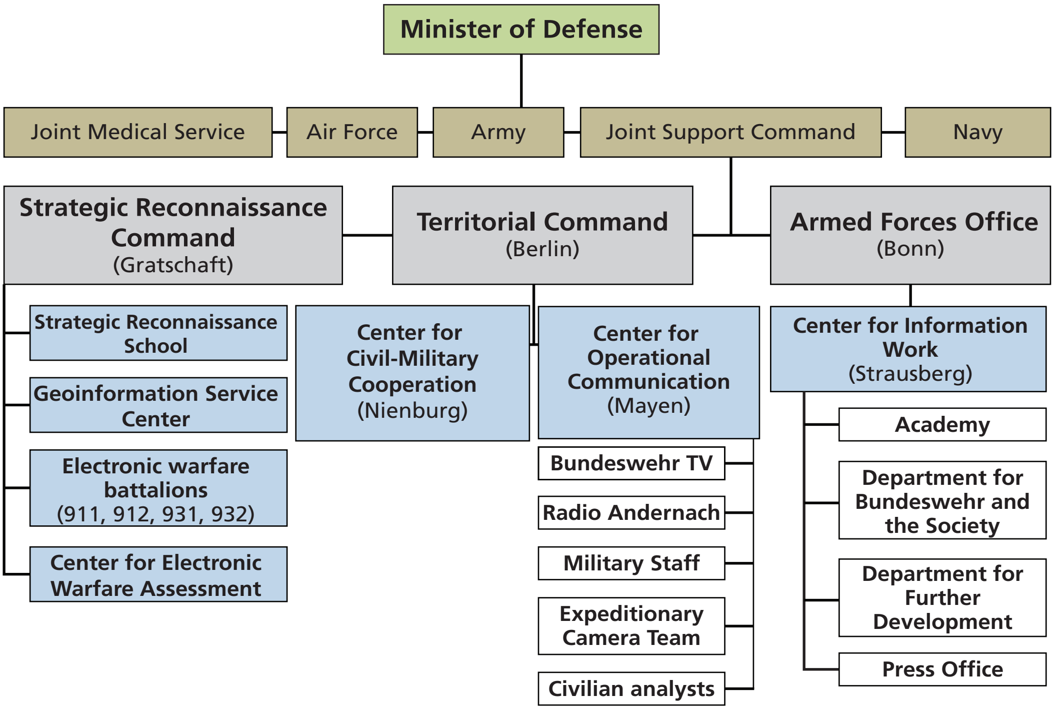
[47] Dausend, 2015.

reflects the shift in the Bundeswehr's strategy: away from the "distortions and lies" of the Cold War, when all focus was on degrading the enemy, and toward moral superiority and "demonstrative openness."[48]

In responding to threats from Russia, German policy has been steadfast in rejecting "half-truths and lies." As Bader argues, these have been proven to undermine a state's credibility and are an "absolute no-go."[49]

The Bundeswehr's Center for Operational Communication is subordinate to the Federal Armed Forces' Territorial Command (which reports to the Bundeswehr's Joint Support Command).[50] Figure 4.2 shows where all IO-related elements reside within the broader military structure.

Figure 4.2
Hierarchy of IO Personnel in the German Armed Forces


Minister of Defense
Joint Medical Service
Air Force
Army
Joint Support Command
Navy
Strategic Reconnaissance Command (Gratschaft)
Territorial Command (Berlin)
Armed Forces Office (Bonn)
Strategic Reconnaissance School
Geoinformation Service Center
Electronic warfare battalions (911, 912, 931, 932)
Center for Electronic Warfare Assessment
Center for Civil-Military Cooperation (Nienburg)
Center for Operational Communication (Mayen)
Bundeswehr TV
Radio Andernach
Military Staff
Expeditionary Camera Team
Civilian analysts
Center for Information Work (Strausberg)
Academy
Department for Bundeswehr and the Society
Department for Further Development
Press Office

SOURCE: Bundeswehr Joint Support Service, 2017a. RAND translation.
RAND *RR1925z2-4.2*

[48] Dausend, 2015.

[49] Dausend, 2015.

[50] Bundeswehr Joint Support Service, "Organisation," web page, last updated February 1, 2017a.

IRCs Employed/Available

As Figure 4.2 indicates, three commands of the German armed forces house IO-related elements, all of them subordinate to the Joint Support Command.

EW, strategic reconnaissance, and geoinformation analysis are housed under the Bundeswehr's Strategic Reconnaissance Command [Kommando Strategische Aufklärung]—the home of German military intelligence.[51] In addition to engaging in intelligence gathering, the Strategic Reconnaissance Command contributes to joint force development, education, and information sharing. Its overarching mission is to support the information needs of the Bundeswehr at the tactical level.[52] Its specific tasks are carried out by the Strategic Reconnaissance School, Geoinformation Service Center, Center for Electronic Warfare Assessment, and four distinct EW battalions.[53] Battalion 911, for example, specializes in both mobile and stationary signals intelligence collection and is equipped to address threats posed by both state and nonstate (paramilitary) actors.[54] Through its mobile assets, Battalion 911 is tasked with force protection when German troops are deployed abroad, including in the ongoing KFOR mission in the Balkans.[55] The education of troops assigned to the battalion includes three months of basic training after an evaluation of mental and physical abilities.[56] Battalion 912 operates three service boats that allow the Bundeswehr to collect signals intelligence at sea.[57] It has been deployed in support of the ISAF mission in Afghanistan, the UN Interim Force mission in the Mediterranean, and KFOR.[58]

The Bundeswehr's Territorial Command [Kommando Territoriale Aufgaben] houses two relevant centers: the Center for Civil-Military Cooperation [Zentrum Zivil-Militärische Zusammenarbeit] and the Center for Operational Communication. The Center for Civil-Military Cooperation is the Bundeswehr's "third-generation" CIMIC organization and consists of 300 service members and civilian staff.[59] The center is dedicated to supporting foreign deployments and was stood up during the Balkan wars to assist with infrastructure development and to help bridge the civil-military gap in

[51] Bundeswehr Joint Support Service, "Kommando Strategische Aufklärung" ["Strategic Reconnaissance Command"], web page, last updated June 1, 2016b.

[52] Bundeswehr Joint Support Service, 2016b.

[53] Bundeswehr Joint Support Service, 2016b.

[54] Bundeswehr Joint Support Service, "Bataillon Elektronische Kampfführung 911: Über uns" ["Electronic Warfare Battalion 911: About Us"], web page, last updated June 1, 2016a.

[55] Bundeswehr Joint Support Service, 2016a.

[56] Bundeswehr Joint Support Service, 2016a.

[57] Bundeswehr Joint Support Service, "Bataillon Elektronische Kampfführung 912: Über uns" ["Electronic Warfare Battalion 912: About Us"], web page, last updated July 28, 2017c.

[58] Bundeswehr Joint Support Service, 2017c.

[59] Bundeswehr Joint Support Service, "Zentrum Zivil-Militärische Zusammenarbeit der Bundeswehr" ["Center for Civil-Military Cooperation of the Bundeswehr"], web page, last updated June 3, 2016c.

operations abroad. The Center for Operational Communication consists of approximately 900 personnel assigned to Bundeswehr TV or Radio Andernach who serve as expeditionary camera team specialists, military staff (who may be embedded in other units of the Bundeswehr), or civilian analysts.

Training and Preparation

German units that focus on information and psychological warfare regularly train with allied forces and share lessons learned from recent deployments to the Balkans, the Middle East, and Africa. In March 2014, for instance, PSYOP Battalion 950 trained with U.S. soldiers in a complex exercise simulating convoy operations. U.S. Army Sergeant Maran Shaker observed that there were many differences in procedures between the U.S. and German troops—from exiting vehicles to approaching villagers—but that the exercise captured important lessons learned and fostered better understanding between the two forces.[60] In 2011, U.S.-German annual training included weapon manipulation, radio, and signal procedures, as well as medical emergency preparedness.[61] Similarly, many training events take place under the NATO aegis and with other partners in the alliance.

Equipment or Specialized Gear

IO personnel often deploy as embedded experts with other units and sometimes as independent supporting units, and the German military has acquired specialized equipment for them. For instance, in 2012, it tested a vehicle-mounted loudspeaker for direct communication in theater on a Dingo 2 A3 heavily armored infantry mobility vehicle, which replaced a previous lightweight all-terrain platform.[62] Information on specific acquisitions related to IO work was not readily available. However, our review did not suggest anything particularly remarkable in terms of equipment for transmission, broadcasting, or messaging.

Organizations/Functions Considered Wholly Part of IO Enterprise

The key operational focus of the Center for Operational Communication is collecting information on behalf of senior military leadership, partly by using the capabilities of Germany's special operations forces and partly through multinational deployments.[63] In addition, they serve as key providers of information to local populations, using such

[60] Iggy Rubalcava, "German, American Soldiers, Polizei Train Together," U.S. Army, April 7, 2014.

[61] The United States was represented by the Army's 557th Medical Company. See Christopher Fincham, "U.S. Army Medics Train German Psyops Soldiers," U.S. Army, June 29, 2011.

[62] Army Recognition, "New Dingo 2 A3 Armoured Vehicle PSYOPS: Psychological Operations of German Army," web page, March 26, 2012.

[63] Dausend, 2015.

means as brochures, posters, leaflets, videos, CDs and DVDs, mobile speakers, and even hiring "intercultural consultants."[64]

In Afghanistan, for instance, the center introduced flyers offering local children and youth schoolbooks in exchange for turning in their weapons, and it produced videos that aired on local television explaining the mission of the Bundeswehr in the area of Hindu Kush and educating local farmers about alternatives to growing opium poppies. This, however, did not stop the locals from doing so: Afghanistan now produces more opium than it did before the campaign.[65]

Media used for PSYOP during the Cold War era included radio, film, flyers and posters, photo series, and special newspaper editions.[66] Since then, most communication has been adapted to local needs in areas where the forces are deployed, relying generally on printed media, television programming, and radio broadcasting. For soldiers and other audiences in Germany, the Bundeswehr has developed a relatively robust presence on social media and other channels (such as an online livestream of Radio Andernach and Bundeswehr TV).

Key IE-Affecting Organizations and Functions That Are Not Part of IO

In an interview with a senior commander in the German Bundeswehr, we learned that other IO-related capabilities, such as electronic and cyberwarfare, are not part of the more narrowly defined IO-enterprise but belong to the German military's general capabilities. Given the relatively narrow scope of German IO, IO expertise is typically provided to combat units directly by the Center for Operational Communication.[67]

Information Operations in Practice

Assessment of German IO Effectiveness

With the recent modernization and streamlining of its IO capability, Germany has developed a robust military press and media capability, continues to excel in operations security and denial measures, and has a very strong social media presence and capability. It is also believed that Germany's EW capability is among the best in NATO, although capability assessments are classified. Germany exhibits several weaknesses, not unlike its NATO peers: Given the restrictions on the use of IO domestically, the Bundeswehr

[64] Dausend, 2015.

[65] Dausend, 2015.

[66] Ralf E. Streibl, "Psychologische Kriegführung und Information Warfare" ["Psychological Warfare and Information Warfare"], in Gert Sommer and Albert Fuchs, eds., *Krieg und Frieden: Handbuch der Konflikt- und Friedenspsychologie* [*War and Peace: A Handbook of Conflict and Peace Psychology*], Weinheim, Germany: Beltz, 2004.

[67] Phone interview with the authors, April 7, 2016.

has displayed a limited ability to influence domestic public opinion,[68] has resorted to presenting a broad set of facts rather than a single narrative about conflicts in which it has participated (this is, however, seen as a strength and source of moral high ground in the country), and has made moderate investments in cyber defense.[69] Similarly to other NATO members, Germany's doctrine prevents it from engaging in deception and manipulation, puts limitations on the use of IO in fire/maneuver (IO units are generally embedded within combat units and have a relatively narrow mandate), and lacks specifics on collaborating with "proxies" (and there is limited political willingness to do so).

Examples of Interesting German IO Efforts

The German Parliament mandated the deployment of German troops in Kosovo alongside other NATO troops in late 1998. Tornado fighters conducted almost 500 sorties, and more than 3,100 troops deployed as part of NATO's humanitarian relief operations.[70] Since then, German troops have contributed to other reconstruction efforts, initially in an emergency relief role and later by commencing development cooperation.[71] Both civilian and military forces have been deployed to Kosovo as part of the UN mission there, NATO'S KFOR mission, and the European Union's EULEX missions, starting with 8,500 troops at the height of the operations. As of March 2016, Germany maintained a contingent in Kosovo of approximately 700 troops.[72] German troops have mostly been engaged at the headquarters level of NATO's KFOR mission, in the military hospital, and as part of the U.S.-led multinational battle group in the east of the country.[73]

As part of KFOR's Multinational Brigade South, German troops responsible for operational communication have been leading the publication of the magazine *Dritarja* and the monthly youth newspaper *FORYOU*.[74] Similarly, French troops publish the magazine *Bonjour* in their area of responsibility.[75]

[68] A majority of Germans have expressed a reluctance to uphold Article 5 of the Washington Treaty if another member state is attacked by Russia. See, for instance, Simmons, Stokes, and Poushter, 2015.

[69] The Cyber Defense Center was launched in April 2011 and has focused mostly on critical infrastructure. See German Federal Ministry of the Interior, *Cyber Security Strategy for Germany*, Berlin, February 2011.

[70] German Federal Ministry of Defence, *The Bundeswehr on Operations: Publication to Mark the 15th Anniversary of the First Parliamentary Mandate for Armed Bundeswehr Missions Abroad*, 2nd ed., Berlin, June 2009.

[71] German Federal Foreign Office, "Kosovo," web page, last updated April 2017.

[72] Bundeswehr, "Der Einsatz im Kosovo, ["Deployment to Kosovo"], web page, last updated May 24, 2017.

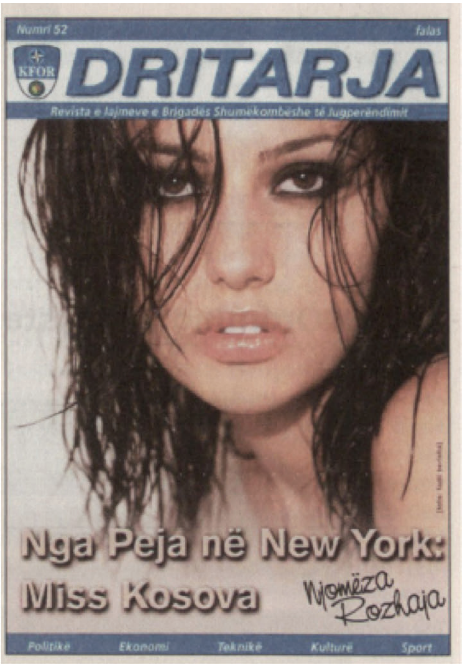
[73] Bundeswehr, 2017.

[74] Julia Egleder, *Peace Through Peace Media? The Media Activities of the International Missions (KFOR and UNMIK) and Their Contribution to Peacebuilding in Kosovo from 1999 Till 2008*, dissertation, Regensberg and Münster, Germany: University of Regensburg and LIT Verlag, 2013, p. 253.

[75] See Egleder, 2013, p. 253. This was not a natural move: The French were reluctant to engage in psychological operations after the debacle in Algeria in the 1950s and 1960s, and they did not trust U.S. PSYOP personnel in

Figure 4.3 shows one of the front pages of *Dritarja*, which is aimed at broad audiences. The Albanian-language magazine and the related Serbian-language *Prozor* began publication in 2001 and within two years had a circulation of approximately 35,000.[76] Other forms of engagement have included posters, information leaflets, and flyers. Moreover, KFOR has established contractual arrangements with ten local stations in Kosovo to broadcast *KFOR-Café*, *KFOR News*, and other programs to local populations in three languages (Albanian, Serbian, and Bosnian). Finally, tactical PSYOP-trained troops are deployed whenever quick-turn missions are conducted, during demonstrations, and to engage in face-to-face communication with locals (civilian and

Figure 4.3
Cover of a 2004 Issue of *Dritarja*



SOURCE: Oscar A. M. Bergamin, "Miss Kosovo als 'Operative Waffe'" [Miss Kosovo as an 'Operational Weapon'"], *Allgemeine schweizerische Militärzeitschrift* [*General Swiss Military Magazine*], Vol. 170, No. 1, January 2004, p. 40.
RAND *RR1925z2-4.3*

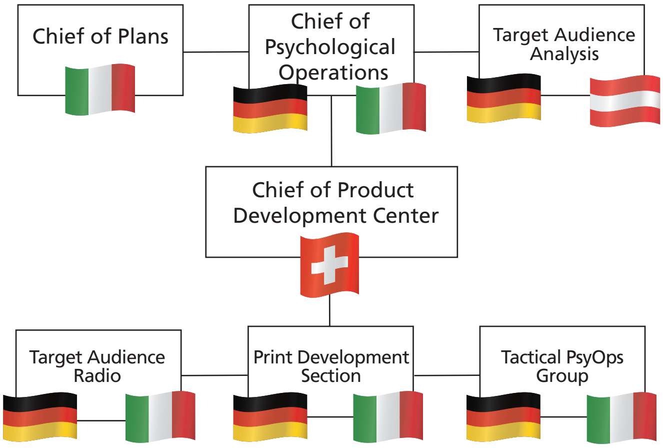
Bosnia. They ultimately began to engage with U.S. units specializing in PSYOP and started their own radio station in Bosnia and, later, in Kosovo. See Steven Collins, "Army PSYOP in Bosnia: Capabilities and Constraints," *Parameters*, Summer 1999.

[76] Javier Yrayzoz, "MNB Southwest Distributes 35,000 Magazines," *KFOR Chronicle*, January 31, 2003; Bergamin, 2004, p. 40.

military alike) to communicate mission intent and assess the "psychological state" of the population.[77]

In 2008, Germany was among the first nations to recognize the sovereignty of Kosovo and has provided it with around €500 million in development aid.[78] A case study in a Swiss military newspaper cited the "substantive German experience in the field of operational information," given its deployments in Somalia (1993–1994), Bosnia and Herzegovina (1997), Kosovo (since 1999), and Afghanistan (since 2001), as well as engagements in Croatia and Macedonia.[79] Together with their Swiss, Italian, and Austrian counterparts, German personnel have been leading KFOR's engagement in the south of Kosovo; Figure 4.4 shows the distribution of these roles. The key principle of Germany's Center for Operational Information—"Who lies once will lie always"—has resulted in a significant emphasis in KFOR IO to present truthful and honest information to local audiences.[80]

Figure 4.4
Structure of the PSYOP Brigade Support Element of Multinational Brigade South in Kosovo


Chief of Plans
Chief of Psychological Operations
Target Audience Analysis
Chief of Product Development Center
Target Audience Radio
Print Development Section
Tactical PsyOps Group

SOURCE: Bergamin, 2004, p. 41.
RAND *RR1925z2-4.4*

[77] Bergamin, 2004, p. 40.

[78] German Federal Foreign Office, 2017.

[79] Schäfer, 2001; Bergamin, 2004, p. 40.

[80] Bergamin, 2004, p. 40.

In NATO, the term *PSYOP* is seen as one that falls under the concept of perception management.[81] Then-LTC Steven Collins of the U.S. Army (later chief of NATO PSYOP at Supreme Headquarters Allied Powers Europe) observed that, in fact, European experiences with PSYOP—in Bosnia and Herzegovina, as well as Kosovo—provide learning opportunities for both the United States and the United Kingdom, particularly with respect to postconflict environments.[82] Already in 2003, Steven Collins observed a tendency to shift away from the more contentious term *PSYOP* to "more acceptable expressions like 'information operations.'" Yet, he was critical of the virtual equivalence the definitions of both terms have attained and the confusion that this has created among military planners. He argued that placing PSYOP under the category of IO may undermine its importance and access to senior commanders. Collins concluded, however, that there must be no connection between PSYOP abroad and public information activities at home that "seek to provide an accurate and truthful account of events." The use of *PSYOP*, according to Collins, would be accepted by domestic constituencies when directed toward audiences in combat zones and crisis-stricken regions, and it is superior to the "watered-down" term *IO*.[83] In Germany, public discourse about privacy and security has focused on the work of intelligence agencies, but it is likely that widespread opposition would emerge if any military-sponsored activities were revealed to target domestic audiences.

In discussing NATO's capability-building efforts in 2003, Collins argued that only a handful of countries had a strong capacity to engage in PSYOP, citing Belgium, the Czech Republic, Germany, Poland, Spain, the United Kingdom, and the United States as leaders in pursuing advanced capabilities.[84] Today, U.S., UK, and German specialists train NATO troops prior to deployment in their home countries.[85] Given the experience of Battalion 950 and its multiple deployments since the end of the Cold War, German PSYOP experience is seen as one of the most advanced in NATO.[86] German IO troops have been part of the so-called EU battle groups (although they have never been deployed in combat).

Other countries, such as the Czech Republic, developed their specialized capabilities related to IO in the late 1990s, with the Czech CIMIC unit formed 2001 in Tabor and later renamed the 103th Center for CIMIC/PSYOPS in 2013. Like their German counterparts, members of the Czech center have deployed to Iraq, Bosnia, Kosovo, and

[81] Bergamin, 2004, p. 40; Steven Collins, "Mind Games," *NATO Review*, No. 2, 2003.

[82] Collins, 2003.

[83] Collins, 2003.

[84] Collins, 2003.

[85] Czech Ministry of Defense, "Když se řekne psychologické operace" ["About Psychological Operations"], web page, undated(b).

[86] Czech Ministry of Defense, undated(b).

Afghanistan and have coordinated their activities with civilian actors abroad and educated domestic audiences about their work.[87]

Key IO Initiatives or Programs

Use of Social Media

The Bundeswehr has operated a Twitter account since March 2010. As of October 2017, it had almost 60,000 followers, but many of its recent posts appear to be generated by bots and refer to website updates.[88] Its other channels on Facebook, YouTube, Flickr, and Instagram have more tailored content. Its YouTube platform is particularly popular, with more than 250,000 subscribers and more than 120 million views of its videos since 2006.[89] In addition, its Facebook page is now followed by more than 413,000 people, and the Bundeswehr's press office engages with followers in the comment sections of individual posts (each response is personally signed), encouraging frank but measured discussions.[90] Its most popular videos—with dramatic music and high production values—attract tens of thousands of viewers within hours of their posting. The team supporting social media is based in Berlin and housed within a dedicated unit for public relations.[91]

Similar to its U.S. counterpart, the German military long resisted the shift toward greater engagement with the public using social media. Only in mid-2012 did the Bundeswehr publish its *Recommendation on the Safe Use of Social Media*, and it did not make social media guidelines available on its website until January 2014.[92] Those documents outline the key principles of the Bundeswehr's engagement with the public via social media:

- All military staff are allowed to use social media for private purposes but are asked to clearly distinguish personal opinions from facts.
- All individuals are responsible for their contributions to the media landscape.
- Users must maintain transparency and honesty, particularly when representing the Bundeswehr in an official capacity, and must not violate information classification rules.

[87] Czech Ministry of Defense, "103. centrum CIMIC/PSYOPS: O nás" ["103rd CIMIC/PSYOPS Center: About Us"], web page, undated(a).

[88] "Bundeswehr," Twitter account, undated.

[89] "Bundeswehr," YouTube account, undated.

[90] Consider, for instance, Bundeswehr's Facebook post on Naval Squadron 5 humanitarian assistance/disaster relief operations, March 22, 2016.

[91] "Bundeswehr," YouTube account, undated.

[92] German Federal Ministry of Defence, "Journalismus über Militär und Krieg im digitalen Zeitalter" ["Journalism on Military and War in the Digital Age"], web page, last updated January 7, 2015.

- Military staff and their families must comply with the law, such as in the use and attribution of intellectual property.
- Users must respect opposing views and refrain from provocations and threats.
- Users are encouraged to consult with information specialists in the Bundeswehr in cases of ambiguity or uncertainty about the application of a specific guideline.

National Security Culture and a Changing Information Landscape

As the German Ministry of Defense acknowledges, there are few online media sources specializing in national security, in contrast to the many U.S. periodicals and blogs dedicated to the field (it cites, for example, *Small Wars Journal* and IISS's *Military Balance Blog*).[93] Yet, the ministry also acknowledges the changing media landscape and the need to use social networks to reach world audiences. After all, NATO Supreme Commander James Stavridis initially announced the end of NATO's intervention in Libya on October 21, 2011, on Twitter and Facebook. (The operation officially ended ten days later.)[94]

Anticipated Developments

As we confirmed in our interviews, it is unlikely that the Bundeswehr's new centralized structure devoted to PA and IO will be adjusted as new experience is collected and new tactical means are developed. Hence, it is difficult to predict future developments within the Center for Operational Communication.

As we have shown, there are many reasons to believe that new geopolitical risks in Europe will continue to affect German defense planning, and with the Bundeswehr's expansion plans announced in May 2016, it is likely that additional resources will be provided to nonkinetic warfare, including IO.[95]

Vulnerabilities in German IO

With a rapidly changing security environment in Europe, the German military faces a number of strategic challenges, one of which is the use of alternative tools to influence public opinion by the adversary. Given that German IO are conducted only vis-à-vis foreign populations and limited resources are available to fight propaganda domestically (and the majority of that work is implicitly delegated to the media and the intel-

[93] German Federal Ministry of Defence, 2015.

[94] James Stavridis, NATO Supreme Commander, Twitter post, October 21, 2011.

[95] Justin Huggler, "Germany Expands Its Army for First Time Since Cold War in Response to Threat of Isil," *The Telegraph*, May 10, 2016.

ligence community), German military and law enforcement agencies must continually adjust to new realities in the information landscape. This is particularly true for the German fight against Russian state-sponsored propaganda and the 2014 expansion of the RT (formerly Russia Today) German franchise.[96]

In operations abroad, the exclusive dependence on evidence-based information may pose short-term operational challenges, particularly given the bureaucratic requirements associated with verifying information that is disseminated to local population. Yet, it is clear that the current model is based on the assumption that the costs of doing so are outweighed by the benefits this provides—chiefly, the trust and credibility such approach helps nourish during German operations abroad. As the operational structure supporting IO-related capabilities of the Bundeswehr matures, it is likely that challenges associated with coordination, bureaucratic hurdles, and inefficiencies in information sharing will be addressed.

Lessons from German Operations in and Through the IE

As a country with a complex military and political history, Germany has advocated for a narrower definition of IO than the United States and, in many cases, decisively led the general European approach to engaging local populations in areas of deployment. The key distinctions of German IO include a commitment to unvarnished truth and an evidence-driven messaging strategy, significant cultural and language training that allows the effective use of local resources and proficient communication with local authorities (both formal and informal), clear restrictions on the use and collection of data through social media, the inability to use military intelligence to shape domestic public opinion, and recent historical experience ensuring the psychological defense of the nation's troops and domestic audiences against foreign propaganda. However, today, Germany faces new challenges. In this section, we describe the key differences and potential lessons learned for the U.S. context.

German IO in Contrast with U.S. IO

As we have shown, Germany conducts IO in areas of foreign deployment and also uses its IO-related capabilities to collect and disseminate information to its own troops. While strictly emphasizing the use of evidence-driven information only, it has built an effective institutional framework to support IO-related efforts across its military and is considered one of the leaders in the field among NATO allies.

[96] Janina Semenova, "Behind Russia's TV Propaganda Machine," *Deutsche Welle*, September 2, 2015.

There are several key characteristics of Germany's approach to IO, some of which distinguish it from U.S. engagement in the information domain:

- a greater focus on information sharing with local populations and less on affecting decisionmaking or behavior
- a heavy emphasis on building morale, trust, and a sense of integrity among German troops through significant investments in psychological defense
- a significant emphasis on training allied partners in conducting IO during deployments abroad
- a dynamic presence on social media and an increasingly strategic use of these platforms, particularly its YouTube and Facebook accounts, which have tens of thousands of followers
- IO-related leadership experience during allied missions in Bosnia, Kosovo, and Somalia, which have been highly effective and resulted in low numbers of casualties.

Based on these characteristics, German IO strategy could be mistaken for an expanded public affairs function. This is a crude simplification, however, and does not do justice to Germany's successes. With significant operational experience in foreign deployments, German troops have built lasting relationships with local populations and become leaders in NATO IO. While Germany's commitment to evidence-based tactics may pose challenges, it also allows its military to present itself in the best possible light and build confidence in its strategy among local populations in the areas to which it deploys, as well as domestically. With a well-resourced and capable social media presence, an integrated IO function in all German expeditionary operations, and a strategic investment in EW, military intelligence, and related functions, the German military represents a vital IO capability within NATO.

Key Takeaways

As this chapter illustrates, Germany epitomizes a broader difference between the European and U.S. conceptions of information warfare. Independent of allied forces, Germany is closely in sync with NATO's conception of PSYOP and is seen as a leader in engaging local populations and defending its troops against an adversary's influence. With new national security threats at home, however, the German military and other security institutions now face one of the greatest tests of their ability to protect the German population from propaganda and sabotage of the information landscape—and they may lack the resources to do so in the short term. The Bundeswehr's recent, future-looking reform and founding of the Center for Operational Communication are evidence of the awareness that senior military commanders in Germany have of their vulnerability to attacks in the information domain—and of their lack of tools just a few years ago. It is incumbent upon the current political leadership to provide the resources needed to build a strong military force that can conduct effective military operations abroad while defending the homeland in emerging domains that, until recently, have been neglected.

The U.S. Army can learn from several aspects of German activities in and through the IE. Germany has worked to modernize and streamline IO capabilities, is constantly reevaluating the effectiveness of its IRCs, and genuinely seems to have a firm grasp of the importance of resourcing these capabilities. It places much importance on training other allied forces in IO, staking out a legitimate claim as a leader in this area within NATO.

Another area in which the U.S. Army could learn from Germany is in the extent to which German troops engage with local populations in countries where they are deployed or could be deployed in the future. Not only does this help the German military establish a baseline knowledge of a country, its culture, and its customs, but it also facilitates face-to-face interactions to clearly communicate mission intent.

Finally, Germany continues to work toward mastering efforts in and through the IE using open-source information, including social media. Germany has recognized the ubiquity of social media and its centrality to many peoples' lives, including those of its own soldiers.

CHAPTER FIVE

China

> To get someone to do something for himself that he thinks is in his own interests, but which is actually in your interests, is the essence of strategy, according to Mao.
>
> —LTC (ret.) Timothy Thomas, Foreign Military Studies Office,
> U.S. Army Training and Doctrine Command[1]

Case Summary

The People's Republic of China is actively and aggressively pursuing goals to persuade the global population of its resurgence while limiting access to information at home in an effort to maintain a one-party system.[2] To do this, China has aggressively entered the IE, systematically developing capabilities and then exercising them in real-world operations. Indeed, over the past 25 years, it has closely followed the actions of the United States in the IE; it has taken these concepts, blended them with Soviet-era doctrine, and added its own traditional tactics and concepts to create a uniquely Chinese approach to information warfare (*xinxi zhanzheng*). The targets of these *information operations*—a U.S. term—are global audiences, internal audiences, and the West, particularly the U.S. public and policymakers. Many of the operations Beijing is pursuing are designed to sway public opinion, acquire U.S. technologies, and counter U.S. action throughout the IE. It wants to do this without physically engaging the United States in open conflict, and it is developing its IRCs, doctrine and policy, force structure, and legal frameworks—as well as adding resources—to accomplish these tasks. Indeed, China and, by extension, the People's Liberation Army (PLA), are already actively engaged in multiple 'warfares'—psychological, public opinion, and legal—

[1] Timothy L. Thomas, "Asia Pacific: China's Concept of Military Strategy," *Parameters*, Vol. 44, No. 4, Winter 2014–2015, p. 39.

[2] See Reporters Without Borders, "China," web page, undated.

even though there is no active conflict.[3] The PLA has gone through a massive reorganization in which it has consolidated all IO forces into the Strategic Support Force, which it has designated a fifth service branch, indicating its high level of importance. The United States recognizes that certain PLA actions are designed to bolster regional territorial claims and diminish U.S. influence in the region, but it is not fully prepared for the suite of capabilities that the PLA is currently employing. This case study examines China's actions, capabilities, and developments with the aim of raising Army leadership awareness.

Background and Overview

China places strong value on history, with a worldview stemming from a civilization that is more than 5,000 years old and has experienced countless wars and massive loss of life. The Middle Kingdom, as China still refers to itself, is a geographical reference that places China central to the world. Over centuries, China has been invaded by foreign powers that destroyed the country and killed millions of its citizens. To counter this, Confucian teachings and, later, a tradition of legalism gained root in Chinese society as a way for Chinese emperors to avert warfare, maintain order, and control the population. Both traditions emphasize that the individual is subservient, and less important, than the will of the many. These themes are still present in China today and help frame Chinese actions domestically and internationally. When placed into this history, it is not surprising that China regards international norms—developed and maintained by the West—as a reflection of the underlying power imbalance between states. As such, it views the power relationships between countries as primary and its own conduct with respect to international norms and behaviors as a secondary consideration.[4] In this world, weaker countries maneuver around stronger countries. Despite suffering a century of humiliation from 1839 to 1949, China has traditionally characterized itself as a stronger power.

The PLA traces its history to August 1, 1927, when it was established as a peasant guerrilla force. It has since grown into the world's largest army, with more than 2 million armed personnel. Initially, the PLA drew heavily on Soviet doctrine, which emphasized quantity over quality. During this early period, its information warfare capabilities were focused on EW techniques, such as jamming, deception, and inter-

[3] Dean Cheng, "Winning Without Fighting: The Chinese Psychological Warfare Challenge," Washington, D.C.: Heritage Foundation, Backgrounder No. 2821, July 11, 2013.

[4] Scott Warren Harold, Martin C. Libicki, and Astrid Cevallos, *Getting to Yes with China in Cyberspace*, Santa Monica, Calif.: RAND Corporation, RR-1335-RC, 2016.

ception of adversary communications and radar.[5] The PLA also expanded Soviet tactical preferences for precision air, missile, and artillery strikes.[6] Psychological warfare was one of the core responsibilities of the PLA's General Political Department during this period. It targeted nationalist and Japanese forces during World War II and continued to refine and use these techniques on U.S. and Korean forces during the Korean War. From these roots, the PLA's information warfare activity has continued to evolve.

The 1990s saw PLA doctrine evolve from a largely defensive people's war construct in favor of new concepts under the rubric of active defense, which called for tactics that were far more aggressive. A turning point in the PLA's development and use of IO occurred in the wake of the Gulf War against Iraq. The manner in which the United States executed combined-arms operations with precision guided munitions and networked C4ISR led to a realization that the PLA was incapable of dealing with a modern, technologically advanced adversary. As Larry Wortzel of the U.S.-China Economic and Security Review Commission notes, "For almost a decade, virtually all of the publications from PLA institutions quoted from or cited American military doctrine or manuals."[7] China recognized the importance of information dominance on the battlefield and the new technologies that would make this possible. China's so-called revolution in military affairs called for a radical transformation within the PLA and highlighted the importance of "informatization"—dominance in IT and cyberspace.[8] As part of its military modernization strategy, the PLA began creating an all-inclusive information master network. This system of systems is based on the national C2 architecture and allows commanders to communicate in real time with forces in their area of operations.

In the mid-2000s, the PLA began developing its own doctrine on IO. These developments involved both planning for operations on the physical battlefield and preparing to conduct political warfare, a concept known as the "three warfares," discussed in greater detail later in this chapter.[9] The Chinese Communist Party approved this new warfare concept in 2003. Once implemented, the PLA viewed it as a natural extension of information warfare in which operations conducted during peacetime allowed the PLA to collect information and persuade adversaries in the political, economic, technical, and military realms. The PLA would use this information to develop

[5] Larry M. Wortzel, *The Chinese People's Liberation Army and Information Warfare*, Carlisle Barracks, Pa.: U.S. Army War College, Strategic Studies Institute, March 2014, pp. 2–3.

[6] Wortzel, 2014, p. xi.

[7] Wortzel, 2014, p. 26.

[8] Daniel Ventre, "China's Strategy for Information Warfare: A Focus on Energy," *Journal of Energy Security*, Vol. 18, May 2010.

[9] Cheng, 2013, p. 1.

operational plans, calculate gains and losses in a conflict, control the level of attack, identify targets, and pursue the best strategic course.[10]

Movement from mechanized conditions to operations in "informative conditions" gained momentum in 2006, when an editorial in the *PLA Daily* called on the military to take advantage of information technologies.[11] The PLA subsequently began updating its mechanized and joint operations doctrine to align it with its doctrine on EW and precision strike. This new model of warfare was *warfare and precision strike*. Wortzel writes,

> In a book published by the PLA Academy of Military Science, Ye Zheng describes information age operations as "a new type of operations that are derived from the basis of mechanized operations moving from "platform-based operations" to systematic operations and network-centric operations.[12]

To accomplish this, the PLA began developing and fielding satellites, communication systems, and other advanced technologies in support of IO.

Since 2009, the PLA has continued to evolve its special-purpose, conventional, nuclear, and IO forces. The concept of informatization has gained significant traction among PLA think tanks and military leadership, leading to improved unmanned aerial vehicles, reconnaissance satellites, and other information-collection platforms. Furthermore, signals intelligence and EW capabilities have expanded into cyber and space warfare. Doctrine is keeping pace with these expanded roles, with the PLA developing new strategies to expand its reach.

Concepts and Principles for Operations in and Through the IE

China is famous for its historical strategic thinkers who focused intently on achieving operational dominance over an opponent. Military strategists, such as Zhuge Liang, Sun Tzu, and Wang Jingze, wrote extensively on the concepts of deception, misdirection, and diversion. Many of the strategies employed over the centuries came from the *Book of Qi* by Wang Jingze and *The Art of War* by Sun Tzu. The PLA continues to expand upon many of these earlier concepts. In fact, the 1997 *Chinese Military Encyclopedia* defines *strategy* and other strategic concepts, such as strategic cover, strategic

[10] Li Naiguo, *New Theories of Information War*, Beijing: Academy of Military Science Press, 2004a, p. 154.

[11] Li Naiguo, *Xinxizhan Xinlun* [*A New Discussion on Information Warfare*], Beijing: National Defense University Press, 2004b, pp. 35–45.

[12] Wortzel, 2014, p. 6, quoting Ye Zheng, *Xinxihua Zuozhan Gailun* [*An Introduction to Informationalized Operations*], Beijing: Military Science Press, 2007, pp. 17–18.

concept, strategic targeting, and strategic thought, more than 100 times.[13] While little has changed in the official definition of *strategy* in the past 20 years, the emerging need for information-focused strategies has become apparent. To meet this need, in 2003 the Chinese Communist Party's Central Military Commission approved an overall conceptual framework on the use of information warfare: the three warfares (*san zhong zhanga*). These three mutually reinforcing strategies (1) coordinate the use of PSYOP (psychological warfare), (2) utilize overt and covert media to manipulate public opinion (media warfare), and (3) establish legal justifications for Chinese military actions (legal warfare).[14]

Strategic Goals/Vision

There are three overarching constructs that guide the PLA: active defense, local war, and people's war. Active defense has been the guiding strategy of the PLA since Mao Zedong. China's active defense policy states that the military will only strike after it is attacked. Local war under conditions of informatization is a more modern concept that has been official PLA doctrine since 1993. It states that near-future warfare will occur primarily along the Chinese periphery, that it will be limited in scope, duration, and means, and that it will be fought using advanced computer systems, IT, and communication networks to gain operational advantage over an opponent.[15] *People's war* describes how the Chinese population will support military operations during times of warfare. Support can come in many forms, including logistical, political, and operational, and from different sources, including militias, civil defense forces, and reserve forces. These contributions are seen as vital to the success of military operations in local wars.[16] These concepts are what China uses to posture, shape, and fight at the strategic level, which in Chinese terms is the campaign level of war. Recent unclassified literature has increasingly focused on ideas developed over the past five years, leading to debates on the PLA's direction in terms of force structure, military spending, and weapon procurement. From this guidance, the PLA has evolved its doctrine to prioritize fighting and winning local wars against adversaries, specifically technologically superior ones.

How Information Warfare Fits Within China's Overall Strategic Goals

As mentioned earlier, the Central Military Commission approved the three warfares concept as a PLA nonmilitary information warfare tool to be used prior to and during

[13] Thomas, 2014–2015. In comparison, the U.S. military defines strategy or strategic concepts just 14 times in Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*.

[14] Michael Raska, "China and the 'Three Warfares,'" *The Diplomat*, December 18, 2015.

[15] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2011*, Washington, D.C., March 2011, p. 3.

[16] Peng Guangoian and Yao Youzhi, eds., *The Science of Military Strategy*, English translation, Beijing: National Military Science Publishing House, 2005, p. 376.

military operations.[17] During peacetime and war, the concepts aim to create a political advantage that can be used to sway internal and external public opinion.

Psychological Warfare

China has been involved in PSYOP for thousands of years. These types of operations traditionally involved the use of stratagem (*moulue*), or deception techniques. The target was an enemy's will to fight, and the approach was designed to reduce the efficiency of an adversary's forces by creating dissent, disaffection, and dissatisfaction in their ranks.[18] PSYOP are not unique to China, but the recent emphasis on these operations in PLA doctrine has elevated their role in Chinese military strategy. According to Dean Cheng, a research fellow at the Heritage Foundation, "Psychological warfare is in some ways the most far-reaching of the 'Three Warfares.' It involves the application of specialized information and media in accordance with a strategic goal and in support of political and military objectives."[19] Chinese psychological warfare efforts target friends, allies, and partners, as well as enemies and those that are uncommitted. As in media (public-opinion) warfare, there is a heavy reliance on media across a 24-hour news cycle that continually competes for viewership.[20] However, the nature of modern technology and speed with which information can be exchanged has dramatically altered the way China targets various audiences (see Figure 5.1).

When viewed through this lens, the PLA is actively engaged in all four areas and across multiple informational domains. According to Wortzel,

> The PLA is not solely focused on information superiority in in the cyber and electromagnetic spectrum. The General Political Department—often in coordination with the Communist Party's International Liaison Department, its Propaganda Department, and military intelligence—also has modernized traditional propaganda and psychological operations for wars in the information age.[21]

Media Warfare

Media or public-opinion warfare uses all forms of media to influence public opinion both domestically and internationally. The goal is to inform audiences about the morality and correctness of China's goals, motivations, and actions. These operations use all

[17] Office of the Secretary of Defense, 2011, p. 26.

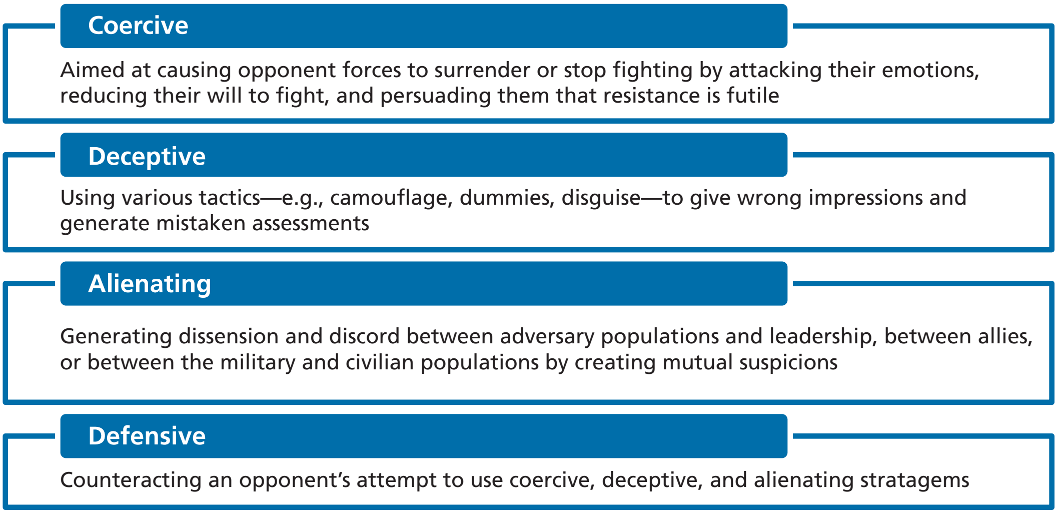
[18] Mark Stokes, "The Chinese Joint Aerospace Campaign: Strategy, Doctrine, and Force Modernization," in James Mulvenon and David Finkelstein, eds., *China's Revolution in Doctrinal Affairs*, Arlington, Va.: Center for Naval Analyses, 2002, pp. 271–274

[19] Cheng, 2013, citing Guo Yanhua, *Psychological Warfare Knowledge*, Beijing: People's Liberation Army National Defense University Press, 2005.

[20] Cheng, 2013, citing Nanjing Political Academy, Military News Department Study Group, "Study of the Journalistic Media Warfare in the Iraq War," *China Military Science*, No. 4, 2003, p. 30.

[21] Wortzel, 2014, p. 28.

Figure 5.1
Types of Psychological Warfare



Coercive

Aimed at causing opponent forces to surrender or stop fighting by attacking their emotions, reducing their will to fight, and persuading them that resistance is futile

Deceptive

Using various tactics—e.g., camouflage, dummies, disguise—to give wrong impressions and generate mistaken assessments

Alienating

Generating dissension and discord between adversary populations and leadership, between allies, or between the military and civilian populations by creating mutual suspicions

Defensive

Counteracting an opponent's attempt to use coercive, deceptive, and alienating stratagems

SOURCE: Derived from Cheng, 2013, citing 100 case studies assembled by PLA analysts (Ci Weixu, ed., *100 Questions About Psychological Warfare*, Beijing: Liberation Army Press, 2004).
RAND *RR1925z2-5.1*

forms of media to convey these messages: television, newspapers, radio, social media, and other outlets that are not immediately evident to the public as modes of message delivery. While many techniques are transparent, others are not, and deception regularly plays a part in China's dissemination campaigns. The similarities between media warfare and traditional propaganda tactics cannot be denied: Some are deliberate deception operations while others are directed at perception management.[22] Paramount among China's stated goals for media warfare is countering the dominance of Western media. To this end, the Chinese Communist Party actively engages the public, promoting its positions and views through its own outlets.

Legal Warfare

The goal of legal warfare, or "lawfare," is to establish legal justification for military actions in advance of a conflict. In the mid-2000s the General Political Department sought ways to develop domestic laws that could be leveraged in the international legal system prior to Chinese military action. The PLA views war as a comprehensive struggle—spanning the military, political, economic, diplomatic, and legal domains. Therefore, for the PLA, "international law is a powerful weapon to expose the enemy, win over sympathy and support of the international community [for China], and gain

[22] Perception management is designed to direct a subject's behavior in ways that favor the original actor's objectives. See Collins, 2003.

the position of strategic initiative."[23] According to Wortzel, Chinese doctrine views legal warfare as a kind of "political preparation of the battlefield." He elaborates that China sees "legal arguments, propaganda, and international agreements worked in advance as justifying any necessary military action."[24]

Preestablishing legal justification for a conflict is not new to China; it has demonstrated its expertise in this domain over the years. For example, before PLA troops entered the Korean War, China announced its intent and reasons by way of the Indian government.[25] In the 1962 Sino-Indian War and again in the 1969 War with the Soviet Union, China meticulously established its legal positions before the onset of hostilities. It has also used domestic law to attack international law by setting a precedent in Chinese law and then attempting to apply it to the international legal system. Examples include the 1992 Territorial Seas Law and the 2005 Anti-Secession Law; the latter targets Taiwan, which China considers a province, and justifies potential military action against it should it declare independence.[26] These events clearly demonstrate that the Chinese road to war is preceded by legal justification for the conflict.

Doctrinal Principles

Information warfare is one of the main principles under the local wars concept, one of the three overarching constructs that guide the PLA, and it will play an integral part in any future conflict. PLA doctrine directs its forces to quickly seize and retain information superiority, actively access and process information from C4ISR networks, and simultaneously deny that ability to the enemy. C2, integrated network EW, cyberwarfare, and the three warfares concept all fall under the purview of IW.

Command and Control

The degree to which individual units or combat platforms are truly integrated into a data-sharing and command system in the PLA varies by organization. The PLA has been working to network its national command structure and units in the field since the 1990s with the ultimate goal of connecting its global C2 systems with satellite assets.[27] The recent realignment of PLA forces into regional commands may have been an attempt to consolidate the force's gains in the communication sector over the past two decades.

[23] Wortzel, 2014, p. 38, quoting Peng and Yao, 2005, p. 79.

[24] Wortzel, 2014, p. 40; see also Liu Zhongshan, "Ziweiquan yu Zhuquan" ["Sovereignty and the Right of Self-Defense"], *Zhanlue yu Guanli* [*Strategy and Management*], No. 1, 2002, p. 50.

[25] Wortzel, 2014, p. 40; see also Alexander L. George, *The Chinese Communist Army in Action: The Korean War and Its Aftermath*, New York: Columbia University Press, 1967.

[26] Mark A. Ryan, David M. Finklestein, and Michael A. McDevitt, eds., *Chinese Warfighting: The Experience of the PLA Since 1949*, Armonk, N.Y.: M. E. Sharpe, 2003, pp. 173–197.

[27] Wortzel, 2014, p. 6; see also Shen Weiguang, Jie Xijiang, Ma Ji, and Li Jijun, eds., *Zhongguo Xinxi Zhan* [*China's Information Warfare*], Beijing: Xinhua Press, 2005, p. 122.

Integrated Network Electronic Warfare

Since the mid-2000s, the PLA has been developing and integrating capabilities to attack enemy C4ISR systems, as called for in its doctrine.

To effectively use integrated network EW attacks, the PLA realizes that it must combine them with integrated firepower.[28] One of the stated goals of this strategy is to blind the enemy and cut off communications between its frontline troops and headquarters by destroying its C4ISR. According to Wortzel,

> [T]he PLA also wants to inflict battlefield casualties on an enemy force and to disrupt logistics, resupply, and personnel systems in the enemy's homeland so that combat losses cannot be restored and the deployed force cannot sustain battle.[29]

Cyberwarfare

China is heavily invested in cyber activities and computer network operations, and it is actively conducting offensive and defensive cyber operations. Chinese cyberwarfare has evolved under the concept of "local war under conditions of informatization" and was highlighted as a major strategic issue by President Xi Jingping in 2014.[30] Other Chinese documents have further identified cyberspace as a new pillar of economic and social development and a new domain for national security. The PLA conducts cyber operations primarily for the following reasons:

1. To strengthen political and economic control in China [repression]
2. To complement other forms of intelligence collection and gather economic, military, or technology intelligence and information [intelligence gathering]
3. To reconnoiter, map, and gather targeting information in foreign military, government, civil infrastructure, or corporate networks for later exploitation or attack
4. To conduct exploitation or attacks using the collected information
5. To develop defenses or conduct defensive operations in the PLA's (and China's) own cyber systems.[31]

[28] Wortzel, 2014, p. 10.

[29] Wortzel, 2014, p. 15

[30] Anthony H. Cordesman, Steven Colley, and Michael Wang, *Chinese Strategy and Military Modernization in 2015: A Comparative Analysis*, Washington, D.C.: Center for Strategic and International Studies, updated October 10, 2015.

[31] Wortzel, 2014, p. 17; see also Larry M. Wortzel, Commissioner, U.S.-China Economic and Security Review Commission, "China's Approach to Cyber Operations: Implications for the United States," testimony before the U.S. House of Representatives Committee on Foreign Affairs at the hearing "The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security and Trade," March 10, 2010. See also Office of the Secretary of Defense, 2011.

"While armed conflict between the United States and China is not a certainty, a cyber conflict is already in under way," Wortzel wrote in 2014. The PLA has been infiltrating U.S. systems to collect intelligence, map infrastructure, and prepare for future real-world conflict.[32] The PLA has expanded its potential targets in an armed conflict to include C2 and communication systems, as well as the information infrastructure of nonmilitary U.S. government agencies, private-sector companies, and even individuals.[33] Former National Security Director ADM Michael McConnell, former Secretary of Homeland Security Michael Chertoff, and former Deputy Secretary of Defense William Lynn stated in a 2012 op-ed in the *Wall Street Journal* that "the Chinese government has a national policy of espionage in cyberspace. In fact, the Chinese are the world's most active and persistent practitioners of cyber espionage today." They concluded that "it is more efficient for the Chinese to steal innovations and intellectual property than to incur the cost and time of creating their own."[34]

Targets and Audiences

The PLA and the Chinese government routinely target two main audiences with their messaging: Chinese nationals and foreign audiences. The government controls the flow of information into the country and the type of information that Chinese citizens can access. It actively ensures that the public is guided toward supporting Chinese Communist Party policy and objectives.[35]

China's international public-opinion efforts have become increasingly sophisticated and more narrowly targeted, harnessing both traditional forms of media and social media platforms. One approach is to insert paid advertisements written like news articles into American or other foreign newspapers highlighting mutual economic interests and downplaying ongoing international concerns about China's human rights record.[36] Like Russia, as we discuss in Chapter Eight, China has built up its media influence abroad by launching television stations with programming friendly to its political objectives. China Central Television operates a 24-hour English-language news network, the China Global Television Network. Before converting to its all-news format, the channel also broadcasted documentaries and other cultural-interest programming. Another example is China's growing influence in Hollywood, which has sparked concerns about more Chinese propaganda in American films.[37] At

[32] David E. Sanger, "U.S. Blames China's Military Directly for Cyberattacks," *New York Times*, May 6, 2013.

[33] Wortzel, 2014, p. 20.

[34] Mike McConnell, Michael Chertoff, and William Lynn, "China's Cyber Thievery Is National Policy—and Must Be Challenged," *Wall Street Journal*, January 27, 2012, quoted in Wortzel, 2014, p. 24.

[35] Wortzel, 2014, p. 31.

[36] Wortzel, 2014, p. 31.

[37] Ana Swanson, "China's Influence over Hollywood Grows," *Washington Post*, September 24, 2016.

the same time, China bans any information that is deemed sensitive or perceived to threaten the regime—sometimes arresting artists and authors as part of this policy. The international market for these works is much harder for it to control, however.[38] Influencing public opinion extends beyond the media into physical interactions as well. The Chinese Communist Party's United Front Work Department and Ministry of Education has established Confucius Institutes in foreign universities with an objective to "'use foreigners as a bridge' to promote and convey the message of the Chinese government and Communist Party."[39]

The dispute over Taiwan's independence reflects the persistence of Beijing's messaging efforts over time and across audiences. Since the founding of the People's Republic of China in 1949, it has engaged in a campaign targeting its own population, its neighbors, and the international community to promote the concept of "one China," denying the sovereignty of the Republic of China. China's message over nearly seven decades has been that Taiwan is a province of the People's Republic of China, and it has relied on both propaganda and legal warfare to cement this claim. The United Front Work Department engages in initiatives to build support for the Chinese Communist Party and for reunification among Taiwanese populations living on the mainland as well as influential groups within Taiwan. These and other "soft-power" efforts to project a message of Chinese authority over Taiwan and to deny it international recognition as a sovereign state are backed up by the threat of military action—a result of China's practice of preestablishing legal justification for military action.[40]

Information Operations/Information Warfare Organization

Structure

The Central Military Commission, the governing body of the Chinese military, underwent a profound change on December 31, 2015. The former general headquarters and department system, which included the General Staff Headquarters, General Political Department, General Logistics Department, and General Armament Department, were converted into 15 functional departments (see Figure 5.2).[41]

Since the reforms, the PLA has been structured in a manner similar to the U.S military. The services took on a more prominent role in training, staffing, and equipping.

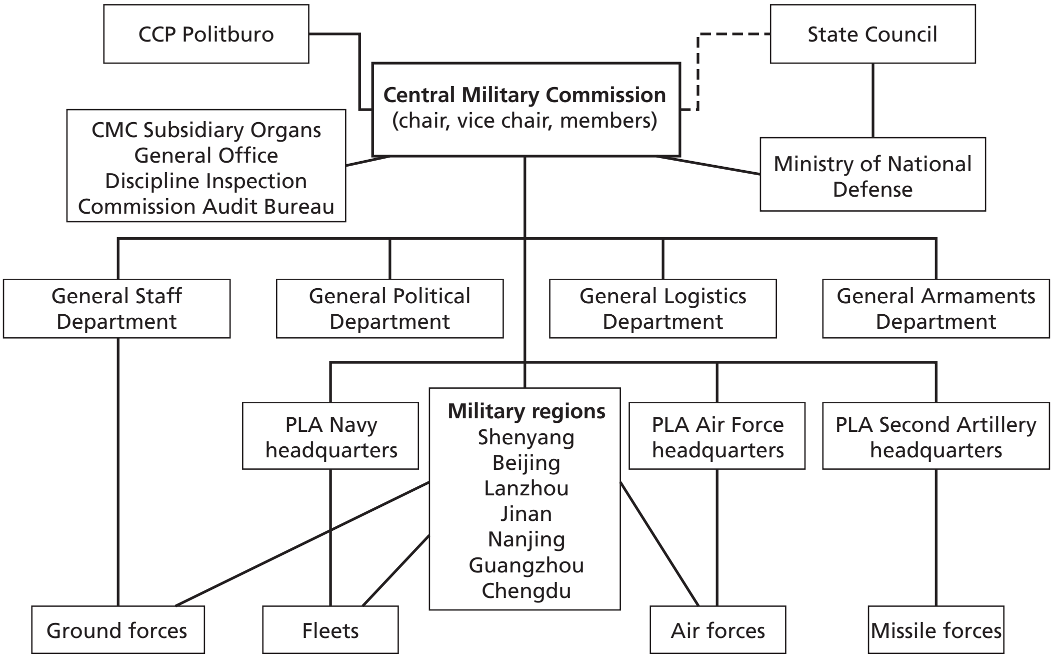
[38] Michael Forsythe and Andew Jacobs, "In China, Books That Make Money, and Enemies," *New York Times*, February 4, 2016.

[39] Wortzel, 2014, p. 32.

[40] See Yimou Lee and Faith Hung, "Special Report: How China's Shadowy Agency Is Working to Absorb Taiwan," Reuters, November 26, 2014.

[41] Guo Yuandan, "PLA Sets Up Overseas Operations Office to Strengthen Overseas Rapid Reaction," *China Military Online*, March 25, 2016.

Figure 5.2
PLA Structure Before 2016 Reforms



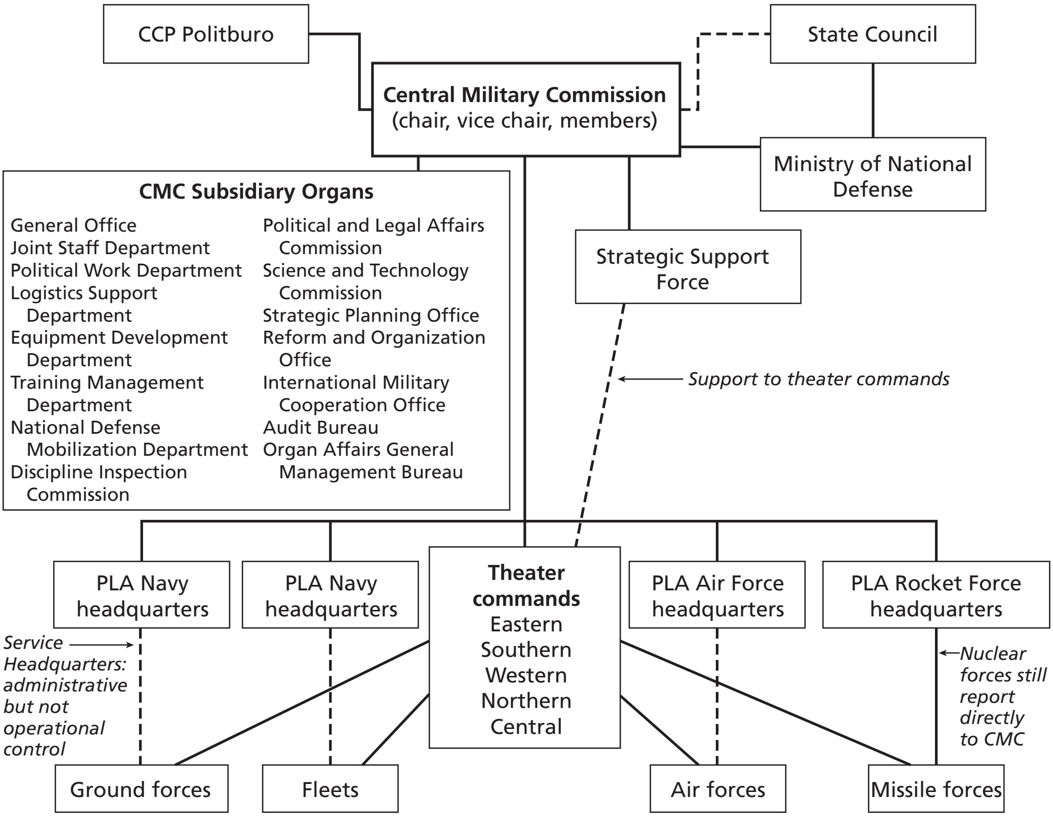
SOURCE: Phillip C. Saunders and Joel Wuthnow, "China's Goldwater-Nichols? Assessing PLA Organizational Reforms," *Strategic Forum*, Washington, D.C.: National Defense University, April 2016, p. 2, Figure 1.
NOTES: CCP = Chinese Communist Party. CMC = Central Military Commission.
RAND *RR1925z2-5.2*

Theater commands replaced the military regions, taking on more of an operational role in the PLA. Additionally, elevating the Strategic Support Force, which forms the core of the PLA's Information Warfare force, to the status of a fifth service reflects the importance of IW capabilities among the highest levels of Chinese leadership (see Figure 5.3). The role of this new force will be to seamlessly incorporate information-related activities to the theater commands.

Funding

The scale of China's annual investment in foreign propaganda activities is hard to pinpoint for three primary reasons. First, the sheer scale of activities is vast, and no single identifiable individual or agency controls this budget. Second, the Chinese government funds these activities in a variety of ways that are not openly reported. Rough estimates range between $7 billion and $10 billion, but these numbers include

Figure 5.3
PLA Structure After the 2016 Reforms


CCP Politburo
State Council
Central Military Commission (chair, vice chair, members)
Ministry of National Defense
CMC Subsidiary Organs
General Office
Joint Staff Department
Political Work Department
Logistics Support Department
Equipment Development Department
Training Management Department
National Defense Mobilization Department
Discipline Inspection Commission
Political and Legal Affairs Commission
Science and Technology Commission
Strategic Planning Office
Reform and Organization Office
International Military Cooperation Office
Audit Bureau
Organ Affairs General Management Bureau
Strategic Support Force
Support to theater commands
PLA Navy headquarters
PLA Navy headquarters
Theater commands
Eastern
Southern
Western
Northern
Central
PLA Air Force headquarters
PLA Rocket Force headquarters
Service Headquarters: administrative but not operational control
Nuclear forces still report directly to CMC
Ground forces
Fleets
Air forces
Missile forces

SOURCE: Saunders and Wuthnow, 2016, p. 3, Figure 2.
NOTE: CCP = Chinese Communist Party. CMC = Central Military Commission.
RAND *RR1925z2-5.3*

only the subsidies given to media targeting non-Chinese foreigners.[42] The actual amount could be far higher. Meanwhile, the U.S. Department of State spent $666 million on public diplomacy in fiscal year 2014 (see Figures 5.4 and 5.5).[43]

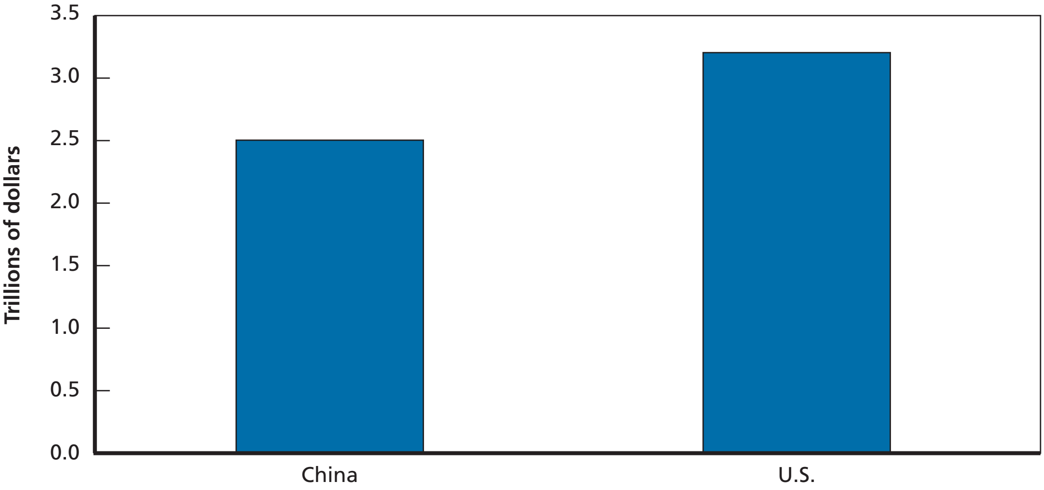
Doctrine

"The Chinese military has adopted information warfare concepts suited to its own organization and doctrine," writes Wortzel, "blending its own traditional tactics, concepts from the Soviet military, and U.S. doctrine to bring the PLA into the information age." Simultaneously, the PLA has modernized its PSYOP capabilities and

[42] Anne-Marie Brady, "China's Foreign Propaganda Machine," *Journal of Democracy*, Vol. 26, No. 4, October 2015; David Shambaugh, "China's Soft-Power Push," *Foreign Affairs*, June 16, 2015.

[43] Shambaugh, 2015.

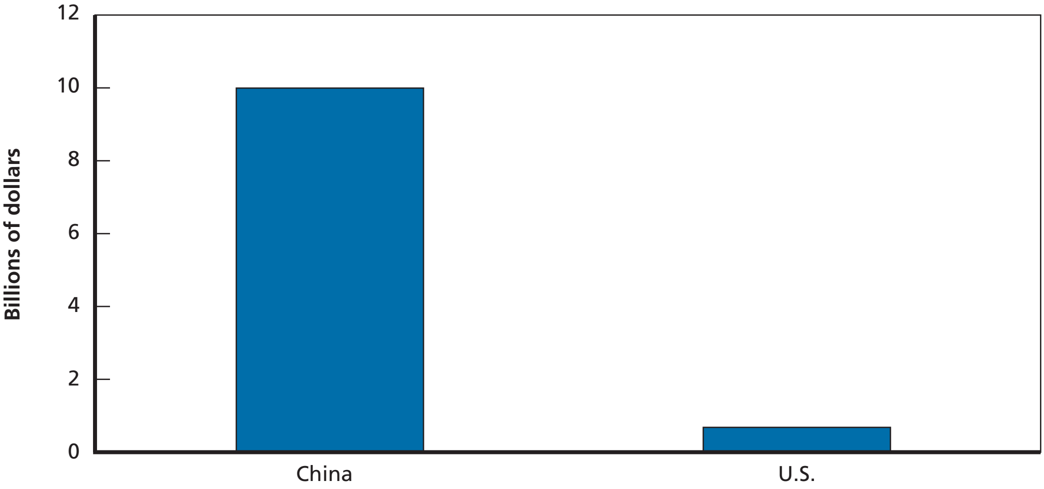
Figure 5.4
Comparison of U.S. and Chinese Budgets, FY 2014



SOURCE: Data from Koh Gui Qing, "China Budgets 2014 Fiscal Deficit of 2.1 Percent of GDP," Reuters, March 4, 2014; Office of Management and Budget, Executive Office of the President of the United States, *Fiscal Year 2014 Budget of the U.S. Government*, Washington, D.C., 2013.

RAND *RR1925z2-5.4*

Figure 5.5
Comparison of U.S. and Chinese Propaganda and Public Diplomacy Budgets, FY 2014



SOURCE: Data from James Smyth, "China's $10bn Propaganda Push Spreads Down Under," *Financial Times*, June 9, 2016; Office of Management and Budget, 2013.

RAND *RR1925z2-5.5*

engaged in legal warfare to justify military action and territorial claims.[44] The goals of PLA information warfare are to destroy the enemy's information collection and processing systems, and PLA doctrine has evolved to reflect changing technology.[45] While the motivation is to maintain information superiority over the enemy, disrupt its C4ISR capabilities, and protect PLA information systems and capabilities, the operational concepts for employing traditional signals intelligence and EW have also expanded to include cyberwarfare and other operations across the EMS.[46]

According to Wortzel,

> The truly distinguishing characteristic of operations in the information age in PLA doctrine, however, is that "information power and various types of firepower are merged" so that mobility and precision fires are integrated to increase their operational effects. Ultimately, the PLA must execute integrated operations combining computer network warfare, networked firepower warfare, electronic warfare, and sensor systems.[47]

Taking a cue from U.S. operations in Iraq and the Balkans, China has elevated EW to a strategic level of war. It has also added funding and manpower to augment these change in doctrine.

Information Operations in Practice

The PLA's General Political Department and other elements of the Chinese government, including the Chinese Communist Party's International Liaison Department and the PLA's Military Intelligence Department, sponsor visits and tours by foreign groups with military affiliations, as well as veterans' groups. These tours often include contact with selected PLA personnel who are part of the military intelligence community. The Sanya Initiative is one such program. Run by the General Political Department in conjunction with the China Association for International Friendly Contact, the Sanya Initiative brings together retired senior U.S. military officials with their retired PLA counterparts on an annual basis. The U.S.-China Economic and Security Review Commission expressed concern about the meetings' ties to Chinese propaganda efforts,

[44] Wortzel, 2014, p. xi.

[45] Zhang Yuliang, ed., *Zhanyi Xue* [*The Science of Military Campaigns*], Beijing: National Defense University Press, 2006, p. 155.

[46] Douglas C. Lovelace, forward to Wortzel, 2014, pp. vi–vii.

[47] Shen et al., 2005, pp. 227–229

highlighted the national security risks of the initiative, and traced U.S. participants' advocacy on behalf of Chinese interests and business activities in the country.[48]

According to Wortzel, "Another tactic in media warfare is to open for selective study parts of the PLA that help deliver the message that the [General Political Department] and the Propaganda Department wants delivered to foreign audiences while concealing other areas of PLA activity."[49] These actions, which are misdirection techniques at best or MILDEC at worst, are a common tactic that serves the PLA well. They effectively communicate the message that the PLA wants to put out to foreign audiences while reinforcing an image of stability and cohesive communist party leadership. By concealing and reorganizing its various functions, the PLA can create new entities that actively engage in IO without the knowledge of U.S. forces.[50]

Lessons from China's Operations in and Through the IE

Effectiveness of Chinese Information Warfare

After the Gulf War in the early 1990s, the Chinese military underwent a revolution in military affairs that radically altered the way that it viewed IT and cyberspace. Consequently, it realigned personnel, funding, and other resources to ensure increased competency in the IE. These changes have made the PLA a very savvy and capable adversary. It has continued to increase its experience and capacity to dominate the IE through exercises and other planned events that showcase the effectiveness and sophistication of Chinese capabilities.

The PLA Navy routinely engages in psychological warfare through its maritime and coastal patrol organizations and through the use of civilian fishing vessels. China has staged incidents involving foreign navies or foreign fishing fleets to establish a pretext for a conflict. These actions intimidate neighbors and other regional actors—particularly the countries that hold claims to disputed territories in the South and East China Seas. The PLA's actions remind its adversaries that it is prepared to use force if they act against Chinese interests.[51]

This example shows China's adeptness in using military presence to influence and manipulate an adversary's cognitive decisions. It also plays into the long-running narrative that the South and East China Seas are, in fact, Chinse territory. Once an action has been initiated, the Chinese media capitalizes on the event, informing the

[48] Bill Gertz, "China Using Retired U.S. Officers to Influence Policy," *Washington Times*, February 7, 2012; Ralph Z. Hallow, "Republicans Fear Exchange Program Put National Security at Risk," *Washington Times*, April 19, 2012.

[49] Wortzel, 2014, p. 33.

[50] The PLA's recent reorganization has dramatically complicated the organizational chart, as seen in Figure 5.3.

[51] Wortzel, 2014, p. 36.

domestic population of the incident in a manner favorable to China. Events like these also show how the government will use both military (PLA Navy) and civilian and proxy forces (fishing vessels) to achieve its goals.

China has also worked hard to integrate maneuver and fires for both operational and informational gains. The PLA is developing operational plans under the concept of *integrated network EW*. It has continued to integrate its forces into a consolidated C2 network, with the major ground formations (infantry, armor, artillery) networked down to the regimental level.[52] Most PLA Navy surface combat ships and submarines are networked. The PLA Air Force is in a similar position and has networked its combat and support aircraft. The same is true of Second Artillery Corps missile-firing battalions.[53] While C2 is integral to the integrated network EW concept, it is only with the addition of EW and offensive cyber actions that China can truly leverage its capabilities in the information domain. The recent reorganization of the PLA, which moved all cyberattack and defense capabilities under one "service," is an example of how it plans to streamline and consolidate this effort.

Key Takeaways

Doctrine

Chinese military doctrine has steadily evolved, becoming more refined and sophisticated in the process. Original concepts were derived from both Soviet and U.S. doctrine, and much of China's early doctrine on information warfare was adopted in response to U.S. operations in the Balkans and Operation Desert Storm. More recently, China has been studying the U.S. Navy's network-centric warfare capabilities.[54] In the cyber domain, the PLA continues to develop new doctrine, but it is constrained by its modernization efforts. At the same time, it is taking advantage of its recent reorganization to capitalize on existing strengths in EW, electronic information collection, precision attack, and massed firepower.[55] As China continues to review and refine its integrated network warfare approach and other concepts, perhaps it is time for the United States to look to Chinese doctrine and concepts to replicate.

[52] As of 2013, infantry battalions were still not fully networked.

[53] Wortzel, 2014, p. 9

[54] Wortzel, 2014, p. 11; see also Wang Zhengde, ed., *Jiedu Wangluo Zhongxin Zhan* [*Interpretation of Network-Centric Warfare*], Beijing: National Defense Industries Press, 2004, pp. 316–318.

[55] Wortzel, 2014, p. 8; see also Dai Qingmin, "Lun Duoqu Zhi Xinxi Quan" ["On Seizing Information Supremacy"], *China Military Science*, Vol. 16, No. 2, April 2002b.

Operations

The PLA has increased its operational capacity outside of mainland China and now has more forces stationed overseas—for example, as attachés at Chinese embassies, assisting with recovery efforts after disasters, or participating in UN peacekeeping missions. With its military operating in other countries' sovereign territory and facing strict diplomatic oversight on the movement of personnel and equipment, Chinese officials have suggested that the country "join or sign more conventions, treaties, memoranda, agreements and other bilateral and multilateral legal documents to provide legal protection for the promotion of the normalization of China's overseas operations."[56] To obtain favorable terms, China is likely to rely on public opinion and legal warfare strategies.

Information Warfare

The PLA routinely acts globally in its media and propaganda campaigns and is increasingly able to do so in a nuanced way. China's "peaceful rise" in the early to mid-1990s was an example of a relatively successful major propaganda campaign. It was designed to reassure China's neighbors and the world that China had peaceful intentions. The PLA contributed primarily by organizing a series of regional military-to-military dialogues.[57] However, the campaign unraveled as China took "a generally more aggressive policy on disputed territories, resource claims, and fishing rights in the South China Sea . . . and China's maritime surveillance authorities undermined years of diplomatic effort."[58]

Cyber Operations

The United States must think through how it intends to respond to the PLA's cyber activities. Defensive measures are important, but Congress and private-sector U.S. companies are discussing the potential for offensive cyber operations designed to disrupt the networks of attackers. One proposed option is to create traps to lure hackers, allow them to extract bad information, and trace the hackers' origin or hack back.[59]

Organization

Whereas Chinese military commanders are tasked with furthering the political objectives of the Chinese Communist Party, the role of the political commissar is to further these political objectives within the PLA. In that capacity, political commissars are directed to disseminate party messages and themes to PLA personnel

[56] Guo Yuandan, 2016.

[57] Wortzel, 2014, p. 46; see also China State Council Information Office, *China's Peaceful Development Road*, Beijing, 2005.

[58] Wortzel, 2014, p. 46.

[59] Ellen Nakashima, "To Thwart Hackers, Firms Salting Their Servers with Fake Data," *Washington Post*, January 2, 2013.

and are mandated to maintain party control of the army. Their primary role includes ensuring loyalty to the Chinese Communist Party; enhancing the morale of the troops; monitoring the beliefs of military personnel and their conduct with regard to rules, regulations, and policies; overseeing public relations; and reporting.[60] The political commissar is independent of the PLA and has the sole responsibility to maintain party loyalty to the Chinese Community Party. As such, it is the primary mouthpiece for regime propaganda in the PLA. There are no parallels within the U.S. military.

The elevation of the Strategic Support Force to the status of a fifth service—consolidating information warfare, space, and cyber capabilities—shows the importance that the Central Military Commission places on IRCs. The new service is responsible for ensuring that IRCs are seamlessly incorporated into theater command activities.

Personnel

The PLA has invested heavily in modernizing its personnel systems. It realizes that it remains behind the United States. According to Wortzel,

> For decades, military culture in China emphasized the importance of people, not equipment, in warfare and employed massed forces or weapons—the strengths China brought to bear in the Korean War, the Sino-Indian War, and the Sino-Vietnam War.[61]

The information age requires personnel with specific skill sets that are not readily found in the current PLA structure, and the PLA lacks personnel with the requisite expertise in complex systems.

> Chinese military leaders, however, recognize this weakness and intend to develop a talent pool of troops who can conduct and plan joint military operations, manage information systems and cyber technology, and use or maintain advanced weapon systems. The PLA's goal is to have these personnel by 2020.[62]

Despite these developments, the PLA is likely to remain a conscript-based military for the foreseeable future. Recruiting and training efforts are under way to attract personnel with the requisite skill sets, but the PLA must also compete with the civilian economy. Recruitment remains strong in less developed areas of China, particularly in the west. The PLA has used different methods to attract the talent it needs, including patriotism, higher pay, and guarantees of job security. In the past

[60] Srikanth Kondapalli, *China's Political Commissars and Commanders: Trends and Dynamics*, Singapore: Institute of Defense and Strategic Studies, October 2005, p. 4.

[61] Wortzel, 2014, p. 5.

[62] Wortzel, 2014, p. 9.

decade, the PLA created a new NCO corps, mainly employing personnel with high-tech jobs, and it has started hiring civilian contractors to augment its manpower. The PLA has also emphasized professional military education and has been expanding educational opportunities for its forces. For example, soldiers deployed to the Spratly Islands can now take correspondence classes via broadband satellite links.[63] PLA military leaders are aware of strengths and weaknesses across the force, particularly the PLA's shortfalls in the skill sets necessary to leverage current technologies and information systems. Like the U.S. military, the PLA consists of personnel with varying educational backgrounds, and it may not be possible to fulfill these needs with existing personnel. To address these challenges, the PLA has increased its recruitment efforts to gain specific technological expertise. One method that it is exploring is to increase the number and types of internships offered through academic and technology institutions and companies. These opportunities are helping the PLA adapt its personnel systems with the goal of attracting higher-caliber personnel.

[63] Jane's Sentinel Security Assessment, "China: Armed Forces," May 15, 2017.

CHAPTER SIX

North Korea

Case Summary

More than 60 years of isolation and inflammatory posturing have left the North Korean regime with limited options to influence regional and global actors. It relies on nuclear and ballistic missiles and a huge standing army, along with other asymmetric capabilities—such as EW, cyberwarfare, and information warfare—to deter aggression from outside entities. Coupled with its leadership's bellicose rhetoric, North Korea's deterrence strategy is designed to intimidate other countries and maintain regime control.

The regime focuses its efforts on influencing two audiences: (1) external actors, including its regional neighbors, the West, and the international community writ large, and (2) groups inside North Korea, including regime elites, the Korean People's Army (KPA), and the North Korean public. The regime is specifically worried about dissent from its domestic audience and therefore devotes significant effort to controlling access to information and creating a god-like "cult of personality" around supreme leader Kim Jong-un.

Background and Overview

North Korea is dominated by rugged mountains and harsh terrain, limiting access to the interior of the country. Gross domestic product ranks 176th in the world, and the average North Korean has relatively few economic opportunities.[1] Although its hermit kingdom nickname is often assumed to be derived from the separation of North and South Korea after World War II, the first such reference to North Korea was in 1882 in William Elliot Griffis's book *Corea: The Hermit Nation*.[2]

Today, North Korea is just as secluded, secretive, and detached from the rest of the world as it was in the 1800s. However, this should not be interpreted to mean that

[1] Central Intelligence Agency, "Korea, North," *World Factbook*, undated(b).

[2] William Elliot Griffis, *Corea: The Hermit Nation*, New York: Charles Scribner's Sons, 1894.

the country is unsophisticated or disengaged from regional and global politics. On the contrary, North Korea actively threatens regional and international stability in pursuit of its national interests. To the rest of the world, North Korea is seen as a belligerent, nuclear-armed state that is determined to conquer its southern neighbor. To North Korean citizens, fed a constant stream of controlled (dis)information, the perception is of a West hell-bent on destroying the country and reunifying the peninsula under South Korean rule.

The extreme nature of the regime in Pyongyang means that a great deal of emphasis is given to internal affairs and propaganda. Today, North Korea is the most closed and security-conscious society in the world, and the regime exerts a tremendous amount of effort to manage internal perceptions. Since 1950, North Korea has been ruled by only three supreme leaders, successive generations from the same family: Kim Il-sung, Kim Jong-il, and Kim Jong-un. Technically an oligarchy but functionally a dictatorship, ultimate control and power rest with the supreme leader. Most of North Korea's military and civilian leadership consists of second- and third-generation leaders who are either friends or family of the current leader, Kim Jong-un. Those who are close to the ruler can obtain considerable benefit and live a life of relative luxury when compared with the millions of typical North Koreans.

Because of North Korea's continued development of nuclear weapons and disregard for international law, the UN has passed four resolutions against it since North Korea's first nuclear test in 2006.[3] Individual nations have also enacted their own unilateral sanctions against the regime. The most recent round enacted by the United States, the North Korea Sanctions and Policy Enhancement Act of 2016, was put in place in January 2016 after North Korea tested its fourth nuclear weapon.[4] The sanctions are designed to limit the country's acquisition of the technology and equipment necessary to continue advancing its nuclear research and development. They also limit the ability of the North Korean government and its leaders to engage with the international community, effectively isolating the country.[5] While in some ways they have been effective, the sanctions also serve to bolster the regime's claims that it is being targeted by the West, and they further limit North Korea's access to the outside world.

Limiting access to information and cultivating a sieged mentality among its population are two hallmarks of the North Korean regime. It relies heavily on perception management, control of access to information, and indoctrination and other psychological methods to get its citizens to either fear or follow the regime's direction. In a state in which all information comes to citizens through official government channels,

[3] Anna Fifiled, "Punishing North Korea: A Rundown on Current Sanctions," *Washington Post*, February 22, 2016.

[4] Fifield, 2016.

[5] Elise Labott and Ryan Browne, "U.S. Sanctions North Korean Leader for First Time over Human Rights Abuses," CNN, July 7, 2016.

the North Korean government has a monopoly. To achieve its goals, it has developed robust information warfare capabilities. Many of these capabilities are dual-use: They target both the country's own population and actors in the international community. This case study examines those capabilities and draws applicable lessons for the U.S. Army in terms of capabilities it should be prepared to counter or possibly adopt.

Concepts and Principles for Operations in and Through the IE

Strategic Goals/Vision

North Korea's goals are framed by the regime's political isolation, economic deprivation, deteriorating conventional military capabilities, and the economic, political, and military growth of its neighbors.[6] The country has three primary goals:

- Maintain the authoritative position of Kim Jong-un and his family within the regime through the ideological control of the country's population.
- Unify the Korean Peninsula under North Korean control.
- Remain an independent state, free of outside interference—especially from the West.[7]

The two foundational institutions that help maintain the regime's position are the KPA and the Workers' Party of Korea; both institutions are heavily funded and controlled by the regime. Between 20 and 33 percent of North Korea's gross domestic product is dedicated to military spending.[8] However, despite its huge standing army, ballistic missiles, and nuclear weapon tests to deter outside aggression, the country is relatively constrained in offensive actions. As a result, North Korea has focused increasingly on asymmetric warfare capabilities to broaden the options available to its leaders, including a considerable focus on the IE.[9] There are specialized military and government units dedicated to EW, computer warfare, and information warfare. North Korea also has surprisingly sophisticated computer and informational capabilities, along with the institutional base to support these activities.

Table 6.1 highlights the types of asymmetric threats that North Korea has traditionally wielded. In the table, "Frequency" indicates how often the activity occurs, and "Intensity" indicates the level of effort that the regime has traditionally devoted to

[6] Office of the Secretary of Defense, *Military and Security Developments Involving the Democratic People's Republic of Korea: Report to Congress*, Washington, D.C., 2015.

[7] LtGen. Vincent R. Stewart, Director, Defense Intelligence Agency, "Statement for the Record: Worldwide Threat Assessment," statement to the U.S. House of Representatives Armed Services Committee, February 3, 2015; Office of the Secretary of Defense, 2015, pp. 6, 201.

[8] NationMaster, "North Korea Military Stats," web page, undated; Jeremy Laurence and Danbee Moon, "North Korea Spends About a Third of Income on Military: Group," Reuters, January 18, 2011.

[9] Jane's World Armies, "North Korea—Army," March 27, 2017.

Table 6.1
Major North Korean Asymmetric Threats

Threat Type	Frequency	Intensity
Nuclear threats, taking hostages	High	Medium
Threats to "turn Seoul into a sea of flames"	High	Medium
Threats to the Five West Sea Islands (Yeonpyeong, Baengnyeongdo, Daecheongdo, Socheondgo, and U Island, under South Korean governance)	High	High
Rear disturbance and infiltration of South Korea	Medium	Medium
Cyberattack	Low	High
Electromagnetic threats	Low	Medium
Political-psychological offensive threats	Low	High
Mixed symmetric-asymmetric attack	High	Very low

SOURCE: Adapted from Duk-Ki Kim, "The Republic of Korea's Counter-Asymmetric Strategy: Lessons from ROKS Cheonan and Yeonpyeong Island," *Naval War College Review*, Vol. 65, No. 1, Winter 2012, p. 61, Table 1.

the threat. The table is not comprehensive, but it does reflect the variety of asymmetric tactics that North Korea uses in the IE.

How Information Warfare Fits Within North Korea's Overall Strategic Goals

North Korea is focused on extracting economic aid and diplomatic concessions from the international community while simultaneously defending its regime against any perceived threat, either internal or external. Managing the IE is a critical element of regime survival and a primary method used to extract concessions from the international community. The regime will likely use all elements at its disposal to maintain power and will likely blend its capabilities in the IE with more conventional capabilities to achieve maximum effectiveness. However, much of North Korea's conventional capabilities are antiquated, having been built in the 1940s–1960s. As a result, recent force modernization efforts have emphasized defensive and asymmetric attack capabilities that focus on countering the technologically superior forces of South Korea and the United States. Consequently, North Korea will continue to use the IE, in which it faces a relatively low threat of retaliation, to offset its aging military capabilities.

One form of information warfare in which North Korea regularly engages are psychological campaigns, which it employs against both internal and external audiences. Internally, the regime has almost total control of information that North Korean citizens receive across all mediums—television, radio, newspapers, and the Internet. While Internet access is extremely limited and the typical North Korean cannot access the global Internet at all, the use of cell phones and social media is growing throughout the country, though it is also strictly monitored.[10] Current estimates put the share of citizens with access to a landline telephone at less than 5 percent, but cell phone use continues to rise, with 1.5–2 million users, mainly the elite, who do not have the ability to make international calls.[11]

North Korea routinely uses misinformation (information that is false, but the person disseminating it believes it to be true) and disinformation (information that is false, and the person disseminating it knows it is false) to sway public opinion toward regime goals. Multiple entities within the regime, including the KPA and the Workers' Party of Korea, are dedicated to monitoring the population—often with overlapping responsibilities to ensure obedience—and to propagating information friendly to the regime. Externally, the regime conducts many of the same kinds of information campaigns; however, these campaigns tend to have less effect on foreign populations because of the free access to information. When specifically focused, however, North Korean information warfare tactics can be quite effective. The regime uses other forms of propaganda, including leaflets distributed through various aerial delivery techniques, in an attempt to persuade South Koreans to align more closely with North Korean ideology.[12]

Targets and Audiences

Internal Audience

The largest target audience for the North Korean regime—the North Korean population—can be broken into three distinct categories. The first audience is the 20,000 elites who live in Pyongyang. These individuals form the core of the regime and owe their elevated status to the supreme leader. They typically hold positions within the government or military and tend to be the most fanatical because they have the most to lose in the event of a regime collapse. The second audience is the KPA. As a tool of the regime, North Korea's military forces are often the most publicly visible government apparatus; they control the weapons and are a devoted element of the regime. The third audience is the North Korean public.

To effectively influence these three audiences, a cult of personality has been deliberately cultivated around the regime leadership. Indoctrination starts at the earliest ages, and North Koreans are only fed information about their leader that positions him in the most favorable light. Intimidation and coercion are two of the regime's most

[10] Hewlett Packard Enterprise, "HP Security Briefing, Episode 16—Profiling an Enigma: North Korea's Cyber Threat Landscape," August 27, 2014.

[11] Eric Talmadge, "North Korea Clamps Down on Already Spare Internet Access," *Christian Science Monitor*, July 6, 2015.

[12] V. Stewart, 2015; Jane's Sentinel Security Assessment, "Korea, North—Armed Forces," July 2, 2014a; Jane's Sentinel Security Assessment, "Korea, North—Army," August 28, 2016a; Jane's Sentinel Security Assessment, "North Korea—Strategic Weapons Systems," July 23, 2014b.

frequently used tools to foster and maintain loyalty, but preferential treatment of the elite in Pyongyang and of select military units is also used.

As mentioned, information is strictly controlled, and North Koreans rely almost exclusively on state-run media content, which is carefully crafted and monitored for public consumption. All newspapers, television shows, and radio broadcasts are controlled by the government. Newspapers include *Rodong Sinmun*, a Korean Workers' Party daily paper; *Joson Inmigun*, a KPA daily paper; *Minju Choson*, a government paper; and *Rodong Sinmum*, a trade union publication.[13] Television stations are limited to Korean Central Television, a Korean Workers' party outlet that also broadcasts content online; a station dedicated to educational programming; and Mansudae Television, which broadcasts cultural events.[14] Most radios are designed to pick up the frequencies of preapproved official government stations only, such as the Korean Central Broadcasting Station. Movie theaters must show only government-approved movies, and even the animation industry is required to conform to government standards and controls. To get around these restrictions, North Koreans—at risk of punishment by the regime—purchase smuggled DVDs and USB drives containing contraband media, such as South Korean films and soap operas, and some have learned to successfully "jailbreak" their pretuned radios to pick up broadcasts by the BBC, Voice of America, and other outlets operating in South Korea, despite the regime's attempts to jam these signals.[15]

The Kwangmyong is North Korea's limited version of the Internet. By restricting online access to approved sites, the regime ensures that its citizens are not exposed to outside information that is counterproductive to indoctrination or in conflict with any regime ideals. This has the added benefit of shifting the population's negative sentiments toward external entities and maintaining ignorance of the regime's own economic hardships, brutality, and systemic incompetence.[16] Access to broader, unfiltered online content is extremely limited; most of the few thousand citizens with Internet access have jobs with the government, and their browsing is routinely monitored.[17] North Koreans caught with illegal media of any type are often harshly punished and could be sent to labor camps. Collective punishment targeting the families and asso-

[13] "North Korea—Media Profile," BBC News, August 24, 2017; Central Intelligence Agency, undated(b).

[14] "North Korea—Media Profile," 2017; Central Intelligence Agency, undated(b).

[15] Leslie Young, "Soap Operas and Short-Wave Radio: How North Koreans Learn About the Outside World," Global News (Canada), September 29, 2017.

[16] Curtis M. Scaparrotti, Commander, United Nations Command, United States–Republic of Korea Combined Forces Command, and U.S. Forces Korea, statement before the U.S. House of Representatives Armed Services Committee, Washington, D.C., April 2, 2014.

[17] Talmadge, 2015.

ciates of lawbreakers is also a common practice, and some sources estimate that more than 200,000 North Koreans are in labor camps.[18]

External Audiences

North Korea routinely targets foreign audiences with its messaging. External audiences can be broken down into allies, countries with which the regime has relationships due to its weapons export business, and adversaries. The only countries that could be considered allies of North Korea are China and Russia, although the government does not fully trust either. The second category are countries to which the regime routinely exports weapons, despite U.S.-led international efforts to stop the practice; these countries include Cuba, Egypt, Iran, Libya, Pakistan, Syria, Uganda, the United Arab Emirates, and Yemen.[19] While these countries are not friends of North Korea, they benefit from the sale of light weapons, ballistic missiles, and missile technology. The third category includes countries that North Korea views as hostile actors. It sees the United States, South Korea, and Japan as particularly threatening and determined to destroy the regime in Pyongyang. Finally, the greater international community is viewed as a puppet of the West and kept at a distance. North Korea maintains a besieged worldview in which attack from outside actors could manifest at any time. It uses the constant threat of attack as justification for the country's harsh living conditions and the many sacrifices that North Korean citizens must make for the regime.

Foundational Principles Junche and Songun

The political ideology of North Korea is *juche*, instituted in 1972 and based on the ideologies of Kim Il-sung. It emphasizes self-reliance, mastering revolution, reconstruction inside North Korea, independence from other people and countries, displaying one's strengths, defending oneself, and taking responsibility for solving one's own problems.[20] This philosophy explains North Korea's disdain for outside cultural and political influence while simultaneously asking North Koreans to sacrifice for the regime. This ideology challenges North Koreans to contribute to the nation's *chaju*, or national sovereignty and independence, and *charip*, the prosperity of the nation. As Figure 6.1 shows, *juche* is the military policy that influences the country's military strategy by giving direction to how North Korea will fight.

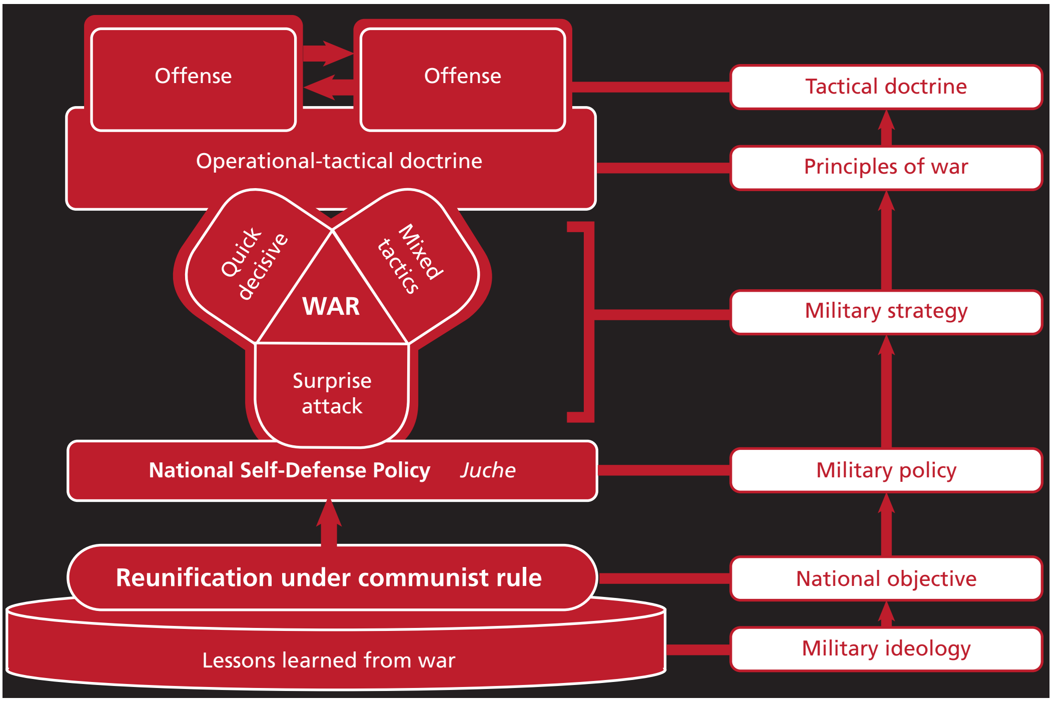
Songun is North Korea's military-first doctrine. It was developed under Kim Jong-il and focused on the development of military capabilities, internal security, and coercive diplomacy. Specifically, the strategy was designed to compel acceptance of the

[18] Dominic Midgley, "What's the Truth About North Korea's Prison Camps?" *Daily Express (UK)*, March 20, 2016.

[19] Jane's Sentinel Security Assessment, 2016a; Jane's Sentinel Security Assessment, "Korea, North—External Affairs," August 28, 2016b.

[20] Hewlett Packard Enterprise, 2014.

Figure 6.1
Building Blocks of KPA Tactical Doctrine



SOURCE: Adapted from James M. Minnich, *The North Korean People's Army: Origins and Current Tactics*, Annapolis, Md.: Naval Institute Press, 2005, p. 66, as modified by U.S. Army Training and Doctrine Command G-2 (Intelligence Directorate).
RAND *RR1925z2-6.1*

regime's diplomatic, economic, and security interests while allowing for the development of strategic military capabilities to deter external aggressions. It prioritizes the military for resource allocation above other political and economic considerations and dominates the ideological landscape of most North Koreans. The philosophy is emphasized from an early age and ingrains the concept that hardship is expected because the majority of resources are designated for military use. It also directly challenges the South Korean–U.S. alliance."[21]

History and Evolution of Information Warfare

Conventionally, the KPA uses a combination of tactics based on old Soviet doctrine (mechanized units operating in large formations to destroy the enemy's rear support), Chinese irregular warfare tactics (people's war, guerrilla warfare, and political-psychological warfare), and lessons learned by the North Koreans during the 1950–1953

[21] Hewlett Packard Enterprise, 2014.

Korean War.[22] Organizationally, the KPA identifies as a Maoist-style army that relies heavily on large armor, infantry, and artillery formations. In the IE, the KPA routinely acts as the public face of the regime. It is also attuned to current global engagements and monitors U.S. operations in Afghanistan, Iraq, and other locations around the world with a critical eye toward how the United States uses information to sway domestic and international support.[23]

Numerous conventional military actions in the past ten years, including the incident on Yeonpyeong Island on November 23, 2010, have showed the weakness of the KPA's conventional forces; as a result, the regime has placed more emphasis on asymmetric and information warfare capabilities. These asymmetric capabilities include chemical, biological, and radiological weapons; special operations forces; nuclear weapons; information and cyberwarfare; and EW.[24] Two of these capabilities, in particular, have received a large amount of attention from the regime: information warfare and cyberwarfare. North Korea's use of both has largely been viewed as successful. When coupled with conventional capabilities and a strong nuclear deterrent capability, North Korea's military options are greatly strengthened.

North Korea's Information Warfare Organization

Structure

The three highest-ranking governing bodies in the regime are the State Affairs Commission, the Cabinet, and the Workers' Party of Korea. The State Affairs Commission succeeded and expanded the mandate of the National Defense Commission in 2015; it is the highest branch of the government and controls the military and sets the policy for the regime.[25] Multiple organizations report directly to the State Affairs Commission, two of which—the Ministry of State Security and the Ministry of People's Armed Forces—have units that routinely monitor communications and conduct hacking operations. The Cabinet also has several organizations for which it is responsible, including the Central Scientific and Technological Information Agency, which collects, analyzes, and processes data (often procured from China, Russia, and Japan).[26] The Workers' Party of Korea oversees, among other organizations, Unit 35, which is

[22] Jane's Sentinel Security Assessment, 2014a; Kim, 2012.

[23] Steve Herman, "Secret Manual Gives Glimpse of North Korean Military Tactics," Voice of America, September 18, 2010; STRATFOR, "Dispatch: Korea's Refocusing Policy Postures," November 18, 2010; Charles Scanlon, "North Korea: Past Lessons Will Affect the Next Move," BBC News, April 4, 2013.

[24] Kim, 2012.

[25] Chloe Sang-Hun, "Kim Jong-un Takes an Additional Title in North Korea," *New York Times*, June 29, 2016.

[26] Stephen C. Mercado, "Hermit Surfers of P'Yongyang: North Korea and the Internet," *Studies in Intelligence*, Vol. 48, No. 1, last updated June 27, 2008.

responsible for technical operations and training cyber warriors, as well as Unit 204 and Office 225, which are heavily involved with internal and external PSYOP.[27]

Training

Computer warfare is an area of special emphasis for North Korean training. The country has a large and competent computer technology base that includes the Korea Computer Center, Pyongyang Informatics Center, and several universities, such as Kim Chaek University of Technology and Kim Il-sung University's School of Computer Science.[28] Individuals are selected for training from a very early age and receive math- and science-focused education. Many North Korean citizens aspire to be "cyber warriors" because they can receive better pay and living conditions.

IRCs Employed/Available

Electronic Warfare

EW activities are conducted across the EMS to control or deny an adversary's military's capabilities. North Korea routinely conducts EW operations as a means of information warfare, often directed at the South Korean and U.S. militaries. Much of North Korea's hardware is outdated and has limited capability, however. What capability it does have is focused on the ability to exploit, deceive, degrade, damage, or destroy sensors, processors, and C2 nodes. For example, the North Korean military routinely exercises its capabilities and has attacked and otherwise disrupted South Korean GPS-dependent systems.[29] It also uses signals intelligence and ground sensors to detect enemy movement near North Korea's borders.

Computer Warfare

In the cyber domain, North Korea has continued to build its offensive cyber capabilities, which have reached an advanced level of sophistication. These activities range from hacking, system mapping, and denial of service to inserting malicious software (viruses, worms, logic bombs, or Trojan horses).[30] For example, the Sony Pictures hack in 2014 showed North Korea's infiltration capabilities: After stealing an administrative password, hackers were able to fully map out Sony's infrastructure. The hackers also used numerous sophisticated software tools in the attack, including listening implants, a lightweight backdoor module (a tool used to breach open ports, execute commands,

[27] Hewlett Packard Enterprise, 2014.

[28] Jenny Jun, Scott LaFoy, and Ethan Sohn, "What Do We Know About Past North Korean Cyber Attacks and Their Capabilities?" Washington, D.C.: Center for Strategic and International Studies, December 12, 2014.

[29] James Johnson, "South Korea Claims North Korea Is Jamming GPS Signals on Planes," *The Inquisitr*, May 2, 2012; "N.K. Continues GPS Jamming," *Korea Herald*, May 7, 2012. It is important to note that there is no South Korean GPS. There are only systems and platforms that rely on U.S. GPS.

[30] Mike Lennon, "Hackers Used Sophisticated SMB Worm Tool to Attack Sony," *Security Week*, December 19, 2014.

and perform other functions), proxy tools, destructive hard-drive tools, and destructive cleaning tools.[31] Other examples of North Korean cyber capabilities include the routine use of computer warfare against the South Korea government, the United States, and private industry. By some reports, North Korea spends 10–20 percent of its military budget on cyberwarfare.[32]

Information Warfare

North Korea operates an effective internal information campaign that uses propaganda and other methods against its own citizens, bolstering national pride while deceptively encouraging citizens to distrust anyone from a foreign country. Limited access to information allows the regime to shape North Korean thoughts and attitudes, and anyone who questions the regime message may be sent to one of its political prison camps.

Multiple organizations are responsible for propaganda in North Korea, with one of the most prolific being Unit 204. It uses posters, traditional media outlets, websites, and social media to internally shape the views of the North Korean citizens. The regime also attempts to persuade foreign audiences to view it in a positive manner, typically through internal and external digital channels. North Korea Today has profiles on Twitter and Facebook for external consumption.[33] North Korean propaganda even features altered photos of past supreme leader Kim Jong-il, making him appear younger and healthier in an attempt to change the North Korean people's perceptions of their late leader. The regime can also air-deliver leaflets to South Korea through a variety of methods, including balloons and unmanned aerial vehicles. U.S. military personnel and South Koreans have found these propaganda leaflets for decades in the demilitarized zone and just south of the border.[34]

Information Operations in Practice

In practice, North Korea operates from a compromised position and has limited informational tools at its disposal. However, its focus on the development of nuclear capabilities, maintaining a large standing army, and developing its IRCs has led it to excel in several areas. Heavily invested in IO for years, the regime has centered its efforts on electronic and cyberwarfare and controlling internal media to maintain its power base and to create a state of fear toward the West. The regime exercises complete con-

[31] Lennon, 2014.

[32] Pierluigi Paganini, "A High-Profile Defector Warns That North Korea's Cyber Army Has the Capability to Run Cyber Attacks That Could Cause Loss of Human Lives," *Security Affairs*, May 30, 2015.

[33] @uriminzokkiri is the official North Korean Twitter account, and it can be found under Uriminzokkiri on Facebook.

[34] Hewlett Packard Enterprise, 2014, pp. 58–59.

trol over the media to censor domestic access to information and to project information that the regime deems palatable. Its focus on information dominance has led to a robust information security apparatus, strong control of information, and advanced cyber operational capabilities.

Lessons from North Korean Operations in and Through the IE

Dual-Focused Regime

North Korea places a heavy emphasis on internal control of information. The regime spends significant time, energy, and resources to ensure that its people receive only the message the regime wants them to hear. This domination of information over the North Korean population allows the cult of personality around Kim Jong-un to flourish. Consequently, devotion to the supreme leader is effectively unanimous, with any deviation from adherence to government direction met with harsh punishment. This is exemplified by the hundreds of thousands of North Koreans who are in labor camps. This large number of political prisoners is an undeniable sign of public alienation and discontent within North Korea.

The regime is fearful of messages that espouse freedom, democracy, and human rights, which, it feels, could trigger unrest or a public uprising. This is the main reason that North Korea is posturing itself in an increasingly antagonistic position toward the West, particularly through the use of nuclear and ballistic missile tests. For example, the North Korean regime is so threatened by anti-Pyongyang propaganda messages broadcast by South Korea via loudspeakers across the shared border that it has threatened war over their use.[35]

Cyber Capabilities

North Korea continues to see cyber operations as a means to intimidate and coerce internal and external populations, and it has expended massive resources training and developing cyber capabilities. Training in math and science begin at the earliest ages to identify talented children who are then selected for further training. This allows North Korea to continue to grow and professionalize its cyber warrior cadre. Current estimates place the number of dedicated cyber professionals working for the government and military at 6,000.[36]

China assists this effort by allowing North Korean hackers to operate from its soil. Much of North Korea's cyber hardware is located across its border in several Chi-

[35] Foster Klug, "North Korea Threatens Strikes Over S. Korean Propaganda Broadcasts, Denies Role in Mine Blasts," Associated Press (*U.S. News and World Report*), August 14, 2015.

[36] David E. Sanger, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More," *New York Times*, October 15, 2017.

nese cities. This allows North Korea to maintain plausible deniability, and it shields the country's internal systems from external access and attack. Another added benefit of conducting operations from China is the links it generates to organized crime syndicates, an often-used source of revenue for the regime.

Key Takeaways

The North Korean government knows that South Korea and Western powers do not want another active war on the peninsula; as such, its bellicose threats often lead to success at the negotiating table. North Korea will continue to actively employ information warfare tactics because there is no punishment for their use and, to the regime, they yield results at a level low enough not to trigger open conflict.

Most of North Korea's IRCs are dual-use: The regime can monitor and control its own population and target external entities. The regime is highly skilled at controlling and altering information to suit its needs, and it targets all three primary internal audiences—elites, the KPA, and the public writ large—with sophisticated, targeted messages that appeal to each. For outside audiences, the regime is specific in its targets and the messages it sends. While its messages to the international community tend to be viewed as comical, when coupled with other asymmetric capabilities, the threats can be credible.

To counter North Korea's efforts, it is critical to be aware that its society is extremely information-starved and that the medium through which a message is delivered is just as important as the message itself. Messages must be crafted separately to target elites, the military, and the average citizen, as each group receives different benefits—and faces different threats—from the regime. Furthermore, the power of the truth cannot be discounted; as more North Koreans become aware of the brutal nature of their regime, the large numbers of their fellow citizens in labor camps, and the continued threat of collective punishment, cracks in the social fabric will start to emerge. The situation in North Korea cannot be changed overnight. However, the persistent pressure of information from outside North Korea, coupled with the influence of popular culture, will create opportunities over time to more effectively engage North Korea's citizens.

Takeaways for the U.S. Army

There are several important takeaways for the U.S. Army with respect to North Korean activities in and through the IE. A critical observation is that operating in and through the IE is not viewed as a luxury for North Korea, but, rather, a necessity. The primary objective is regime survival, which, in turn, is dependent on a pliant and sycophantic domestic population. Those in charge of inculcating the population with propaganda have done a masterful job of portraying North Korea as a victim, constantly under threat from external powers—chiefly the United States—and urging the importance of internal cohesion, unity, and, above all, loyalty to the regime.

That regime propaganda and indoctrination have been generational lends a certain sense of legitimacy through consistency and repetition. The regime develops narratives and sticks with them, coordinating across the whole of government, a feat obviously enabled by the highly centralized structure of the communist party. Any future contingencies involving the U.S. Army in North Korea would be complicated by the fierce resistance that soldiers would likely face from the North Korean population, which has been harangued over decades about the danger posed by an American invasion.

North Korea's actions in and through the IE are viewed as a force multiplier, and the regime effectively synchronizes its propaganda and official statements with bellicose actions, including missile launches, in an attempt to reinforce the severity of its threats. Since the leadership likely recognizes that it will never close the gap with Western militaries from a conventional standpoint, it is likely that Pyongyang will continue to pursue what it views as game-changers, including nuclear weapons and a larger, more effective cyber arsenal.

CHAPTER SEVEN

Iran

Case Summary

Iranian influence operations are directed at multiple audiences. Domestically, the goal is to promote the view that the country is unfairly targeted by the rest of the world, particularly the United States and Israel. Across the broader region, Iran's efforts in the IE are largely directed toward its ongoing proxy conflict with Saudi Arabia, in which Tehran supports Shia populations in Iraq, Yemen, Lebanon, Syria, Bahrain, and elsewhere. The Iranian Revolutionary Guard Corps (IRGC) Quds Force is an elite military unit used by the regime to train proxy forces abroad as a means of extending Iranian foreign and security policy across the Middle East.

On a more fundamental level, Iran is beginning to devote a significant portion of its resources, attention, and energy to cyberspace. It has employed cyber capabilities less to exercise real aggression than to signal its capability and to act as a deterrent, which involves both having punitive capabilities and demonstrating a resolve and willingness to use them. Iran has used technical IRCs in exactly this way. Iranian hackers have progressed far beyond website defacing or distributed denial-of-service attacks; they are now capable of developing sophisticated software to probe U.S. systems for vulnerabilities, inject malware, and gain control. In its operations in and through the IE, Iran has no compunction about disseminating falsehoods or manipulating information and relies extensively on the use of informational combat power in operations short of war.

Background and Overview

Iran is a country of approximately 81 million people located at the crossroads between the Middle East and Central Asia. Formerly known as Persia, Iran's population is 99 percent Muslim, and the overwhelming majority (between 90 and 95 percent) are Shia.[1] The story of contemporary Iran begins with the 1979 Islamic Revolution and

[1] Central Intelligence Agency, "Iran," *World Factbook*, undated(a).

continues forward with the legacy of Ayatollah Ruhollah al-Musavi Khomeini. The revolution gave Khomeini the confidence to preach the benefits of theocratic rule, and he declared Iran an example of how a country can succeed by following Islam and installing a truly Islamic government.

According to Khomeini, Allah believed Islam should be implemented thoroughly, and he would see to it that Iran would build a model Islamic state and spread the Revolution throughout the region.[2] As Barry Rubin notes, Khomeini "had rejected this idea that 'Islam in the present day is incapable of administering a country.'"[3] Iran fought a bloody eight-year war against Iraq from 1980 to 1988, and that conflict shaped the mindset of many of its senior military leaders. Since the United States invaded Iraq and toppled Saddam Hussein in 2003, Iran has steadily increased its influence over the Shia-dominated government in Baghdad, and it controls several prominent militias operating in Iraq. In addition to funding, training, and equipping Iraqi Popular Mobilization Force units, Iran also relies on proxies in Lebanon (Hezbollah), Syria, and Yemen.

Concepts and Principles for Operations in and Through the IE

The Iranian approach relies on the "deft use of the media and other propaganda tools to influence popular sentiment," and Iran often uses misinformation, deflection, or hyperbole to frame its positives while accentuating any potential negatives of its adversaries, including Israel, the United States, and Saudi Arabia.[4] Iran is well aware of its own disadvantages in terms of power projection and conventional military capability, and it attempts to use the IE to achieve an asymmetric advantage. In short, Iran believes that propaganda is critical to revolutionary movements and success in warfare.[5]

Strategic Goals/Vision

Where the government's reach is less robust, particularly in some rural areas of Iran, the IRGC and Basij (paramilitary militia) leadership stress the necessity of media cooperation and seek to promote a "culture of sacred defense." These are subtle ways

[2] Vali Nasr, *The Shia Revival: How Conflicts Within Islam Will Shape the Future*, New York: W. W. Norton, 2006, p. 125.

[3] Barry Rubin, *The Tragedy of the Middle East*, Cambridge, UK: Cambridge University Press, 2002, p. 124.

[4] Frederic Wehrey, David E. Thaler, Nora Bensahel, Kim Cragin, Jerrold D. Green, Dalia Dassa Kaye, Nadia Oweidat, and Jennifer J. Li, *Dangerous but Not Omnipotent: Exploring the Reach and Limitations of Iranian Power in the Middle East*, Santa Monica, Calif.: RAND Corporation, MG-781-AF, 2009, p. 54.

[5] Michael Eisenstadt, "The Missing Lever: Information Activities Against Iran," Washington, D.C.: Washington Institute for Near East Policy, Policy Notes No. 1, March 2010, p. 3.

of coercing less formal media outlets into cooperating with Tehran's agenda.[6] The IRGC produces publications to recruit new members into its ranks and to spread the leadership's Islamic ideology. For example, it produces various books, booklets, and pamphlets that focus on the geopolitical context of Iranian foreign policy, explaining or justifying Iran's involvement in conflict outside of its borders and its deep connections to Islam and Shia history.[7]

How Operations in and Through the IE Fit Within Iran's Overall Strategic Goals

Iran employs IO to attain several overarching strategic goals, including regime self-preservation, regional hegemony (which extends to the use of proxy forces in Lebanon, Syria, Iraq, Yemen, and elsewhere), and global expansion. The leadership views IO as a subset or complement to political warfare, which is the employment of all means at a nation's command, short of war, to achieve national objectives.[8] Iran engages in civil-military operations and civil affairs–like activities through its patronage in the Middle East, but especially in Syria since the beginning of the civil war there in 2011. According to Ahmad Majidyar, a fellow and managing editor at the Middle East Institute's Iran Program,

> The high-profile celebrations of Iran's Islamic Revolution across Syria—organized by Iranian government entities or Iranian-funded cultural and religious organizations—are one illustrative example of how the Islamic Republic uses soft power tools to expand its ideological, cultural and political spheres of influence across the Middle East.[9]

Targets and Audiences

Iran uses media operations to influence a range of actors, including its own domestic constituency, Arab governments in the region (those both friendly and unfriendly to Tehran), the citizens within these countries, and a litany of adversarial countries, chief among them Israel and the United States. Indeed, if post-Revolution Iran has an official slogan, it might very well be, "Death to America," although some Iran analysts are keen to point out the distinction between a dislike or hatred for U.S. foreign policy and

[6] Frederic Wehrey, Jerrold D. Green, Brian Nichiporuk, Alireza Nader, Lydia Hansell, Rasool Nafisi, and S. R. Bohandy, *The Rise of the Pasdaran: Assessing the Domestic Roles of Iran's Islamic Revolutionary Guards Corps*, Santa Monica, Calif.: RAND Corporation, MG-821-OSD, 2009, p. 51. See also Ray Takeyh, "Iran's Revolutionary Guards Are Shaping the Future of the Middle East," *Defense One*, June 17, 2016.

[7] Afshon Ostovar, *Vanguard of the Imam: Religion, Politics and Iran's Revolutionary Guards*, Oxford, UK: Oxford University Press, 2016, p. 124.

[8] U.S. Army Special Operations Command, "Counter-Unconventional Warfare White Paper," September 26, 2014, p. 12.

[9] Ahmad Majidyar, "Celebrations of Iranian Revolution Across Syria Shows [sic] Iran's Soft Power Hegemony," Washington, D.C.: Middle East Institute, February 13, 2017.

attitudes toward American people.[10] In December 2012, the Iranian regime launched its own YouTube channel, *Mehr*, dedicated to influencing domestic audiences with content approved by the government.[11]

Foundational Principles

Iran's soft power initiatives have focused on its near abroad, including generous investments in economic and development aid for reconstruction and infrastructure projects in both Iraq and Afghanistan, as well as strategic investments in media, finance, and other quasi–private-sector outlets.[12] Iran values soft power immensely and finds it an effective means of translating resources into leverage; its leadership has elevated the spread of Persian culture as a means of securing influence beyond the country's border.

History and Evolution

Iranian activities in and through the IE are closely tied to the country's media, which can vacillate from moderate to hardline, depending on the makeup of the government. Iran's 1979 revolution set the tone for the next several decades as first Khomeini and then Khamenei stressed the export of the revolution's values to regional Shia and Arab constituencies. The bloody eight-year war against Saddam Hussein and Iraq took a heavy toll on the Iranian military, further reinforcing the importance of low-cost force multipliers, like activities in and through the IE.

For most of the 1990s, Iran's military budget was relatively modest and focused more on defense than offense.[13] The IE *within* Iran opened up significantly during the tenure of President Mohammad Khatami, when hundreds of reformist newspapers and journals were allowed to operate openly.[14]

Organization for Operations in and Through the IE

Iran's leadership understands and appreciates the value of psychological warfare. In a 2006 report, *The Role of the Media in Political and Cultural Conflict*, the leadership lauded the role of radio, television, and other media in helping to promote Islamic

[10] Hooman Majd, *The Ayatollah's Democracy: An Iranian Challenge*, New York: W. W. Norton, 2010, p. 163.

[11] David Murphy, "Iran Launches 'Mehr,' Its Own YouTube-Like Video Hub," *PCMag*, December 9, 2012.

[12] Wehrey, Thaler, et al., 2009, p. 2.

[13] Daniel Byman, Shahram Chubin, Anoushiravan Ehteshami, and Jerrold D. Green, *Iran's Security Policy in the Post-Revolutionary Era*, Santa Monica, Calif.: RAND Corporation, MR-1320-OSD, 2001, p. 100.

[14] Sara Beth Elson, Douglas Yeung, Parisa Roshan, S. R. Bohandy, and Alireza Nader, *Using Social Media to Gauge Iranian Public Opinion and Mood After the 2009 Election*, Santa Monica, Calif.: RAND Corporation, TR-1161-RC, 2012, p. 13.

ideals, generating and sustaining support for Hezbollah, and clarifying what it viewed as misperceptions of Iran and its theocratic style of government.[15]

Structure

Besides the supreme leader and his close cadre of confidantes, the next most powerful entity within Iran is the IRGC.[16] In addition to its primary military and security functions, the IRGC administers two universities, two think tanks, assorted policy journals, and several media outlets, including the major state-sponsored media corporation.[17] The Basij, a paramilitary volunteer militia, established a network of spies and informants to help gather intelligence on any activities deemed to be anti-regime. This network was so pervasive that it became known colloquially as the "36 million [member] information network."[18]

In terms of cyber activities, the supreme leader's office, the IRGC, and the Basij are responsible for defending Iranian cyberspace and monitoring international cyberspace. The degree of cooperation and the division of labor between these entities is opaque, just as it is in other areas of security and defense.[19]

Funding

There are no clear numbers on Iran's total military expenditures; however, the total budget for the Ministry of Information and Communication Technology in 2014–2015 was approximately $1.36 billion, an astonishing 95-percent increase from the prior year. The 2015–2016 budget increased spending by an additional 34 percent.[20]

Key Leaders

Ayatollah Ali Khamenei ascended to the status of supreme leader of Iran, replacing Khomeini in 1989. In the process, he inherited a wealth of challenges, including an economy in tatters from eight years of continuous war. Commenting on the death of Khomeini, who died of a heart attack at the age of 86, one observer remarked, "[T]he charismatic symbol of the revolution was replaced by men of more modest proportions who would now have to address the daunting, if mundane, challenges of

[15] Jerrold D. Green, Frederic Wehrey, and Charles Wolf, Jr., *Understanding Iran*, Santa Monica, Calif.: RAND Corporation, MG-771-SRF, 2009, p. 36.

[16] Karim Sadjapour, "The Islamic Republic Will Never Be the Same," Washington, D.C.: Carnegie Endowment for International Peace, June 26, 2009.

[17] Green, Wehrey, and Wolf, 2009, p. 13.

[18] Wehrey, Green, et al., 2009, p. 26.

[19] Dina Esfandiary and Ariane Tabatabai, "Iran's Cyberattacks Are Likely to Increase. Here's Why," *Washington Post Monkey Cage Blog*, November 18, 2015.

[20] Small Media, *Iranian Internet Infrastructure Policy Report*, London, January 2014.

post-revolutionary Iran."[21] Tensions between Iraq and Iran were at an all-time high at this time, and Khomeini had vowed to pursue the war with Iraq until Saddam Hussein was defeated.

Khamenei was elevated to succeed Khomeini mainly due to his popularity among conservative clerics in Iran, but outside of Tehran, he was still an unknown quantity. On the battlefield, IRGC commander Qassem Suleimani oversees the elite Quds Force, which is responsible for Iran's most important missions beyond its borders.[22]

IRCs Employed/Available

Driven in large part by two major events—the 2009 Green Movement and the 2010 Stuxnet attack—Iran has markedly increased its investment in offensive and defensive cyber capabilities.[23] Cyber is integrated directly into Iran's broader strategy to operate in and through the IE, and, according to commentators, "Tehran dials its cyber activities up or down depending on the signal it wants to send to its adversaries."[24] Moreover, unlike other countries with sophisticated cyber capabilities, Iran's activities focus less on espionage and theft and more on wreaking havoc and destruction within the networks of its adversaries.[25]

Although Iran is investing heavily in its cyber capabilities, its Arabic-language al-Alam News Network remains the "centerpiece of Tehran's strategic communication strategy in the Arab world." Organizationally, it is a part of Iran's state-run media apparatus, the Islamic Republic of Iran Broadcasting, itself headed by an ex-IRGC commander appointed by Khamenei.[26]

Iranian messaging frequently references conspiracy theories suggesting that the United States and Israel are working to undermine the regime and replace it with a pro-Western government friendly to Washington and Tel Aviv. More recently, the nascent regional proxy conflict between Saudi Arabia and Iran led Tehran to direct significant ire toward Riyadh, and its mullahs blame the kingdom for spreading the Wahhabist ideology underpinning the rise of ISIL. The government meddles more directly in the media during times of unrest, as seen during the 2009 protests against the reelection of then-President Mahmoud Ahmadinejad and in favor of the opposition candidate, Mir-Hossein Mousavi, who was perceived to be more moderate and reform-minded

[21] Augustus Richard Norton, *Hizballah of Lebanon: Extremist Ideals vs. Mundane Politics*, New York: Council on Foreign Relations, 1999, p. 18.

[22] Dexter Filkins, "The Shadow Commander," *New Yorker*, September 30, 2013.

[23] Jay Solomon, "U.S. Detects Flurry of Iranian Hacking," *Wall Street Journal*, November 4, 2015.

[24] Esfandiary and Tabatabai, 2015.

[25] Sam Jones, "Cyber Warfare: Iran Opens a New Front," *Financial Times*, April 26, 2016.

[26] Wehrey, Thaler, et al., 2009, p. 131.

than his opponent.[27] This dynamic was apparent once again in the anti-regime protests in early 2018.

Organizations/Functions Within or Aligned with IE Efforts

In addition to employing official state media, Iran also seeks to co-opt nongovernmental organizations and grassroots movements to help promote its agenda.[28] For such groups or organizations, the government actually prefers a layer of ambiguity, which makes it seem that its propaganda is organic rather than directed from the highest levels of the Iranian government.[29]

Coordination/Integration Efforts/Challenges

Iran's tendency to operate through multiple proxy forces occasionally poses a challenge to C2 in the IE. Operating through a proxy can be effective, but transmitting directives to different countries, with different cultures, languages, and contexts is not always a smooth process. Moreover, Iran's actions in Lebanon, Iraq, and Syria have been perceived, at times, as unnecessary meddling by the domestic populations of these countries, further attenuating Iran's ability to influence events on the ground.

Information Operations in Practice

Iranian IO consists primarily of influence operations in support of its quest for regional dominance and to establish an advantage in its regional proxy conflict with Saudi Arabia. Tehran supports Shia populations in Iraq, Yemen, Lebanon, Syria, Bahrain, and elsewhere; in Bahrain, specifically, Iran issues political statements calling for peace in an attempt to undermine the Saudi-backed government.[30] IRGC Quds Force commanders and Hezbollah militants (supported by Iran) are active in both Syria and Iraq.

Examples of Interesting Iranian Efforts

Through Islamic Republic of Iran Broadcasting, the country is quietly pursuing an expansionist agenda on a global scale, promoting Iranian culture and civilization to an international audience. In addition to al-Alam News Network, which focuses on Iraq, Lebanon, Palestine, and Africa, Iran operates four other international news channels, including a Spanish-language station broadcasting in Spain and Latin America and a

[27] Abbas Milani, "The Green Movement," in Robin Wright, ed., *The Iran Primer: Power, Politics and U.S. Policy*, Washington, D.C.: United States Institute of Peace, 2010.

[28] Pierre Pahlavi, "Understanding Iran's Media Diplomacy," *Israel Journal of Foreign Affairs*, Vol. 6, No. 2, 2012, p. 27.

[29] We thank Alireza Nader at RAND for this observation.

[30] Jason Rivera, "Iran's Involvement in Bahrain: A Battleground as Part of the Islamic Regime's Larger Existential Conflict," *IO Sphere*, Winter 2015, p. 13.

24-hour English-language channel, Press TV, which launched in 2007. International media operations are complemented by websites available in target-audience languages and in Persian.[31]

Noteworthy Capability Demonstrations or Practices

Iranian IO can be tailored to specific target audiences to focus on niche policy issues, including its nuclear negotiations with the West or the status-of-forces agreement between the U.S. military and the Iraqi government. When the agreement was being negotiated in 2009, both al-Alam and Hezbollah's al-Manar television network aired highly critical programming in an attempt to derail the agreement altogether. Iran portrayed the issue as one of Iraqi sovereignty when, in reality, it was obvious that Tehran was more concerned with limiting the presence of the U.S. military in a neighboring country. When the agreement was ultimately approved, Iranian media was highly critical of the decision.[32]

Anticipated Developments

Iran is likely to continue developing its cyber capabilities, a current major line of effort for the regime and one that appears to be paying dividends: Iran is often mentioned alongside Russia, China, and North Korea as a nation-state with robust cyber capabilities.

Efforts of Others to Counter Iranian Efforts in the IE and Their Effectiveness

The West—and the United States, specifically—is on constant guard against Iranian cyberattacks. As part of its efforts, Iran has used the IRGC to target industrial control systems in both the public and private sectors, including supervisory control and data acquisition systems that are essential to the functioning of utilities and industrial automation.[33] In response, the United States took an unprecedented step in March 2016, indicting several Iranian citizens whom it alleges were working as hackers for the IRGC and Iranian government. These hackers are accused of conducting cyberattacks against the New York Stock Exchange, NASDAQ, Bank of America, J. P. Morgan Chase, and AT&T, as well as the Bowman Avenue Dam in Rye, New York, where hackers gained unauthorized remote access to a computer controlling the dam's floodgate.[34]

[31] Edward Wastnidge, "The Modalities of Iranian Soft Power: From Cultural Diplomacy to Soft War," *Politics*, Vol. 35, Nos. 3–4, November 2015, p. 372.

[32] Wehrey, Thaler, et al., 2009, p. 121.

[33] Frederick W. Kagan and Tommy Stiansen, *The Growing Cyberthreat from Iran: The Initial Report of Project Pistachio Harvest*, Washington, D.C.: American Enterprise Institute, April 2015, p. 14.

[34] Erik Larson, Patricia Hurtado, and Chris Strohm, "Iranians Hacked from Wall Street to New York Dam, U.S. Says," Bloomberg (*Business Times*), March 24, 2016.

Lessons from Iranian Operations in and Through the IE

Iran uses influence operations to convince its people that they are targeted by the rest of the world, particularly the United States and Israel. Over the past decade, Iran has significantly increased investment in its cyber capabilities, and Iranian hackers have progressed far beyond website defacing or distributed denial-of-service attacks. They are now capable of developing sophisticated software to probe U.S. systems for vulnerabilities, inject malware, and gain control.[35]

Effectiveness of Iranian Operations in the IE

Besides using information in an offensive manner, a major line of effort with respect to Iran's activities in and through the IE is defensive. Indeed, Iran excels in censorship and information control, and it dedicates significant resources to this end. One aspect of the regime's efforts to censor information is the creation of a parallel or "second" Internet with the goal of isolating the Iranian population from the broader Internet.[36] A dedicated unit known as the "cyber police" is responsible for monitoring the activities of journalists, reporters, and activists who rely on the Internet to disseminate and access information.[37] Both Facebook and Twitter are banned in Iran, but tens of millions of Iranians use the encrypted messaging app Telegram. In August 2016, it was revealed that Iranian hackers belonging to a group called Rocket Kitten successfully hacked Telegram messaging accounts in Iran. The spear-phishing campaign used Persian-language references and was similar to ones used in the past by the IRGC.[38] Iran has demonstrated enough capability to operate in and through the IE, especially in the cyber domain, to give the United States and the West serious pause when considering the wisdom of rattling sabers against Tehran. As such, it would be logical to conclude that Iran's capabilities constitute an effective deterrent against Western encroachment, especially as Iran continues to devote significant resources to further developing these capabilities.

Vulnerabilities in Iranian Operations in the IE

Iranian IO efforts can be either defensive or offensive, with the former attempting to insulate the population "against corrosive foreign cultural influences, subversive political messages, and purported U.S. psychological warfare activities" and the latter

[35] Kagan and Stiansen, 2015.

[36] Ilan Berman, vice president, American Foreign Policy Council, "The Iranian Cyber Threat, Revisited," statement before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, March 20, 2013.

[37] "Internet Censorship in Iran," University of Pennsylvania Annenberg School of Communications, Iran Media Program, March 13, 2013.

[38] Joseph Menn and Yeganeh Torbati, "Exclusive: Hackers Accessed Telegram Messaging Accounts in Iran—Researchers," Reuters, August 2, 2016.

aiming to establish an Iranian narrative on issues of primary concern to Iran.[39] The Islamic Republic relies on IO to shape perceptions of the United States in Iraq. The launch of al-Alam coincided with the U.S. invasion in 2003, and Iran's involvement in Iraqi politics is seen as a bulwark against American influence.[40] Still, Iranian efforts in other countries are not always met with success. Reflecting the Arab-Persian divide, Iranian involvement is occasionally construed as meddling. For example, in November 2007, tribal leaders in southern Iraq protested what they perceived as Iranian efforts to destabilize the country.[41]

Key Takeaways

A major line of effort for Iran's IO is influencing Arab opinion throughout the region, which it pursues by broadcasting messages through local media and its own international outlets (including its Arabic-language satellite channel, al-Alam) in support of the mullahs' broader agenda. Iranian messaging has focused on myriad issues, from boilerplate anti-American and anti-Israel themes to support for Hezbollah and the Palestinians.[42]

Capabilities or Practices That the U.S. Army Might Want to Replicate (or Access Through Joint, Interagency, International, or Multinational Efforts)

In terms of C2, although the IRGC maintains a comprehensive IO portfolio, some IRCs have been decentralized and outsourced to actors outside of official government structures. This is obviously a double-edged sword, as Iran loses some control over the message, but at the same time it retains a modicum of plausible deniability and ambiguity in terms of where the operations originate.

Distinctive Features

Iran employs signaling as a form of IO and tends to be more aggressive closer to home. Several incidents are noteworthy. In 2007, Iranian naval forces captured at gunpoint 15 British sailors and marines on a routine mission inspecting merchant ships in Iraqi waters. Iran claimed that the personnel had illegally entered Iranian waters. The incident occurred at the same time Iran was facing immense pressure from the UN

[39] Ali Alfoneh, *Indoctrination of the Revolutionary Guards*, Middle Eastern Outlook No. 2, American Enterprise Institute, February 2009, p. 5.

[40] Alireza Nader, *Iran's Role in Iraq: Room for Cooperation?* Santa Monica, Calif.: RAND Corporation, PE-151-OSD, 2015.

[41] Michael Eisenstadt, Michael Knights, and Ahmed Ali, *Iran's Influence in Iraq: Countering Tehran's Whole-of-Government Approach*, Washington, D.C.: Washington Institute for Near East Policy, Policy Focus No. 111, April 2011, p. 15.

[42] Wehrey, Thaler, et al., 2009, p. xix.

Security Council over its failure to comply with International Atomic Energy Agency inspections.[43]

In January 2016, the Iranian Navy detained ten U.S. sailors after their vessel experienced engine trouble and drifted into Iranian waters. The detainment was videotaped and shown on Iranian state television, with one clip showing an American sailor apologizing for the incident. The seizure occurred just days before the Iran nuclear deal was expected to enter into force, and perhaps it was intended as a face-saving measure or signal that Iran would not subordinate itself to the West.[44]

Takeaways for the U.S. Army

A major takeaway for the U.S. Army is that Iran is using technical IRCs for signaling, opening up the possibility of responding to aggression in different domains. As discussed earlier, Iran's activities are often tied to developments on the domestic front, reinforcing the necessity of monitoring domestic Iranian politics to anticipate a wave or surge in cyberattacks. Iran has begun to make significant investments in capabilities to conduct cyber operations. Like other state actors, Iran uses its cyber capabilities in aggressive ways. Distinctively, it also uses its cyber capabilities for signaling and deterrence more than for true aggression. By letting potential adversaries know some of what it is capable of, Iran hopes to dissuade certain kinds of aggression. Deterrence involves both having punitive capabilities and demonstrating the resolve and willingness to use them. Iran has used technical IRCs in exactly this way.

The ayatollahs have no compunction about employing falsehood or manipulation in messaging targeting the Iranian population. Furthermore, there may be opportunities to counter Iran's narrative that it is a victim of U.S. aggression by highlighting the regime's brutal suppression of opposition figures in its own country, as witnessed during the 2009 Green Revolution and again in early 2018. Along similar lines, Iran has squandered significant blood and treasure in Syria propping up Bashar al-Assad, a brutal dictator guilty of slaughtering his own people. The longer the Syrian civil war rages, the more coffins will return to Iran, leading the population to question the military's involvement in civil war in an Arab country. And most recently, Iran has been fighting a proxy war with Saudi Arabia in Yemen, where it supports the Houthi rebels. Saudi Arabia and its allies allege that Iran has armed the Houthis and, with Hezbollah's assistance, facilitated attacks against Saudi border towns and infrastructure.[45]

Iran is overmatched physically by its principal potential antagonists, which drives it to seek asymmetric advantages. It relies extensively on the use of informational

[43] Mary Jordan and Robin Wright, "Iran Seizes 15 British Seamen," *Washington Post*, March 24, 2007.

[44] Sarah N. Lynch, "U.S. Sailors Captured by Iran Were Held at Gunpoint: U.S. Military," Reuters, January 18, 2016.

[45] Joshua Koontz, "Iran's Growing Casualty Count in Yemen," *War on the Rocks*, June 1, 2017.

combat power in operations short of war, engaging in information warfare and political warfare in addition to more overtly kinetic activities.

Finally, Iran excels in outsourcing, using proxy militias and franchising to extend the reach of its IRCs. The IRGC Quds Force is an elite military unit used by the regime to train proxy forces abroad as a means of propagating Iranian foreign and security policy throughout the Middle East. Iran supports Shia populations and nonstate irregular forces in Iraq, Yemen, Lebanon, Syria, Bahrain, and elsewhere; although Iran often only partially controls these forces, the threat and reality of these proxies have powerful effects in the IE.

CHAPTER EIGHT

Russia

Case Summary

Engaging opponents in the IE is not part of a forgotten Cold War past in Russia; rather, it is a key component of its current foreign *and* domestic policy. The past few years have illustrated the breadth and depth of the Russian information apparatus, which the state has nimbly adapted to the digital age with significant investment in efforts to influence public opinion via the Internet and in foreign countries. Remarking on the capabilities that Russia has built and its willingness to deploy them domestically and internationally, General Philip Breedlove bluntly referred to the country's current efforts in the IE at the 2014 NATO Summit in Wales as "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[1]

Despite its economic woes, Russia has reinforced its military by developing rapid-reaction, highly deployable units and, with that, well-trained information warfare staff and a surrounding infrastructure of state-controlled media, tight controls on information shared with the public, and a brutal strategy of intimidating and silencing its critics.[2] These developments pose significant challenges for the United States and its allies, which have focused on avoiding military confrontation on NATO's Eastern flank and internally limiting the influence of Russia and its proxies among their own populations.

Background and Overview

Russia's information warfare history can be summarized as "adaptation by trial and error."[3] While the notion of subversion campaigns bears resemblance to the Cold War

[1] Peter Pomerantsev, "Russia and the Menace of Unreality: How Vladimir Putin Is Revolutionizing Information Warfare," *The Atlantic*, September 9, 2014.

[2] Andrew E. Kramer, "More of Kremlin's Opponents Are Ending Up Dead," *New York Times*, August 20, 2016.

[3] Keir Giles, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, London: Chatham House, March 2016.

days, Russia's current methods have reached significant levels of sophistication and coordination. As part of its military modernization strategy, Moscow has invested heavily in its civilian and military information capabilities by (1) exercising strong control over media targeting both domestic and foreign audiences; (2) using social networks and the Internet as a "force multiplier"; (3) engaging foreign audiences in their native language, often relying on well-resourced proxies; (4) developing an advanced EW capability; and (5) combining civilian and military capabilities in ways that effectively undermine opponents' defensive measures.[4]

History

Russian academics and policymakers have been deliberating the requirements for prevailing in conflict since the dissolution of the Soviet Union. In the mid- to late 1990s, the notion of integrating the military and other forms of national power to achieve strategic objectives was publicly discussed and later incorporated into Russian military doctrine (a topic we address later in this chapter).[5] Some analysts have gone as far as to argue that in the 1990s, the Russian and U.S. approaches to information warfare were quite similar: Both sought to develop new EW capabilities, advance their C2 systems, transition to the use of digital technology and information management in planning combat operations, and enhancing their capabilities to engage in PSYOP.[6] However, Russia has heavily invested in deception (*maskirovka*) and reflexive control, and it has effectively blended civilian and military resources in pursuit of its desired outcomes.[7] There are other important contextual differences between the Russian and U.S. approaches, chiefly due to the countries' respective socioeconomic contexts after the end of the Cold War.

Post–Cold War Developments

At the end of the Cold War, both the Russian Federation and the United States had similarly sized populations, but per capita income in Russia was lower than in the United States. Russia remained excessively dependent on natural resource exports—primarily oil and gas—and spent up to a quarter of its gross domestic product on its military.[8] In short, economic conditions in Russia continued to stagnate, and many

[4] Giles, 2016; Joe Gould, "Electronic Warfare: What U.S. Army Can Learn from Ukraine," *Defense News*, August 2, 2015.

[5] V. V. Kruglov, "О вооруженной борьбе будущего ["On Future Armed Conflict"]," Военная мысль [*Military Thought*], No. 4, September–October 1998, p. 58.

[6] Timothy L. Thomas, "Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations," *Journal of Slavic Military Studies*, Vol. 11, No. 1, March 1998.

[7] Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies*, Vol. 17, 2004.

[8] Steven M. Efremov, *The Role of Inflation in Soviet History: Prices, Living Standards, and Political Change*, thesis, Johnson City, Tenn.: East Tennessee State University, August 2012.

industries were left struggling in an environment of flourishing corruption, steep inflation, and chaotic privatization. Assistance from the International Monetary Fund and several G7 countries helped stabilize the ruble in 1995, but much-needed government reforms had barely started.[9]

Beyond the economic realm, Russia faced numerous other challenges, including a poorly trained military and a disillusioned populace. As a result, separatist actors saw a unique opportunity to pursue independence from the Russian Federation, and multiple conflicts broke out in its republics, including Dagestan and Chechnya. In addition, conflicts over control in the newly independent republics, such as Georgia, Tajikistan, Moldova, and Ukraine, erupted in the years that followed—and many have been simmering ever since. Table 8.1 lists selected conflicts in which Russia was involved after the dissolution of the Soviet Union, three of which were ongoing as of this writing.

Table 8.1
Selected Post–Cold War Conflicts with Russian Participation

Conflict	Duration
War of Transnistria	1992
East Prigorodny Conflict	1992
War of Dagestan	1999
War of Dagestan	2008
Annexation of Crimea	2014
War in Abkhazia	1991–1993
Georgian civil war	1991–1993
Civil war in Tajikistan	1992–1997
First Chechen War	1994–1996
Second Chechen War	1999–2009
Russo-Georgian War	2008
North Caucasus insurgency	2009 (ongoing)
Tajikistan insurgency	2010–2012
War in Donbass	2014 (ongoing)
Intervention in Syria	2015 (ongoing)

SOURCE: Compiled from various historical sources.

[9] Anders Åslund, "Why Has Russia's Economic Transformation Been So Arduous?" paper prepared for the Annual World Bank Conference on Development Economics, Washington, D.C., April 28–30, 1999; John Odling-Smee, *The IMF and Russia in the 1990s*, Washington, D.C.: International Monetary Fund, 2004. G7 (Group of Seven) countries are Canada, France, Germany, Italy, the United Kingdom, and the United States.

Information Warfare in Modern History

First Impetus for Cyber Capabilities

As a totalitarian state, the Soviet Union was heavily invested in controlling the flow of information, laying the foundation for Russia's highly aggressive operations in the IE in the post–Cold War era. Russia's capabilities first manifested during the second Chechnya war (1999–2009), in which it engaged in strict censoring of the media (aimed at influencing both domestic and foreign audiences) and launched cyberattacks against independent websites reporting on the conflict—an effort summarily described as an "information blockade."[10] Yet, it also experienced a relative setback: Despite Russian military superiority and attempts to control the information sphere, Chechen freedom fighters proved to be surprisingly adept in the use of the Internet, then a new technology. Relatively early in the 21st century, therefore, the Russian Federal Security Service (FSB), successor to the Soviet Committee for State Security (KGB), started developing its cyber capabilities.[11]

Military Modernization

During its war with Georgia (2008), Russia won militarily (the conflict resulted in the expansion of Abkhazia and South Ossetia) but faced stiff international opposition. Despite Russia's diplomatic pressure, the semiautonomous states it supported were recognized by just three countries: Nicaragua, Venezuela, and Nauru.[12] Moreover, the Russian contingent faced considerable resistance from the many-times-smaller Georgian military, exposing the weaknesses of its large but badly equipped and trained military. This hard-won victory provided another impetus for military reform. Since 2008, Russia has invested in better training and equipment for its expeditionary units and has considered forming a force of "information troops."[13] It was thought that this highly trained force would include "hackers, journalists, specialists in strategic communications and psychological operations, and, crucially, linguists to overcome Russia's now perceived language capability deficit."[14] Yet, such a force was ultimately not developed, and the FSB continued to play the key role in information warfare, chiefly by investing heavily in sophisticated cyber capabilities.[15]

[10] Graeme P. Herd, "The 'Counter-Terrorist Operation' in Chechnya: 'Information Warfare' Aspects," *Journal of Slavic Military Studies*, Vol. 13, No. 4, 2000; Giles, 2016.

[11] Giles, 2016.

[12] Ellen Barry, "Abkhazia Is Recognized—by Nauru," *New York Times*, December 15, 2009.

[13] Giles, 2016.

[14] Giles, 2016.

[15] Giles, 2016.

Controlling Domestic Opposition

Another turning point for the Kremlin's approach to the IE happened relatively recently. During the Arab Spring revolutions in the Middle East (2010–2012), Russian elites were surprised by the agility and speed with which protest movements in otherwise tightly controlled regimes were able to change the course of history.

During the protests that followed Putin's 2012 announcement that he would again run for president, Russian security forces employed a number of advanced techniques, including targeted distributed denial-of-service attacks, a mass flooding of the online space by Twitter bots, and other messaging efforts, to discredit Putin's critics.[16] This was supplemented by mass arrests. More than 1,000 people were detained during the protests, including leading opposition figures Alexei Navalny and Boris Nemtsov. Many were held and sentenced on fabricated charges, including Nikolay Kavkazsky, a human rights activist later discharged to house arrest, and Mikhail Kosenko, a critic of Vladimir Putin who was sentenced to indefinite, forced psychiatric treatment, a Soviet-era method for isolating and pressuring dissidents and a cruel violation of international law.[17] The Kremlin's new strategy thus began to materialize: By seamlessly deploying significant control over the information landscape, Russia has been able to prevent its citizens from receiving objective information about protest movements and their underlying motivations, and by deploying crude force and ostensibly intervening in the judicial process, Moscow increased the pressure on those opposing its policies. In the year after Putin's election in 2012, more than 186,000 Russians left the country, and 40,000 applied for asylum elsewhere.[18]

While only some emigration can be linked to government policy, and much of this movement reflects economic realities, analysts agree that the increase in migration after 2009 reflects the tightening of government controls over Russian society and disillusionment associated with Putin's reelection.[19] Figure 8.1 shows the number of people who left the Russian Federation between 2005 and 2014.

Prominent emigrants from recent years include the chess player and political activist Garry Kasparov, economist Sergei Guriev, entrepreneur Pavel Durov, and journalist Leonid Bershidsky.[20]

[16] Giles, 2016.

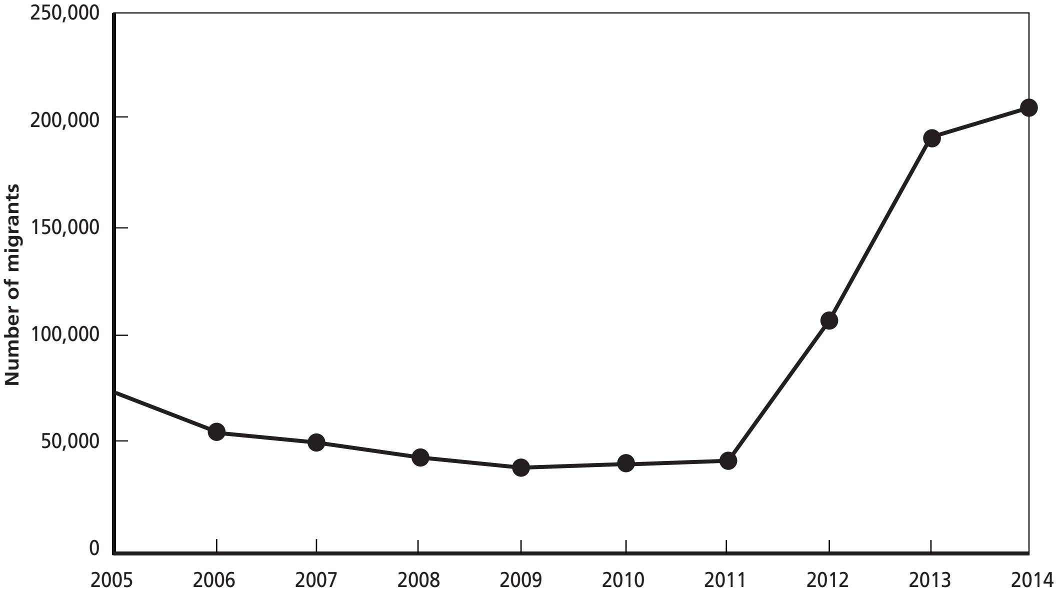
[17] Valeri Stepchenkov, Olga Petrova, and Alissa de Carbonnel, "Mikhail Kosenko, Putin Critic, Sentenced to Detention in Psychiatric Ward," Reuters (*Huffington Post*), updated January 23, 2014; Joshua Yaffa, "The Insanity of Protesting Against Putin," *New Yorker*, October 9, 2013.

[18] Stephen Ennis, "Russia Brain Drain After Putin Crackdown," BBC News, October 2, 2014.

[19] Ksenia Semenova, "A New Emigration: The Best Are Leaving, Part 1," New York: Institute of Modern Russia, April 7, 2015; Robert Coalson, "Twelve Who Left: A New Wave of Russian Emigration," Radio Free Europe/Radio Liberty, May 21, 2015; Ankit Panda, "Russian Emigration Spikes in 2013–2014," *The Diplomat*, July 25, 2014.

[20] Ennis, 2014.

Figure 8.1
Emigration from Russia, 2005–2014



SOURCE: K. Semenova, 2015; Panda, 2014; Migration Policy Centre, *Russia: The Demographic-Economic Framework of Migration, the Legal Framework of Migration, the Socio-Political Framework of Migration*, Florence, Italy, June 2013.
RAND *RR1925z2-8.1*

In an article explaining his departure from the country, Bershidsky wrote,

> I would love to not only see how future events unfold in Russia, but to play a part in them by helping to create a truly free press—the kind that, as in the U.S., would publish the revelations of men like former National Security Administration leaker Edward Snowden.
>
> Now that work has ended for me. That is not to say I accomplished nothing. In fact, some of the media outlets that I had the opportunity to help create remain independent and refuse to compromise to this day.
>
> But overall, my dreams were defeated. Now Russia's mainstream media ranges from the bulging-eyed hyperbole of pro-Kremlin television anchor Dmitry Kiselyov, to the intellectual "we're talking but nobody's watching" Dozhd television programs. That's about it. Those that fall somewhere in the middle are not only uninteresting, but bear no relationship to the media's primary function—namely, to protect the weak from the strong.[21]

[21] Leonid Bershidsky, "No Illusions Left, I'm Leaving Russia," *Moscow Times*, June 18, 2014.

While the crackdown on protestors was rapid and achieved its primary goals, Putin's government further invested in building its capacity to direct or prevent online debate and comment using thousands of new employees stationed in secretive locations around the country and abroad.[22] These new job openings had salary levels significantly higher than those in traditional media—an attempt to draw the more educated Russians into the propaganda apparatus as well.[23]

Targeting Journalists

As part of its strategy, the Kremlin has not shied away from targeting individual journalists: The most prominent critics were exposed to intimidation, interrogation, and censorship, and dozens have been killed, including Anna Politkovskaya (2006), Natalya Estemirova (2009), and Akhmednabi Akhmednabiyev (2013).[24] A *Khimkinskaya Pravda* journalist, Mikhail Beketov, died in 2013, five years after a brutal attack that left him unable to speak and with an amputated leg, ostensibly connected to his investigation of corruption linked to Vladimir Strelchenko, the mayor of Khimki.[25]

According to the New York–based Committee to Protect Journalists, at least 58 journalists covering corruption, business, crime, human rights, politics, conflicts, or culture have been killed in Russia since 1992, with more than half of the murderers never punished.[26] The organization estimates that 36 percent of these murders were sanctioned by military officials, 20 percent by government officials, 17 percent by criminal groups, and the rest by other actors.[27] The vast majority of journalists targeted (69 percent) worked for newspapers and other print publications; 28 percent worked for television stations, and 7 percent worked for online media outlets.[28]

In short, the Kremlin has pursued or sanctioned information and manipulation campaigns against its own people almost as intensively, if not more, as against foreign targets.

Concepts and Principles for Operations in and Through the IE

Given the dual focus of Russian activities in and through the IE—targeting both domestic and foreign audiences—and the loose legal framework within which they

[22] Giles, 2016; Adrian Chen, "The Agency," *New York Times Magazine*, June 2, 2015.

[23] Giles, 2016.

[24] Committee to Protect Journalists, "Journalists Killed in Russia Since 1992," web page, undated.

[25] "Russian Khimki Forest Journalist Mikhail Beketov Dies," BBC News, April 9, 2013.

[26] Committee to Protect Journalists, undated.

[27] Committee to Protect Journalists, undated.

[28] Committee to Protect Journalists, undated.

are conducted, a number of concepts and principles can be seen as crucial for Russia's success:

- willingness to use disinformation or manipulated or outright fabricated information to achieve information security goals
- disregard for domestic and international law in conducting operations of high significance by delegating their execution to government-sponsored proxies
- indirect influence on foreign political developments by financing opposition parties, presidential candidates, and other activists willing to give voice to a pro-Russian agenda (or just sew chaos)
- using multiple sources and circular referencing to flood the IE with false, unverified information and hoaxes to confuse general audiences
- employing strict controls over the IE by censoring state-sponsored media and intimidating independent and foreign journalists
- forcing foreign entities operating in Russia to comply with often-arbitrary regulations to reduce their impact on local populations, particularly in revealing corruption and manipulation in government ranks
- investing heavily in digital media and supporting a highly trained cadre of coders, hackers, and thousands of digital influencers in several target languages (sometimes based abroad).

Russian information concepts include and embrace concepts rarely seen in the West, including propaganda and media censorship, while experimenting with pushing the limits in previously untested areas. For example, Russia used an aggressive disinformation campaign to justify the annexation of Crimea, attempted to sabotage the electoral process in the United States, and has provided financing to pro-Russian political actors across Europe and around the world.

Strategic Goals/Vision

In official statements, the Russian Ministry of Defence outlines four functions of its armed forces:

1. Deterring the military and political threats to the security or interests of the Russian Federation
2. Supporting economic and political interests of the Russian Federation
3. Mounting other-than-war enforcement operations
4. Using military force.[29]

[29] Russian Ministry of Defence, "Mission and Objectives of the Russian Armed Forces," web page, undated(a).

To succeed in these functions, the ministry engages in a number of activities, including "staging and conducting information counter-balancing operations."[30] While this terminology suggests strictly defensive operations in the IE, practical implementation has included activities aimed at undermining the willingness of opponents to fight, coordinating deception with other Russian national security actors, and using economic and geopolitical leverage to shape developments in countries of interest that have not pursued military confrontation with Russia.

Information Security as a Key Component of National Security

In its doctrine (as discussed in the next section), Russia aims to achieve "information security," which is defined as

> security of the individual, society and state from internal and external threats in the information domain that enables the enjoyment of constitutional rights and freedoms by the citizens of Russian Federation, a good quality and standard of life, sovereignty, territorial integrity, a sustainable socio-economic development of the Russian Federation and its defense as well as national security.[31]

In the current geopolitical environment, Russia has been perceived as an unpredictable actor and has openly undermined the territorial and national integrity of Ukraine and Georgia, and it has supported the regime of Bashar al-Assad in the bloody civil war in Syria. Since the decision to abstain from UN Security Council Resolution 1973 allowing NATO's intervention in Libya in 2011, it has pursued an openly confrontational strategy vis-à-vis NATO and its allies and has strengthened both its kinetic and information warfare capabilities. Today, Russian influence is tangible in many social domains in most European countries and North America—ranging from direct financial support to candidates in Italy, France, Germany, the Czech Republic, and elsewhere to various types of political interference in the United Kingdom (Brexit) and the United States (the 2016 presidential election).[32] It has been experimenting with a number of tools in the information domain that have not been countered by the United States or its allies. Moreover, it has pursued its signature strategy, *maskirovka*, by weaponizing information and interfering with the independence of the press by supporting online influencers across the developed world. Finally, Russia has successfully oppressed domestic opposition largely through intimidation, propaganda, and censorship—tools that are often at odds with its own laws.

[30] Russian Ministry of Defence, undated(a).

[31] Security Council of the Russian Federation, "The National Security of Russia," September 26, 2016.

[32] See, for example, Arne Delfs and Henry Meyer, "Putin's Propaganda Machine Is Meddling with European Elections," Bloomberg, April 19, 2016; Dana Priest, Ellen Nakashima, and Tom Hamburger, "U.S. Investigating Potential Covert Russian Plan to Disrupt November Elections," *Washington Post*, September 5, 2016; and Peter Foster and Matthew Holehouse, "Russia Accused of Clandestine Funding of European Parties as U.S. Conducts Major Review of Vladimir Putin's Strategy," *The Telegraph*, January 16, 2016.

Aside from distinct tactical and operational goals, analysts have argued that the overarching Russian military objective has been to undermine the integrity and influence of Western institutions.[33] While the extent of such an effort remains an open question, it is unambiguous that Russian information warfare contributes to effects beyond the specific operational contexts in which capabilities have been deployed.

Tactical Approach of Russian Information Warfare

The relative success of Russian IRCs should not be confused with overall military strength. While Russia has used IO boldly and with little restraint in recent years, its military impasses in Georgia, Ukraine, and now Syria illustrate the broader weaknesses of its armed forces: poor training, ineffective internal communication, inconsistencies in protecting "its own," and largely outdated equipment.[34] With the exception of nuclear warfare, it is unlikely that Russia would enjoy military superiority in a confrontation with an advanced Western adversary. To bridge the capability gap with the West while continuing to achieve its strategic objectives, Russia has resorted to Soviet-era information warfare tactics—blurring the lines between peacetime and war, civilian and military operations, and domestic and foreign audiences.

In 2010, an official from the Central Research Institute of the Russian Ministry of Defence identified three subsystems of network-centric warfare: sensory, informational, and military.[35] The official characterized the components of "information superiority" as intelligence collection enabled by technical means (hardware and software), high levels of IO-related training, and information awareness among the troops.[36]

Table 8.2 lists some of the numerous concepts and terms used to describe IO campaigns that Russia has conducted at home and abroad since the end of the Cold War.

Active Measures

Russia's history of targeting other countries dates to the so-called active measures of the Soviet era: publishing fabricated stories that were intended to spread through routine news channels to millions of readers or viewers—for example, that HIV/AIDS was a U.S. Central Intelligence Agency (CIA) invention. Today, such measures focus heavy on influencing public perceptions but have less of an ideological component than those employed during the Cold War.[37]

[33] Anne Applebaum and Edward Lucas, "The Danger of Russian Disinformation," *Washington Post*, May 6, 2016.

[34] Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*, Washington, D.C.: Institute for the Study of War, September 2015.

[35] Vasily Mikhailovich Burenok, Базис сетецентрических войн—опережение, интеллект, инновации . . . ["The Basis of Network-Centric Warfare Is Proactive, Intelligence, Innovation . . ."], *Independent Newspaper (Russia)*, February 4, 2010.

[36] Burenok, 2010.

[37] MacFarquhar, 2016.

Table 8.2
Selection of Russian IW Concepts and Principles

Concept	Definition	Example	Domestic/Foreign/ Hybrid Use
Active measures	Using false or intentionally misinterpreted information to undermine the opponent's legitimacy or military power; using various forms of political repression to silence critics.	Forging letters about the implications of Sweden's future membership in NATO.	Hybrid
Deception (*maskirovka*)	A complex set of actions meant to deceive the enemy and hide true intentions through surprise, camouflage, deception maneuvers, concealment, use of decoys and dummies, or disinformation.	The appearance of "little green men" in Ukraine despite Russian denials of military involvement in the country.	Foreign
Reflexive control	"Conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[a]	Disseminating information about alleged fascists in Ukraine and would-be benefits for citizens of eastern Ukraine if it became part of Russia.	Hybrid
Propaganda (black, gray, and white)	The use of information in a selective (white), partly true (gray), or outright wrong (black) manner that aims to convince the recipient to take or fail to take certain actions.	Information strategy employed by state-sponsored Russian media at home and abroad when reporting on Russian international engagements.	Hybrid
Censorship	Limiting freedom of expression under certain conditions, enforced either actively (e.g., through physical interruptions to digital connectivity) or through indirect influence (e.g., leading to self-censorship).	Active Russian control of domestic media and the Internet and preventing opposition figures from developing a large following.	Domestic
Intimidation	Influencing individual choices by implicitly threatening retaliation for undesirable choices or using nonlethal force, sham court trials, and other tools to indicate which behaviors are at odds with the interests of the intimidator.	Intrusions into the apartments of foreign journalists based in Moscow.	Domestic

SOURCES: Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *New York Times*, August 28, 2016; Lucy Ash, "How Russia Outfoxes Its Enemies," *BBC News Magazine*, January 29, 2015; Robert C. Rasmussen, "Cutting Through the Fog: Reflexive Control and Russian STRATCOM in Ukraine," Center for International Maritime Security, November 26, 2015; "Russian Spy Agency Targeting Western Diplomats," *The Guardian*, September 23, 2011.

[a] Thomas, 2004.

Such stories have long been a part of Russia's domestic information landscape but have only recently emerged in many Western countries. For example, discussions about potential Swedish accession to NATO have triggered a flood of pro-Russian publications in Sweden, mostly containing untrue or heavily manipulated information about the nature of NATO membership.[38] In addition to misleading narratives, forgery has been a component of pro-Russian agents, who fabricated a letter from the Swedish Ministry of Defense instructing a Swedish firm to sell weapons to Ukraine.[39]

Russian propaganda—partly executed by independent actors but largely authorized and sanctioned by the highest echelons of the administration—now targets both foreign elites and regular citizens abroad alike, aiming to make any objective assessment of a situation as difficult as possible and coordinated resistance to Russian intentions unlikely.

Deception (Maskirovka)

Cold War–era Soviet doctrine taught MILDEC as a basic principle of warfare of all types. *Maskirovka* is "designed to conceal" Russian troops, equipment, and intentions "from enemy intelligence and to mislead [the enemy] regarding the location, amount, and composition of forces and the actions and intentions of the troops."[40] Through a wide variety of methods, Russia can lull an enemy to reduce its defenses or cause it to overreact. In the words of Timothy L. Thomas, a senior analyst in the U.S. Army's Foreign Military Studies Office, "Military deception . . . can be achieved through disinformation, demonstration, simulation, or deformation. The latter is the deliberate distortion of a facility, material, or weapons."[41]

Reflexive Control

Another basic tenet of Russian military planning is the concept of reflexive control, or presenting information with the purpose of eliciting a desired behavior and controlling an enemy's decisionmaking.[42] An example of strategic reflexive control is displaying in a military parade intercontinental ballistic missiles that appear larger than normal, causing an enemy to invest heavily in countermeasures against a fake threat. In the information realm, reflexive control may include "camouflage (at all levels), disinformation, encouragement, blackmail by force, and the compromising of various officials and officers."[43]

Russian information warfare writings devote a great deal of attention to securing Russia's own information. This is a kind of deception: The use of defensive phrasing is often a euphemism for offensive operations.[44]

[38] MacFarquhar, 2016.

[39] MacFarquhar, 2016.

[40] Timothy L. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness*, Fort Leavenworth, Kan.: U.S. Army Foreign Military Studies Office, 2011, p. 109.

[41] Thomas, 2011, p. 117.

[42] Thomas, 2011, p. 118.

[43] Thomas, 2011, p. 124.

[44] Jolanta Darczewska, *The Anatomy of Russian Information Warfare: The Crimean Operation, a Case Study*, Warsaw, Poland: Centre for Eastern Studies, May 2014.

Thresholds

It has become apparent that certain observable conditions must be met before there is a collective or bureaucratic decision that Russia will respond with force. Below this threshold, no action will be taken, ensuring impunity of Russian actions against an adversary's interests.[45]

Faced with the fog of war, a dearth of information, Russian disinformation, and overwhelming propaganda, friendly-force commanders may feel that they do not have enough information to act, or they may not trust the information and the sources they do have.

Gerasimov Doctrine

Russian information warfare is constantly evolving, and a stated goal is to "informatize" the country's armed forces. As President Dmitry Medvedev has made clear, "today's computer is a weapon, which is of no smaller importance than a rifle or a tank."[46]

The Gerasimov Doctrine has been widely misinterpreted as advocating "hybrid warfare," and it was applied to Crimea and Donbass in the recent conflict in Ukraine. In light of Russia's goal to informatize its military, it is obvious that General Valery Gerasimov has pursued a multifaceted approach to warfare with informational dimensions.[47]

In Ukraine, a combination of military, intelligence, and information-related operations has been essential to achieving Russian strategic goals in Crimea and undermining the integrity of governance in the eastern parts of Ukraine.

While Gerasimov did not specifically mention the cyber aspects of the battle, hackers have been part of the conflict. Indeed, the conflict in Ukraine was one of the first manifestations of a highly sophisticated form of information war. In addition to cyberattacks and deception, Russia employed a number of tools to support its objectives, ranging from propaganda to suppressing media reporting, hiring trolls, and strictly controlling the information flow in and out of the contested area.

Doctrine: 2000 as a Turning Point

After Vladimir Putin's designation (and later election) as the president of Russia in 2000, the government adopted several key documents that would inform its future approach IO—chiefly, the National Security Concept and the Information Security

[45] Andrew Monaghan, "Putin's Way of War: The 'War' in Russia's 'Hybrid Warfare,'" *Parameters*, Vol. 45, No. 4, Winter 2015–2016.

[46] Thomas, 2011, p. 304.

[47] Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows*, July 6, 2014.

Doctrine of the Russian Federation.[48] We discuss the importance of each in the following section.

National Security Concept of 2000

In his first national security concept, Putin's administration highlighted several components of information security. First, the concept notes the importance of "economic, political, science and technological, environmental and information factors" in the "global transformation" and defines national interests in the "information sphere" as

> observance of its citizens' constitutional rights and freedoms to receive and make use of information, . . . the development of modern telecommunication technologies, and . . . protecting the state's information resources from unsanctioned access.[49]

Moreover, it was relatively explicit about the nature of the threats the country was likely to face in the information domain:

> There is an increasing threat to national security in the information sphere. The striving of a number of countries to dominate the global information space and oust Russia from the external and internal information market poses a serious danger, as do the elaboration by a number of states of a *concept of information wars that envisages creation of means of dangerous influence on the information spheres of other countries of the world*; disruption of the normal functioning of information and telecommunication systems and of storage reliability for information resources; and gaining of unsanctioned access to them.[50]

More specifically, despite not being involved in a direct confrontation with NATO (in fact, the NATO-Russia Council was founded 2002 to foster mutual relations and improve information exchange), Russia named NATO as an entity of concern, likely due to its involvement in military operations in the Balkans:

> NATO's shift to the practice of using military force outside its zone of responsibility and without UN Security Council authorization is fraught with the danger of destabilizing the entire strategic situation in the world.[51]

Highlighting the importance of information security in ensuring national security, the concept proposed the following strategy:

[48] Russian Ministry of Foreign Affairs, "National Security Concept of the Russian Federation," decree of the President of the Russian Federation No. 24, January 10, 2000.

[49] Russian Ministry of Foreign Affairs, 2000.

[50] Russian Ministry of Foreign Affairs, 2000. Emphasis added.

[51] Russian Ministry of Foreign Affairs, 2000.

> The major tasks in ensuring the information security of the Russian Federation are:
>
> - realization of the constitutional rights and freedoms of the citizens of the Russian Federation in the sphere of information activities;
> - improvement and protection of the national information infrastructure and the integration of Russia into the world information space;
> - *counteraction against the threat of rivalry in the information sphere*.
>
> Effective use and all-round development of *intelligence and counterintelligence capabilities* with a view to the timely detection of threats and determination of their sources has a special significance for ensuring the national security of the Russian Federation.[52]

And while the concept did not provide specific reasons, it also noted possible threats to Russia's "cultural, spiritual and moral legacy, historical traditions and the norms of social life" and justified government's involvement in regulating the domestic information space—essentially laying the foundation for the censorship later observed in the country and the use of the Russian language as a tool to gain dominance over Russian-speaking populations outside the Russian Federation.

> Ensuring the national security of the Russian Federation also includes protection of the cultural, spiritual and moral legacy, historical traditions and the norms of social life, the preservation of the cultural wealth of all the peoples of Russia, the formation of government policy in the field of the spiritual and moral education of the population, and the imposition of a *ban on use of air time* in electronic mass media for distribution of programs *propagandizing violence and exploiting low instincts*, along with counteraction against the negative influence of *foreign religious organizations and missionaries*.
>
> The spiritual renewal of society is impossible without the preservation of the role of the Russian language as a factor of the *spiritual unity of the peoples of multinational Russia* and as the language of *interstate communication between the peoples of the member states of the Commonwealth of Independent States*.[53]

Information Security Doctrine of 2000 and 2016

In September 2000, just six months after his election as president, Vladimir Putin signed the nation's first information security doctrine. At its outset, it noted the "increasing role of the information sphere" and consisted of four components, as shown in Table 8.3.[54]

[52] Russian Ministry of Foreign Affairs, 2000. Emphasis added.

[53] Russian Ministry of Foreign Affairs, 2000. Emphasis added.

[54] Russian Federation, 2000.

Table 8.3
Components of Russian Information Security Defined in 2000

Component	Definition	Threats (examples)
Constitutional rights and freedoms of man and the citizen	"Observance of the constitutional rights and freedoms of man and the citizen to receive and use information, the assurance of a spiritual renewal of Russia, and the preservation and reinforcement of the moral values of society, traditions of patriotism and humanism and the cultural and scientific potential of the country."	• Monopolies on forming, receiving, and disseminating information within Russia through the use of telecommunication systems or other means • Irrational, excessive restrictions on access to socially necessary information • Information manipulation (e.g., disinformation, information concealment and distortion)
Information support for the state policy of the Russian Federation	"Information support for the state policy of the Russian Federation that involves conveying to the Russian and international public trustworthy information about the state policy of the Russian Federation and about its official position on socially significant events in Russian and international life, with the provision of access for citizens to open government information resources."	• Monopolization of individual sectors or all of the Russian information market by domestic and foreign entities • Blocking activities of state media in providing information to Russian and foreign audiences
National information industry	"Promoting modern information technologies, boosting the national information industry (the industries of informatization, telecommunication, and communication facilities in particular), securing the satisfaction of domestic market requirements with its products, and their entry into the world market, and providing for accumulation, storage reliability, and effective utilization of national information resources."	• Government purchases of imported means of informatization, telecommunication, and communication when domestic analogues are available and not inferior • Ousting Russian producers of informatization, telecommunication, and communication technologies from the domestic market • An increase in the outflow of specialists and intellectual property rights holders going abroad
Security of information and telecommunication systems and facilities	"Protecting information resources against unsanctioned access, and securing the information and telecommunication systems whether already deployed or being set up on the territory of Russia."	• Illegal information gathering and use • Discrediting of cryptographic information-protection keys and means • Use of uncertified domestic and foreign information technologies, information-protection means and informatization, and telecommunication and communication facilities in setting up and developing the Russian information infrastructure

SOURCE: Russian Federation, *Information Security Doctrine of The Russian Federation*, September 9, 2000.

In its definition of information security components, the doctrine also named more than 40 specific threats Russia faces in the information domain, a sampling of which are shown in the table. The doctrine also distinguished between internal and external threats to Russia's information security. Examples of Russia's perceived external threats included political, economic, military, and intelligence activities by foreign countries directed against Russian interests, with a particular focus on these countries' technology investments and strategies in the information domain.[55] Perceived internal threats addressed in the doctrine included organized crime, coordination among government agencies for the purposes of developing and implementing a unified national information strategy, an insufficiently developed legal and regulatory system for activities in the information domain, and insufficient state control of the Russian "information market."[56]

There were few surprises in Russia's 2000 information security doctrine, but developments since it was issued have clearly undermined the principles it set out. For example, as we discuss later in this chapter, the Russian government has implemented laws that constrict rather than expand the provision of "objective information to the population about socially significant events of public life," and, by exercising control over state-owned media, the Kremlin has effectively exposed the Russian society to (rather than protected it from) the "distorted and untrustworthy information" it warned against in the 2000 doctrine.[57]

Interestingly, the doctrine included a number of information security goals, one of which was "prohibiting the development, spread and use of the 'information weapon.'"[58] This is perhaps the most striking contradiction to actual Russian IO strategy that followed the adoption of this document. Finally, the doctrine was generally defensive and omitted, for example, the state's role in the cyber domain.

An updated version of Russia's information security doctrine that was released in 2016 reflected a significant shift in Russian thinking over a period of a decade and a half.[59] Although Russia retains its focus on defensive activities and continues to perceive many of the same internal and external threats to its national interests and security in the information domain as it did in 2000, the 2016 doctrine describes "a trend among foreign media to publish an increasing number of materials containing biased assessments of State policy of the Russian Federation." It also states that "Russian mass media often face blatant discrimination abroad, and Russian journalists are prevented

[55] Russian Federation, 2000, p. 7.

[56] Russian Federation, 2000, pp. 7–8.

[57] Russian Federation, 2000, p. 27.

[58] Russian Federation, 2000, p. 25.

[59] Russian Federation, *Doctrine of Information Security of the Russian Federation*, December 5, 2016.

from performing their professional duties."[60] As we discuss later in this chapter, the shift since 2000 in how Russia uses both mass and social media to disseminate pro-Russian messages and misinformation abroad has prompted international backlash that allows the Russian government to act the part of a victim when its state-sponsored media outlets are accused of disseminating propaganda.

Military Doctrine of 2010

In February 2010, Russia adopted a new military doctrine, codifying insights from Georgia (2008) and the cyberattacks against Estonia that were likely conducted by non–state-sponsored Russian actors.[61] The document contains multiple references to information warfare, including statements that "the intensification of the role of information warfare" is a likely feature of future military conflicts and that information warfare is likely to be conducted both "without the utilization of military force and, subsequently, in the interest of shaping a favourable response from the world community to the utilization of military force."[62] It tasked the military with developing forces and resources to conduct information warfare and mandated the creation of an "information field" within the military, in addition to investing heavily in technology and IT systems:

> The tasks of equipping the Armed Forces and other troops with armaments and military and specialized equipment are . . . :
>
> d) to improve the quality of means of information exchange on the basis of the use of up-to-date technologies and international standards, as well as the single information field of the Armed Forces and other troops as part of the Russian Federation's information space; . . .
> g) to create basic information management systems and integrate them with the systems for command and control of weapons and the automation systems of command and control organs at the strategic, operational-strategic, operational, operational-tactical, and tactical levels.[63]

Some have argued that the lack of a state-level cyber capability during the 2007 Estonia hacking and the 2008 campaign in Georgia prompted Moscow to invest in tools that allow it to pursue operations that are more advanced than the previous "unsophisticated distributed denial-of-service attacks against government, media, and

[60] Russian Federation, 2016.

[61] Azhar Unwala and Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict," *Military Cyber Affairs*, Vol. 1. No. 1, Article 7, 2015.

[62] Russian Federation, *The Military Doctrine of the Russian Federation*, February 5, 2010.

[63] Russian Federation, 2010.

financial websites [which] generated little lasting damage with limited payoff."[64] In the case of Georgia, a lack of coordination led to indiscriminate attacks targeting American websites, potentially leading to unintended escalation, and allowed Georgia to rebuild its digital infrastructure very quickly in the aftermath.[65]

Notably, the doctrine of 2010 actively uses the phrase *information warfare*, in contrast to the predominant use of *information security* and *information operations* in earlier doctrinal publications.

A 2011 report by the Russian Ministry of Defence specified some high-level notions about activities in the information space:

- Military conflict in the information space is a form of *interstate or intrastate conflicts* with the use of information weapons.
- Armed Forces cyberspace activities imply the *use of military information* resources to solve defense and security problems.
- Information Security of the Armed Forces is the security of the information resources of the Armed Forces against the attack using the *information weapons*.
- Information War is the confrontation between *two or more states* in the information space with the purpose of *inflicting damage* to information systems, processes and resources, critical and other structures, *undermining the political, economic and social systems, a massive psychological manipulation of the population* to destabilize the state and society, as well as *coercion of the state* to take decisions for the benefit of the opposing force.
- Information infrastructure is a combination of technical tools and systems of formation, creation, transformation, transmission, usage and storage of information.
- *Information weapons are comprised of information technologies, means and methods* used to conduct the information warfare.
- Information space includes a scope of activities associated with the formation, creation, transformation, transmission, usage, storage of information which influences the individual and community awareness, information infrastructure and information itself.
- Information resources make up the information infrastructure, as well as information itself and information flows.
- Crisis situation is a stage of conflict escalation characterized by the use of military force to resolve it.
- International information security is a state of international relations that excludes the violation of global stability and buildup of a security threat to nations and the international community in the information space.

[64] Unwala and Ghori, 2015.

[65] Unwala and Ghori, 2015.

- *Information security management system of the Russian Federation is an element of the national security system* of this country intended for the implementation of state policy in the sphere of information security.[66]

Military Doctrine of 2014

The most recent military doctrine, published in 2014, describes a trend that Russia sees as changing its security environment:

> There is a tendency towards shifting the military risks and military threats to the information space and the internal sphere of the Russian Federation. At the same time, despite the fact that unleashing of a large-scale war against the Russian Federation becomes less probable, in a number of areas the military risks encountered by the Russian Federation are increasing.[67]

Among the perceived threats are "information and communication technologies . . . aimed against sovereignty, political independence, territorial integrity of states and posing threat to the international peace, security, global and regional stability." In section 13, the new doctrine describes several internal threats related to the information domain:

> a) activities aimed at changing by force the constitutional system of the Russian Federation; *destabilizing domestic political and social situation in the country*; disrupting the functioning of state administration bodies, important state and military facilities, and information infrastructure of the Russian Federation. . . .
>
> c) *subversive information activities* against the population, especially young citizens of the State, aimed at undermining historical, spiritual and patriotic traditions related to the defense of the Motherland.[68]

It also describes modern conflicts as integrating "military force and political, economic, informational or other non-military measures implemented with a wide use of the protest potential of the population and of special operations forces."[69]

Targets and Audiences

Domestic

The Russian elite has used sophisticated methods to undermine domestic political opposition by intimidating journalists (as we describe later), staging political trials with

[66] Russian Ministry of Defence, "Russian Federation Armed Forces' Information Space Activities Concept," web page, undated(b). Emphasis added.

[67] Russian Federation, *The Military Doctrine of the Russian Federation*, December 25, 2014.

[68] Russian Federation 2014. Emphasis added.

[69] Russian Federation, 2014.

activists and businesspeople, and leveraging control of the media landscape to censor information.

Russian domestic audiences rely mostly on television and newspapers for information about politics and current events. There are three state television stations (Rossiya, Pervyj Kanal, and NTV) covering the vast majority of Russian territory and audiences, and two newspapers control the print market (*Komsomolskaya Pravda* and *Rossiyskaya Gazeta*), both of which have indirect or direct ties to the Russian government.[70] State control of key media, together with the significant roadblocks hindering the development of independent outlets and opposition parties, has effectively marginalized any unofficial sources of information for the Russian public.

Foreign

With respect to foreign audiences, Russia's information strategy has differed by country. It is now thought that pro-Russian proxies conduct a large part of these activities, including disseminating propaganda and flooding the information space, with financial and political support but without direct guidance from Moscow.

Among the prime targets are—to varying degrees—NATO and EU countries, other leading democracies (Switzerland, Australia, and Japan), and populations in areas of military interest (such as Georgia, Ukraine, and Syria).

In advanced democracies, Russia has taken advantage of the emergence of extremist parties on the political left and right alike.[71] In countries of interest, moreover, it has engaged in massive propaganda campaigns and supported foreign political leaders sympathetic to Russian interests (in the United Kingdom, Czech Republic, France, Italy, and Germany), including those advocating for Brexit. Russia has even been suspected of sponsoring highly sophisticated cyberattacks against the Democratic National Committee in the United States.[72] In one extreme case, Russia's foreign minister publicly chastised Germany for welcoming refugees and immigrants over a rape accusation that had already been debunked.[73]

In its information campaign aimed at foreign audiences, Russia has been very careful to take into account historical, cultural, language, and religious factors, particularly

[70] Natalya Krasnoboka, *Russia*, Maastricht, Netherlands: European Journalism Centre, undated.

[71] MacFarquhar, 2016.

[72] In the Czech Republic alone, around 40 pro-Russian websites have been spreading rumors and propaganda, and some have been as popular as other mainstream media. See, for example, Jakub Janda and Veronika Víchová, *Fungování českých dezinformačních webů* [*The Function of Czech Disinformation Sites*], Prague: Evropske Hodnoty, July 26, 2016. For more on large-scale Russian propaganda campaigns conducted internationally, see MacFarquhar, 2016, and Czech Security Information Service, *Annual Report of the Security Information Service for 2015*, Prague, January 9, 2016. On the vulnerability of the U.S. election system, see Geoff Dyer, "FT Explainer: Can the U.S. Election Be Hacked?" *Financial Times*, August 30, 2016.

[73] MacFarquhar, 2016.

in Europe. (Paying close attention, for example, to what resonates in the former East Germany, which may not be persuasive or appealing to western German populations).

Increasingly, Russia has been targeting foreign organizations, including human rights organizations, activists, and other sources of potentially compromising information. In an August 2016 incident, an Armenian political analyst was banned from entering Russia until 2030 on the grounds of having taken part "in activities of international organizations that are not desired to be present on the Russian territory."[74]

Russian Diaspora

The large Russian diaspora remains an important target of the Russian information campaign. Through the state-funded RT television station, ethnic Russians in the United States (about 2.6 million), Germany (0.5 million), and other countries are exposed to pro-Russia messages.[75] Russian speakers and co-ethnics represent potentially fertile ground for Russian propaganda and create the possibility of an artificially aggrieved minority as a theme in that propaganda.

Russian Information Warfare Organization

Details on the structure, organization, and location of information warfare capabilities within the Russian military are not publicly available. Analysis of exercises involving Russian units (after the military modernization was initiated, first focusing on airborne troops, then the armed forces broadly) identified the likely composition of a standard Russian motorized rifle brigade, the military's most common formation, which included a communication battalion, a reconnaissance company, and a radio-EW company.[76]

During the war in Georgia in 2008, Russia deployed two reconnaissance special task force regiments, believed to support information warfare functions and consisting of highly trained special operations forces—one in South Ossetia, one in Abkhazia.[77]

In the next section, we describe the functions of high-level bodies that contribute to the development, oversight, and execution of IO capabilities in the Russian Federation.

[74] Radio Free Europe/Radio Liberty, "Russia Refuses Entry to Armenian Political Analyst," September 1, 2016.

[75] Angela Brittingham and G. Patricia de la Cruz, *Ancestry: 2000, Census 2000 Brief*, Washington, D.C.: U.S. Census Bureau, June 2004; Russia Beyond the Headlines and Russia Today, "Über das Verhältnis von Russen und Deutschen" [On the Relationship Between the Russians and Germans"], *Deutschland und Russland*, April 4, 2012.

[76] Dmitry Boltenkov, Aleksey Gayday, Anton Karnaukhov, Anton Lavrov, and Vyacheslav Tseluiko, eds., *Russia's New Army*, Moscow: Centre for Analysis of Strategies and Technologies, 2011.

[77] Boltenkov et al., 2011.

Authorities

Russia's 2016 information security doctrine described the key actors involved in protecting national information security:

- Russian policymaking and regulatory bodies, such as the Council of the Russian Federal Assembly, the State Duma, the Security Council of the Russian Federation, federal executive agencies, the Central Bank of the Russian Federation, the Military-Industrial Commission, the judiciary, and interagency and local-level entities involved with information security.[78]
- Nongovernmental entities, such as media outlets and the communications industry, financial institutions, companies that develop information security technologies, and organizations that educate the public in information security.

With this number of actors, coordination of information activities remains a challenge in Russia and happens through a number of avenues, such as the Russian Security Council at the highest level and the provincial executive bodies at the regional level.

One of the best-resourced agencies within the government is the FSB, with 66,000 uniformed personnel, 4,000 armed special forces, and more than 160,000 border troops; it is also headed by vital members of the Security Council.[79] Although the FSB focuses predominantly on domestic security (leaving the area of espionage to the 10,000- to 15,000-strong Foreign Intelligence Service),[80] it has absorbed some of the capabilities of the former Federal Agency of Government Communications and Information (the Russian equivalent of the U.S. National Security Agency), and it uses advanced information gathering and dissemination techniques.

Several journalists, activists, and diplomats operating in Russia have reported on the FSB's "campaign of intimidation," which has included break-ins, harassment of embassy staff, email hacks, obvious phone bugging, and other scare tactics aimed at shortening the duration of their stay in the country.[81] The strategies now employed by the FSB were well-documented in the days of its predecessor agency, the KGB.[82]

Supporting/Coordinating Russian Organizations

Russian information warfare efforts would not be possible without the active support of all other parts of the government.

[78] Russian Federation, 2016.

[79] Richard Sakwa, *Russian Politics and Society*, 4th ed., New York: Routledge, 2008, p. 98.

[80] Sakwa, 2008, p. 98.

[81] "Russian Spy Agency Targeting Western Diplomats," 2011; Luke Harding, "Enemy of the State: How Luke Harding Became the Reporter Russia Hated," *The Guardian*, September 23, 2011.

[82] Harding, 2011.

Intelligence

Russian intelligence is split between operational and analytic elements. Russian operatives can conduct covert, clandestine, and overt activities in support of national intelligence efforts. In the Soviet era, *active measures* were a key part of information warfare against the West and included supporting (or undermining) political movements abroad, fostering mistrust in government among foreign populations, and propagating hoaxes and other disinformation campaigns. There is no reason to believe that these activities have not continued.

The preponderance of reporting maintains that the FSB is in charge of Russian information warfare efforts, although at this time it cannot be proven from open sources, nor does Russia acknowledge it.[83] Media reports indicate that Putin adviser Vladislav Surkov is also involved in directing these activities and played a particularly important role in Russian operations in Ukraine in 2014.[84]

Military

During Russian operations in Donbass, it was revealed that the military incursion into Ukraine was not as successful as an observer might expect. Front-line, elite military forces were used only in extraordinarily surgical applications, and the vast majority of forces were "volunteers," locals, mercenaries, and Russian soldiers "on vacation." Consequently, there were miscues, stalled actions, and ineffectual operations. When success was mandatory, professional Russian soldiers backed up, augmented, and occasionally replaced the Russian proxy troops. Even then, the Russian regular soldiers were not particularly successful, and they experienced approximately five casualties for every lost Ukrainian soldier. The Russian military in Crimea also relied on naval infantry forces from the Black Sea Fleet already docked in Crimea, along with Spetsnaz, FSB, Foreign Intelligence Service, and Main Intelligence Directorate personnel.

Legal Apparatus

Russia supports warfare using legal resources; this is commonly called lawfare.[85] For example, in 2015, Russia attempted to reopen a legal case against Lithuanians who had refused to complete their Soviet military service after Lithuania declared independence in 1990. Although the Lithuanian government refused to cooperate with the request, it did advise those targeted not to travel to Russia or other countries where they could be detained on the charges.[86]

[83] Catherine A. Fitzpatrick, "Russia This Week: Here Comes the Kremlin's Troll Army (2–7 June)," *The Interpreter*, June 6, 2014; Alexander S. Martin, "FSB's Snowden War: Using the American NSA Against Itself," *Modern Diplomacy*, May 24, 2016.

[84] Anton Zverev, "Ex-Rebel Leaders Detail Role Played by Putin Aide in East Ukraine," Reuters, May 11, 2017.

[85] "About Lawfare: A Brief History of the Term and the Site," *Lawfare Blog*, undated.

[86] "Lithuania Says Russia Reopens Soviet Conscript Cases," BBC News, September 8, 2014.

Russia also threatened legal action against Ukraine on at least two occasions. First, it challenged the legality of Ukraine's independence from the Soviet Union, though this dispute was eventually resolved through treaties specifying the disposal of Soviet weapons and other military equipment based in Ukraine, as well as Ukraine's continued economic dependence on Russia. The second challenge is ongoing, with Russia forcing Ukraine to pay several billion dollars owed for Russian natural gas.

Russian Security Council

The initial plan for the invasion of Crimea was developed during an all-night session of the council on February 22, 2014, the night Ukraine's ousted president, Viktor Yanukovych, fled the country. In this and other operations, Russian information warfare is dependent on the approval of the Russian Security Council.

Observers outside of Russia have published numerous accounts of the disinformation that characterizes Russian media messaging.[87] Russia uses the alternative reality promoted through propaganda to justify its actions in the political-military realm. A significant component of this justification is skewing statements from Western governments to be seen as a provocation so that Russia may defend itself from Western aggression.

Funding

The Russian propaganda apparatus is very well funded. The state-run news agency Rossiya Segodnya is the overall media lead and is responsible for organizing much of the Russian government's propaganda efforts.[88] In 2014, Rossiya Segodnya dissolved the government funded but editorially independent international news agency RIA Novosti and launched Sputnik News in its place. Sputnik operates radio stations and websites in several languages and has emerged as an important tool in the spread of misinformation, conspiracy theories, and propaganda.[89]

Propaganda is one of the basic instruments of Russian information warfare, blocking opposing influences and leaving governments and legitimate media outlets struggling to correct mistruths that propagate at the speed of social media. The Russian propaganda apparatus achieves its desired outcomes through a few basic principles:[90]

[87] Pomerantsev, 2014.

[88] Although *Rossiya Segodnya* translates to *Russia Today*, it is completely separate from the international Russian television network RT, which was formerly known as Russia Today.

[89] Lizzie Dearden, "NATO Accuses Sputnik News of Distributing Misinformation as Part of 'Kremlin Propaganda Machine,'" *The Independent*, February 11, 2017.

[90] Darczewska, 2014.

- ongoing promotion of themes and memes, such as *banderivtsi* propaganda, to discredit Ukrainians opposed to Russian policies on Crimea[91]
- spreading so-called core information, such as that Russia will protect the rights of Russians and Russian-speaking people and that the Russian language has been banned by foreign governments
- fomenting emotional agitation, leading the target audience to act without much thought—even irrationally
- emphasizing clarity and simplicity, with simple messages, black-and-white terms, and loaded keywords, such as *Russophobe*
- creating an illusion of obviousness, through which repeated terms become so commonplace that they are associated with false stories.

These tools are most useful in influencing domestic audiences; Russia's leadership understands that preventing a color revolution is of the utmost importance. An audience external to Russia is secondary but still a target of Russian information campaigns that incorporate these principles.

Russian propaganda has changed significantly since the Soviet era. Quality control, simplicity, consistency, and believability are no longer top priorities.[92] Being the first to publish is now most important. The idea is no longer to convince people of the evil of the West. Rather, it is to plant small examples of the West's descent into chaos and depravity. These stories are used to undermine the West, especially NATO and the EU, whenever possible. For example, a common Russian propaganda theme is to say the CIA is proficient and has mastered brainwashing using the Internet.[93]

Blurring of Civilian and Military Lines

The flagships of Russian state-controlled media are *Rossiyskaya Gazeta*, Rossiya Segodnya, RT, and Sputnik News. The government's official outlet is *Rossiyskaya Gazeta*, the government-owned daily newspaper of record which publishes in print and online the official decrees, statements, and documents of state bodies.

These media outlets operate from within Russia's borders, although RT and Sputnik News have regional bureaus around the world (including in Washington, D.C.). Many of the websites operated by the Russian state-run media apparatus have .ru extensions, but some use .com.

[91] *Banderivtsi* is a pejorative Russian expression that references Ukrainian political activist Stepan Bandera, a pivotal character in the historical Ukrainian independence and nationalist movements.

[92] Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016.

[93] Igor Panarin, "Вторая мировая информационная война. Как в ней победить России?" ["The Second World Information War: Can Russia Win?"], *KM Online*, September.28, 2015.

State-Controlled Media

In the Soviet Union, the news organization Novosti headed up the state's propaganda machine.[94] Novosti continued to be financed by the state but developed into an award-winning international media outlet, RIA Novosti, with the dissolution of the Soviet Union. In 2013, RIA Novosti once again fell under state control when Rossiya Segodnya was established by presidential decree.

Pro-Russian Proxy Media

Pro-Russian proxy media outlets are usually located outside Russia but carry at least a small number of Russian stories. Content from these websites is frequently cited by Russian trolls who carry messages to social media and the comments sections of legitimate news articles. Many of the sites, such as Media Lens and InfoWars, specialize in challenging mainstream news organizations' coverage of current events.

Some pro-Russian proxy websites are also known for publishing wholly fabricated stories, stories based on only a kernel of truth, and stories with a strong bias in favor of Russia or that undermine the West.[95]

Russian and Pro-Russian Trolls

A fairly new and unique part of the Russian information war is the use of paid and patriotic trolls.[96] A 2015 *New York Times* article probed the shadowy network of trolls and hoax propagators, reporting on "industrialized" trolling operations in St. Petersburg, Russia, where approximately 400 staff churned out blog posts, comments, and social media content 24 hours a day from a nondescript office building.[97] The organization behind the operation, Internet Research Agency, is funded by Yevgeny Prigozhin, a restaurateur with close informal ties to Putin's inner circle.

The disruptive effects of pro-Russian trolls have been enormous. Fabricated disasters have left government officials and legitimate media outlets struggling to correct the record. At one point in early 2014, the Guardian's website fielded almost 40,000 comments per day on anything it posted that was remotely related to Russia or Ukraine.[98]

In March of that year, investigators obtained a *temniki*, or guidance sheet for pro-Russian trolls, bots, and proxy outlets, that served as evidence of central Russian infor-

[94] Alexei Baranovsky, "The Information War over the Conflict in South Ossetia: The Analysis and Conclusions," osetinfo.ru, November 11, 2008.

[95] For a list of suspected pro-Russian proxy outlets, see Joel Harding, "Russian News, Russian Proxy News Sites and Conspiracy Theory Sites," *To Inform Is to Influence*, November 15, 2015.

[96] Chris Elliot, "The Readers' Editor on . . . Pro-Russia Trolling Below the Line on Ukraine Stories," *The Guardian*, May 4, 2014.

[97] Chen, 2015.

[98] Fitzpatrick, 2014.

mation control.[99] It was later discovered that Alexandr Dugin, a Russian information warfare philosopher, wrote the initial guidance for the trolls.[100]

Cyberwarfare

Part of the reason Russia did not engage in cyberwarfare in the lead-up to its annexation of Crimea was the short period between initial planning and the actual launch of the invasion. With the operation planned in one overnight meeting between President Putin and the Russian Security Council on February 22, 2014, there was insufficient time to test Ukraine's networks in preparation for a sophisticated cyber exploit or mount an effective cyberattack.[101]

After the initial phase, however, the cyberattacks did not rise beyond harassment—mostly distributed denial-of-service attacks.[102] Later attacks were leveled against the Ukraine power grid in 2016, and zero-day exploits have targeted both Ukraine and NATO without major consequences. The electrical grid attacks were exacerbated by simultaneous attacks against Ukraine's telecommunication network, mostly telephone lines, which increased the effectiveness of the attack against the electrical grid.

After Russian cyberattacks against Estonia in 2007, potential targets appear better prepared every year. For example, Ukraine benefited from the support of NATO's Cooperative Cyber Defense Centre of Excellence, established as a result of the 2007 attacks. Immediately after the initial invasion of Crimea, the center quickly came to Ukraine's aid.

Information Operations in Practice

Conflict in Ukraine

After the fall of Ukrainian President Yanukovych in February 2014, Russia sent soldiers without insignias to the country to help secure the annexation of the Crimean Peninsula. Concurrently, pro-Russian protests broke out in eastern Ukraine, chiefly in the Donetsk and Luhansk oblasts. There, heavy military engagement by Russian forces led to the deaths of more than 6,000 soldiers and civilians between April 2014

[99] Kevin Rothrock, "'Anonymous International' Leaks Kremlin's Instructions to Russian TV," Global Voices, March 28, 2014.

[100] Darczewska, 2014. The document was titled *The Rules of Polemics with the Internal Enemy*.

[101] "Putin Reveals Secrets of Russia's Crimea Takeover Plot," BBC News, March 9, 2015.

[102] Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression Against Ukraine*, Talinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

and April 2015.[103] The region, however, has a longer history of Russian engagement, some of which has included operations in the information domain. Moreover, Russia has employed sophisticated IO against Western countries with the goal of deterring them from providing assistance to Ukraine, acting militarily, or implementing costly measures against Russian interests. Nonetheless, Russia has achieved many of its objectives in the region—halting the pro-European movement in Ukraine, undermining NATO's unity, and deepening instability in Europe—despite displays of Western support and cooperation on Ukraine. As a result, the Russian engagement in the country, starting shortly after the failed Orange Revolution in 2004, may serve as a vital case study to understand its strategy in the information domain and its integration of the IO with kinetic and other means.

Setting the Stage

Since the Orange Revolution, Russia has continually increased its pressure on Ukrainian authorities, leading to President Yanukovych's November 2013 decision to halt talks on Ukraine's future accession to the European Union. As a result, more than 100,000 people protested in Kiev, demanding Yanukovych's resignation, but police took control of the situation.[104] Russian pressure was not just political, however. Russian hackers used Snake malware to access Ukrainian government and diplomatic systems as early as 2010. Alongside other tools, particularly interruptions to Ukraine's gas supply, campaigns to undermine Ukraine's government have helped Russia gain leverage with both political elites and the broader populace.[105] Between 2009 and 2014, Russia expanded its cyber espionage operations, using Sandworm malware to target EU and NATO institutions, an effort that intensified before and during the conflict in Ukraine in 2014.[106]

By winter 2013–2014, the protest movement in Ukraine had grown, with around 800,000 people rallying in Kiev in December. In response, Putin offered Yanukovych assistance with debt restructuring and reduced the contractual price of oil by about a third.[107] Nonetheless, protests continued in Donetsk, Luhansk, and Kiev, and Ukrainian Prime Minister Mykola Azarov resigned in late January 2014. The peak of the violence occurred in February 2014, when at least 88 people died in just two days. It was Ukraine's worst bout of violence since World War II.[108]

[103] United Nations Office for the Coordination of Humanitarian Affairs, *Ukraine*, Situation Report No. 34, April 3, 2015.

[104] Oksana Grytsenko, "Ukrainian Protesters Flood Kiev After President Pulls Out of EU Deal," *The Guardian*, November 24, 2013.

[105] Sam Jones, "Ukraine: Russia's New Art of War," *Financial Times*, August 28, 2014.

[106] Unwala and Ghori, 2015.

[107] "Ukraine Crisis: Timeline," BBC News, November 13, 2014.

[108] "Ukraine Crisis: Timeline," 2014.

Yanukovych fled the country again shortly after failed negotiations with opposition leaders, and Ukraine's parliament adopted a number of highly controversial measures, including renouncing Russian as a second official language—though it later retracted this decision—and disbanding the Berkut police unit that was responsible for some of the crackdowns on protestors.[109] Within two days of Olexandr Turchynov's appointment as interim president, however, pro-Russian gunmen took control of key positions in Simferopol, the capital of Crimea, including its airport.[110]

Before the Military Incursion

The Russian information campaign against Ukraine was heavily focused on collecting information about potential Ukrainian responses to Russian actions by means of espionage, specifically targeting the "computers and networks of journalists in Ukraine, as well as Ukrainian, NATO, and EU officials."[111] These activities were enabled by the Russian origins and sometimes even ownership of Ukrainian telecommunication networks, including VimpelCom and Vodafone Ukraine, even disseminating chilling messages to participants in anti-Russian demonstrations, saying, "Dear subscriber, you are registered as a participant in a mass disturbance."[112] Vodafone Ukraine itself was reported to have more than 22 million subscribers in the country, allowing pro-Russian forces to effectively target a large part of the population.[113] Similarly, Russia targeted the phones of the members of Ukraine's parliament, and recordings of phone conversations between American diplomats were later released by unidentified sources.[114] Yet, the phone companies denied any involvement, blaming "pirate base-stations" for disseminating anti-protest messages.[115] Analysts have suggested that for such coordinated and massive engagement of anti-Russian groups, foreign intelligence agencies must have been involved, pointing to the FSB.[116]

During the Military Incursion

On March 1, 2014, the Russian parliament approved President Putin's request to use force in Ukraine "to protect Russian interests." A referendum on Crimea's secession

[109] "Ukraine Crisis: Timeline," 2014.

[110] "Ukraine Crisis: Timeline," 2014.

[111] Unwala and Ghori, 2015.

[112] Andrew E. Kramer, "Ukraine's Opposition Says Government Stirs Violence," *New York Times*, January 21, 2014.

[113] Patrick Tucker, "Why Ukraine Has Already Lost the Cyberwar, Too," *Defense One*, April 28, 2014.

[114] Pavel Polityuk and Jim Finkle, "Ukraine Says Communications Hit, MPs Phones Blocked," Reuters, March 4, 2014.

[115] Heather Murphy, "Ominous Text Message Sent to Protesters in Kiev Sends Chills Around the Internet," *New York Times*, January 22, 2014.

[116] Unwala and Ghori, 2015.

took place just two weeks later, with Putin formally accepting the accession of Crimea to Russia on March 18, 2016.[117] Over the next few weeks, pro-Russian protests erupted in other Russian-speaking regions of Ukraine, with epicenters in Donetsk, Luhansk, and Kharkiv. Ukraine's acting president, Olexandr Turchynov, formally launched military operations against the separatists in the east in April 2014 but did not prevent the separatists in Donetsk and Luhansk from declaring independence on May 11.

Military clashes continued throughout the summer and included the downing of a Malaysian passenger airliner, MH17, over pro-Russian territory on July 17, 2014, which killed all 298 people onboard.[118] While this event ultimately led to an agreement on new sanctions against Russia in late-July, the Russian government tried to weaken European and U.S. unity by promulgating false hypotheses on the causes of the tragedy.

On August 26, Ukraine released videos of captured Russian paratroopers, officially documenting Russian military involvement in the country. Despite the September peace agreement signed in Minsk and a retreat of Russian troops from close to Ukraine's borders, NATO documented Russian tanks, artillery, air defense systems, and combat troops crossing into Ukraine in early November 2014. (The Russian Ministry of Defence denied sending any troops to eastern Ukraine.) It was also suspected that Russia deployed "nuclear-capable weapons to Crimea."[119]

The pro-Russian cyber campaign increased in intensity after the annexation of Crimea: Cyber Berkut, a group of Ukraine-based pro-Russian hackers, executed distributed denial-of-service attacks against Ukrainian and NATO websites and communications between Ukraine and the United States.[120] Given the relatively low level of sophistication of these attacks, it is not likely that they were part of the Russian military apparatus.[121]

Lessons Learned from the Conflict

In the ongoing Russia-Ukraine conflict, Russia's effective use of multiple types of IO has allowed it to quickly create a fog of war. Although they were often not compatible, the plethora of narratives disseminated by pro-Russian actors essentially "poisoned the well" before an objective investigation could be conducted.[122] The United States and its allies must be prepared for such a strategy and have plans in place to deter such operations. Article 5 of the Washington Treaty is no longer sufficient if "little green men" enter a NATO country without any response from the alliance.

[117] "Ukraine Crisis: Timeline," 2014.

[118] "Ukraine Crisis: Timeline," 2014.

[119] "Ukraine Crisis: Russian Troops Crossed Border, NATO Says," BBC News, November 12, 2014.

[120] Unwala and Ghori, 2015.

[121] Unwala and Ghori, 2015.

[122] Paul and Matthews, 2016.

Russia's post-Crimea strategy has been characterized by expanded goals. Rather than focusing on the single issue of the territorial integrity of Ukraine, Russia has pursued a greater objective: questioning the post–Cold War status quo.[123] It has been well documented in investigations that followed the conflict that Russia's use of multiple levers to achieve strategic uncertainty and cast doubts on Western moral integrity was effective in undermining NATO's willingness to provide lethal support to Ukraine.

The strategy used by Russian operatives—including the ministers of foreign affairs and defense—consisted mostly of rejecting objective information (such as the incursion of Russian soldiers into Crimea or Donbass) and creating an environment of uncertainty in which the regime could achieve its operational goals.[124]

Response to Information Operations in Practice

While many Russian efforts in and through the IE are not coordinated from one center, the information gathered by intelligence agencies is often used to inform the Kremlin's military and information strategy. This points to a weakness that many countries in the West have not overcome: how to respond to low-intensity, nonkinetic engagement of a nuclear power in an era of borderless IT and high levels of dependence on critical infrastructure that is vulnerable to digital attack. In other words, despite Western cumulative superiority to Russia's military capabilities, Russia's approach has leveraged the unquestionable strength of the Putin regime and a willingness to break domestic and international laws and blur lines between civilian and military engagements in ways that the West cannot emulate.

Effectiveness of Russian Information Warfare

As we have observed, Russian information warfare has been successful in several previous conflicts and is thought to have enabled a "winning" strategy, as in the country's annexation of Crimea. Russia has excelled in exercising strong control over official messaging and public relations announcements (often disseminated by the Presidential Executive Office or by other senior officials and supported by pro-government media). It also has a strong influence capability and is willing to openly interfere in the domestic affairs of other countries—for example, leveraging political frictions and pro-Russian sentiments in several European countries and pursuing advanced deception and manipulation strategies. As discussed earlier, Russia has some of the most advanced technological tools to jam military communications and radio broadcasting, and it has

[123] Jones, 2014.

[124] Margarita Jaitner, "Russian Information Warfare: Lessons from Ukraine," in Geers, 2015.

invested heavily in cyberattack capabilities (both within and outside of government agencies). It also exhibits a moderately strong OPSEC capability (though a reliance on poorly trained personnel often undermines its operations security), and it has successfully integrated its IO capability with its maneuver and fire units, particularly for intelligence collection and analysis.[125] Finally, Russia is deft at engaging proxies and other allies, often in foreign territory,[126] and it has been extremely proficient in monitoring and communicating via social media.

Despite Russia's investments in the information space, a 2015 Pew Research Center survey found that the country's standing had largely weakened around the world.[127] The majority of populations surveyed in developed countries perceived Russia more negatively than positively (with the least positive views held by Poles, Jordanians, Germans, French, Americans, Italians, and Ukrainians), while the areas with the highest level of support for Russia included Vietnam, China, and Ghana (more than 50 percent in each).[128] In all parts of the world, Russia was seen less positively than the United States. [129]

Nonetheless, Russia has achieved strategic and tactical victories in recent years, many of which can be attributed to effective IO drawing on advanced human psychology research.[130] In Ukraine, for instance, Russia was able to not only confuse its adversary and prevent the international community from forging a military coalition against the Russian proxies behind the annexation of Crimea, but it also expanded "the spectrum of Russian exit strategies from the conflict."[131] Given an absence of an official military conflict, moreover, the burden to prove the links between combatants and the Russian government fell to the Ukrainian government and its allies. Russia was able to reinforce its strategy through engagement in many Western countries. As a result, the willingness of NATO or individual countries to stand up to Russia militarily has been extremely low. This may be partly explained by the level of sophistication and decentralization employed by pro-Russian actors, as well as their mastery of human psychology.[132]

[125] Consider the use of social networks by Russian soldiers who were secretely deployed in Ukraine.

[126] Consider Russian support for the Assad regime in the ongoing conflict in Syria or its support for pro-Russian rebels in eastern Ukraine.

[127] Bruce Stokes, "Russia, Putin Held in Low Regard Around the World," Washington, D.C.: Pew Research Center, August 5, 2015.

[128] B. Stokes, 2015.

[129] B. Stokes, 2015.

[130] Snegovaya, 2015; Paul and Matthews, 2016.

[131] Snegovaya, 2015.

[132] Paul and Matthews, 2016.

In the United States, viewership of the RT channel has increased to more than 2.8 million people per week, and the estimated viewership for all of Europe is just about a million people (about 0.2 percent of the population).[133]

The success of Russian media abroad should not be the only indicator of Russia's effectiveness in IO: The growth of pro-Russian populist parties across Europe has been seen as a risk that can grow into a significant opportunity to further weaken European unity and willingness to stand up for its eastern neighbors.

Efforts to Counter Russian Information Warfare

In Ukraine, the government has countered Russian influence by blocking access to Russian television channels, reducing the otherwise virtually captive audience by half, to just about 9 percent of the population.[134] In Western countries, such as Germany, the effect has been rather tempered: RT Germany and Sputnik News have not gained a massive following, and many of their supporters likely held pro-Russian views even before the start of the information campaign.

In most advanced countries, investigative reports on Russian propaganda, cyberattacks, and other operations, have undermined the effectiveness of these campaigns and generated evidence of the risks they pose.

Russia seems not to have been deterred by economic sanctions and these other setbacks. If anything, it has redirected significant resources to information warfare in its many forms.

Lessons from Russian Operations in and Through the IE

While adapting to new realities will take more than a few months, the United States can take active steps to strengthen its ability to fight Russian IO, but it should also support its NATO allies and others in building such a capability in the midst of the highest tensions seen since the end of the Cold War. Given the characteristics of Russian information warfare, several lessons emerge.

State-Sanctioned Deception

Russia has not shied away from using misinformation, manipulation, and propaganda both at home and abroad. It has effectively blurred the lines between law enforcement, intelligence, and the armed forces. Its winning strategy is largely based on attempts to tailor messages to specific characteristics of the target audience, yet it has also deployed

[133] Snegovaya, 2015.

[134] Snegovaya, 2015.

a "firehose of falsehood" approach, particularly in situations of high urgency (such as the downing of MH17). The United States can address both the targeting and dissemination of untrue information by supporting investigative, democratic media and building trust between the national security community and the public. While this approach is likely to take years and will require a steadfast commitment to disseminating objective, evidence-based information, it could pay dividends in the future.

Violations of the Law

Russian disregard for domestic and international law poses new, unforeseen challenges, particularly as Putin tests the thresholds for Western response and uses operations in the IE to build opposition to any decisive response from the West. While the current regime poses a threat to the international system, it has only limited international support—largely in other nondemocratic nations—and it is not likely to change the character of the international order unless it succeeds in undermining Western unity and NATO's willingness to fight for its members.

Reliance on Proxies

Russian use of proxies and other means of influencing foreign political developments is a particular source of concern in most Western countries, however. From elections in Kiev to elections in the United States, Russian actions have been well calibrated, highly professional, and timed to achieve the maximum impact favoring pro-Russian interests. The government's willingness to resort to such actions is a source of concern, especially at a time when Russian oligarchs maintain tight connections to many European and American elites and are able to leverage them to undermine the democratic process in other countries. Only limited resources have been devoted to investigating and countering such operations in many NATO countries, resulting in a significant risk to these countries' democratic processes in the coming years.

Countering Russian Narratives with Reliable Evidence

Russian proxies and the many other voices that support Russia's narrative have been particularly effective while allowing the government to avoid directly engaging domestic or foreign actors. While investigations of such schemes are likely to take many years, effectively countering these operations will require cooperation between investigators and law enforcement—and these efforts should begin as soon as possible, receive appropriate resources, and be conducted by highly capable personnel.

The Role of Independent, Reliable Information in Fighting Propaganda

Domestic controls on media and information dissemination are not new in Russia, but they have affected the ability of the West to reach audiences in the country. As a result, the majority of Russians—particularly those who live outside of major cities—have heard different interpretations of developments in Ukraine, Georgia, Syria, and elsewhere, making support for the regime stronger than it would be otherwise. The West may not be able to counter censorship that is used for national security purposes, but it should support Russian-language alternatives in news and entertainment that are not controlled by the Kremlin. Moreover, it should consider measures against websites that are based abroad and target foreign audiences with rumors, conspiracies, and misinformation. Support for political prisoners and journalists standing trial in Russia should leverage the collective diplomatic, economic, and moral power of NATO countries. Investigations of local or national-level corruption, money laundering (including billions of dollars laundered through Switzerland and the United Kingdom), and organized crime must receive the best available support from government and nonprofit organizations alike, and the results should inform policymaking in the most advanced countries. Trading with entities tied to Russian oligarchs should be limited or completely abandoned.

Leveraging the Cyber Domain and Additional Tools to Counter Attacks

Cyberattacks against Western interests are also not new in Russia, but their intensity and strategic goals indicate that Russia and pro-Russian actors have built a strong cyber capability worldwide. Russian IO often succeed only if they permit access to compromising information. Greater transparency and effectively fighting domestic corruption may be the best way to avoid the conditions that give power to such material. Nonetheless, the West must build a new capability to counter Russian information aggression in the same range of languages used to disseminate Russian messages. There is also a pressing need for additional research to clarify the specific dynamics of Russian information warfare in the military and civilian domains alike.

Key Takeaways

Russian efforts in and through the IE have been distinct from those employed by most other state actors. Ranging from civilian to military measures, their success has relied not on a high degree of coordination but, rather, on a firehose of falsehood aimed at foreign audiences, alongside broad-ranging censorship and disinformation vis-à-vis domestic audiences. Given its willingness to violate domestic and international law—while preserving a clout of indifference and even victimhood—Russia has leveraged its historical experience with *maskirovka* and applied it to the modern age. Having invested in both EW and the hiring of thousands of online trolls, it has illustrated its ability to quickly take control of both developments on the ground and the broader narrative that featured most prominently in the Ukraine conflict.

The United States and its allies will likely face new threats from Russian information warfare in the future. From using its cyber capabilities to undermine elections and spreading false information about its engagement abroad to conducting cyberattacks against high-level targets, Russia's focus abroad has largely been on developing strategic uncertainty about its national security interests and its means of achieving them. As a result, it has built the means to deter NATO adversaries with more-advanced conventional military capabilities, and it has avoided large-scale military confrontations with countries on its periphery.

The response necessary from the West will be manifold, including vigorous support for independent media at home and abroad, strengthening NATO members' commitment to Article 5 of the Washington Treaty, investigating Russian oligarchs based abroad who use foreign institutions to launder money, countering Russian narratives through traditional and digital channels, and building stronger capabilities to defend Western interests in the cyber domain and with respect to EW. As a willing adversary that is capable of attacking foreign interests with no advance notice and with immense sophistication, Russia poses a significant threat to U.S. interests around the globe.

More so than perhaps any other country, including the United States, Russia recognizes and has embraced the importance of allocating resources to operations in and through the IE. The United States has already been compelled to dedicate more resources to countering Russian influence, but it should not assume a strictly defensive posture. There are several important steps that the United States can adopt that will help blunt the effectiveness of Russian information activities in and through the IE, including forewarning audiences of misinformation, or merely reaching them first with the truth, rather than retracting or refuting false "facts." It should also prioritize efforts to counter the effects of Russian propaganda and focus on guiding the propaganda's target audience in more productive directions. Other options include competing with Russian propaganda, working to prevent Russia from dominating the IE, and, finally, increasing the flow of information that diminishes the effectiveness of propaganda while, in the context of active hostilities, attacking the means of dissemination.[135] Perhaps most important, because Russian disinformation is a global threat and much of it targets democracies, the U.S. government should step up collaboration with other like-minded governments to counter the onslaught. U.S. concerns gain credence and reinforcement when others also express them.[136]

[135] Paul and Matthews, 2016.

[136] Christopher Paul and William Courtney, "Russian Propaganda Is Pervasive, and America Is Behind the Power Curve in Countering It," *U.S. News and World Report*, September 12, 2016.

CHAPTER NINE

Hezbollah

Case Summary

Hezbollah is a Shia terrorist organization based in Lebanon and supported by Iran that has been active since the early 1980s. Over the past several decades, Hezbollah has professionalized its military and developed a comprehensive appreciation of the value of effects in and through the IE. Hezbollah's IRCs have narrowed the divide between what was once a parochial militia and the region's most powerful military, the IDF. Among violent nonstate actors, Hezbollah is certainly the first group to truly appreciate the importance of an "information-first" operational mindset, which has undoubtedly contributed to its longevity and tactical success. Hezbollah is important for the U.S. Army to consider because it is an example of what violent nonstate actors can achieve in the IE by investing substantial resources in media, propaganda, and the integration of IRCs into a broader defense architecture.

Background and Overview

Literally translated as "the Party of God," Hezbollah was formed in the midst of an internecine civil war that would wreak havoc in Lebanon for 15 years, ending only in 1990.[1] The group emerged from the extremely complex patchwork of ethnic and religious groups in Lebanon and draws its support almost exclusively from Shia communities in the country's capital city, Beirut, and its environs, southern Lebanon, the Bekka Valley, and the Hirmil region.[2] Similar to other insurgent movements throughout the Middle East, Hezbollah receives support and is influenced by powerful actors in

[1] We use this particular transliteration—Hezbollah—throughout this discussion. Note that there are other common transliterations, including Hizbullah, Hezballah, Hisbollah, and Hizb Allah. For a detailed discussion of the Lebanese civil war, see Dilip Hiro, *Lebanon Fire and Embers: A History of the Lebanese Civil War*, New York: St. Martin's Press, 1992; Marwan George Rowayheb, "Political Change and the Outbreak of Civil War: The Case of Lebanon," *Civil Wars*, Vol. 13, No. 4, 2011; and Walid Khalidi, *Conflict and Violence in Lebanon: Confrontation in the Middle East*, Cambridge, Mass.: Harvard University, Center for International Affairs, 1979.

[2] Augustus Richard Norton, *Hezbollah: A Short History*, Princeton, N.J.: Princeton University Press, 2007, p. 6.

the region, including Syria and Iran, with the latter being the "principal moving force" behind the group's creation.[3]

Concepts and Principles for Operations in and Through the IE

More than any other nonstate actor, Hezbollah appreciates the importance of IO and treats operations in the IE as a warfighting function.[4] Hezbollah operates by the mantra, "If you haven't captured it on film, you haven't fought."[5] The group has grasped the importance of documenting its successes from a very early stage. Indeed, in late 1994, Hezbollah fighters and a cameraman infiltrated an Israeli military compound in Lebanon and raised a flag inside the base, capturing the event on film and scoring a significant propaganda coup. Overall, Hezbollah's IO portfolio relies on a broad-based platform that includes newspapers, social media outlets, and television programming. Hezbollah operates summer camps for children and boasts a robust public works program in the areas under its control. In essence, many of Hezbollah's activities connect directly to its recruitment efforts and allow the group to maintain political legitimacy and high levels of popular support for its agenda.

Strategic Goals/Vision

Hezbollah's main goal since its founding has been to expel Israel from Lebanese territory. It achieved this goal in 2000. When the Israelis unilaterally withdrew from Lebanon, there was a major discussion within the highest ranks of Hezbollah about which way to steer the organization. Would the group turn inward to focus on the Lebanese state and attempt to tackle issues of corruption and domestic politics? Or would it maintain its "resistance posture" in Lebanon and the Middle East while presenting itself as the most viable option to defend the Lebanese people? While the group did assume a more direct role in the Lebanese political system, the lion's share of its efforts continued to be devoted to waging a campaign of guerrilla warfare against Israel, even though the 18-year IDF occupation had ended.[6] Over the years, Hezbollah has demonstrated the priority it gives the IE by promoting its leader, Hassan Nasrallah, through various media platforms, as we discuss later in this chapter.

[3] Kenneth M. Pollack, *The Persian Puzzle: The Conflict Between Iran and America*, New York: Random House, 2004, p. 201.

[4] Caldwell, Murphy, and Menning, 2009, p. 4. A warfighting function is a group of tasks or systems (people, organizations, information, and processes) united by a common purpose that commanders use to accomplish missions or objectives.

[5] Ron Schleifer, "Psychological Operations: A New Variation on an Age Old Art: Hezbollah Versus Israel," *Studies in Conflict and Terrorism*, Vol. 29, No. 1, 2006, p. 6.

[6] Norton, 2007, p. 90.

How Operations in and Through the IE Fit with Hezbollah's Overall Strategic Goals

Hezbollah propaganda is well honed, targeted, and specific, with such themes as resistance ideology, martyrdom, and legitimacy through the provision of social services.[7] The group's leadership has long understood that it would need support beyond its immediate Shia constituency. As such, Hezbollah has used its information efforts to promote itself as a much more inclusive organization, marked by flexibility and adaptability in its ideology. In this way, it has expanded its base of operations and garnered support throughout Lebanon among Christians and Sunnis. In the words of Frederic Wehrey, during its fight against Israel in South Lebanon, Hezbollah waged "psychological campaign of persuasion, communication, and the shaping of perception."[8]

Targets and Audiences

Hezbollah's target audiences include populations within Lebanon and, specifically, southern Beirut, as well as the "enemy audience" in Israel and neutral parties—in Lebanon, Israel, and the wider region—who have not made up their minds about the Lebanese militia.[9] During the 18-year conflict with Israel in southern Lebanon, Hezbollah also directed its propaganda against the South Lebanon Army (SLA), a proxy Christian-Shia militia group.[10] In targeting each audience, Hezbollah has carefully crafted themes and messages to appeal to their respective demographics. For example, messages targeting Hezbollah's home audience often include such words and phrases as *unity*, *Jerusalem*, *the justice of our path*, *the long struggle*, *demonizing*, and *God's will.*

Unity as a theme reflects Hezbollah's attempt to widen its constituency, broadening its appeal to all Lebanese (e.g., Christian, Sunni, Druze). Evoking *Jerusalem* is an attempt to use the Israeli-Palestinian conflict to mobilize Muslims throughout the Middle East, as Jerusalem maintains religious significance to many Muslims. *The justice of our path* plays to such themes as defeating infidels and the righteousness of Hezbollah's cause. *The long struggle* refers to Hezbollah's willingness to sustain losses and fight a war of attrition. *Demonizing* is Hezbollah's method of framing Israel through apocalyptic religious terms, highlighting the hardline Zionist beliefs of the Jewish state. Finally, the phrase *God's will* reinforces the notion that the ongoing battle

[7] Frederic Wehrey, "A Clash of Wills: Hezballah's Psychological Campaign Against Israel in South Lebanon," *Small Wars and Insurgencies*, Vol. 13, No. 3, 2002.

[8] Wehrey, 2001, p. 54.

[9] Schleifer, 2006, pp. 6–10.

[10] Augustus Richard Norton, "Hizballah and the Israeli Withdrawal from Southern Lebanon," *Journal of Palestine Studies*, Vol. 30, No. 1, Autumn, 2000, p. 23. For a detailed analysis of the SLA, see Austin G. Long, Stephanie Pezard, Bryce Loidolt, and Todd Helmus, *Locals Rule: Historical Lessons for Creating Local Defense Forces for Afghanistan and Beyond*, Santa Monica, Calif.: RAND Corporation, MG-1232-CFSOCC-A, 2012, pp. 107–130.

between Hezbollah and Israel is predetermined and part of a broader religious struggle predicted by the Quran and Islamic prophets throughout history.[11]

Messages directed toward enemy audiences are crafted around entirely different themes, marked by such key terms as *determination*, *futility*, *a well-defined political aim*, and *guilt* (*the long struggle* also makes appearances in these messages), with secondary messages like *getting bogged down in the Lebanese quagmire*. *Determination* is an attempt to intimidate Israel with messages stressing Hezbollah's indefatigability, as evidenced by the death of Nasrallah's son in battle and promises of an endless supply of suicide bombers. *Futility* denotes an attempt to convince the IDF that Israeli military action in Lebanon is ineffective and that the blood and treasure spilled in Lebanon will never result in a positive outcome for Israel. *A well-defined political aim*, a consistent Hezbollah message, was used to target Israelis who wanted the IDF to withdraw from Lebanon, impressing upon that segment of society that doing so would help bring an end to the Jewish state's suffering. *Guilt*, an admittedly more complex emotion to manufacture through IO, sought to tug on the heartstrings of Israelis through images of dead Lebanese civilians and stories about vast human rights abuses. With martyrdom central to Hezbollah's ideology, *the long struggle*, as directed toward the enemy, reinforces the notion of a decades-long conflict—something antithetical to Israel's democracy, which is more responsive to the writ of its citizens.[12]

Finally, messages directed toward "neutrals" have focused on issues like human rights.[13] The range of themes allows Hezbollah to target multiple demographics within Israel, from policymakers and the military to civilians and the general public.

Foundational Principles

Recall that Hezbollah's foundational operational principle is, "If you haven't captured it on film, you haven't fought." Hezbollah seeks to fight guerrilla warfare psychologically, with casualties and attacks filmed and disseminated as a force multiplier. The group's operational principles and its principles for operating in and through the IE are one in the same. In other words, kinetic operations and the provision of social services are not just two more IRCs to the group's members. For Hezbollah, the concept of IO is interwoven with its military planning and conceived of as a force multiplier. For some insurgent groups (and indeed some nation-states), it is taken for granted or treated as an afterthought. But for the Party of God, these operations have long been considered indispensable to its asymmetric capabilities more broadly.

[11] Schleifer, 2006, pp. 10–11.

[12] Schleifer, 2006, pp. 11–12.

[13] Schleifer, 2006, p. 13.

History and Evolution

A major source of Hezbollah's politico-military success stems from its prioritization of information effects, which the group considers integral to its operations. Thus, it earmarks the resources necessary to keep its IRCs current. Hezbollah has the resources to pursue top-end capabilities dedicated to IO, and it is continuously seeking to upgrade these capabilities, evolve, and adapt. Hezbollah is a learning organization, and this evolution extends to IO. Starting in 1991, Hezbollah's television station, al-Manar (*the Beacon*), began trying to influence Israeli public opinion by broadcasting actual battlefield footage that showed Israeli soldiers being killed and maimed.[14] Hezbollah combat units, known as the Islamic Resistance, use violence as a psychological tool to wear down the morale of the IDF and the Israeli public in a deliberate attempt "to get into every [Israeli's] mind and affect Israeli public opinion." Within five years, al-Manar's Hebrew Observation Department was monitoring Israeli radio and television broadcasts around the clock.[15] After the destruction of Hezbollah territory in southern Lebanon, the group erected billboards on the rubble of buildings that said, "Made in the USA," in English. It is crucial to note that through al-Manar, Hezbollah is not just pushing messages but responding to events as they unfold. Al-Manar is not merely a Lebanese phenomenon. Rather, its popularity has facilitated its growth into one of the leading news organizations of the Arab world.

Hezbollah's Organization for Operations in the IE

Structure

As shown in Figure 9.1, Hezbollah's information unit falls directly under its executive council and garners the same notoriety as other critical organizational units, including finance and external relations. That it is so prominent in the group's organizational structure is further evidence of how important Hezbollah considers information and media affairs to its overall performance, from both a military and political perspective.

Funding

Al-Manar broadcasts worldwide via satellite and runs on an annual budget of roughly $15 million.[16] Most of its 40 reporting staff (as of the early 2000s) are former Hezbollah fighters.[17] The Lebanese government conferred al-Manar with official licen-

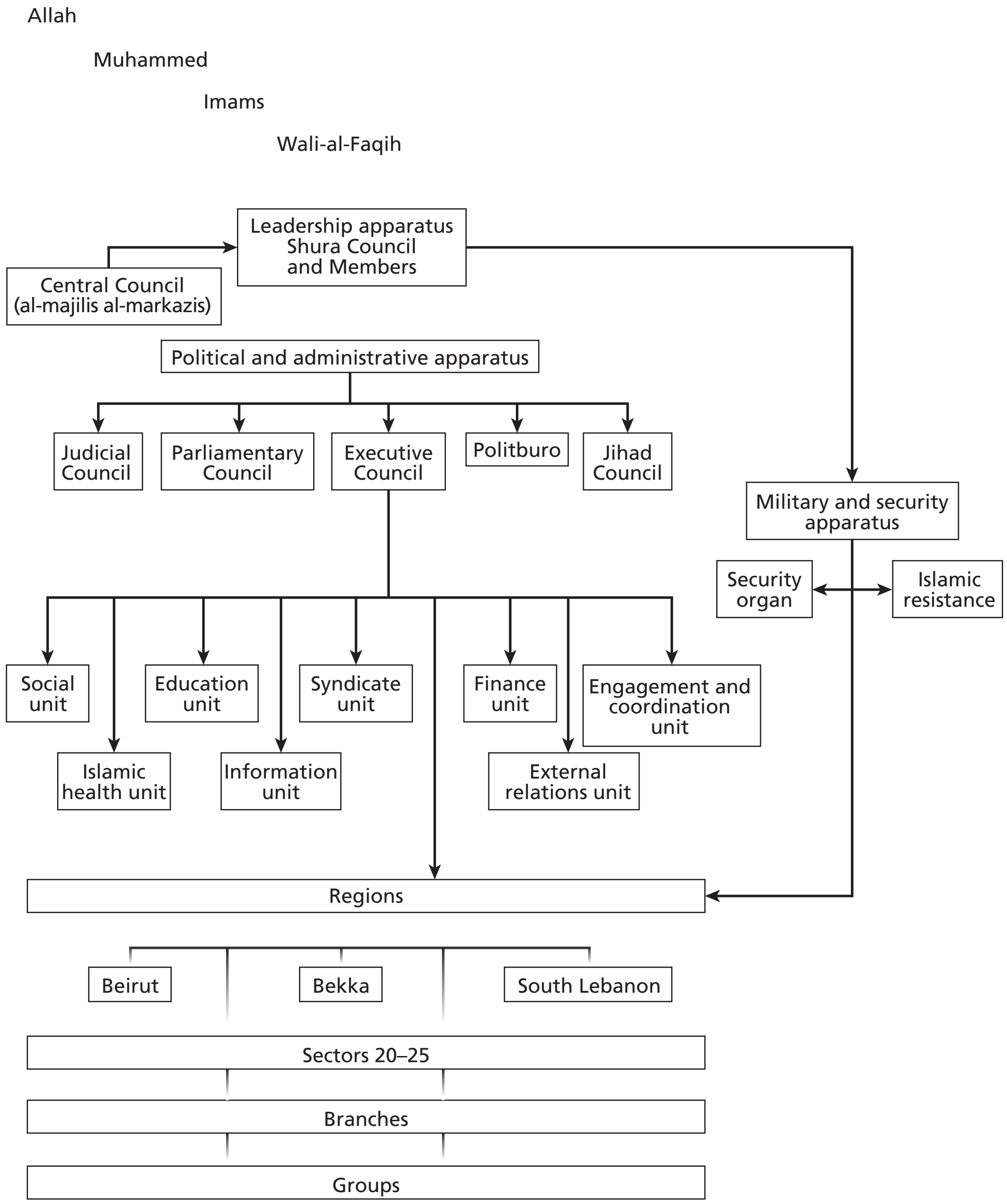
[14] Avi Jorisch, *Beacon of Hatred: Inside Hezbollah's Al-Manar Television*, Washington, D.C.: Washington Institute for Near East Policy, October 2004b.

[15] Wehrey, 2001, p. 66.

[16] Gabriel Weimann, "Hezbollah Dot Com: Hezbollah's Online Campaign," in Dan Caspi and Tal Samuel-Azran, eds., *New Media and Innovative Technologies*, Tel Aviv, Israel: Ben-Gurion University Press, 2008, p. 7.

[17] Robert Fisk, "Television News Is Secret Weapon of the Intifada," *The Independent*, December 2, 2000.

Figure 9.1
Hezbollah's Organizational Structure



SOURCE: Ahmad Nizar Hamzeh, *In the Path of Hizbullah*, Syracuse, N.Y.: Syracuse University Press, 2004, p. 46, Figure 4.1. Used with permission.

RAND *RR1925z2-9.1*

sure to broadcast in October 1996, and the network is financed by wealthy expatriate Lebanese donors, commercial receipts from the sale of its shows, and various Iranian community organizations. Al-Manar broadcasts throughout the Middle East and in Africa, Europe, and North and South America.[18] The Lebanese government takes a *laissez faire* approach to addressing Hezbollah's activities partly because there is little that Beirut can actually do: Hezbollah members staff key government ministries and provide a critical function to the Lebanese state by maintaining law and order in parts of the country where the government has little writ. Indeed, some analysts have speculated that, since around 2011, Hezbollah has become "the de facto ruling party of Lebanon."[19]

Key Leaders

Just as impressive as Hezbollah's television and video production is the group's extensive use of new media and information technologies, including its widespread presence on the Internet.[20] Its leader, Hassan Nasrallah, has his own personal website, complete with archives of his speeches and a photo gallery divided into various sections, including military operations, Lebanese brigade, Islamic Resistance, al-Aqsa intifada, attacks, the Qana massacre, the Mansoura massacre, and "other massacres."

Functional/Organizational Divisions

Hezbollah maintains a unit dedicated to psychological warfare, which specializes in promoting Hezbollah's image. This unit works closely with Al-Manar.[21]

IRCs Employed/Available

Hezbollah promotes its propaganda and messages through a broad portfolio of channels, from postcards, posters, videos, keychains, and billboards to videogames and elaborately constructed websites. The group offers or has offered a range of journals and weeklies, including *al-Ahd*, *al-Bilad*, *al-Wahda*, *el Ismaileya*, and *al-Sabil*.[22] It also operates several radio stations, including The Voice of Islam, The Voice of the Oppressed, and al-Nahar, and it controls two television stations: the aforementioned al-Manar and another, al-Fajr. Hezbollah's radio broadcasts directly reinforce the theme that Israel consistently abandons its clients and proxies. The content available on Hezbollah's websites, sometimes referred to as *cyber-Katyushas*, after the Russian-

[18] Warren Singh-Bartlett, "Al-Manar Molds Itself to Changing Situation," *Daily Star (Lebanon)*, January 3, 2001.

[19] Bennett Seftel, "Hezbollah's Many Faces," *Cipher Brief*, July 14, 2016b.

[20] For more on Hezbollah's technology use, see A. J. Dallal, "Hezbollah's Virtual Civil Society," *Television and New Media*, Vol. 2, No. 4, 2001.

[21] Pahlavi, 2007, p. 17.

[22] *Al-Ahd*, the main Hezbollah newspaper, launched in 1984 and had a circulation of 15,000 copies per week by the late 1990s.

made rockets, reflects the group's diverse agenda. This content includes news and information, welfare and social services resources, religious indoctrination literature, personal information about Hezbollah leaders, anti-Israel messages, message boards, and youth-oriented features.[23] Since the beginning of the war in Syria, Hezbollah has dramatically ramped up its efforts to recruit new and much younger members. By 2016, there were reports of a graduation ceremony for Hezbollah's youth organization, the Imam al-Mahdi Scouts, in which approximately 70,000 new members were welcomed into Hezbollah's junior ranks.[24]

In 2010, to further engage the younger generation, Hezbollah developed an online videogame in which players waged a war against Hezbollah's enemies, mainly the IDF. Before the game began, a player would take rounds of target practice against a lineup of well-known Israeli politicians.[25] When Israeli hackers interrupted service to the two major Hezbollah-run websites during the July 2006 war, Hezbollah's own hackers hijacked the communication portals of private companies, cable providers, and web-hosting servers in south Texas and suburban Virginia, as well as in Delhi, Montreal, Brooklyn, and New Jersey.[26]

Hezbollah has perfected the messaging aspect of IO and is now working to enhance its technical capabilities. The IDF banned personnel from using cell phones to call their families for fear that Hezbollah was intercepting the calls and gleaning valuable intelligence. Restricting the use of cell phones had the effect of isolating IDF soldiers operating in southern Lebanon. Hezbollah's communication system has also improved dramatically over time and now includes radio networks, copper-wire phone systems, cellular and fiber-optic networks, voice-over-Internet networks, and virtual private networks.[27]

Primary Organizations/Functions of IE Efforts

Hezbollah deliberately combines its information campaign with the kinetic aspects of its operations, and often to great effect. Taking the information effects of military operations into account during the planning phase has allowed Hezbollah to combine conventional and psychological warfare to create a "whole new PSYOP idiom." As Ron Schleifer has noted, "Hezbollah did introduce and make extensive use of one innovative PSYOP stratagem—that of subjecting virtually all its military action to its

[23] Weimann, 2008, p. 11.

[24] Nour Samaha, "Hezbollah's Crucible of War," *Foreign Policy*, July 17, 2016.

[25] Elisabeth Ferland, "Hezbollah and the Internet," Washington, D.C.: Center for Strategic and International Studies, March 4, 2010.

[26] Hilary Hylton, "How Hezbollah Hijacks the Internet," *Time*, August 8, 2006.

[27] Carl Anthony Wege, "Hezbollah's Communication System: A Most Important Weapon," *International Journal of Intelligence and Counterintelligence*, Vol. 27, No. 2, 2014.

propaganda and mass media requirements."[28] The use of video has enabled Hezbollah to magnify largely symbolic gestures far beyond their actual tactical value, thus highlighting these actions and transforming them (occasionally after the fact) into the objective of the operation. Using rather simple equipment, like video cameras, Hezbollah has given its attacks a force multiplier effect, which helped score devastating psychological blows against Israel. According to a UN observer, "75 percent of Hezbollah's war was the videotapes."[29]

Organizations/Functions Considered Partially Within or Aligned with IE Efforts

The history of Hezbollah's efforts to operate in and through the information environment is best told through the story of the evolution of its active media arm, al-Manar, which is available via satellite to televisions around the world.[30] Hezbollah transmitted its first broadcast on al-Manar in 1991 and began regularly scheduled programming on the network a mere three years later. Al-Manar is also known as Qanat al-Moqawama, or the Station of Resistance, and serves a critical function as the main dissemination point for Hezbollah news and propaganda. In addition to al-Manar, Hezbollah maintains an extensive media operation that includes al-Nour Radio, *al-Intiqad Weekly Journal*, and *Baqiatollah Islamic Magazine*, as well as a network of more than 50 websites in several languages, including English, French, German, and Arabic.[31]

From its inception, al-Manar has played an instrumental role in providing a Shia-Lebanese perspective of politics in the Middle East. Al-Manar is not just a Lebanese phenomenon, however. Its popularity has facilitated its growth into one of the leading news organizations in the Arab world. Its reach becomes increasingly important during flashpoints of conflict between Hezbollah and its adversaries—principally Israel. When the IDF conducted airstrikes against a Lebanese village in 1996 and again during the 2006 war, the Qana massacres, which killed more than 100 Lebanese civilians taking shelter at UN compound and resulted in the collapse of civilian residences, respectively, received considerably more attention on al-Manar than on most mainstream media outlets. In both cases, Israel maintains that the civilian casualties were unintentional and exacerbated by Hezbollah's practice of using civilians as human shields.[32]

Overall, al-Manar has been extremely useful as a tool for spreading Hezbollah propaganda and is regarded as a powerful and effective medium for Hezbollah's messages about the group itself, its adversaries (especially Israel), the wider Lebanese com-

[28] Schleifer, 2006, p. 5.

[29] John Kifner, "In Long Fight with Israel, Hezbollah Tactics Evolved," *New York Times*, July 19, 2000.

[30] Al-Manar operates as a part of Hezbollah's information department, which is also responsible for radio and newspaper campaigns, in addition to television.

[31] Weimann, 2008, p. 5. See also Avi Jorisch, "Al-Manar: Hezbollah TV, 24/7," *Middle East Quarterly*, Vol. 11, No. 1, Winter 2004a.

[32] Martin Asser, "Qana Makes Grim History Again," BBC News, July 31, 2006.

munity (after the Israeli withdrawal in May 2000, a widely circulated bumper sticker read, "Without al-Manar, victory would have been elusive"), and even the Lebanese government.[33]

Coordination/integration Efforts/Challenges

Hezbollah, like most organizations focused on operating in and through the IE, faces a number of challenges. First, while the level of coordination between Hezbollah's main IO cadre and the leadership in Iran remains unclear, Ayatollah Khamenei undoubtedly lacks the same currency with Hezbollah's leadership as his predecessor, Khomeini. And although, in theory, Khamenei has the final say in major decisions, he has never overruled a decision made by Hezbollah's leadership.[34] His influence via Hezbollah is *de jure* rather than *de facto*, and his approval has been reduced to little more than a rubber stamp.

The relationship between Iran and Hezbollah is based on a shared ideology and financial backing that provides Hezbollah with both money and weapons to ensure that Israel accounts for the threat on its border. Nevertheless, Hezbollah does not take orders from Tehran, nor does it operate at the behest of the Iranian government, the Pasdaran, or its Supreme Leader.[35] Most experts agree that Iran had no operational involvement with the planning and execution of Hezbollah's 2006 conflict with Israel.[36]

Information Operations in Practice

Hezbollah is hyperaware of its status in the Middle East and constantly attempts to appeal to multiple audiences, both domestic to international. In a nod to the "us-versus-them" dynamic of conflict throughout the broader Middle East, mentions of Israel are always placed in quotation marks, and Israelis are frequently referred to in pejorative shorthand on Hezbollah-affiliated websites.

Examples of Interesting Hezbollah Efforts

In a direct attempt to degrade IDF morale and to influence Israeli policymakers and the Israeli public, al-Manar ran a series in 2000 titled, "Who is Next?" in reference to

[33] Wehrey, 2001, p. 65.

[34] "Hezbollah: Rebel Without a Cause?" Brussels: International Crisis Group, Middle East Briefing Paper, July 30, 2003, p. 4.

[35] Graham E. Fuller, "The Hezbollah-Iran Connection: Model for Sunni Resistance," *Washington Quarterly*, Vol. 30, No. 1, Winter 2006–2007, p. 143.

[36] Robert Grace and Andrew Mandelbaum, *Understanding the Iran-Hezbollah Connection*, Washington, D.C.: United States Institute of Peace, September 2006.

its daily segments showing soldiers being killed and IDF troops retreating from Hezbollah attacks.[37] Hezbollah was cognizant of the chord this struck in Israeli society, which prides itself on an image of survival and a strong military tradition. Much of Hezbollah's intelligence about its enemy was gleaned through Israel's proxy army, the SLA. About ten years into the conflict, conscripted SLA fighters, nearly three-quarters of whom were Shia, suffered from extremely low morale as they fought their fellow citizens on behalf of a culturally alien occupying force.[38] Hezbollah recognized this vulnerability and took advantage of it, encouraging SLA fighters to abandon their units and using them as "a source of invaluable military, political, and psychological information" in its effort to persuade Israel to withdraw.[39]

Not only does Hezbollah push its propaganda, but it is also well poised to respond to and take advantage of any Israeli mishaps. After Israel's disastrous 1996 Operation Grapes of Wrath, which targeted and effectively destroyed large swaths of Beirut's civilian infrastructure, Hezbollah responded by rebuilding the community, earning the respect and praise of a cross-section of Lebanese citizens; one headline in a centrist Christian newspaper read, "We Are All Hezbollah."

The group is also adept at crafting and spreading messages about its own successful attacks. It regularly distributes its videos to international news agencies, including the Associated Press and Reuters, and the footage has eventually ended up on Israeli television. Hezbollah has also held press conferences in which it encouraged SLA defectors to implore their comrades to abandon the fight. In one elaborately staged press conference, Hezbollah invited a group of 70 journalists and offered them a rundown of recent Israeli casualties, including a description of the weapons used in Hezbollah attacks.[40] Hezbollah also used its information capabilities to circulate rumors in its favor, a masterful act of deception to bring about strategic effect. For example, in the late 1990s, Hezbollah ambushed an elite Israeli naval unit in southern Lebanon, killing a dozen commandos. Shortly thereafter, Hezbollah began circulating rumors that it was able to pull off the ambush because one or more of its members had penetrated Israeli intelligence. In response, the IDF halted counterinsurgency operations, ceding land and the initiative to Hezbollah.[41]

Noteworthy Capability Demonstrations or Practices

Several well-known events in on-again, off-again conflict between Hezbollah and Israel have been caught on tape by Hezbollah media personnel:

[37] Wehrey, 2001, p. 66.

[38] Al J. Venter, "South Lebanese Army Combats Internal Disintegration," *Jane's International Defense Review*, Vol. 29, August 1996, p. 58.

[39] Schleifer, 2006, p. 5.

[40] Wehrey, 2001, p. 67.

[41] Kifner, 2000.

- In February 1997, Hezbollah fighters hiding in a grove of banana trees ambushed an Israeli special forces commando operating near Sidon.
- In February 1999, Hezbollah mounted a lethal attack against IDF commander General Erez Gerstein, who was killed by an improvised explosive device.
- In January 2000, a bombing killed Colonel Akel Hashem, deputy commander of the SLA, an Israeli proxy militia.
- During the 2006 conflict, the Israeli naval destroyer *Hanit* was hit by missiles. Within minutes, Hezbollah Secretary General Hassan Nasrallah announced the strike on al-Manar with accompanying footage for distribution by regional media and YouTube.[42]

Anticipated Developments

As Iran continues to make progress in developing its cyber capabilities, it is widely believed that Hezbollah will be a major beneficiary. The ongoing conflict in Syria will likely have a major effect on the future of Hezbollah as a fighting force. Hezbollah fighters are gaining critical experience by fighting against diverse enemies and in myriad settings, using new equipment and weaponry (including drones), and operating in a range of terrain, including deserts, coastal fronts, and urban areas.[43] Some estimates suggest that in the past three years alone, somewhere between 800 and 1,200 Hezbollah fighters have been killed in the fighting in Syria.[44] This includes some extremely high-ranking fighters and leaders within the group, including top military commander Mustafa Badreddine.[45]

Efforts of Others to Counter Hezbollah Operations in the IE and Their Effectiveness

Hezbollah's move away from copper-wire to fiber-optic networks was a deliberate decision to enhance the group's data streaming capacity and to ensure a more robust defense against Israeli EW capabilities. Not only was Hezbollah successful in preventing Israeli EW units from jamming its networks south of the Litani River in the July 2006 war, but it also reportedly had its own assets in place to jam Israel's radar and communication systems.[46] For OPSEC reasons, Hezbollah migrated to closed telephone circuits that were operationally independent of Lebanese government networks.[47] In fighting in the Syrian town of Qusair in June 2013, Hezbollah again showed its penchant for

[42] Rid and Hecker, 2009, p. 51.

[43] Jamie Dettmer, "Hezbollah Develops New Skills in Syria, Posing Challenges for Israel," Voice of America, April 27, 2016.

[44] Samaha, 2016.

[45] Robin Wright, "The Demise of Hezbollah's Untraceable Ghost," *New Yorker*, May 13, 2016.

[46] STRATFOR, "Lebanon: Hezbollah's Communication Network," May 9, 2008.

[47] Walid Phares, "Hezbollah's Communication Network Confirms Its Terror Goals," *World Defense Review*, May 21, 2008.

OPSEC by dividing the territory into operational sectors and using code numbers to identify specific locations and objectives. This allowed Hezbollah fighters to talk freely on open radio channels without much concern about conversations being intercepted.[48]

Lessons from Hezbollah's Operations in and Through the IE

One of the primary lessons from Hezbollah efforts in the IE is the extent to which a nonstate actor can achieve high-level capabilities and how these capabilities can evolve over time. In the case of Hezbollah, the group has clearly benefited from Iranian assistance, in terms of resources, training, and tacit knowledge transfer. Still, that Hezbollah has been able to make such strides in integrating IO into its overall military approach is impressive and has been evident in both the group's longevity and its success on the battlefield.

Effectiveness of Hezbollah Efforts in the IE

Hezbollah has adroitly manipulated themes picked up in the Israeli press, including that Lebanon was not a "war of necessity" but a "war of choice," and consistent references to the conflict as a morass on the level of "Israel's Vietnam."[49] Other successful Hezbollah IO tactics have included airing embarrassing footage of IDF troops retreating and failing to counterattack, as well as documenting inconsistencies between what was happening on the battlefield and what was being reported in the Israeli press. The embarrassing footage led retired Israeli soldiers to denigrate the quality of currently enlisted IDF troops, further hurting morale, while Hezbollah's ability to highlight the disconnect between what was being reported and what was actually happening on the battlefield spurred widespread protests from a group in Israel called Four Mothers, which argued that their sons and daughters were fighting and dying in Lebanon while the government whitewashed the severity of casualties and setbacks.[50] In some cases, Hezbollah battlefield footage served as explicit proof contradicting statements from Israel that certain attacks never took place, thus sapping IDF credibility within Israel.

Vulnerabilities in Hezbollah Efforts in the IE

In March 2006, The U.S. Treasury Department designated al-Manar's television operation, al-Nour Radio, and the Lebanese Media Group (the parent company of both al-Manar and al-Nour Radio) as specially designated global terrorist entities. Stuart Levey, Under Secretary of the U.S. Treasury for Terrorism and Financial Intelligence, proclaimed, "Any entity maintained by a terrorist group—whether masquerading as

[48] Nicholas Blanford, "Hezbollah Applies New Training Practices in Syria," *Daily Star (Lebanon)*, June 8, 2013.

[49] Wehrey, 2001, p. 64.

[50] Wehrey, 2001, p. 66.

a charity, a business, or a media outlet—is as culpable as the terrorist group itself."[51] In addition to supporting Hezbollah, al-Manar has also aided the Palestinian Islamic Jihad and al-Aqsa Martyrs' Brigade. The U.S. State Department placed al-Manar on its terrorist exclusion list back in December 2004, in effect barring individuals who engaged in a range of actions involving al-Manar from entering the United States.

Key Takeaways

There are several key takeaways for the U.S. Army from Hezbollah's ability to operate in and through the IE:

- The group has the resources, personnel, and capabilities necessary for effective operations in the IE.
- Hezbollah continuously and meticulously seeks to improve its technical capabilities.
- Because Hezbollah treats IRCs as a warfighting function, the integration is seamless. This strategy has been extremely effective against adversaries with far superior military capabilities, such as the IDF.
- Hezbollah is not just pushing messages but responding to events as they unfold.
- Hezbollah is largely unconstrained by laws or authorities in Lebanon and is able to operate with relative impunity in terms of dedicating the necessary resources toward IO and IRCs.
- All members are trained in the importance of the IE. It is not strictly the domain of a specific wing of the organization. From its leadership down to the lower levels, there is buy-in regarding the importance of IO as a force multiplier and asymmetric warfare tool.
- Target audiences and segmentation are selected with great care to address specific vulnerabilities. As mentioned earlier, Hezbollah radio broadcasts directly targeted the SLA, relentlessly reminding the proxy soldiers that Israel had historically abandoned its clients during some point in the conflict.

Capabilities or Practices That the U.S. Army Might Want to Replicate (or Access Through Joint, Interagency, International, or Multinational Efforts)

One practice in particular that is worth the Army's consideration is the priority and prominence that Hezbollah gives IO in its operations. This emphasis on information is embedded in planning at all levels and inculcated in the culture of Hezbollah's military arm. Moreover, as mentioned throughout this chapter, Hezbollah carefully selects themes for its messaging campaigns and reemphasizes these themes with steadfast consistency. In turn, this allows Hezbollah to integrate IO with its military operations with little friction. More than any other nonstate actor, Hezbollah appreciates the

[51] Cliff Kincaid, "Bombing Terror Television," *Accuracy in Media*, August 4, 2006.

importance of efforts in and through the IE and treats them as its own “warfighting function.” Finally, the Army can learn from mistakes made by the IDF over the course of its 18-year occupation of southern Lebanon and subsequent battles against Hezbollah. For example, the IDF’s restrictions on media access in the security zone ensured that reporting would remain biased in Hezbollah’s favor.

CHAPTER TEN

Al-Qaeda

Case Summary

As the perpetrator of the deadliest terrorist attack in history on U.S. soil, al-Qaeda has demonstrated an intuitive understanding of the information value of kinetic operations. “Spectacular” attacks like those launched against New York City and Washington, D.C., on September 11, 2001, have echoes in the IE that equal—or even surpass—the actual physical effects. Al-Qaeda’s media production is sophisticated, both aesthetically and historically. However, its messages are often wide-ranging and unfocused. Since 9/11, core al-Qaeda’s propaganda has abated significantly, and it is now more appropriate to think of the group’s operations in and through the IE in terms of its franchises and affiliates (e.g., al-Qaeda in the Arabian Peninsula [AQAP], al-Qaeda in the Islamic Maghreb [AQIM], al-Shabaab).

Although its propaganda has slowed down, it lives forever on the Internet. ISIL has clearly learned from, improved upon, and surpassed al-Qaeda’s tactics, which included footage showing attacks on U.S. troops, al-Qaeda militants assembling improvised explosive devices, and suicide bombers’ martyrdom tapes, complete with anti-American and anti-Israeli vitriol. Deterring, disrupting, or destroying the physical organization does not put an end to the influence that a group can have, as evidenced by the popularity of Anwar al-Awlaki, whose YouTube sermons have inspired terrorist attacks long after his death. Media distributed by violent nonstate actors, such as al-Qaeda, can reinforce the group’s strategy while also having a more tactical effect (e.g., conveying instructions for constructing homemade bombs in *Inspire*, the manual that Dzhokhar and Tamerlan Tsarnaev used to build the bombs for the Boston Marathon attack).

Background and Overview

Al-Qaeda's origins can be traced to an organization called Maktab al-Khidamat, established by a Palestinian jihadist named Abdulla Azzam.[1] That organization's early efforts focused on recruiting Arab fighters to join the resistance in Afghanistan, where the mujahideen, or holy warriors, were fighting to expel Soviet troops from the country.[2] Early members of Maktab al-Khidamat, which was founded in 1984, included Azzam, Osama bin Laden, and the Algerian Abdullah Anas. Soon after, bin Laden met and joined forces with Ayman al-Zawahiri, the current leader of "core" al-Qaeda. Zawahiri eventually merged key members of his group, Egyptian Islamic Jihad, with al-Qaeda once it emerged as its own entity in the late 1980s. At that point, Maktab al-Khidamat had become more focused on humanitarian efforts rather than actual fighting.[3] Al-Qaeda has continued to evolve over the years. Now entering its third decade, al-Qaeda is many things—terrorist organization, global jihadist network, brand, and franchise group for Salafist jihadists throughout the world. Although this case study focuses primarily on what is known as core al-Qaeda, it also touches on several al-Qaeda affiliates where relevant, including AQAP, based in Yemen, and AQIM, based in North Africa, as well as al-Qaeda in Iraq (AQI), now ISIL, and al-Nusra Front, al-Qaeda's Syria affiliate, which rebranded itself as Jabhat Fateh al-Sham in August 2016.[4]

Concepts and Principles for Operations in and Through the IE

Throughout his tenure as al-Qaeda's leader, Osama bin Laden consistently used the group's media platforms—from newsletters to audio cassettes and video messages—to address issues that many in the Arab and Muslim worlds were passionate about, including the liberation of Palestine, the U.S. occupation of Iraq, and the corruption of apostate governments and regimes throughout the Middle East and South Asia.[5] Al-Qaeda is acutely aware of the importance of the IE, and nowhere is this more evident than in captured correspondence—since made public—between al-Qaeda's then-deputy, Ayman al-Zawahiri, and AQI chieftain Abu Musab al-Zarqawi over the former's protestation of AQI's wanton slaughter of Shia populations. Zawahiri

[1] Al Qaeda has been translated variously as "base of operation," "foundation," "precept," or "method." Al Qaeda, al-Qaeda, al-Qa'ida, and several other variants are used interchangeably in the literature. For more, see Bruce Hoffman, "The Changing Face of Al Qaeda and the Global War on Terrorism," *Studies in Conflict and Terrorism*, Vol. 27, No. 6, 2004, p. 551.

[2] R. Kim Cragin, "Early History of Al-Qa'ida," *Historical Journal*, Vol. 51, No. 4, December 2008.

[3] Cragin, 2008, p. 1056.

[4] Core al-Qaeda is sometimes referred to as the al-Qaeda Core, al-Qaeda Central, or the al-Qaeda Senior Leadership. It is important to note that the core group's affiliates are in a constant state of flux.

[5] Marc Lynch, "Al Qaeda's Media Strategies," *National Interest*, Vol. 83, Spring 2006.

admonished Zarqawi in the letter and reminded him that “more than half of this battle is taking place in the battlefield of the media.”[6] Like his Salafist cohorts, Zawahiri is no fan of Shias, who are often the target of even more scorn than Christians and Jews, but he was apparently so concerned about the damage that Zarqawi was inflicting on the al-Qaeda brand in his quest to instigate sectarian war in Iraq that he felt compelled to reach out directly.

If al-Qaeda’s media production seems high-quality and refined, that is because the group has been producing media since its inception, but over the years, the themes have changed and its presentation has grown more nuanced.[7] Zawahiri reportedly prizes the “jihadi information media” as an indispensable element of al-Qaeda’s war against the United States.[8] Al-Qaeda’s media production is sophisticated—both aesthetically and in its ability to manipulate its audience’s understanding of history. Its propaganda routinely references colonial injustices of the past, including the Sykes-Picot Agreement, which carved up the Middle East between France and Britain. After its falling out with ISIL, al-Qaeda and its erstwhile offshoot consistently traded barbs through their respective media outlets, mocking each other’s leaders and attacking their religious credentials. The irony was lost on Zawahiri, at least, who, in August 2015, remarked, “We once conquered the world with our media. . . . Today, their media has divided us.”[9] He revisited this theme of division in a video released in August 2016. In “Be Not Divided Among Yourselves,” Zawahiri castigates ISIL as a divisive force and urges true believers among the global jihadist movement to “rally around the emirate,” a reference to the Taliban.[10]

Strategic Goals/Vision

Al-Qaeda’s “Declaration of War against the Americans Occupying the Land of the Two Holy Places,” published in 1996 in the London-based newspaper *al-Quds al-Arabi,* was the opening salvo in the information war against the United States and its allies—including what the jihadists viewed as apostate regimes in the Middle East, such as Egypt and Saudi Arabia. Many scholars believe that this *fatwa* was “a turn-

[6] Quoted in Lawrence Wright, “The Master Plan,” New Yorker, September 11, 2006. See also Catherine A. Theohary and John Rollins, *Terrorist Use of the Internet: Information Operations in Cyberspace*, Washington, D.C.: Congressional Research Service, March 8, 2011, p. 3.

[7] Michael Scheuer, “Al Qaeda’s Media Doctrine: Evolution from Cheerleader to Opinion-Shaper,” *Terrorism Focus*, Vol. 4, No. 15, May 30, 2007. See also Manuel R. Torres, Javier Jordán, and Nicola Horsburgh, “Analysis and Evolution of Global Jihadist Media Propaganda,” *Terrorism and Political Violence*, Vol. 18, No. 3, 2006.

[8] Philip Seib, “The Al-Qaeda Media Machine,” *Military Review*, May–June 2008, p. 79.

[9] Hassan Hassan, “Threats from Two Fronts: Al-Qaeda and IS Define Their Strategies,” Washington, D.C.: Tahrir Institute for Middle East Policy, May 25, 2016.

[10] Thomas Joscelyn, “Zawahiri Calls on Muslims to Support Taliban, Reject Islamic State,” *Long War Journal*, August 21, 2016.

ing point" in al-Qaeda's media operations, "both in terms of form and content."[11] The *fatwa* outlined new objectives and new themes for al-Qaeda and announced its place as the preeminent jihadist group taking aim at the West. The primary achievement of bin Laden's *fatwa* was to frame parochial conflicts in the Middle East and South Asia as key components of a global struggle between Islam and the West.

In many ways, al-Qaeda's ideology reflects its self-perception as a defender and vanguard of Muslims everywhere, the *ummah*. In declaring jihad, bin Laden argued that the West—and particularly the United States—was hostile to Islam and that the only way to respond to this aggression was with force or violence, the only language that the United States understands. In his speeches, bin Laden exhorted his followers to fight back and defend Muslims from the United States, which was responsible for "an ocean of oppression, injustice, slaughter and plunder."[12] Therefore, the next logical step was jihad. In essence, the core of al-Qaeda's ideology is individual jihad fused with collective revenge.[13]

From an intellectual standpoint, the jihadist totalitarian ideology is a closed system, but it also allows for disagreements over strategy, tactics, and other critical issues.[14] An analysis of the group's internal documents revealed a group at ease with internal disagreement and debate among its members and leadership.[15] One well-known ideological divide in al-Qaeda has been between those who wish to strike "the far enemy" and those who prefer to target what they perceive as apostate regimes throughout the Muslim world.

How Operations in the IE Fit Within al-Qaeda's Overall Strategic Goals

Zawahiri's vision of an Islamic caliphate is al-Qaeda's long-term strategic goal, though it should be noted that, unlike ISIL, Zawahiri warns against rushing into the declaration of a caliphate and instead views it as the culmination of a seven-stage plan first articulated by al-Qaeda's operational chief, Saif al-Adl.[16] The first phase is known as "the awakening" and launched with al-Qaeda's attacks on September 11, 2001. Several intermediate phases are focused on galvanizing the *ummah* and uniting the Muslim world behind the group's agenda. The final phase, "definitive victory," signals the

[11] Rid and Hecker, 2009, p. 187.

[12] Michael Scheuer, *Imperial Hubris: Why the West Is Losing the War on Terror*, Washington, D.C.: Brassey's, 2004, p. 129.

[13] Bruce Hoffman, "Al Qaeda Trends in Terrorism and Future Potentialities: An Assessment," paper presented at a meeting of the Council on Foreign Relations, Washington D.C., May 8, 2003, p. 5.

[14] David Aaron, *In Their Own Words: Voices of Jihad*, Santa Monica, Calif.: RAND Corporation, MG-602-RC, 2008, p. 73.

[15] Cragin, 2008, p. 1066.

[16] Bruce Hoffman, "Al Qaeda's Master Plan," *Cipher Brief*, November 18, 2015.

establishment of a global Islamic caliphate under which infidels and unbelievers will be vanquished.[17]

IRCs figure prominently in al-Qaeda's strategic goals. This is evident in the text *The Management of Savagery*, in which Islamist strategist and al-Qaeda ideologue Abu Bakr Naji stressed the importance of the media in destroying the United States' image while also building the self-confidence of Muslims worldwide.[18] Bakr Naji also urged his followers to study Western writing on management, military principles, political theory, and sociology to better understand the strategies that Western governments employ and how to exploit U.S. and European vulnerabilities.[19] He even implored his followers to study the Arabic translation of Paul Kennedy's *The Rise and Fall of the Great Powers*.

Bakr Naji also advocated attacks on the U.S. economic and financial infrastructure, including tourist sites and oil facilities. He argued that these attacks should be carefully planned to avoid harming other Muslims, so as not to alienate potential followers and supporters.[20] Al-Qaeda has deliberately made it a point to stress the importance of integrating military and media activities. For example, Abdel Aziz al-Muqrin, former leader of AQAP, believed that the synchronization of military and media activities was at the forefront of the group's objectives and served as a force multiplier.[21]

Targets and Audiences

Al-Qaeda has always maintained an impressive awareness of the targets and audiences it seeks to influence with its messaging. Understanding that terrorism is political violence, the *raison d'etre* of al-Qaeda's violence is not, as some have suggested, simply hatred for American values and the American way of life—although, to be sure, Western values are certainly inimical to the Salafist jihadist platform. Rather, al-Qaeda attacks the West to change policy. In April 2004, al-Qaeda released an audiotape in which bin Laden offered "a truce to the European countries that do not attack Muslim countries" and that refrain from interfering "in [Muslim countries'] affairs."[22]

This appeal to the body politic of Western countries aligns with a major aim of al-Qaeda's overall media strategy. An analysis of the media strategies employed by

[17] Bill Roggio, "The Seven Phases of the Base," *Long War Journal*, August 15, 2005.

[18] Sometimes referred to as the Administration of Savagery, or *the Management of Barbarism*, depending on the translation. The subtitle reads, "The Most Dangerous Stage Through Which the *Ummah* Will Pass." See Michael W. S. Ryan, *Decoding Al-Qaeda's Strategy: The Deep Battle Against America*, New York: Columbia University Press, 2013, p. 163.

[19] Jarret M. Brachman and William F. McCants, "Stealing Al Qaeda's Playbook," *Studies in Conflict and Terrorism*, Vol. 29, No. 2, 2006, pp. 310–312.

[20] Brachman and McCants, 2006, p. 311.

[21] Rid and Hecker, 2009, p. 203.

[22] Dana Priest and Walter Pincus, "New Target and Tone," *Washington Post*, April 16, 2004.

both al-Qaeda and ISIL revealed that al-Qaeda consistently employed attrition to compel changes in the West's policy and behavior.[23] Al-Qaeda consistently sought to warn, intimidate, and cajole Western publics, viewed by al-Qaeda as "neutrals," that the actions on behalf of their governments were the reason they were being targeted. After mounting a series of coordinated bombings in London on July 7, 2005, al-Qaeda released a martyrdom tape featuring Mohammed Sidique Khan, who warned British citizens and the West in a thick Yorkshire accent about interfering in Muslim lands, declaring, "Our words are dead until we give them life with our blood."[24]

Bakr Naji believed that al-Qaeda's media strategy should focus on two groups specifically: "ordinary people" who could be convinced to join the jihad and enemy soldiers who could be intimidated into defecting from their respective militaries in the wake of impossible odds.[25] Al-Qaeda has also used its media platform to threaten enemies other than the West. In February 2012, Zawahiri addressed the "Lions of the Levant," peppering his message with warnings for Alawites, Hezbollah, and Iran. Finally, the group has relied on messaging to attract recruits and funding for its activities. In March 2013, it launched a new e-journal, *Balagh* (*Message*); the publisher called itself the Levant News Battalion and urged followers to join the fight and send money to support those already fighting.[26]

Foundational Principles

For as long as the United States has been at war with al-Qaeda, the terrorist group has recognized the importance of fighting back in the IE. To be sure, Mohammed bin Ahmad al-Salem's 2003 publication, *39 Ways to Serve and Participate in Jihad*, emphasized the importance of what he called electronic jihad.[27] But beyond using IO for propaganda purposes and to inform, influence, and persuade, al-Qaeda also uses information to instruct. More specifically, it relies on its media as a conduit to transfer the technical know-how for bomb making, ambush techniques, and a range of other guerrilla TTPs. Al-Qaeda—like any reputable organization mindful of its image—is concerned about copycats or "wanna-bes" diluting its brand. As such, to maintain the

[23] Attrition is one of five strategic logics outlined by Kydd and Walter in their study of terrorist organizations. Put simply, attrition strategies are intended to convince the enemy that the terrorists are willing and able to inflict a high cost if a specific policy continues to be enforced. See Andrew H. Kydd and Barbara F. Walter, "The Strategies of Terrorism," *International Security*, Vol. 31, No. 1, Summer 2006. The comparative analysis of al-Qaeda and ISIL appears in Celine Marie I. Novenario, "Differentiating Al Qaeda and the Islamic State Through Strategies Publicized in Jihadist Magazines," *Studies in Conflict and Terrorism*, Vol. 39, No. 11, 2016.

[24] Nicholas J. O'Shaughnessy and Paul R. Baines, "Selling Terror: The Symbolization and Positioning of Jihad," *Marketing Theory*, Vol. 9, No. 2, 2009, p. 234.

[25] Michael Ryan, 2013, p. 177.

[26] Bruce Hoffman, "Al Qaeda's Uncertain Future," *Studies in Conflict and Terrorism*, Vol. 36, No. 8, 2013, p. 643.

[27] Rid and Hecker, 2009, p. 194.

integrity and credibility of its media, it warns against those who distribute media in al-Qaeda's likeness "without official sanction."[28]

History and Evolution

Before the rise of ISIL, al-Qaeda's media savvy among terrorist groups was rivaled only by that of Hezbollah. After being expelled from Saudi Arabia to Sudan, bin Laden created the Advice and Reform Committee, based in London, which distributed newsletters and emails to prominent Muslim clerics, scholars, and judges who shared the al-Qaeda founder's views on Islamic jurisprudence.[29] Even during the nascent stages of al-Qaeda's formation, when it was known as Maktab al-Khidamat, bin Laden was conscious of the importance of the IE. By the early 1990s, electronic journals, such as *al-Ansar*, *al-Neda*, *Mu'askar al-Battar,* and *Sawt al-Jihad,* began to appear.[30] Over the years, al-Qaeda continued to expand the technical sophistication of its communications, as well as increase their geographic reach and overall frequency. The group released six videos in 2002, 11 in 2003, 13 in 2004, 16 in 2005, 58 in 2006, and 97 in 2007.[31]

Organization for Operations in the IE

Al-Qaeda is commonly referred to as a terrorist network, yet it comprises elements of a bureaucracy. The group is headed by its emir, currently Zawahiri, who sits atop the al-Qaeda Shura, or advisory council. Beneath this body are six core committees, one of which is the information committee, sometimes referred to as the committee on propaganda and media affairs (and at one point led by a jihadist nicknamed Abu Reuters).[32]

Structure

According to Bruce Hoffman, al-Qaeda is "more an idea or a concept than an organization" and is "an amorphous movement tenuously held together by a loosely networked transnational constituency rather than a monolithic, international terrorist organization with either a defined or identifiable command and control apparatus."[33] At least 13 established media production and distribution entities can be linked to the group, but the three most prominent are al-Fajr Media Center, the Global Islamic Media

[28] Rid and Hecker, 2009, p. 204.

[29] Rid and Hecker, 2009, p. 187.

[30] Rid and Hecker, 2009, p. 188.

[31] Rid and Hecker, 2009, p. 203.

[32] Daniel Byman, *Al Qaeda, The Islamic State and the Global Jihadist Movement: What Everyone Needs to Know*, New York: Oxford University Press, 2015, p. 95.

[33] Hoffman, 2004, p. 551.

Front, and the al-Sahab Institute for Media Production. The relationship between al-Qaeda and disparate jihadist groups can be mutually beneficial. Al-Qaeda is lionized as the vanguard of Islamic resistance (one of its stated aims), and each time an attack is executed in its name somewhere in the world, the al-Qaeda "brand" is strengthened and its image burnished among its followers. The group that carries out the attack, for its part, gains the credibility of association with the al-Qaeda brand, and a successful operation can even result in follow-up funding to plan and execute future attacks.[34]

The franchise model also has its downsides, because al-Qaeda's central leadership exerts little control over its affiliates beyond offering periodic praise and suggesting potential targets.[35] The murder of innocent Muslims is a topic widely debated in jihadist forums both online and in print, and it was the main point raised in Zawahiri's 6,000-word letter to Zarqawi that was intercepted by the U.S. military in October 2005.[36] The importance of information was not entirely lost on Zarqawi, who, as the emir for AQI, organized an information wing that included his personal press secretary.[37]

Funding

Although there are no universally accepted figures on al-Qaeda's operating budget, especially in terms of how much funding is dedicated to media and propaganda activities, the highest-end estimate suggests that, during the 2000s, al-Qaeda earned as much as $1 billion per year from its financing efforts.[38] Others suggest that, before the 9/11 attacks, al-Qaeda sustained itself on roughly $30 million annually.[39] In a 2004 journal article, Mark Basile claimed that al-Qaeda operated a financial network valued

[34] An example of this is AQIM. That group was formerly known as the Salafist Group for Preaching and Combat but adopted the al-Qaeda name in an attempt to gain notoriety and credibility, potentially raising its profile with other jihadists. AQIM used this brand to redress local grievances but has scant interest in expanding its activities elsewhere. And, despite the group's former name, it shares little of the Salafist ideology of the main branch of al-Qaeda. This is noted by Jean-Luc Marret in "Al-Qaeda in Islamic Maghreb: A 'Glocal' Organization," *Studies in Conflict and Terrorism*, Vol. 31, No. 6, 2008.

[35] While many commentators on terrorism have put forth strong arguments for the franchise analogy, including Lowell E. Jacoby, "Five Years After 9/11: What Needs to Be Done?" Philadelphia, Pa.: Foreign Policy Research Institute, February 2007, Joshua McLaughlin makes a compelling case for using the term *conglomerate* to describe al-Qaeda (Joshua McLaughlin, "The Al Qaeda Franchise Model: An Alternative," *Small Wars Journal*, January 31, 2010).

[36] Susan B. Glasser and Walter Pincus, "Seized Letter Outlines Al Qaeda Goals in Iraq," *Washington Post*, October 12, 2005.

[37] Susan B. Glasser and Steve Coll, "The Web as Weapon," *Washington Post*, August 9, 2005.

[38] Angel Rabasa, Peter Chalk, Kim Cragin, Sara A. Daley, Heather S. Gregg, Theodore W. Karasik, Kevin A. O'Brien, and William Rosenau, *Beyond Al-Qaeda: The Global Jihadist Movement*, Part I, Santa Monica, Calif.: RAND Corporation, MG-429-AF, 2006, p. 59.

[39] Juan Miguel del Cid Gómez, "A Financial Profile of the Terrorism of Al-Qaeda and Its Affiliates," *Perspectives on Terrorism*, Vol. 4, No. 4, October 2010, p. 3.

at more than $300 million and that it dispersed between $30 million and $40 million per year to run the organization.[40] The CIA also estimated that, prior to 9/11, the cost of sustaining al-Qaeda was approximately $30 million per year.[41] An assessment of the group's finances in 2010 concluded that it was being squeezed financially but that paying for "publicity" was inexpensive, and maintaining a sophisticated media operation was still "relatively cheap."[42]

Key Leaders

Besides bin Laden, al-Qaeda's main Salafist ideologues have included Ayman al-Zawahiri, Abu Musab al-Suri (captured), Anwar al-Awlaki (deceased), and Abu Yahya al-Libi (deceased).[43] These modern-day insurgent-theorists have offered followers advice on strategy, operations, and tactics (in addition to a host of other issues, including diet, grooming, and marriage),[44] and they have all been highly adept at propagating the narrative that the Muslim *ummah* is being oppressed by the U.S.-Israel (or Crusader-Zionist) nexus.[45]

Abu Musab al-Suri is a Syrian jihadist with Spanish citizenship and, prior to his capture, was al-Qaeda's most prolific author on insurgent and terrorist strategy and tactics. Dubbed the architect of the new al Qaeda, perhaps no other individual has done more to shape the group's new strategy since 9/11.[46] Al-Suri brought a wealth of experience to al-Qaeda's media operations, having previously worked with the Armed Islamic Group of Algeria's *al-Ansar* journal, *al-Fajr* of the Libyan Islamic Fighting

[40] Mark Basile, "Going to the Source: Why Al Qaeda's Financial Network Is Likely to Withstand the Current War on Terrorist Financing," *Studies in Conflict and Terrorism*, Vol. 27, No. 3, 2004, p. 170.

[41] Victor Comras, "Al Qaeda Finances and Funding to Affiliated Groups," in Jeanne K. Giraldo and Harold A. Trinkunas, eds., *Terrorism Financing and State Responses: A Comparative Perspective*, Stanford, Calif.: Stanford University Press, 2007, p. 115.

[42] Greg Bruno, "Al-Qaeda's Financial Pressures," backgrounder, Council on Foreign Relations, February 1, 2010.

[43] Abu Musab al-Suri is also known as Mustafa Setmariam Nasar. On Anwar al-Awlaki, see Scott Shane, *Objective Troy: A President, A Terrorist and the Rise of the Drone*, New York: Deckle Edge, 2015. On Abu Yahya al-Libi, see Declan Welsh and Eric Schmitt, "Drone Strike Killed No. 2 in Al Qaeda U.S. Officials Say," *New York Times*, June 5, 2012.

[44] There are a number of emerging jihadist pundits in the virtual arena. Some of the most prolific Internet authors have included Asad al-Jihad, Abd al-Rahman al-Faqir, Hafid al-Hussain, Shaykh Abu Abd al-Rahman al-Yafi'i, Abu Shadiyah, Ziyad Abu Tariq, Shaykh Abu Ahmad, al-Rahman al-Masri, and Yaman Mukhaddab. For more information, see Jarret Brachman, "The Worst of the Worst," *Foreign Policy*, January 22, 2010.

[45] For more on narratives, see William D. Casebeer and James A. Russell, "Storytelling and Terrorism: Towards a Comprehensive 'Counter-Narrative Strategy,'" *Strategic Insights*, Vol. 4, No. 3, March 2005.

[46] Paul Cruickshank and Mohannad Hage Ali, "Abu Musab al-Suri: Architect of the New Al Qaeda," *Studies in Conflict and Terrorism*, Vol. 30, No. 1, 2007, p. 1. For more on al-Suri and his influence on current jihadist strategy, see Colin P. Clarke and Daveed Gartenstein-Ross, "How Will Jihadist Strategy Evolve as the Islamic State Declines?" *War on the Rocks*, November 10, 2016.

Group, and *al-Mujahidun*, a publication produced by Egyptian Islamic Jihad. Indeed, Thomas Rid and Marc Hecker remarked that "his career epitomizes how jihad and media operations have effectively merged."[47] Al-Suri penned a 1,600-page tome, *The Call for Global Islamic Resistance*, which argued that individual terrorism should replace al-Qaeda's hierarchical structure. His *magnum opus* argued that a decentralized, looser network would present more problems for the West, especially if cells formed spontaneously and autonomously. The result would be "thousands, even hundreds of thousands of Muslims participating in *Jihad*."[48]

Eclipsing al-Suri as the vanguard of al-Qaeda's thinking on insurgency was a former member of the Libyan Islamic Fighting Group, Abu Yahya al-Libi. At one point referred to as bin Laden's successor, al-Libi was seen as "young, media-savvy, ideologically extreme, and masterful at justifying savage acts of terrorism with esoteric religious arguments."[49] Unlike AQI's former leader and cult hero Abu Musab al-Zarqawi, al-Libi blended jihadist credentials with scriptural knowledge. He fought against the Soviets in Afghanistan, trained insurgents in Libya and Mauritania, and was arrested by Pakistani intelligence only to escape from Bagram prison in Afghanistan while under the watch of U.S. soldiers. In other words, his *bona fides* were genuine, and he had "street cred" with jihadist fighters and scholars alike. The ability to boast leaders with a mastery of both the Quran and the AK-47 has made al-Qaeda not just a terrorist group but an "intellectual and religio-ideological insurgency."[50]

If al-Suri was the strategist and al-Libi represented the new guard, then al-Qaeda's current leader, Zawahiri, is the group's operational planner.[51] In his seminal work, *Knights under the Prophet's Banner*, Zawahiri laid out a two-phase strategy to instigate a global Islamic insurgency.[52] First, he proposed a focus on the "near enemy," including the corrupt and apostate regimes of the Middle East, with his native country of Egypt drawing particular ire. After an Islamic caliphate is restored in Egypt, he argued, the caliphate would be used as a staging ground to launch attacks against the West, eventually usurp the United States and its allies, and reclaim al-Qaeda's rightful place as a global example of strength and wisdom.

In March 2008, al-Sahab published a nearly 200-page document by Zawahiri, *A Treatise Exonerating the Nation of the Pen and the Sword from the Blemish of the Accusation of Weakness and Fatigue*, which presents the case against Crusaders, Zionists, and apostate Arab regimes. Some of Zawahiri's ideas closely resemble those of one of his

[47] Rid and Hecker, 2009, pp.188–189.

[48] Cruickshank and Ali, 2007, p. 10.

[49] Jarret Brachman, "The Next Osama," *Foreign Policy*, September 10, 2009.

[50] Brachman, 2009.

[51] See "The Operations Man: Ayman al-Zawahiri" *The Estimate*, Vol. 13, No. 17, September 21, 2001.

[52] David Kilcullen, "Countering Global Insurgency," *Journal of Strategic Studies*, Vol. 28, No. 4, 2005, p. 598.

Egyptian Islamic Jihad and al-Qaeda counterparts: Sayed Imam Abdulaziz al-Sharif, author of *The Master in Making Preparation for Jihad*, which has been translated into numerous languages, including English, French, Turkish, and Urdu.

Functional/Organizational Divisions

Al-Qaeda divided its media operations along two lines: a "guidance center" and "resistance call units." The former was enabled by the Internet and responsible for supervising and distributing ideological material, a doctrinal program, educational materials, and communiques; the resistance call units were more ad hoc, established in a decentralized manner on an as-needed basis.[53] But just as al-Qaeda relies on dedicated cells within its organization to propagate its information and propaganda, so too does it accept help from willing accomplices living abroad who possess the technical skills and abilities to help spread its core messages. A case in point is that of Younis Tsouli, an IT student at a London university who became the chief architect of *al-Ansat*, one of al-Qaeda's most prolific web forums in the mid-2000s.

IRCs Employed/Available

While al-Qaeda relies primarily on propaganda, it has also employed various IRCs at different points. There are myriad examples of cyberattacks initiated by al-Qaeda–linked militants and sympathizers over the years, though most qualify as low-level incidents of hacking Internet servers to share documents or defacing websites.[54] Operations security appears to be a paramount concern, according to Dorothy Denning:

> The al-Qa'ida training manual emphasizes security and integrates it into such topic areas as housing, communications, transportation, training, meetings, and operations. Under telephone communications, for example, members are instructed to use phones in public places and to use codes or speak in general terms in case their conversations are being monitored. Under apartments, they are told that nobody should know the location except those who use it, and that it is preferable to rent apartments using false names, appropriate cover, and non-Muslim appearance. Members are also told to prepare secret locations in their apartments for hiding documents, records, arms, and other important items.[55]

Al-Qaeda's security priorities also extend to data encryption (of computers and satellite data communications) and steganography. An al-Qaeda training manual includes instructions for deception, cover identities, and the use of false documents,

[53] Rid and Hecker, 2009, p. 192.

[54] Dorothy Denning, "Information Operations and Terrorism," in Lars Nicander and Magnus Ranstorp, eds., *Innovative Terrorism in the Information Age: Understanding the Threat of Cyber-Warfare*, London: Hurst, unpublished, 2005.

[55] Denning, 2005.

lessons that may draw on the success of several of the 9/11 hijackers who attempted to blend into local communities and avoid suspicious activities.

Coordination/Integration Efforts/Challenges

Al-Qaeda's main coordination and integration challenges today result from the near-constant onslaught of U.S. counterterrorism strikes targeting the organization. Core al-Qaeda is still based in Pakistan, although the group and its leadership have been driven deep underground, complicating the ability to disseminate relevant and timely media products. Moreover, its franchise groups are geographically dispersed (e.g., across Yemen, North Africa, and other locations), and it has been losing adherents to ISIL, with groups previously affiliated with al-Qaeda abandoning the brand for ISIL in parts of Nigeria, Somalia, Afghanistan, and elsewhere.

Information Operations in Practice

The products al-Qaeda disseminates vary and include glossy books, short articles, videos, and audio-recorded lectures. A one-month snapshot from July 2007 demonstrates the volume of al-Qaeda's media production at its peak: The group and its affiliates published approximately 450 unique media products.[56] Al-Qaeda or affiliated groups have displayed their propaganda on more than 4,000 websites and have used thousands of other websites to convey their messages. Al-Qaeda's production company, al-Sahab, releases dozens of videos each year, which have been translated to German, French, Italian, Dutch, Turkish, Pashtu, Urdu, and Russian, among other languages.[57] In March 2004, the group launched *Muskar al-Battar*, or *Camp of the Sword*, offering information on jihadist attacks in Saudi Arabia and Iraq.[58] *Sawt al-Jihad*, or *Voice of Jihad*, is an online magazine aimed at mobilizing public support for the group and justifying its actions to its core constituency.[59]

Al-Qaeda has used the Internet not only for propaganda but also for financing, logistics, and recruitment.[60] European governments have struggled to deal with the "dynamic two-way process" wherein engagement with jihadist groups like al-Qaeda

[56] Ninety percent of these products were text-based, 9 percent were videos, and 1 percent were audio and image files. See Daniel Kimmage, *The Al-Qaeda Media Nexus: The Virtual Network Behind the Global Message*, Washington, D.C.: Radio Free Europe/Radio Liberty, March 2008.

[57] Rid and Hecker, 2009, p. 197.

[58] Rid and Hecker, 2009, p. 197; Hoffman, 2004, p. 553.

[59] Yariv Tsfati and Gabriel Weimann, "www.terrorism.com: Terror on the Internet," *Studies in Conflict and Terrorism*, Vol. 25, No. 5, 2011.

[60] For more on the planning aspect of al-Qaeda's media capabilities, see Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" *Parameters*, Vol. 33, No. 1, Spring 2003.

can originate either from an Internet user or the terrorists themselves.[61] As of 2014, the three most important password-protected/access-controlled jihadist websites—*Shumukh al-Islam*, *al-Fida*, and *Ansar al-Mujahideen*—focused almost exclusively on the deteriorating situation in Syria.[62]

Examples of Interesting Al-Qaeda Efforts

Before ISIL was capturing headlines with its beheading videos, al-Qaeda broadcasted the beheading of American journalist Daniel Pearl, and AQI released video of the beheading of hostage Nicholas Berg, which was copied and downloaded more than half a million times in 24 hours.[63] In 2006, al-Qaeda's media distribution wing, known as the Global Islamic Media Front, released the film *Jihad Academy*, which included footage of attacks on U.S. troops, al-Qaeda militants assembling improvised explosive devices, and suicide bombers' martyrdom messages, complete with anti-American and anti-Israeli vitriol.[64]

One innovative way that al-Qaeda approached the IE was by having Zawahiri answer questions submitted to a web forum in December 2008; nearly 2,000 questions were posed. Events like this, even if perceived as publicity stunts, make al-Qaeda seem more relevant to younger generations of aspiring jihadists in an age of new media.

Noteworthy Capability Demonstrations or Practices

Perhaps one of the most noteworthy demonstrations of al-Qaeda's capabilities—and concrete evidence that terrorism can be effective—was the March 2004 attack on a Madrid commuter train that killed 191 people. The decision to attack Spain was a deliberate strategy designed to force Spain's withdrawal from the coalition fighting in Iraq. Three months before the Madrid attack, Global Islamic Media released a four-page "Message to the Spanish People" directing Spanish citizens to convince their government to withdraw its military forces from Iraq. Al-Qaeda explicitly detailed its strategy for physically attacking Western nations while pairing the attacks with an information campaign focused on the injustices committed against Muslims in Iraq.[65] A week after the attack, Spain elected a socialist prime minister who vowed to (and ultimately did) withdraw Spanish troops from Iraq.

Anticipated Developments

As al-Qaeda is further squeezed by ongoing U.S. counterterrorism operations, its media presence has steadily declined. More recently, when al-Qaeda does release an audio-

[61] Rid and Hecker, 2009, p. 197.

[62] Hoffman, 2013, p. 643.

[63] Naya Labi, "Jihad 2.0." *Atlantic Monthly*, July–August 2006.

[64] Seib, 2008, p. 75.

[65] Denning, 2005.

tape, the target is ISIL and not the United States. However, where the United States and its allies fall short of their own ideals, al-Qaeda seeks to exploit these opportunities for its media and propaganda. To date, Abu Ghraib, Guantanamo Bay, and the extraordinary rendition of prisoners, some of whom were waterboarded by the United States, have served as a rallying cry for the group. More recently, inflammatory political rhetoric around the 2016 U.S. presidential election galvanized jihadists worldwide. In early 2016, al-Shabaab released a video of Donald Trump announcing a call to ban Muslims from the United States, juxtaposed with a clip of Anwar al-Awlaki warning Muslims that "the West will eventually turn against its Muslim citizens."[66]

Efforts of Others to Counter Al-Qaeda in the IE and Their Effectiveness

Some scholars, including Yemen and AQAP expert Gregory Johnsen, have argued that the counterterrorism mission has been distracted by too much focus on al-Qaeda propagandists like al-Awlaki, who, at least according to Johnsen, was afforded influence by the Obama administration far beyond his true position as a "midlevel religious functionary." Johnsen went on to point out that far more dangerous individuals should have been a higher priority, including AQAP's leader Nasir al-Wuhayshi, its deputy commander Said Ali al-Shihri, its top religious scholar Adil al-Abab, its chief of military operations Qasim al-Raymi, its bomb-maker Ibrahim al-Asiri, and its leading ideologue Ibrahim Suleiman al-Rubaish.

Lessons from Al-Qaeda Operations in and Through the IE

While the United States and its coalition partners have received high marks for disrupting and dismantling core al-Qaeda based in Pakistan—first by expelling the group from Afghanistan and then by conducting an aggressive drone campaign targeting the organization's leadership—most analysts agree that the West has not been nearly as successful in its quest to counter the narrative proffered by the group. Bruce Hoffman believes that this is due, at least in part, to "our [the West's] failure to effectively counter our enemies' effective use of propaganda and related information operations."[67] As Evan F. Kohlman notes, in countering the media strategies of terrorist groups (al-Qaeda foremost among them), "technological sophistication is no longer a luxury" but instead "a basic survival skill" for law enforcement and intelligence agencies.[68]

[66] Josh Sanburn, "Al-Qaeda Group Uses Donald Trump in Recruitment Video," *Time*, January 2, 2016.

[67] Bruce Hoffman, "Combating Al Qaeda and the Militant Islamic Threat," testimony before the U.S. House of Representatives Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats, and Capabilities, February 16, 2006.

[68] Evan F. Kohlmann, "The Real Online Terrorist Threat," *Foreign Affairs*, Vol. 85, No. 5, 2006, p. 124.

As highlighted in U.S. Army Field Manual 3-24, *Counterinsurgency*, insurgents and terrorists seek to shape the IE by broadcasting suicide attacks and roadside ambushes as a means of inflating perceptions of their capabilities.[69] Counterprogramming should focus less on defending U.S. actions and more on pointing out inconsistencies and contradictions between what al-Qaeda says it believes in and what it actually does or how the group behaves, especially with respect to the murder of Muslim civilians.

Effectiveness of Al-Qaeda Operations in and Through the IE

There is little doubt that the legacy of AQAP propagandist Anwar Al-Awlaki, the American-born, English-speaking ideologue who perfected the ability to preach al-Qaeda's rhetoric over the Internet, lives on today.[70] Al-Awlaki's lectures have inspired several jihadist plots, and he is thought to have communicated directly with Fort Hood shooter Nadal Hassan. Al-Awlaki successfully established a cult of personality that continues to influence and inspire jihadist attacks.

Far more than just another ideologue in the broader jihadist universe, Abu Musab al-Suri through his writings has significantly influenced other high-profile jihadists, including former AQI leader Abu Musab al-Zarqawi and Anwar al-Awlaki, whose YouTube sermons frequently cite al-Suri's teachings. According to the Counter Extremism Project, 88 known extremists in the United States and Europe—including those who have committed acts of terrorism—have had ties to Awlaki.[71]

Moreover, al-Suri's call to arms has not fallen on deaf ears, as evidenced by the 46 incidents of domestic radicalization and recruitment in the United States alone between September 11, 2001, and 2010.[72] Those incidents involved 125 people, with individuals accounting for about half of the cases.[73] The prospect of lone-wolf terrorism on U.S. soil becomes more of a reality with each passing year, as terrorist attacks in Chattanooga, San Bernardino, and Orlando suggest.[74] Al-Suri, al-Awlaki, bin Laden, and Abdullah Azzam have all been identified as al-Qaeda–linked orators with a par-

[69] Headquarters, U.S. Department of the Army, *Insurgencies and Countering Insurgencies*, Field Manual 3-24/Marine Corps Warfighting Publication 3-33.5, Washington, D.C., May 2014.

[70] Haroro J. Ingram and Craig Whiteside, "The Yemen Raid and the Ghost of Anwar al-Awlaki," *The Atlantic*, February 9, 2017.

[71] Scott Shane, Richard Pérez-Peña, and Aurelien Breeden, "'In-Betweeners' Are Part of a Rich Recruiting Pool for Jihadists," *New York Times*, September 22, 2016. See also Counter Extremism Project, *Anwar al-Awlaki's Ties to Extremists*, New York, September 2016.

[72] Toni Johnson, "Threat of Homegrown Islamist Terrorism," backgrounder, Council on Foreign Relations, last updated September 30, 2011.

[73] Brian Michael Jenkins, *Would- Be Warriors: Incidents of Jihadist Radicalization in the United States Since September 11, 2001*, Santa Monica, Calif.: RAND Corporation, OP-292-RC, 2010.

[74] For more on lone-wolf terrorism, see Ramón Spaaij, "The Enigma of Lone Wolf Terrorism: An Assessment," *Studies in Conflict and Terrorism*, Vol. 33, No. 9, September 2010.

ticular gift for deploying propaganda that successfully transforms tacit supporters into active ones willing to engage in acts of political violence.[75]

Al-Qaeda's Vulnerabilities in the IE

Al-Qaeda is vulnerable in the sense that its words and deeds occasionally contradict each other. For example, while claiming to be the protector of Muslims worldwide, many of the civilians killed in the group's attacks in Pakistan, Iraq, and elsewhere have been Muslims (both Sunni and Shia). Moreover, al-Qaeda claims to speak on behalf of a global *ummah*, but the majority of the world's 1 billion Muslims totally disavow violence, murder, and criminality. Another vulnerability is that al-Qaeda often makes threats in its propaganda that are realized only a fraction of the time. For example, the group has repeatedly threatened to deploy a dirty bomb in the United States (Zawahiri has claimed that he purchased suitcase nuclear bombs from former Soviet nuclear scientists), but this threat has proved to be nothing more than an attempt to intimidate U.S. citizens and policymakers. The failure to follow through clearly demonstrates the gap between al-Qaeda's capabilities and the image it seeks to project to its followers and adversaries. In some circles, al-Qaeda's branding has been described as America Online, while ISIL is Google.[76] In other words, al-Qaeda is losing its reputation as the jihadist group most appealing to younger demographics.

Key Takeaways

There are several key takeaways from al-Qaeda's efforts in the IE. First, despite the onslaught of counterterrorism efforts from the world's most powerful military, core al-Qaeda still exists and maintains the ability to transmit messages to its followers. The decentralized nature of al-Qaeda's media operations has allowed it to continue operating, despite the austere conditions of the groups' headquarters in the tribal areas of Pakistan. As such, it seems unrealistic that countering the group's IO will ever be completely successful, and coalition forces have to accept the reality that an insurgent or terrorist group will almost always be able to sustain a modicum of IRCs.

Al-Qaeda's media production is aesthetically sophisticated and demonstrates an understanding of history, though its messages are wide-ranging and sometimes unfocused. But even as core al-Qaeda's propaganda has abated significantly, its franchise groups have filled the void. It is now more appropriate to think of IO in terms of these franchises and affiliates (e.g., AQAP, AQIM, al-Shabaab) rather than al-Qaeda as a monolithic entity. Furthermore, even as the group's propaganda has slowed down, it lives forever on the Internet and continues to influence the next generation of jihad-

[75] Haroro J. Ingram, *Deciphering the Siren Call of Militant Islamist Propaganda: Meaning, Credibility and Behavioural Change*, The Hague, Netherlands: International Centre for Counter-Terrorism, September 2016b.

[76] Josh Kovensky, "ISIS's New Mag Looks Like a New York Glossy—with Pictures of Mutilated Bodies," *New Republic*, August 25, 2014.

ists to carry out and support its platform and objectives. ISIL has clearly learned from, improved on, and surpassed al-Qaeda's tactics, and another group will likely do so after both al-Qaeda and ISIL have faded away.

Deterring, disrupting, or destroying a physical organization does not put an end to the influence a group can have, as evidenced by the popularity of Anwar al-Awlaki, whose YouTube sermons have inspired terrorist attacks long after his death. Media distributed by violent nonstate actors, such as al-Qaeda, can reinforce the group's strategy while also having a more tactical effect.

Capabilities or Practices That the U.S. Army Might Want to Replicate (or Access Through Joint, Interagency, International, or Multinational Efforts)

There are not many applicable lessons for the Army from what al-Qaeda does. After all, it is a global terrorist organization intent on murdering civilians and celebrating these acts. However, al-Qaeda's push to merge media (both its own and also international coverage) with violence has elevated the group far beyond what its capabilities would suggest. Al-Qaeda has harnessed the power of the Internet to increase its reach, ability to recruit, and ability to raise funds. It has effectively infiltrated all corners of the globe and established its brand at the top among Salafi jihadist organizations, although that brand is currently under assault from ISIL.

Other Capabilities or Practices That the U.S. Army Must be Prepared to Contend with

While there are not many al-Qaeda capabilities or practices that the Army might want to replicate, there are a number of issues with which the Army must be prepared to contend. Al-Qaeda, despite losing ground to ISIL, specifically seeks to recruit media savvy youth as it attempts to stay abreast of emerging technologies in the IE. Although the U.S. military has waged a relentless and aggressive kinetic campaign against al-Qaeda and its affiliates, it is crucial to maintain awareness of this group as a persistent and enduring threat and work to maintain political will on the domestic front. The attacks of September 11, 2001, were a spectacular display of al-Qaeda's capability and raised the bar in terms of "propaganda of the deed." The integration of informational and physical power means that this attack continues to resonate with aspiring jihadists and will likely play a role in al-Qaeda's propaganda for the foreseeable future.

Accordingly, there are some vulnerabilities that the Army should be prepared to exploit. First, al-Qaeda's failure to adapt could lead to its further marginalization, particularly among the millennial generation from which it will inevitably seek to recruit. Second, and just as important, al-Qaeda offers an inflexible narrative that is increasingly losing appeal among its target audiences. The narrative was never too compelling to begin with, although the group has benefited from gifted orators, such as Anwar al-Awlaki, whose audio and video recordings live on through YouTube and continue to inspire jihadists.[77] The main lesson here is that deterring or destroying a physical organization does not necessarily put an end to its influence; older, high-quality propaganda preserved on the Internet can continue to circulate for years.

The West in general and the Army more specifically need to work to better understand the complexities and nuance inherent in al-Qaeda's IO. To be sure, al-Qaeda understands Western media much better than the West understands al-Qaeda's approach to the IE.

[77] J. M. Berger, "The Enduring Appeal of Al-Awlaqi's 'Constants on the Path of Jihad,'" *CTC Sentinel*, Vol. 4, No. 10, October 2011. See also Scott Shane, "The Enduring Influence of Anwar al-Awlaki in the Age of the Islamic State," *CTC Sentinel*, Vol. 9, No. 7, July 2016a.

CHAPTER ELEVEN

ISIL/Daesh

Case Summary

Since ISIL stormed through parts of Iraq and Syria in the summer of 2014, the group has cultivated an aura of invincibility among terrorism researchers and policymakers.[1] To be sure, much of what has been said about ISIL amounts to hyperbole: The militants are far from omnipotent, as witnessed by the coalition's recapture of territory in Fallujah, Ramadi, Manbij, and other critical ISIL strongholds. However, one area in which ISIL has indeed lived up to the hype is in its ability to operate in and through the IE. ISIL has been successful in the IE for several reasons. First, information personnel are accorded high levels of prestige or are otherwise well rewarded. Second, the caliphate narrative is incredibly effective, for both unifying the group's operations and messages and providing compelling context for those operations for supporters and potential supporters.[2] Third, the group's major themes are cleanly grouped and tightly focused, which make message discipline easy. The themes are also directly related to several important and diversified subnarratives that specifically target different audiences.

ISIL has taken advantage of social media to disseminate its message and ideology far beyond what al-Qaeda was ever able to achieve.[3] Despite the attention afforded to its execution videos, ISIL actually produces much more material, and on a broader range of topics, than what gets reported in the mainstream media.[4] ISIL propaganda is centered on three major themes. First, ISIL has restored the caliphate, which makes it the only authentic Islamic state in the world and thus worthy of political legitima-

[1] The group is also known pejoratively as Daesh, the Arabic acronym for its former name, the Islamic State in Iraq and Syria.

[2] For a comprehensive account of ISIL media operations, see Craig Whiteside, *Lighting the Path: The Evolution of the Islamic State Media Enterprise (2003–2016)*, The Hague, Netherlands: International Centre for Counter-Terrorism, November 2016.

[3] Bennett Seftel, "What Drives ISIS," *Cipher Brief*, May 5, 2016a.

[4] Aaron Y. Zelin, "Picture or It Didn't Happen: A Snapshot of the Islamic State's Official Media Output," *Perspectives on Terrorism*, Vol. 9, No. 4, 2015.

cy.[5] Second, any existing Islamic entity (state or nonstate) that does not recognize the group's authority qualifies as an apostate and must be vanquished. Finally, ISIL is more capable than al-Qaeda ever was and continues to grow as an organization and an ideology.[6]

Over the course of 2016, however, ISIL media production plummeted, leading some scholars to suggest that the group was in decline.[7] However, even as ISIL has been pushed out of Mosul and Raqqa, it will likely remain highly active and perhaps even increase its reliance on operations in and through the IE.[8]

Background and Overview

ISIL grew out of its predecessor organization, al-Qaeda in the Land of Two Rivers, or AQI, which, itself, was an outgrowth of the group Jamaat al-Tawhid Wal-Jihad, headed by Abu Musab al-Zarqawi.[9] The group currently known as ISIL began metastasizing after the U.S. withdrawal of troops from Iraq in 2011 and continued to rest, rearm, and resupply its ranks until mid-2014, when it began its offensive throughout Iraq.[10] In an effort to build up its operational and organizational capabilities, ISIL took advantage of chaos in neighboring Syria while gaining recruits as a result of the marginalization of Iraqi Sunnis by Iraq's then–Prime Minister Nouri al-Maliki. Under the Maliki administration, sectarianism intensified, pushing Iraqi Sunnis, many of whom were formerly associated with Saddam Hussein's Baath Party, into the arms of ISIL.[11]

[5] Colin P. Clarke and Chad C. Serena, "To Defeat ISIL's Brand, Its Territory Must Be Reclaimed," *National Interest*, July 8, 2016a.

[6] Daveed Gartenstein-Ross, Nathaniel Barr, and Bridget Moreng, "How the Islamic State's Propaganda Feeds into Its Global Expansion Efforts," *War on the Rocks*, April 28, 2016b.

[7] Charlie Winter and Colin P. Clarke, "Is ISIS Breaking Apart? What Its Media Operations Suggest," *Foreign Affairs*, January 31, 2017.

[8] Joseph L. Votel, Christina Bembenek, Charles Hans, Jeffrey Mouton, and Amanda Spencer, "#VirtualCaliphate: Defeating ISIL on the Physical Battlefield Is Not Enough," Washington, D.C.: Center for a New American Security, January 12, 2017. See also Charlie Winter, *Media Jihad: The Islamic State's Doctrine for Information Warfare*, London: International Centre for the Study of Radicalisation and Political Violence, February 2017.

[9] Between its AQI and ISIL classifications, the group was alternatively known as Majlis Shura al-Mujahedin and the Islamic State of Iraq. See Aaron Y. Zelin, "The War Between ISIS and al-Qaeda for Supremacy of the Global Jihadist Movement," Washington, D.C.: Washington Institute for Near East Policy, Research Note 20, June 2014, p. 1.

[10] William Young, David Stebbens, Bryan Frederick, and Omar Al-Shahery, *Spillover from the Conflict in Syria: An Assessment of the Factors that Aid and Impede the Spread of Violence*, Santa Monica, Calif.: RAND Corporation, RR-609-OSD, 2014.

[11] Tim Arango, "Uneasy Alliance Gives Insurgents an Edge in Iraq," *New York Times*, June 18, 2014. See also Anthony H. Cordesman, "The Real Center of Gravity in the War Against the Islamic State," Washington, D.C.: Center for Strategic and International Studies, September 30, 2014.

Current religious conflicts are strengthening rather than abating as the Sunni-Shia schism and ISIL's rise have increased extremism and religious polarization worldwide. As bin Laden's contemporaries who went to Afghanistan became the core of al-Qaeda a decade later, the current generation of youth now being radicalized by ISIL (and other flavors of extremism) will dominate the Sunni extremist scene for the immediate future. U.S. government officials and terrorism experts have argued that the campaign against ISIL is unlikely to be resolved quickly.[12] And several recent and current U.S. commanding generals agree with former President Obama's assertion that the fight against ISIL is best measured in decades, not years.[13]

Concepts and Principles for Operations in and Through the IE

Of all the messages propagated by ISIL, the establishment and implementation of the caliphate is a unique selling point, as it retains historical and religious resonance for the broader Muslim *ummah* and harkens back to Islam's Golden Age.[14] ISIL attempts to communicate to all its potential recruits the core narrative that its caliphate is a triumphant, model society.[15] The group's slogan is "Baqiya wa Tatamaddad" ["Remaining and Expanding"]. Rather than living under apostate regimes in the Middle East or morally bankrupt societies in Western nations, Muslims who join ISIL can enjoy an ideal Islamic community, and those who resist this call will be vanquished. This vision is furthered by videos that focus on the caliphate as a benevolent state committed to public works and Islamic welfare.[16]

[12] White House Office of the Press Secretary, "Statement by the President on ISIL," September 10, 2014; White House Office of the Press Secretary, "Remarks by the President on Progress in the Fight Against ISIL," July 6, 2015. For more background on ISIL, see Charles Lister, *The Islamic State: A Brief Introduction*, Washington, D.C.: Brookings Institution, 2015; William McCants, *The ISIS Apocalypse: The History, Strategy and Doomsday Vision of the Islamic State*, New York: St. Martin's Press, 2015; Hassan Hassan and Michael Weiss, *ISIS: Inside the Army of Terror*, New York: Simon and Schuster, 2015; Jessica Stern and J. M. Berger, *ISIS: The State of Terror*, New York: HarperCollins, 2015a; Patrick Cockburn, *The Rise of Islamic State: ISIS and the New Sunni Revolution*, London: Verso Books, 2015; and Howard J. Shatz and Erin-Elizabeth Johnson, *The Islamic State We Knew: Insights Before the Resurgence and Their Implications*, Santa Monica, Calif.: RAND Corporation, RR-1267-OSD, 2015, pp. 11–15.

[13] Dan De Luce, "Is the U.S. Ready for Endless War Against the Islamic State?" *Foreign Policy*, August 27, 2015. See also Courtney Coren, "Gen. Hayden: Panetta Right, Fighting ISIS Will Take 'Generation Plus,'" *Newsmax*, October 6, 2014, and Anthony Cordesman, "Paris, ISIS, and the Long War Against Extremism," Washington, D.C.: Center for Strategic and International Studies, November 14, 2015.

[14] Charlie Winter, *The Virtual "Caliphate": Understanding Islamic State's Propaganda Strategy*, London: Quilliam Foundation, July 2015b, p. 28.

[15] Charlie Winter and Jordan Bach-Lombardo, "Why ISIS Propaganda Works," *The Atlantic*, February 13, 2016.

[16] Greg Miller and Souad Mekhennet, "Inside the Surreal World of the Islamic State's Propaganda Machine," *Washington Post*, November 20, 2015.

Strategic Goals/Vision: Promoting the Caliphate

While Western media tends to focus on ISIL videos showing gruesome executions, the majority of ISIL output is focused on far less brutal pursuits and includes videos showing fighters singing and drinking tea together in an attempt to highlight the camaraderie that attracts so many recruits to the organization in the first place.[17] Moreover, ISIL IO output has spanned a vast geographic expanse—at its peak, the caliphate maintained a network of 48 official media offices and nine additional centrally administered outlets—and rarely went off message while sustaining a high level of message discipline. In this way, it was able to transmit a carefully constructed narrative of the caliphate as triumphant, defiant, and representative of the broader *ummah*.[18]

Targets and Audiences

ISIL attempts to fit its information efforts with its overall strategic goals by tailoring messages to several specific and distinct audiences to achieve maximum effect: current and potential opponents, international publics, active ISIL members, potential recruits, disseminators, proselytizers, and enlisters.[19] Beyond these specific target audiences, ISIL shapes its messages to encourage foreign fighters and add manpower to the group's ranks, to inspire militant jihadists to join the fight in Iraq and Syria, and—for those who are unable to join the fighting—to take action where they can. Finally, the group attempts to appeal to "fence-sitters" in ISIL-occupied territory whose cooperation is necessary for maintaining control in those areas.[20]

A significant target audience for ISIL propaganda is the foreign fighter contingent that ISIL seeks to attract to its organization. By 2016, thousands of fighters had flocked to join the group, emboldened by its string of military victories and a media campaign unrivaled in its sophistication, technical prowess, and reach. Estimates vary widely, but Chairman of the Joint Chiefs of Staff Joseph Dunford stated in late 2017 that "as many as 40,000 foreign fighters from 120 different countries" had gone to fight with ISIL in Syria and Iraq, making it the most significant transnational jihadist conflict of all time.[21] Fighters have traveled from far afield, including the United States, various European countries, Australia, and even countries not normally associated with global

[17] Charlie Winter, "Islamic State Propaganda: Key Elements of the Group's Messaging," *Jamestown Terrorism Monitor*, Vol. 13, No. 12, June 12, 2015a.

[18] ISIL maintains one media office in each self-declared "province" (19 in Syria and Iraq, seven in Yemen, three in Libya, and various others corresponding to its footholds in additional countries). Winter and Bach-Lombardo, 2016.

[19] Winter, 2015b, pp. 33–40.

[20] Eric T. Olson, "War of Ideas: From the Taliban to the Islamic State," *War on the Rocks*, January 6, 2016.

[21] Ryan Browne and Barbara Starr, "U.S. Military Official: 50 ISIS Foreign Fighters Captured Since November," CNN, December 12, 2017.

jihad, such as Chile and Cambodia. In August 2016, ISIL released a slickly produced video, complete with special effects, aimed at recruiting Kurds into its organization.[22]

ISIL also targets specific demographics, such as millennials.[23] In a 2016 video, the group presented a fictional story with a plot and characters to promote a narrative of personal ideological awakening. In the video, a man in his early 20s named Mohammed is living in Raqqa and grows distraught over continued U.S. airstrikes and the resulting destruction. When Mohammed discovers an ISIL combat video online, he is convinced to join the group that he believes is the only organization willing and able to defend innocent Muslims against the wanton slaughter of civilians by the West.[24]

Foundational Principles

Improving upon the media capabilities of its predecessor, al-Qaeda, ISIL produces consistently high-quality propaganda, exhibiting an in-depth knowledge of the qualities that appeal to modern audiences: graphics packages, clarity of images, frame composition, camera angles, lighting, editing, effects, and pre-/post-production work.[25] Furthermore, ISIL media production is extremely well organized and productive. A study of a single week's output found 123 media releases in six languages, 24 of them videos.[26] Another study identified 1,146 distinct pieces of propaganda in a month.[27] ISIL takes extreme care in producing its videos, which are staged and scripted, with militants performing multiple takes and even reading lines directly from cue cards to make sure that messaging remains consistent.

History and Evolution

As the civil war in Syria escalated in 2013, the organization's propaganda evolved considerably. Among the changes were a newfound focus on Syria, high production values, and a social media outreach campaign targeting Muslims and other audiences beyond the Arabic-speaking Middle East and North Africa. The 49-episode video series *Windows Upon the Land of Epic Battles*, which gained prominence between April 2013 and February 2014, reflects this evolution.[28]

[22] Mohammad A. Salih, "How Islamic State Is Trying to Lure Kurds into Its Ranks," *Al-Monitor*, August 12, 2016.

[23] Anthony Faiola and Souad Mekhennet, "What's Happening to Our Children?" *Washington Post*, February 11, 2017.

[24] Shane Dixon Kavanaugh and Gilad Shiloach, "ISIS Latest Recruiting Film Targets Sensitive Milennials," *Vocativ*, July 12, 2016.

[25] Cori E. Dauber and Mark Robinson, "ISIS and the Hollywood Visual Style," *Jihadology*, July 6, 2015.

[26] "Islamic State: The Propaganda War," *The Economist*, April 15, 2015.

[27] Miller and Mekhennet, 2015.

[28] Alberto M. Fernandez, *Here to Stay and Growing: Combating ISIS Propaganda Networks*, Washington, D.C.: Brookings Project on U.S. Relations with the Islamic World, October 2015.

ISIL Operations in and Through the IE

Despite the barbarity of some of its propaganda videos, violence is far from the only theme that ISIL emphasizes in its messaging. ISIL does attempt to "win hearts and minds" and shows images of otherwise mundane civilian life, offering nuanced discussions surrounding the concept of mercy and highlighting the camaraderie of its members, which is critical for recruitment. Videos show such banal activities as the construction of public markets, religious police on neighborhood patrols, and citizens fishing with their friends and families. Other information-related lines of effort focus on military acumen, counternarratives, religious duties, systems of meaning, and "baiting" as a strategy. It should be noted that while ISIL dedicates much of its propaganda bandwidth to promoting its governance apparatus as multidimensional, sophisticated, and well resourced, there is little doubt that violence is instrumental to strengthening and building the brand. Moreover, not only does ISIL distribute its own messages, but it also blocks Internet access and mobile phone networks in the territory it controls, eliminating other sources of information in the process.[29]

Structure

To disseminate its message, ISIL relies on several central media units, provincial information offices, and a broad support base. The organization's al-Hayat Media Center produces a range of print publications (including *Dabiq* and *Rumiyah*) and videos (e.g., *Flames of War*) in several languages, while its al-Furqan Media division releases statements from ISIL senior leaders and produces other videos (e.g., *Clanging of Swords*). The group's al-Itisam Media division produces Arabic-language content and videos similar in style and format to those produced by al-Hayat Media Center, and its Ajnad Media Foundation produces recitations of *suras* (Quranic verses) and *nasheeds* (hymns). ISIS also relies on an unofficial wire service, the Amaq News Agency, to disseminate its messages.[30]

Amaq has emerged as the go-to source for ISIL claims of responsibility after attacks. And language itself is important. The precise wording used by Amaq can help analysts decipher the group's role in an attack—whether it was likely directly involved, as in the coordinated bombings and shootings in Paris in November 2015 and the March 2016 bombings at the airport and a metro station in Brussels, or merely served as the inspiration for an attack.[31]

[29] Brendan I. Koerner, "#Jihad: Why ISIS Is Winning the Social Media War," *Wired*, March 30, 2016.

[30] Rukmini Callimachi, "A News Agency with Scoops Directly from ISIS, and a Veneer of Objectivity," *New York Times*, January 14, 2016a.

[31] Max Bearak, "When ISIS Claims Terrorist Attacks, It's Worth Reading Closely," *Washington Post*, July 26, 2016. See also Charlie Winter and Haroro J. Ingram, "How ISIS Weaponized the Media After Orlando," *The Atlantic*, June 17, 2016. For more on the different types of ISIS attacks, see Clint Watts, "Inspired, Networked and Directed—The Muddled Jihad of ISIS and Al Qaeda Post Hebdo," *War on the Rocks*, January 12, 2015.

As mentioned, there are three distinct levels to the ISIL media architecture: central media units, provincial information offices, and the broader support base. Provincial information offices produce the bulk of ISIL output and focus on local and regional events, while the group's support base uses social media to amplify its "'unofficial' messaging."[32] This structure allows ISIL to synchronize its information efforts with politico-military action and to use propaganda as the central strategic mechanism to frame its politico-military activities. For example, after the group's June 2014 capture of Mosul, ISIL chief spokesman Abu Muhammad Al-Adnani released a statement detailing a new phase in the group's military strategy to coincide with the victory. In this way, ISIL is able to uphold its reputation as an accountable and transparent authority.

There is disagreement over exactly how much autonomy the regional or provincial media offices have, with some analysts speculating that these offices have free reign to distribute ISIL propaganda,[33] while others insist that all messages must receive approval from the Ministry of Media prior to release.[34] It seems more likely that the provincial offices have gained more autonomy over time, given the volume and speed with which ISIL propaganda is produced. The provincial media offices manage mobile kiosks, or "media points," that distribute ISIL propaganda to newly conquered territory on flash drives and SIM cards.

Funding

While there are no figures available for what ISIL spends on its information and propaganda activities, there have been reports that its media operatives are paid roughly seven times as much as the average fighter.[35] This is an important lesson for the U.S. Army, because it demonstrates exactly how highly ISIL values its information specialists. According to a report by the Combating Terrorism Center at West Point, "it is clear that the group invests heavily in this area," referring to the group's reliance on information-related efforts.[36]

Key Leaders

There is no central ISIL propagandist, although the group's spokesman was Abu Muhammad al-Adnani until he was killed in an airstrike in Syria in late August 2016.

[32] Haroro J. Ingram, "The Strategic Logic of Islamic State Information Operations," *Australian Journal of International Affairs*, Vol. 69, No. 6, 2015.

[33] Koerner, 2016.

[34] Daniel Milton, "The Islamic State: An Adaptive Organization Facing Increasing Challenges," in Muhammad al-Ubaydi, Nelly Lahoud, Daniel Milton, and Bryan Price, eds., *The Group That Calls Itself a State: Understanding the Evolution and Challenges of the Islamic State*, West Point, N.Y.: United States Military Academy, Combating Terrorism Center, December 2014, p. 49.

[35] Koerner, 2016.

[36] Milton, 2014, p. 47.

Adnani was an extremely important figure within the ISIL propaganda architecture; he was responsible for convening a monthly shura with other senior ISIL leaders to decide which videos would be featured as official ISIL content to resonate with recent battlefield developments.[37] Adnani was also responsible for the group's exhortation for Muslims to kill Westerners, or "infidels," during Ramadan—a call that was heeded by many during the particularly bloody summer of 2016.[38] One ISIL fighter who gained notoriety through the group's propaganda was "Jihadi John," also known as Mohammed Emwazi, the British-born jihadist who starred in several ISIL beheading videos prior to his death in November 2015.

Functional/Organizational Divisions

In July 2016, ISIL released a video outlining the structure of the caliphate.[39] While the organization is constantly in flux, Figure 11.1 depicts the ISIL media landscape.

IRCs Employed/Available

Most of what ISIL does seem to fit most accurately under the rubric of media production or propaganda for influence. However, ISIL is also acutely aware of OPSEC, even producing a 34-page guide that its members must consult before conducting certain operations.[40] While ISIL does not boast EW capabilities, there are reports that its members have used the dark web to fundraise and recruit.[41] The group does maintain a nascent hacking capability calling itself the United Cyber Caliphate, though no known major actions have been attributed to it.[42]

In an example of physical capabilities doubling as IRCs, ISIL also seeks to censor and control information within the territory it controls by destroying satellite dishes and restricting Internet access.[43] Furthermore, ISIL is using myriad digital products to mask its online activity—from secure browsers (Tor Browser, Opera) to virtual private networks and proxy servers (F-Secure Freedome, CyberGhost VPN), along with protected email services (Hushmail, ProtonMail, YOPmail, Tutanota), mobile security

[37] Rukmini Callimachi, "How a Secretive Branch of ISIS Built a Global Network of Killers," *New York Times*, August 3, 2016b.

[38] Ben Hubbard, "ISIS Uses Ramadan as Call for New Terrorist Attacks," *New York Times*, July 3, 2016; Zachary Laub and Rukmini Callimachi, "The Islamic State's Bloody Summer," Council on Foreign Relations, August 3, 2016.

[39] Jack Moore, "ISIS Releases New Video Outlining the Structure of the Caliphate," *Newsweek*, July 7, 2016b.

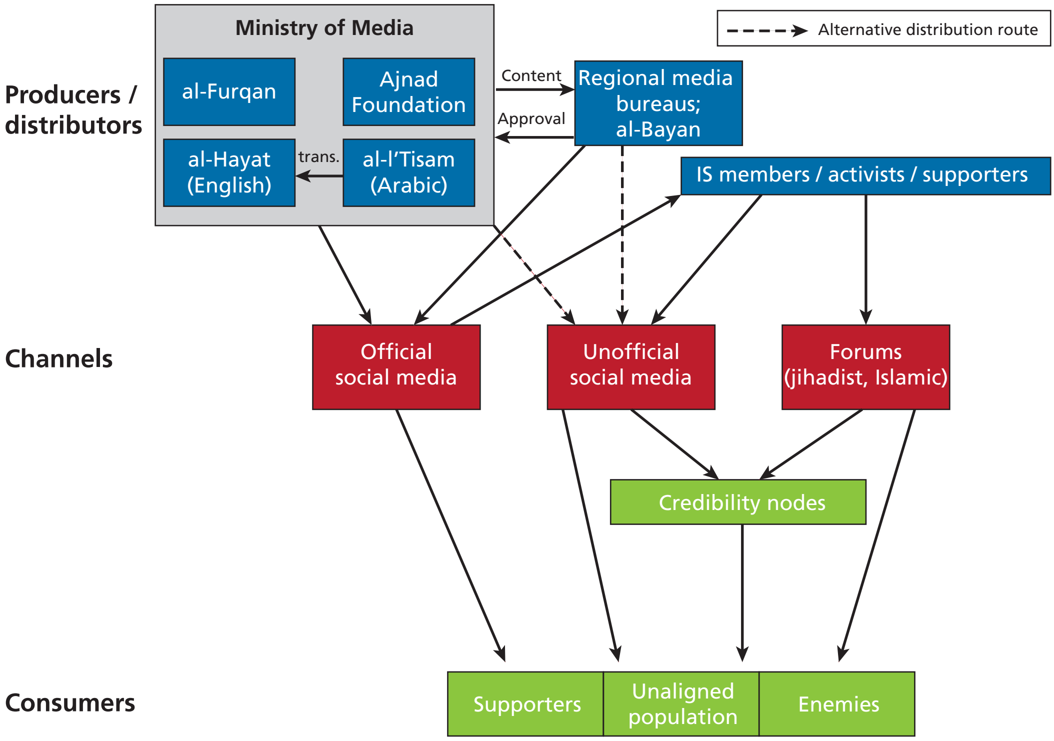
[40] Kim Zetter, "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits," *Wired*, November 19, 2015.

[41] Colin P. Clarke and Isaac R. Porche III, "The Online Fight Against ISIS," *Project Syndicate*, April 1, 2016.

[42] Gilad Shiloach, "ISIS Hackers Respond to U.S. Cyberattacks with Threats," *Vocativ*, April 27, 2016.

[43] J. M. Berger, "The Decapitation Will Not Be Televised," *Foreign Policy*, July 3, 2016. See also Pamela Engel, "How ISIS Monitors and Restricts Internet Access in the Caliphate," *Business Insider*, November 7, 2015, and Maayan Groisman, "ISIS Destroys Syrian Satellite Dishes in Bid to Ban 'Un-Islamic' TV During Ramadan," *Jerusalem Post*, June 2, 2016.

Figure 11.1
The ISIL Media Landscape



SOURCE: Milton, 2014, p. 49.
RAND *RR1925z2-11.1*

apps (automatic lockout/data destruction apps, Fake GPS, D-Vasive Pro, iShredder Pro, Hide.me, DNSCrypt, NetGuard, AFWall), and encrypted messaging apps (Telegram, Threema).[44]

ISIL produces high-quality, timely products in multiple languages to fit the narrative the group seeks to convey to a given target audience.[45] *Dabiq*, one of the group's main propaganda products, outlined the organization's goals and provided updates of its activities and how those activities tied directly to its objectives, while also showcasing personal stories of its fighters and announcing major developments in its struggle against an array of adversaries.[46] ISIL efforts in and through the IE and the release of

[44] Laith Alkhouri and Alex Kassirer, *Tech for Jihad: Dissecting Jihadists' Digital Toolbox*, New York: Flashpoint, July 2016.

[45] Milton, 2014, p. 47.

[46] William McCants and Clint Watts, "Why the U.S. Can't Make a Magazine Like ISIS," *Daily Beast*, January 11, 2016. Dabiq appears to have ceased publication in mid-2016; in its place, ISIL has been releasing a similarly glossy magazine-style publication, *Rumiyah*.

specific media are deliberately timed and coordinated to coincide with military operations, demonstrating the group's keen understanding of politico-military strategy and the force-multiplying effects of coordinating the kinetic and nonkinetic aspects of its operations.

Organizations/Functions Considered Wholly Part of Efforts in the IE

In an example of cyber, PA, and inform, influence, and persuade capabilities, the ISIL media enterprise boasts more than 100 operatives and consists of hackers, engineers, and other recruits with prior experience in media, production, or technology. Recruits without such experience undergo a special month-long training program. It is important to note that senior media operatives are given the title "emir," making them equal in rank to their military counterparts. According to Greg Miller and Souad Mekhennet, "videographers, producers and editors" are all part of a "privileged, professional class with status, salaries and living arrangements that are the envy of ordinary fighters."[47] In August 2016, ISIL released images of its media team, which included a dozen color profile portraits of members of its upper echelon for media affairs. In October of that year, the ISIL media chief Abu Mohammed al-Furqan was killed, a loss widely lamented by ISIL supporters on social media.[48] The message is clear: Information is given the same priority as battlefield acumen.

Coordination/Integration Efforts/Challenges

From an organizational perspective, ISIL faces an array of challenges to IO. First, the group is under near-constant siege from coalition airstrikes, meaning it must devote a significant amount of its resources to survival, first and foremost. Second, as the group is pushed out of some territories and seeks to gain a foothold in others—including Libya, the Sinai Peninsula, and parts of South and Southeast Asia—it must coordinate with provincial offices across vast distances. However, among violent nonstate actors, ISIL has mastered the integration of its physical and information-related activities, becoming what Jared Cohen has called "the first terrorist group to hold both physical and digital territory."[49]

Overall, the lion's share of ISIL messaging is directed toward regional, not global, audiences.[50] Developing targeted messages is challenging because those that appeal to the global jihad might not resonate with a local audience in Libya, for example, or vice

[47] Miller and Mekhennet, 2015.

[48] Jack Moore, "ISIS Confirms Death of Media Emir Abu Mohammed al-Furqan," *Newsweek*, October 11, 2016c.

[49] Emerson T. Brooking and P. W. Singer, "War Goes Viral," *The Atlantic*, November 2016.

[50] Chris Galloway, "Media Jihad: What PR Can Learn in Islamic State's Public Relations Masterclass," *Public Relations Review*, Vol. 42, No. 4, November 2016.

versa.[51] Similarly, it is difficult to deconflict messaging between the core organization in Iraq and Syria and affiliates in its outlying provinces. At the time of this writing, ISIL was losing key terrain in both Iraq and Syria, as well as in some of the countries where its franchise groups were anchored. But even as these affiliated groups released messages proclaiming their staying power and desire to continue to hold territory, ISIL chief spokesman Abu Muhamman al-Adnani (since killed in an airstrike) released his own—and somewhat contradictory—message downplaying the importance of territory and suggesting that the group's plan all along had been to revert to its roots as a guerrilla insurgency.[52] As it becomes more difficult to maintain the organization as a coherent entity, fracturing and splintering will likely give way to mixed messaging and an inability to effectively integrate IRCs across vast distances.[53]

Information Operations in Practice

As recent videos on the Saudi-led Islamic alliance against terrorism, various attacks in Europe, and the refugee crisis demonstrate, if the "base foundation"—akin to corporate headquarters—issues a communiqué, its provincial offices are on standby to respond. ISIL practices information coordination and integration with tactical effect and is unencumbered by the panoply of restraints faced by Western governments and militaries. ISIL understands its audience well and has been able to position itself in opposition to the West as a group with countercultural appeal, so-called jihadi cool.[54]

Examples of Interesting Efforts

ISIL propaganda efforts incorporate roughly a dozen distinct messages that make up the core of the group's branding strategy: brutality/violence, mercy, victimhood, war, camaraderie and belonging, the caliphate as utopia, a winner's message, discrediting the competition, sowing discord in enemy ranks, the illegitimacy of Islamist politics, exploiting sectarian tensions, driving a wedge between Muslims and the West, and, finally, the religious obligation to join the caliphate.[55]

[51] Brian Michael Jenkins and Colin P. Clarke, "In the Event of the Islamic State's Unlikely Demise," *Foreign Policy*, May 11, 2016.

[52] Eric Schmitt, "As ISIS Loses Land, It Gains Ground in Overseas Terror," *New York Times*, July 3, 2016.

[53] Colin P. Clarke and Chad C. Serena, "This Is the Problem with Trying to Destroy the Islamic State," *Washington Post Monkey Cage Blog*, July 12, 2016.

[54] Simon Cottee, "The Challenge of Jihadi Cool: Why ISIS Propaganda Is So Popular," *The Atlantic*, December 24, 2015.

[55] Winter, 2015b; Daveed Gartenstein-Ross, Nathaniel Barr, and Bridget Moreng, *The Islamic State's Global Propaganda Strategy*, The Hague, Netherlands: International Center for Counter Terrorism, March 2016a.

The videos focused on brutality and violence are by now well known, with demonstrations of alleged spies being executed to send the message that defectors or traitors inside the group will meet a similar fate. The theme of mercy is meant to show the organization's pragmatic side. In April 2015, a video titled "From the Darkness to the Light" showed fighters from Nusra, the Free Syrian Army, and the Syrian Arab Army joining ISIL, which was portrayed as benevolent for taking in those who had once fought against it.

Victimhood is a theme that ISIL cultivates in an attempt to appeal to Muslims around the world. For example, it accompanies messages that Muslim civilians, including women and children, are frequently the victims of coalition airstrikes with images of dead and dying children. War is another obvious theme—one celebrated in videos of ISIL fighters battling bravely, clad in matching uniforms, with the intent of showing the group as a real military of professional fighters (in contrast to other militants, who are often regarded as rag-tag militias). Belonging, or finding camaraderie with fellow Muslims, is yet another ISIL theme. Videos of ISIL fighters singing together are meant to appeal to potential recruits by showing them what they are missing by eschewing the group's clarion call to arms. Finally, utopianism is an overarching theme of ISIL IO, with ubiquitous eschatological allusions and references to Armageddon.

Noteworthy Capability Demonstrations or Practices

To spread its messages through informal channels, ISIL relies on a range of social media platforms, including Twitter and Facebook, as well as peer-to-peer messaging apps, such as Telegram and Surespot, and content-sharing systems like JustPaste.it.[56] At various points, the group's provincial branches have maintained official media pages on VKontakte, a well-known and widely used Russian social media site. In some cases, ISIL fighters have strapped GoPro cameras to their heads during combat to simulate first-person shooter videogames.[57] The group has even produced a trailer for its own version of such a game based on *Grand Theft Auto*.[58] It has also designed an app for children on the Android smartphone operating system and has used its news agency, Amaq, to push its plugin for Firefox web browsers.[59]

Efforts of Others to Counter ISIL in the IE and Their Effectiveness

One current effort to counter ISIL efforts in the IE is the Counter Extremism Project, working in concert with Dartmouth University computer scientist Hany Farid and funded in part by Microsoft. The project uses robust hashing, a method of machine

[56] Koerner, 2016.

[57] Berger, 2016.

[58] Ahmed al-Rawi, "Video Games, Terrorism and ISIS's Jihad 3.0," *Terrorism and Political Violence*, August 5, 2016.

[59] Caleb Weiss, "Islamic State Launches Mobile App for Children," *Threat Matrix*, May 11, 2016.

learning that attempts to teach software to recognize images deemed offensive (in this case, ISIL beheadings or other grisly productions) and flag them for immediate removal from the Internet. The project is based on a similar effort to prevent the spread of child pornography and will be distributed to Twitter, Facebook, Google, and other technology companies to stop the distribution of terrorist propaganda online.[60]

Both the U.S. State Department and the U.S. Department of Homeland Security are working to counter ISIL propaganda by identifying individuals who present as credible voices and reach out to those at risk of being radicalized. The State Department tripled the initiative's funding to $16 million in 2016 because its previous efforts were widely lambasted and ridiculed as ineffective. It's strategy includes using Facebook videos, Instagram ads, and other social media designed to convince potential ISIL recruits that joining the group will destroy their families; these emotional appeals stand in contrast to earlier efforts that were characterized as "snarky" and at risk of backfiring.[61] The U.S. Department of Homeland Security recently launched the Countering Violent Extremism Grant Program with $10 million in funding for state and local governments, nonprofit organizations, and educational institutions. It has also been working with about 150 colleges and universities on counter-messaging campaigns.[62]

In 2016, coalition forces dropped leaflets over the ISIL capital of Raqqa with directions for civilians to flee the city, leaving ISIL fighters to wonder whether an imminent assault was being planned.[63] (A Pentagon official admitted that no such operation was forthcoming and that the campaign was an attempt to manipulate ISIL fighters.) Overall, efforts by the coalition to counter ISIL messaging activities have been characterized as "tentative and ineffective."[64] That is not to say that there have been no successes, however. British special forces launched an EW attack against ISIL fighters in Libya, successfully jamming the group's communication network in Sirte, then monitoring the militants' subsequent chatter as they attempted to figure out what just happened. The EW attack was spearheaded by the crew of a Royal Air Force Rivet Joint spy plane.[65]

In the spring of 2016, the United States launched its own campaign to disrupt the group's ability to spread its message, attract recruits, circulate orders from its leader-

[60] Patrick Tucker, "How to Stop the Next Viral Jihadi Video," *Defense One*, June 17, 2016.

[61] Helene Cooper, "U.S. Drops Snark in Favor of Emotion to Undercut Extremists," *New York Times*, July 28, 2016.

[62] Jeff Seldin, "U.S. in 'Crisis Mode' in Fight Against IS Online Messaging," *Voice of America*, July 6, 2016.

[63] Natasha Bertrand, "The U.S.-Led Coalition Is Dropping These Leaflets on ISIS' Capital in Syria to 'Mess with Them,'" *Business Insider*, May 21, 2016.

[64] Haroro J. Ingram, "How to Beat Back ISIS Propaganda," *National Interest*, June 15, 2016a.

[65] Mark Nicol, "UK Special Forces Launch 'Black Ops' Assault on ISIS Using Electronic Warfare to Cripple Jihadists' Communications," *Daily Mail*, May 14, 2016.

ships, and execute critical human resource–type functions, such as paying the salaries of its fighters.[66]

Lessons from ISIL Operations in and Through the IE

There is much to learn from ISIL IO and how these operations nest within the group's overall approach in the IE. The structure and flexibility of ISIL messaging allows the group to respond quickly to situations as they develop on the ground. Furthermore, ISIL messaging platforms are decentralized, blending reactive and proactive responses while fiercely protecting the ISIL brand by attacking its rivals, such as al-Qaeda. Finally, ISIL messaging is not risk averse, and the group seems willing to lose adherents in the process of shaping its brand. ISIL terrorism also takes advantage of the Western media's 24/7 news cycle so that even hours, days, or weeks after an initial attack, the "propaganda of the deed" is being replayed endlessly and analyzed ad nauseam.[67]

Effectiveness of ISIL Operations in the IE

If measured simply by the attention the group has garnered, ISIL IRCs would be considered successful by most standards. Indeed, ISIL continued to attract foreign fighters to its ranks, even while the coalition reclaimed territory from the group in both Syria and Iraq. However, reports at the time of this writing indicated a potential reversal of this trend as many of these fighters returned to their home countries.[68]

ISIL messaging is characterized by reach, relevance, and resonance. *Reach* is a message's ability to access its target audiences, *relevance* relates to the timeliness of messages and their relative sociocultural and situational significance, and *resonance* refers to the ability to influence perceptions.[69] By late 2016, ISIL messaging had declined sharply. At its peak in August 2015, ISIL was pushing out approximately 700 items per day from its official outlets, a number that had dropped to around 200 per day as of October 2016.[70] But even as this decline in media production is a positive sign for the coalition forces arrayed against the militants, individuals who were influenced during

[66] David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat," *New York Times*, April 24, 2016.

[67] Charlie Winter, "ISIS Is Using the Media Against Itself," *The Atlantic*, March 23, 2016.

[68] Christopher Woody and Mike Nudelman, "Here's How Many Foreign ISIS Fighters Have Returned Home from the Battlefield," *Business Insider*, October 26, 2017.

[69] Haroro J. Ingram, "Three Traits of the Islamic State's Information Warfare," *RUSI Journal*, Vol. 159, No. 6, December 2014.

[70] Scott Shane, "ISIS Media Output Drops as Military Pressure Rises, Report Says," *New York Times*, October 10, 2016b. See also Daniel Milton, *Communication Breakdown: Unraveling the Islamic State's Media Efforts*, West Point, N.Y.: United States Military Academy, Combating Terrorism Center, October 2016.

the earlier high-production period are unlikely to change their minds about fighting for ISIL simply because the frequency of video releases has decreased.

Vulnerabilities of ISIL in the IE

ISIL messaging is vulnerable due to its overreliance on social media. As a result of coalition efforts, especially those of the U.S. government, counter-ISIL messages and products are more prolific now than ever before; the quantity of counterpropaganda is snowballing, and social media giants, such as Twitter, are becoming more aggressive in their efforts to hobble ISIL propagandists. A significant step would be to work more consistently across the government (i.e., to take a whole-of-government approach) to ensure unity of effort and the consistency of messages in these campaigns. In 2016, the U.S. State Department restructured its own counterpropaganda apparatus, creating the Global Engagement Center to "more effectively coordinate, integrate and synchronize messaging to foreign audiences that undermines the disinformation espoused by violent extremist groups, including ISIL and al-Qaeda."[71]

J. M Berger and Jessica Stern have pointed out several important vulnerabilities that the coalition should seek to exploit. They recommended the following actions to reduce the effectiveness of ISIL propaganda: Stop exaggerating the group's invincibility, amplify the stories of ISIL family members and defectors, take on the group's version of Islam, highlight the group's hypocrisy and publicize its atrocities against Sunnis, and aggressively suspend ISIL-connected social media accounts.[72] This last recommendation—to suspend the group's social media accounts—dovetails with a finding by Berger and Morgan that "[ISIL's] social media success can be attributed to a relatively small group of hyperactive users, numbering between 500 and 2,000 accounts, which tweet in concentrated bursts of high volume."[73]

Between June and October 2015, Twitter suspended or deleted the accounts of more than 125,000 ISIL sympathizers and members.[74] An August 2016 RAND report noted that if Twitter continued its campaign of account suspensions, this harassment could cost ISIL supporters valuable time reacquiring followers and could ultimately push some to use social media channels that are far less public and accessible than Twitter.[75]

[71] Winter and Bach-Lombardo, 2016.

[72] Jessica Stern and J. M. Berger, "A 6-Point Plan to Defeat ISIS in the Propaganda War," *Time*, March 30, 2015b.

[73] J. M. Berger and Jonathon Morgan, *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*, Washington, D.C.: Brookings Project on U.S. Relations with the Islamic World, March 2015.

[74] Jack Moore, "ISIS's Twitter Campaign Faltering Amid Crackdown," *Newsweek*, February 18, 2016a. See also "Islamic State Finds Diminishing Returns on Twitter: Report," Reuters, February 18, 2016.

[75] Elizabeth Bodine-Baron, Todd Helmus, Madeline Magnuson, and Zev Winkelman, *Examining ISIS Support and Opposition Networks on Twitter*, Santa Monica, Calif.: RAND Corporation, RR-1328-RC, 2016. Still,

ISIL Efforts in the IE in Contrast with U.S. IO

In contrast to U.S. IO, ISIL has several advantages. First, its output need not be truthful, just timely; ISIL has an operational need to maintain the offensive in reaching out to its followers while attempting to intimidate its adversaries. In addition, ISIL IO is highly decentralized, with responsibility for output pushed down to the lowest levels, where operatives are trusted to act responsibility while producing content that remains consonant with the ISIL brand.

Key Takeaways

One of the advantages of the decentralized model for ISIL messaging is that technical deconfliction is less of an issue than it is for U.S. IO. The same is true for content deconfliction, mostly due to the group's adherence to simple, universal themes, such as its vision and promotion of the caliphate. For ISIL, the caliphate is not only its ultimate objective but also an intermediate selling point and a subordinate objective, tying it to the group's supporting narrative. The caliphate is used to recruit members and to differentiate ISIL from al Qaeda in terms of branding. The caliphate narrative is incredibly effective, both for unifying ISIL operations and messages and providing compelling context for the group's operations for its supporters and potential supporters. Cleanly grouped and tightly focused themes make message discipline easy, although as the group loses territory and its affiliates are pressured, message discipline will become a key point of vulnerability that could be exploited.

ISIL fighters are adept at integrating informational and physical power and have been given specific orders to do so. Documents recovered from the battlefield in Benghazi, Libya, show explicit instructions for ISIL fighters to work in tandem with ISIL media operatives. One document instructed fighters to inform the media operatives "of all actions before beginning to undertake them in sufficient time," while another part of the same document warned against "photography with mobiles or cameras in the Dawla's bases or fronts except with prior coordination with the media."[76]

ISIL information personnel are accorded high levels of prestige or are otherwise well rewarded. As mentioned earlier, ISIL pays its media operatives roughly seven times what the average fighter makes and grants these individuals the rank of emir.[77] This is an important lesson for the U.S. Army, because it demonstrates exactly how valuable

others are skeptical that this tactic is effective over the long term. For a more pessimistic view on the effectiveness of shutting down ISIS Twitter accounts, see Amarnath Amarasingam, "What Twitter Really Means for Islamic State Supporters," *War on the Rocks*, December 30, 2015.

[76] Aymenn Jawad Al-Tamimi, "Archive of Islamic State's Administrative Documents," *Pundicity*, January 11, 2016. It is not particularly surprising that the ISIL affiliate in Libya would produce such specific and deliberate instructions. Of all ISIL affiliates, the franchise group in Libya is known to be among the most bureaucratic. See Sudarsan Raghavan, "Inside the Brutal but Bizarrely Bureaucratic World of the Islamic State in Libya," *Washington Post*, August 23, 2016.

[77] Koerner, 2016.

ISIL feels its information specialists are to the organization. Recruits with IRC backgrounds are prized and recognized for their skills—and seen as critical to helping ISIL achieve its objectives.

CHAPTER TWELVE

Mexican Drug-Trafficking Organizations

Case Summary

Mexican drug trafficking organizations (DTOs) have made extensive use of actions with effects in and through the IE, especially since the surge of violence that struck Mexico in the mid-2000s. DTOs operate in constant conflict with Mexican law enforcement, rival gangs, and the threat of vigilante groups of citizens in occupied territories. At the same time, they must construct and protect the infrastructure they use for trafficking. In this environment, DTOs thrive on intimidation and extortion. Public threats and violence, including "narcobanners" or "corpse messages," are a critical means to broadcast threats and demonstrate follow-through. Violence is frequently both the medium and the message. Traditional and social media reporting frequently enhances, extends, and echoes the information effects of these actions. Although many DTO activities are morally repugnant, the organizations give them a positive spin in the context of their mission statements. For example, some groups claim to pursue "divine justice." However, most claim only to be the lesser of all evils. In both cases, DTOs reinforce those justifications by enforcing intense membership rules and slandering the reputations of their rivals.

Background and Overview

Spanning drugs such as cocaine, heroin, marijuana, and methamphetamine, the U.S.-Mexican drug trade is worth tens of billions of dollars per year.[1] Billions more flow to DTOs through exports to Canada, Europe, and Asia. There is intense competition to access and control these lucrative markets.

The Mexican President Peña Nieto's administration has had recent success reeling back the influence of DTOs, disrupting larger groups and breaking them into smaller

[1] The North American illicit drug market has been valued at more than $100 billion, and trade from Mexico is responsible for a substantial portion of that market. See United Nations Office on Drug and Crime, *World Drug Report 2005*, Vienna, Austria, 2005.

organizations. Yet perhaps half a dozen major criminal organizations continue to participate in the Mexican drug trade, each with its own regional base. Mexico's Sinaloa region is home to the Sinaloa Federation and Beltrán Leyva Organization; in Tierra Caliente, the fall of Los Caballeros Templarios (Knights Templar) and La Familia Michoacana coincided with the rise of Cartel de Jalisco Nueva Generación; territory in Tamaulipas is split between Los Zetas and the Gulf Cartel.[2] In this chapter, we focus primarily on three groups:

1. Los Zetas, which Mexico's Secretariat of National Defense described as "the most formidable death squad to have worked for organized crime in Mexican history"[3]
2. La Familia Michoacana
3. Los Caballeros Templarios, which in some sense represents the same organization as La Familia Michoacana at an earlier phase in its evolution.

La Familia Michoacana and Los Caballeros Templarios have largely ceased to operate, having lost key leaders to law enforcement efforts, but Los Zetas remain active.

Very high rates of drug-related violence in Mexico are a recent phenomenon. Mexico's intentional homicide rate nearly tripled from 2007 to 2011 (from 8.1 per 100,000 in 2007 to 23.5 in 2011). Estimates suggest that somewhere between one-third and one-half of these homicides were related to the drug trade, accounting for 10,000 to 15,000 deaths per year during the peak.[4] Much of the violence is attributable to DTOs competing with each other for territory and authority. Many Mexican cities have found themselves in the middle of these power struggles between rival criminal organizations.

Beyond the unprecedented violence, recent years have seen an evolution in the DTOs' traditional organizational models. Earlier generations relied on drug trafficking as their principal source of revenue, but today's DTOs also generate revenue by controlling Mexican towns and cities, especially those close to deep seaports, border towns, and other strategic locations. They also run local crime rackets that impose de facto taxes on a region's economic activity (licit and otherwise), as well as such schemes as kidnapping and ransoming residents, blackmail, and assassination for hire. For some major DTOs, these non–drug-trafficking activities make up more than half of annual revenues.

[2] STRATFOR, "The Geography of Mexican Drug Cartels," January 25, 2016.

[3] Natasha Bertrand, "How 34 Commandos Created Mexico's Most Brutal Drug Cartel," *Business Insider*, March 5, 2015.

[4] Kimberly Heinle, Cory Molzahn, and David A. Shirk, *Drug Violence in Mexico: Data and Analysis Through 2014*, San Diego, Calif.: Justice in Mexico Project, University of San Diego, April 2015.

Concepts and Principles for Operations in and Through the IE

For many DTOs, success in the IE requires developing a reputation conducive to intimidation and coercion. Running a profitable extortion racket requires making credible threats, leading to easier, bigger, and safer ransoms. The public display of violence, whereby threats are followed through on as promised, is a key component of building and sustaining such a reputation.

The public display of violence and threats of violence is a hallmark of DTO information-related activities. DTOs perpetrate violence with the intention of generating effects in the IE—and this violence is not just the medium but also the message itself. Commonly, the intended message is a threat of further violence conditional on a demand, or simply a demonstration of a DTO's power and the impotence of traditional forms of authority. Forms of messaging range from the seemingly harmless (e.g., graffiti) to the macabre, such as corpse messages (a form of *narcomensajes*), in which dead bodies are left in plain sight.

Mexico's journalists are a frequent target of intimidation and extortion, given their influence and highly visible status. They have learned that reporting on a drug-related murder can prompt death threats from local trafficking groups.[5] In one incident, a major newspaper publisher agreed to remove the comments section from its website, yielding to a Zeta threat to blow up its offices.[6] In some places, media outlets have opted to avoid investigating DTO activities out of fear of retribution.

Blogs and social media have come to fill the role of traditional journalism in some DTO-occupied areas, publicizing outbreaks of violence in real time, operating as tip lines, exposing government and police corruption, identifying DTO members, and reporting on the latest kidnappings and other DTO activities. Like journalists, these bloggers and social media users have found themselves targets, their bodies displayed with messages to other "Internet snitches."[7]

Unlike more organized nonstate actors, such as Hezbollah and ISIL, Mexican DTOs do not operate any formal media apparatus. They find different ways to broadcast their messages. DTOs speak with their actions—usually violence—and they strategically place violence in the public sphere to maximize their audience. Even public acts of violence are not often actively broadcast by the DTOs; rather, word of mouth and media coverage bring publicity. In some Mexican cities, DTOs wait until the

[5] Damien Cave, "Mexico Turns to Social Media for Information and Survival," *New York Times*, September 24, 2011.

[6] Nick Miroff and William Booth, "Mexico's Drug War Intrudes on Monterrey, a Booming Metropolis," *Washington Post*, March 16, 2011.

[7] Elizabeth Flock, "Mexican Cartel Decapitates Web Commenter in Latest String of Internet Attacks," *Washington Post*, September 26, 2011; Jason McGahon, "She Tweeted Against the Mexican Cartels, They Tweeted Her Murder," *Daily Beast*, October 21, 2014; Robert Bunker, "The Growing Mexican Cartel and Vigilante War in Cyberspace: Information Offensives and Counter-Offensives," *Small Wars Journal*, November 3, 2011.

start of the six o'clock news to begin killing so that reporters will report the crimes live. The Internet and social media further amplify the effects of these tactics, though the "wrong" kind of attention can prompt retaliatory violence as well. In Mexico, the atrocities committed by DTOs are a common staple on blogs, Twitter accounts, and Facebook feeds, submitted by DTO members and worried citizens alike.

Strategic Goals/Vision

DTOs must balance several activities at once. They must (1) capture and maintain control of territory so that they may act with impunity and avoid retribution from law enforcement; (2) engage in revenue-generating criminal activities, such as trafficking drugs, collecting kidnapping ransoms, or redistributing gas stolen from PEMEX pipelines; (3) prevent or resolve external threats, whether posed by vigilante groups or rival criminal organizations; and (4) build and maintain a loyal and able membership base. IO are used to further each of these objectives.[8]

It can be a key competitive advantage for a DTO to rapidly expand into new territory and form alliances with regional gangs. Los Zetas employ a franchise model, forming business partnerships with independent criminal organizations operating in distant regions. Zetas offer their protection and resources, including the authorized use of the Zeta name, in return for a share of the revenues from criminal activities.

However, a downside of a sprawling and loosely connected organization is that it facilitates the unauthorized use of the organization's name. Unaffiliated criminals might claim to belong to a major organization to better intimidate and influence their victims. Likewise, DTOs might conduct false-flag operations by posting narcobanners or leaving corpse messages scrawled with the signatures of a rival. DTOs try to punish these fraudsters severely, and agreements to police against "McZetas" are a common condition of Zeta franchise agreements with affiliates.[9]

A critical defensive measure for DTOs is to control the flow of information about their own members and their rivals. Confidentiality protects the safety and continued work of collaborators, such as corrupt government officials, informants, and members of the media. These supporters must protect sensitive information about their identities (e.g., where they live, what car they drive) or else risk targeting from law enforcement or retaliation by enemies. Leaking the identities or information about the nefarious activities of rivals can likewise be a potent offensive measure.

[8] John P. Sullivan, "Criminal Insurgency: Narcocultura, Social Banditry, and Information Operations," *Small Wars Journal*, December 3, 2012; John P. Sullivan and Adam Elkus, "Cartel v. Cartel: Mexico's Criminal Insurgency," *Small Wars Journal*, February 1, 2009; Cabel N. Wharton and Daniel E. Welsh, *Net-Warlords: An Information Analysis of the Caballeros Templarios in Mexico*, Monterey, Calif.: Naval Postgraduate School, 2014.

[9] Tom Wainwright, *Narconomics: How to Run a Drug Cartel*, New York: PublicAffairs, 2016.

How Information Efforts Fit Within Strategic Goals

Just as territorial conflicts among DTOs can overflow into city streets, battles also extend to the IE. DTOs constantly attempt to vilify their rivals, accusing them of causing disorder, secretly collaborating with corrupt law enforcement, or attempting to mislead the public. At the same time, DTOs are under pressure to defend against similar attacks, whether they occur in public view on city streets in the form of a narcobanner or as photographs or stories posted on websites or social media.

In controlled territory, DTOs face opposition from rival gangs, law enforcement, residents, and vigilante groups. Actions with effects in the IE play a critical role in winning over or at least silencing these adversaries.

Currying favor with the public helps DTOs maintain a sustainable source of new recruits and induce local populations to acquiesce to or even support the organization. Residents of DTO-controlled territories face serious threats from criminal organizations, risking insecurity and economic disruption; yet, in some regions, residents view DTOs in a positive light. Narco-traffickers and criminals can attain a level of wealth and power that is otherwise out of the reach for many Mexicans, especially those without jobs or education (so-called *ninis*, for *ni trabaja, ni estudia*). Accordingly, one way that DTOs win support is through conspicuous displays of wealth and machismo, implicitly offering new recruits the same opportunity.[10] Another is to engage in philanthropic activity, often shrouded in local culture or religion, for instance by the sponsoring musicians or distributing Bibles.

A common theme is the promotion of DTOs' role in enforcing law and order in otherwise chaotic communities—actions consistent with civil affairs–type IO. Narcobanners and corpse messages frequently denounce criminals who have been caught and punished by DTO members. In one incident, after kidnapping two young men and chaining them to a fence, the Gulf Cartel posted a banner nearby identifying them as local university students and alleging that they were responsible for a recent wave of robberies and kidnappings. The message struck a threatening tone but ultimately concluded mercifully, stating, "This time we forgive them, because they are students and part of the great, respectable communities of Tampico, Madero and Altamira." The message also urged parents to "pay attention to your children because this plaza must be respected," adding that there would be no tolerance for thievery and extortion.[11] It is more common for banners to accompany dead bodies.

DTOs foster a popular culture that approves of the narco lifestyle through philanthropic acts, sponsoring *narcocorridos* (literally, drug ballads), and appropriating cultural icons. Some organizations, especially La Familia Michoacana and Los Caballeros

[10] "Violence in Mexico and Central America: A Lethal Culture," *The Economist*, December 11, 2014.

[11] Luis R., "Los Rojos–CDG Leave 2 Naked, Chained Kidnappers with Manta Message," *Borderland Beat*, November 10, 2015.

Templarios, have gone as far as creating quasi-religious belief systems that mythologize the narco lifestyle and justify and revel in its excesses.

Other actions in the IE are aimed at DTOs' own members. It is not uncommon for key leaders to defect from an organization or for members to act as double agents for law enforcement. Disagreements within a group's leadership may cause it to split, and poor morale can hurt recruiting efforts. Information efforts—specifically, intense recruitment and training ceremonies—help build discipline and loyalty within an organization's ranks. When members are effectively acculturated, they internalize the organization's values, goals, and tactics, discouraging members from defecting or deserting.

Targets and Audiences

There are six primary audiences that DTOs wish to influence or communicate with:

1. rival criminal organizations
2. law enforcement
3. vigilante groups
4. local populations in the territories they control, intended to provide social legitimacy and secure the public's acquiescence if not their cooperation as lookouts or full members
5. the organization's own members, for example to raise morale, coordinate operations, or prevent defection[12]
6. members of the media, to encourage them to cover (or not cover) a particular story or to threaten retaliation for unfavorable coverage, usually with one or more of the other five audiences in mind.

History and Evolution

The public and flagrant use of violence for broader messaging is a relatively new feature of Mexican DTO activity. Prior to the surge in violence in the mid-2000s, DTOs, such as the Sinaloa Cartel, made widespread use of blackmail and bribery of government officials and others to secure influence. This *plata o plomo* approach (*silver or lead*, or a choice between a bribe and a bullet) allowed the cartel to co-opt entire portions of government and law enforcement in the state of Sinaloa, allowing it to operate locally with impunity. Such messaging, however, was traditionally direct and personal.

In 2007, then-President Felipe Calderón's administration began its crackdown on the drug trade as violence surged, Internet access continued to spread throughout Mexico, and the DTOs' approach to the IE evolved. Text analysis shows that the terms now associated with distinctive DTO message-delivery modes originated just before Calderón's crackdown: Narcovideos (2005) and corpse messages (2006) came first, fol-

[12] This is a real threat: Massive defection was key to the demise of Los Caballeros Templarios.

lowed by narcobanners (2007). The first narcovideo dates to 2005 and is an al-Qaeda–style torture-and-execution video of four alleged Zeta members that was received and reported by the *Dallas Morning News*.[13] In 2006, La Familia Michoacana threw five severed heads onto a nightclub floor accompanied by a small cardboard sign, making this one of the first uses of a narcobanner *and* symbolic beheading in the Mexican drug war. Another early use of a narcobanner came in 2008, when someone hung an extended threat against Los Zetas opposite the offices of TV Azteca in Mexico City.[14] This period also saw substantial growth in Internet access. In 2000, only 5 percent of Mexicans had Internet access; by 2012, 30 percent were on Facebook.[15]

The emergence of Los Zetas was a driving force in that change. Leveraging the elite training they had received as members of the Mexico's special forces, and influenced by defectors from the Guatemalan special forces group Los Kaibiles, Los Zetas brought tactical excellence to the drug trade. The group quickly developed a reputation for carrying out acts of public violence, including beheadings, cooking victims into stew, dismemberment, and mutilation. Corpses were left in plain view, frequently hung over highway crossings or on roadsides. Often, they were accompanied by messages. These messages could be subtle and coded, such as gang signs inscribed on a corpse or nearby wall, but, other times, they were complex and explicit, such as banners painted with paragraph-long messages.

Experts disagree about what influenced this group's use of beheadings, but perhaps it was imitating al-Qaeda execution videos influenced by the historic use of this tactic by the Mayan and Aztec civilizations or modern religious cults such as Santa Muerte, or operating with instructions from recruits who defected from Los Kaibiles.[16] Regardless of what influenced Los Zetas, it is clear that the group has, in turn, influenced others. Rival DTOs have added similar tactics into their own arsenals, leading to increasingly brutal displays of violence in the fight for media attention.

Mexican DTOs' Organization for Operations in the IE

Despite the widespread use of effects in and through the IE, none of the DTOs we examined had a specific unit, division, or cell that specialized in information efforts, including planning or carrying out messaging campaigns or executing related capabilities. The decentralized or franchised structure of many DTOs suggests that decisions

[13] Paul K. Eiss, "The Narcomedia: A Reader's Guide," *Latin American Perspectives*, Vol. 41, No. 2, March 2014.

[14] Eiss, 2014.

[15] World Bank, International Bank for Reconstruction and Development, *World Development Indicators 2012*, Washington, D.C., 2012; Eiss, 2014.

[16] Ioan Grillo, "Behind Mexico's Wave of Beheadings," *Time*, September 8, 2008; Will Grant, "Mexico Violence: Fear and Intimidation," BBC News, May 15, 2012.

about information-related activities are often made at the local level or even on an ad hoc basis by individual operatives or leaders.

Structure

DTOs often have pyramidal hierarchies, with the top ranks overseeing a range of lieutenants grouped by functional or regional divisions. Upper leadership ranks supervise (1) plaza-level hierarchies, each headed by a lieutenant or plaza boss, and (2) a flat network of technical or support cells. Cells may specialize in high-skilled operations, such as money laundering or foreign distribution of drugs, or in low-skilled tasks, such as enforcement. Plaza bosses are given substantial autonomy in deciding how to manage their territory as long as they maintain control, hit revenue targets, and forward revenues to upper leadership.[17] Enforcement activities are often outsourced to groups external to the parent organization, making them free to change patrons when self-interest dictates, though they tend to enter into long-term arrangements with a single DTO.[18]

Otherwise, there is little or no structure for coordinating information efforts. To the extent that effects in and through the IE are integrated into standard operations, plaza bosses and other midlevel personnel responsible for controlling regional security are de facto coordinators. Generally, there does not appear to be any formal apparatus above that level with a substantial information-related role. This lack of coordinating structure does not appear to impair the effectiveness of DTOs' efforts, likely because of the simplicity and consistency of their tactics and messages—which so frequently involve drawing attention to the organization's use of violence or defaming adversaries.

An important exception are the publicity-loving groups, such as La Familia Michoacana and its splinter group Los Caballeros Templarios. Their top leaders act as organizational spokespersons or craft elaborate quasi-religious belief systems—for example, La Familia's Nazario "El Mas Loco" ("The Craziest One") Moreno González and Los Templarios' Servando "La Tuta" ("the Teacher") Gómez Martínez. La Tuta, a self-described "narco by heart," made frequent appearances in traditional and social media; Moreno, deferred to on questions of religion and ideology, generally took a backroom role as ideological founder and spiritual leader of both groups.[19] Reportedly, Los Caballeros Templarios kept public relations practitioners on staff, and some media activities (mainly videos posted to social media) were delegated to a senior leader.[20]

[17] Sylvia Longmire, "TCO 101: The Gulf Cartel," *Mexico's Drug War*, 2012.

[18] America Y. Guevara, "Propaganda in Mexico's Drug War," *Journal of Strategic Security*, Vol. 6, No. 3, Suppl., 2013.

[19] Falko A. Ernst, "Seeking a Place in History—Nazario Moreno's Narco Messiah," Insight Crime, March 12, 2014.

[20] Silvia Otero, "'La Tuta' y el Síndrome Ahumada" ["'La Tuta' and the Smoke Signal Syndrome"], *El Universal*, February 27, 2015; Rubén Mosso, "'El Tio' se Escondió en Clóset para Evitar Captura: Rubido" ["'El Tio' Hid in the Closet to Avoid Capture: Rubido"], *El Milenio*, January 27, 2014.

Funding

Although some DTOs are estimated to collect "hundreds of millions" of dollars per year,[21] it is clear that DTOs do not invest much in IRCs. However, they do draw significant benefit from physical efforts that have important effects in and through the IE.

Functional and Organizational Divisions

Given the lack of personnel who specialize in deploying IRCs or coordinating information efforts, DTOs typically do not divide personnel and lines of effort across functions or organizational components. Rather, much of DTOs' information efforts are conducted by rank-and-file members in the course of their routine activities. To the extent that the use of these IRCs is coordinated or supervised at all, it seems likely that coordination is managed by the plaza boss as part of his responsibility for his region's security and profitability. (There is little information detailing how common or intense that level of supervision might be or how it varies across plaza bosses or organizations.) But intimidation and threats are so ingrained in the organizational culture and the overall logic of operations that even the lowliest foot solider can easily intuit the value of violence as a message.

IRCs Employed/Available

DTOs very rarely employ traditional IRCs (e.g., EW, cyber capabilities, PSYOP, PA) and certainly not under those names. But a wide range of "quasi-IRCs" are fundamental to DTOs' daily operations, including those relating to intimidation and displays of violence, the engagement of traditional and social media, and the propagation of religious or quasi-religious belief systems.

Intimidation and Displays of Violence

DTOs have become well known for their use of quasi-IRCs related to intimidation and displays of violence, such as narcobanners. These tactics are commonly employed in territories controlled by DTOs, particularly during times of conflict or instability—for instance, during raids by Mexican law enforcement, when a rival gang enters a territory, or when there is internal conflict within a DTO. Even the simple act of inscribing a gang's symbol can demonstrate control over a territory and inspire terror and compliance.

One of the most common and striking of the quasi-IRCs is corpse messaging, the act of leaving deceased victims of DTO violence in public for maximum exposure. Corpse messages not only announce a killing, but they can also send more detailed messages, depending on the style of the killing or the display of the body. Allegedly, a mutilated hand indicates that the victim was a thief, but placing one of the victim's fingers (often the index finger) in the victim's anus indicates an informant; cutting off

[21] George W. Grayson, *La Familia Drug Cartel: Implications for U.S.-Mexican Security*, Carlisle Barracks, Pa.: U.S. Army War College, Strategic Studies Institute, December 2010, p. 49.

the feet shows that the victim attempted to defect; removing the ears suggests that the victim heard something he was not supposed to hear; a mutilated tongue indicates that the victim said things that he should not have; finally, mutilating the testicles or penis signals that the victim was weak or too cowardly to follow the orders issued by a DTO.[22]

Corpse messaging is an effective means to grab attention, especially when conducted en masse. In the span of a few weeks during a 2012 Zeta-Sinaloa turf war in Nuevo Laredo, authorities found 18 mutilated bodies in vehicles along a roadside, 14 severed heads packed into coolers, and 49 other severely dismembered bodies. Nearby graffiti alleged Zeta responsibility ("Z 100%"), but it remains unclear whether the event was a straightforward attempt by Los Zetas to claim territory or an effort to draw the attention of Mexican law enforcement to enemy territory.[23]

Such demonstrations are taken seriously by other DTOs and can trigger severe responses. After the 2009 death of Beltrán Leyva Organization leader Arturo Beltrán Leyva, photographs surfaced online of his corpse in embarrassing positions, with pants pulled down and covered in bloodied money, an offense serious enough to warrant lethal retaliation against the family members of a Mexican marine killed in the raid (despite the Mexican government's condemnation of the photographs' release).[24]

Narcobanners (*narcomantas*) sometimes accompany corpse messages but are also often used independently. They are hung in the most visible places, including on highway overpasses and along main roads, sometimes introduced with the fanfare of gunfire to attract extra attention. Narcobanners allow DTOs to make direct, clear announcements to the public and adversaries. They may be used for a wide range of purposes, including attributing or denying credit or blame for a recent event, claiming control of territory, implicating members of a rival organization in acts of crime or calling for retaliation or a bounty, and spreading rumors about the strength or actions of rival organizations.

Engagement with Traditional and Social Media

The Internet and social media can enhance, echo, and extend the effects of these tactics. DTOs frequently engage on social media, for instance through anonymous submissions to websites devoted to narco-related news, Facebook and Twitter posts by members, and, in some cases, even self-filmed videos posted on YouTube. There have been multiple prison breakouts organized by DTOs that were filmed and released to

[22] Rocco Palomera, "Narcomutilaciones Tienen un Signficado" ["Narco Mutililations Have a Meaning"], *El Occidental*, June 7, 2010.

[23] Jo Tuckman, "Mexican Drug Cartel Massacres Have Method in Their Brutal Madness," *The Guardian*, May 14, 2012.

[24] Eiss, 2014.

YouTube.[25] In Reynosa, an audio recording of a Gulf Cartel leader discussing plans to launch a campaign to detonate car bombs at police facilities was leaked to social media. In response, the faction hung banners addressing the president, the governor of Tamaulipas, and the mayor of Reynosa denying the charge.[26]

One of the more popular narcovideos featured Cartel de Jalisco Nueva Generación members announcing Los Mata Zetas, or Zeta Killers, a special squad formed to drive Zetas from Veracruz. In the 2009 clip, the narrator calls attention to atrocities carried out by Los Zetas and states that "drug trafficking will not end but we can bring peace to our families." He alleges that Los Zetas have the police and governor working in their stead, calling on citizens to report corrupt members of the Mexican state and name Zeta operatives.[27]

Former La Familia Michoacana leader Servando "La Tuta" Gómez Martínez made exceptional use of YouTube and traditional media to directly engage the public.[28] La Tuta first gained notoriety in 2009 after calling a TV news program and introducing himself as a leader of La Familia, a "self-defense group" seeking to defend Michoacán against the excesses of rival DTOs (especially Los Zetas) and government forces, whom he accused of being accomplices.[29]

La Tuta has authored many other narcovideos with similar themes in which he speaks directly to the camera.[30] In one video, filmed shortly after thousands of federal troops were dispatched to Caballeros Templarios territory, La Tuta speaks in front of a wide range of iconography: a Mexican flag, a statue of a medieval knight, a poster of Che Guevara, and a photo of Fidel Castro.[31] Other media stunts have included repeated public requests for a truce between the La Familia and the federal government, under which the organization would disband if the government agreed to "defend the region against other drug gangs."[32] La Tuta has also used media activity as a threat to influence collaborators, including holding politicians and others accountable or blackmailing them.[33]

[25] Joseph Cox, "Mexico's Drug Cartels Love Social Media," *Vice*, November 4, 2013.

[26] Kristian Hernandez, "Cartel Boss States 'We Are Not Terrorists' Using Narco Banners Throughout Reynosa," *The Monitor (McAllen, Texas)*, November 3, 2015.

[27] "Ejecutan a tres los mata Zetas" ["Zeta Killers Execute Three"], *El Universal*, June 19, 2009.

[28] Patrick Corcoran, "Inside the Moral Code of the Caballeros Drug Gang," Insight Crime, July 20, 2011.

[29] Miriam Wells, "Knights Templar Blame Self-Defense Groups for Violence in Mexico," Insight Crime, April 29, 2013; Miriam Wells, "Mexico's Knights Templar Love Publicity, but Where Will It Get Them?" Insight Crime, February 18, 2014; Corcoran, 2011.

[30] See Solo un Hack, "'La Tuta' en su Rancho Envia Mensaje a EPN y al Gobierno de México" ["'La Tuta' on His Ranch Sends a Message to EPN and to the Government of Mexico"], video, posted April 27, 2013.

[31] Edward Fox, "Knights Templar Leader Makes Rare Video Appearance," Insight Crime, August 31, 2012.

[32] Michael O'Boyle, "Mexican Cult-Like Drug Gang Says Willing to Disband," Reuters, November 29, 2010.

[33] Otero, 2015.

Promotion of Narcocultura

Narcocultura is an umbrella term that encompasses (1) music of the *narcocorrido* genre, narrative-style songs about the exploits of DTOs and their leaders; (2) the worship of narcosaints, narco-themed icons integrated into a religious fabric that is mixed with Iberian Catholicism and religious themes indigenous to Mexico; and (3) the glorification or flagrant display of the lifestyle and wealth associated with members of DTOs.[34]

The *narcocorrido* genre has grown quite popular; the songs are often played on the radio, and the artists perform live across the country. The sponsorship of *narcocultura* can become yet another proxy battlefield in which DTOs vie for supremacy and demonstrate their willingness to commit violence. The notorious head of the Sinaloa Cartel, Joaquín "El Chapo" Guzmán, is one of many DTO leaders who have commissioned musicians to write ballads in their honor. It is also popular to commission attack ballads against other organizations. Despite the risk of becoming a target for retaliation by a sponsor's rivals, many musicians accept DTO sponsorship, whether in the form of commissions for writing narcoballads or funds to release an album or go on tour.

Other DTOs have embraced narcosaints in a similar fashion. Narcosaints were not invented by DTOs, although they have been co-opted and popularized by these groups' imagery and messaging. Some of the more popular narcosaints include Santa Muerte (Holy Death) and Jesus Malverde, a Robin Hood–type figure often called the "generous bandit" or "angel of the poor." Santa Muerte has been condemned by the Catholic Church but has been embraced by leaders of the Gulf Cartel. Her image is frequently found in drug houses, and members pray to her on certain occasions, such as after completing a job or escaping from the police or from jail. Reportedly, Santa Muerte figures outsell figures of the Virgin of Guadalupe, Mexico's patron saint. DTO leadership has shown a commitment to such folk-religious ideas by conducting ceremonial burials, in some cases going to such lengths as to raid morticians' offices to capture the bodies of fallen members.

Efforts to make a contemporary narcosaint out of La Familia leader Nazario "El Mas Loco" Moreno González demonstrate the importance that top DTO leadership has assigned to *narcocultura*. After his rumored death, Moreno served as an inspirational figure and backroom leader for Los Caballeros Templarios; his continued survival was considered "an open secret" in Michoacán.[35] According to Moreno himself, this mythology gave locals "a space to believe," gave his organization and persona a shroud of mystery, and demonstrated the group's strength against the government.[36] Moreno was commonly referred to as "El Señor" or "lord," and after his actual death in

[34] *Narcocorridos* are often said to function similarly to gangster rap, but the style draws on historical narrative-structured folk songs, typically about war. A distinct genre of hardcore narco-rap music is also popular, however.

[35] "Era un Secreto a Voces que 'El Chayo' Estaba Vivo: Castillo" ["It Was an Open Secret That 'El Chayo' Was Alive: Castillo"], *El Milenio*, October 3, 2014.

[36] Ernst, 2014.

2014, shrines devoted to “San Nazario” sprung up across Michoacán, accompanied by a prayer for abundance.[37] A Michoacán chapel built to venerate his image is decorated with the text, “They are lying, Nazario is alive.”[38]

Another example of *narcocultura* is Los Zetas forcing local bars to stock a particular Z-shaped bottle of brandy.[39] Such actions encourage the public to embrace the cultural mindset that encourages support for a DTO, and they make visible people’s commitments to the organization while highlighting the exclusivity of the perks of support.

Recruitment, Training, and Membership Rules

The training techniques used by Los Zetas and other DTOs can be psychologically extreme. Early Zeta leader Heriberto Lazcano sought instruction from defectors from the Kaibiles, a Guatemalan special forces group that operates a training camp (“El Infierno”) near a Zeta outpost in Poptún, Guatemala. At their jungle camp, Kaibiles recruits undergo severe training, including learning to “eat anything that moves, bite heads from live chickens, and kill puppies after bonding with them.”[40] Their motto is, “If I advance, follow me. If I stop, urge me on. If I retreat, kill me.”[41] Although less information is available on Zeta training practices, it seems likely that the group has integrated some of these tactics (as they may have done with symbolic decapitations). It has also been reported that DTO recruits are required to hunt and kill innocent people during training. In one of the most extreme incidents, Zetas halted busloads of farmers, handed them weapons, and forced them into a melee to the death. According to some accounts, this was a means to recruit the few “winners,” although it may have been merely an expression of malice and wrath. (It is unclear whether such activities are part of a deliberate recruiting strategy or the result of malice by individual members.)[42]

La Familia Michoacana and Los Caballeros Templarios took a different approach, focused around a set of quasi-religious beliefs. The two organizations preached a “divine calling” that involved “killing to do good.” La Familia Michoacana marketed itself as an alternative to the drug-fueled chaos that had been wrought on the state of Michoacán under Zeta control. The group emphasized rightful living, initially requiring all potential recruits to achieve sobriety and prohibiting members from selling drugs (although the organization appears to have become more lenient over time). La Familia operated an extensive network of free rehabilitation centers that doubled as recruitment

[37] Ernst, 2014.

[38] Michael Lohmuller, “Rumors Fuel the Legend of the ‘Narco-Saint,’” Insight Crime, February 6, 2014.

[39] George W. Grayson, *The Evolution of Los Zetas in Mexico and Central America: Sadism as an Instrument of Cartel Warfare*, Carlisle Barracks, Pa.: U.S. Army War College, Strategic Studies Institute, April 2014, p. 33.

[40] Grayson, 2014, pp. 3–4.

[41] Tracy A. Bailey, “Ranger Graduates Kaibil School,” *ShadowSpear Special Operations*, December 18, 2012.

[42] Adam Clark Estes, “Mexico’s Tales of Bus Passengers Forced to Fight to the Death,” *The Atlantic*, June 14, 2011.

bases. Patients who recovered successfully were invited to become full-fledged members of La Familia, in the *plata o plomo* sense—such that refusing the offer came with the threat of retaliatory violence. Recruits were sent to a two-month program resembling a cult initiation that included Bible study, periods of silence, and inspirational sermons focused on spiritual rebirth. The program was designed by Rafael "El Cede" Cedeño Hernández, a self-described pastor and an observer appointed to Michoacán's human rights commission, granting it additional credibility.[43]

Doubling as a holy book and doctrinal training manual, the *Code of the Knights Templar* has been distributed on the streets of Michoacán and is even available as a PowerPoint presentation targeting new and prospective recruits.[44] The manual lists 53 commandments, along with proverbs and a mix of political, religious, and operational messages.[45] Operational messages emphasize the importance of the chain of command, constant vigilance against security threats, and "absolute coordination" with the broader organization. For example, one of guidelines reads," "For the use of deadly force, the council's authorization is required."[46] Ethical orders include to "fight against materialism, injustice, and tyranny," to "defend the values of a society based on ethics," and to act with honesty, humility, and chivalry.[47] Authorities have found Templarios with white robes, a red cross, medieval knight–style helmets, and books used for indoctrination.[48]

The code lays out specific punishments for when rules are broken, a greater risk among younger members. (La Tuta lamented, "We can't cure all the muchachos").[49] The code asserts, "That Knight who betrays the Templars will be punished with death, and all his properties will be confiscated, [and] his family will suffer the same fate."[50] It is not clear how often that particular punishment is carried out, but when it is, it is likely done in public to maximize exposure.

Why would such a dangerous organization deliberately make joining so difficult for new members? The economists Kostelnik and Skarbek posit that this helps DTOs solve cooperation problems. They argue that these costly initiation processes and restrictive rules (e.g., requiring sobriety) screen out members who are not fully

[43] Grayson, 2010, p. 38.

[44] Patrick Corcoran, "Revelations of Mexico's Knights Templar Indoctrination Manual," Insight Crime, December 17, 2013.

[45] Corcoran, 2013.

[46] Tribal Analysis Center, *Mexico's Knight Templar and Code of Conduct Implications*, Williamsburg, Va., November, 2013.

[47] Corcoran, 2011.

[48] Miguel García Tinoco, "Criminales del Medievo; Hallan Túnicas de Caballeros Templarios" ["Medieval Criminals: Tunics Found from Knights Templar"], *Excelsior (Mexico)*, July 20, 2011.

[49] Ernst, 2014.

[50] "Excerpts of the 'Code of the Knights Templar' Cartel," Associated Press, July 20, 2011.

loyal to the organization; as a result, members who do pass through those filters may be more trustworthy, potentially preventing future defections and increasing discipline within the organization.[51]

Personnel

DTOs tend to have few if any personnel with roles specific to information efforts. Instead, these efforts are carried out by rank-and-file members.

Otherwise, DTO membership can be split into four clearly identifiable types of personnel: (1) high-level, highly skilled "core" members who are recruited very selectively; (2) midlevel members specializing in such functions as assassinations, kidnapping, or enforcement; (3) low-level foot soldiers who bring few skills but are numerous, knowledgeable about local territories, and often willing to risk their lives; and (4) low-level members of human intelligence networks who feed information to DTOs but have no role in combat, including prostitutes and taxi drivers.

Other areas of expertise may be acquired via kidnapping. More than three dozen IT professionals, communication specialists, engineers, architects, and others with specialty skills disappeared without ransom demands in DTO-occupied territory between 2008 and 2015. Authorities and others familiar with DTO operations suspected that these kidnapping victims were being put to work developing secure communication systems or applying their hacking skills to identifying enemies (including bloggers and vigilante social media users). However, other experts question why DTOs would kidnap specialists to support these activities when they have the means to recruit them into their ranks and fund their training.[52]

Finally, DTOs rely on an extensive network of supporters outside of Mexico—including arms smugglers, U.S.-based gangs, and individuals who transport and distribute drugs on DTOs' behalf and operate fronts for money laundering.[53]

Dependencies, Relationships, Related and Supporting Capabilities, Areas, and Functions

Intelligence Networks

Ground-level human intelligence and communication networks are key assets for DTO information activities. These systems assist DTOs in monitoring strategic areas and rival organizations. In controlled territories, DTOs manage extensive human intelligence networks, drawing on taxi drivers, prostitutes, youths, and others who are equipped with cell phones or radios and are well positioned to monitor the streets for shootouts, movements by law enforcement, and other events. Some lookouts (*halcones*)

[51] James Kostelnik and David Skarbek, "The Governance Institutions of a Drug Trafficking Organization," *Public Choice*, Vol. 156, No. 1, July 2013.

[52] Brian Anderson, "The Drug Cartels' IT Guy," *Motherboard*, March 3, 2015.

[53] Jerry Seper, "Ruthless Mexican Drug Cartel Recruiting in U.S.; Los Zetas Looks to Prisons, Street Gangs," *Washington Times*, July 7, 2013.

also monitor social media channels, picking up on events reported by citizens, rival organizations, and news organizations. To collect and use the information reported by those lookouts, DTOs maintain local safe houses where information is analyzed and passed on via extensive networks of radio towers and repeaters.[54] Some plaza bosses have built closed-circuit TV systems fed by cameras mounted on rooftops and light poles, providing them with round-the-clock situational awareness.[55]

Coordination/Integration Challenges

One might expect DTO information efforts to be chronically self-conflicting and frequently misguided, for two primary reasons. First, IRCs are regularly carried out by low-level, unskilled members, many of whom are connected to the parent organization only by way of a local plaza boss or as a member of a franchised street gang. Second, there is a lack of structure for directing or coordinating the deployment of IRCs across the whole organization.

In fact, there are surprisingly few incidents of self-conflicting messages. DTO information efforts have a simple message, concerned primarily with delivering threats and demonstrating the credibility of those threats. This straightforward strategy guides low-level members responsible for IRCs, such as leaving corpse messages and narcobanners: Be prepared to use threats of violence to achieve your objective, and be shameless in advertising the use of violence as a means to build organizational reputation. Furthermore, the messages are commonly tactical and localized, and they are guided by plaza bosses at the local level. Due to the fragmented nature of DTOs, plaza bosses operating in different regions can take different approaches to managing their territory without the need to coordinate their strategy or messages. They merely adhere to themes universal to all DTOs: power, intimidation, and violence. Finally, recruitment, training, and other membership rules instruct members regarding standard protocol (including punishment for breaking the rules) and foster obedience and loyalty.

However, there are challenges to this structure. Although DTOs are effective at signaling their willingness to use violence, operatives appear to be going through the motions without a broader strategy. In 2010 in Ciudad Juarez, a DTO operative murdered a photojournalist from the local newspaper *El Diario*. It was the second time in two years that a *Diario* journalist had been the victim of DTO violence. Clearly affected but unsure how to react, the newspaper's staff wrote an editorial titled "Que Quieren de Nosotros?" ("What Do You Want from Us?"). The article directly addressed the responsible criminal organization: "We'd like you to know that we're communicators,

[54] For example, in 2011, authorities discovered a 1,000-mile network of antennas, repeaters, computers, and other gear used to link Zetas operating in three Mexican states. Similar busts have occurred elsewhere in Mexico. See Anderson, 2015.

[55] Juan Pablo Becerra-Acosta, "GATES, Policías de Élite que Combaten Narcos en Coahuila, Bajan la Delincuencia" ["GATES, Elite Police That Combat Narcos in Coahuila, Lower Crime"], *El Milenio*, May 30, 2015.

not psychics. As such, as information workers, we ask that you explain what it is you want from us, what you'd intend for us to publish or to not publish, so that we know what is expected of us."[56] This demonstrates a key defect: There is little use in delivering a threat, even a credible threat, if the demands are unclear. (A somewhat different interpretation is that *El Diario* staff intentionally wrote a desperate editorial as a means to get the attention of Mexican federal law enforcement without triggering retaliation from the local criminal organization.)

Information Operations in Practice

The constant conflict waged across Mexico over the past decade has provided DTOs countless opportunities to demonstrate their use of IRCs.

Examples of Interesting Mexican DTO Information Efforts

The emergence of La Familia Michoacana and its splinter group Los Caballeros Templarios demonstrated a consistent and deliberate use of effects throughout the IE, spearheaded primarily by leaders Nazario Moreno González and Servando "La Tuta" Gómez Martínez. In September 2006, a group of 20 masked men entered a Michoacán nightclub, firing shots into the air and throwing five decapitated heads onto the dance floor, marking the first time that severed heads were used purely for propaganda purposes by Mexican criminal organizations.[57] As explanation, the men left a cardboard sign that read, "The family doesn't kill for money. It doesn't kill for women. It doesn't kill innocent people, only those who deserve to die. Know that this is divine justice." Two months later, local newspapers *La Voz de Michoacán* and *El Sol de Morelia* ran display ads announcing a new group, La Familia Michoacana. The ads portrayed La Familia as a defender of Michoacán against a plague of drug abuse and violence, and calling upon the local populace to join in that battle. The lengthy advertisement took on a formal structure, with headers such as "Who Are We?"; "Mission"; "Objective"; "Why Did We Form?"; and "For Reflection." An excerpt reads, "You, Family man, I ask you: Would you like to see your son out on the streets in danger of getting involved in drugs or crime? Would you support this organization in its fight against the maladies that attack our state?"

The advertisement explicitly makes two points. First, it offers a moral justification for La Familia's actions:

[56] "Que Quieren de Nosotros?" ["What Do You Want from Us?"], *El Diario*, September 19, 2010.

[57] Grayson, 2010, pp. 1, 45.

> Unfortunately, to eradicate the ills we have mentioned, we have had to resort to robust strategies, as we have seen that this is the only way to bring order to the state. We will not allow it to get out of control again.[58]

Second, it emphasizes the importance of law and order, stating the group's intent to

> eradicate from the state of Michoacán kidnapping, extortion in person and by telephone, paid assassinations. . . [and] home robberies done by people like those mentioned, who have made the state of Michoacán an unsafe place. Our sole motive is that we love our state and are no longer willing to see our people's dignity trampled on.[59]

Consistent with that goal, La Familia conducts and widely advertises acts of philanthropy and community service. The group is known to distribute Bibles, assist in the repair of schools, and run homeless shelters and rehabilitation clinics.[60] It has even been reported that La Familia offered consumer loans to small businesses, with approvals within 72 hours and at a lower interest rate than that offered by banks. Soon after accepting a loan, customers received a message that said, "Thank you for your trust. Now you're a part of La Familia Michoacán."[61]

La Familia Michoacana came to an abrupt end in 2010, soon to be reborn as Los Caballeros Templarios. Just as La Familia's emergence was steered by the careful deployment of effects in the IE, so was the group's rebranding. After an alleged betrayal within the top leadership, Moreno and La Tuta sought to purge other leadership and "get rid of the stained name."[62] The catalyzing event was a rumor that Moreno had been killed in a conflict with Mexican security forces, spread by way of uncoded communications on open, unsecured radio channels. Moreno's rumored death and the collapse of La Familia were deliberately managed to create a power vacuum that would bring the new group to power. Key to this effort was the close linking of Los Caballeros Templarios to the La Familia. La Tuta announced the group as the successor to La Familia, and efforts were made to deify the rumored-dead La Familia leader Moreno. Los Caballeros Templarios continued to operate in that fashion until the group eventually collapsed after Moreno's actual death in 2014 and La Tuta's capture in 2015.

[58] Grayson, 2010, p. 102.

[59] Grayson, 2010, p. 101.

[60] Grayson, 2010, p. 37.

[61] Grayson, 2010, p. 52.

[62] Ernst, 2014.

Effectiveness of Mexican DTO Information Efforts

Over the past decade, Mexican DTOs have generated tremendous profits while wreaking an immense amount of violence and disorder on Mexican communities—and, for the most part, Mexican authorities have been unable to stop them. The *plata o plomo* approach to intimidation and extortion has been an effective means for DTOs to corrupt and control entire Mexican states. The success of Los Zetas points to the usefulness of this brand of public hyperviolence, which delivers enormous amounts of media coverage and instills terror and fear into communities. Likewise, the short but impactful reign of La Familia Michoacana and Los Caballeros Templarios suggests the usefulness of efforts to build a strong organizational culture through intensive membership rules.

The efforts described in this chapter offer evidence of Mexican DTOs' excellence in influencing audiences, leveraging narrative, and using maneuver and fires as IRCs. Furthermore, some aspects of DTO activity reflect excellence in in controlling information.

Perhaps the most distinctive trademark of Mexican DTOs is their excellence in the use of maneuver and fires as IRCs. Los Zetas, in particular, were path-breaking in their massive deployment of public violence with clear and direct effects in the IE. The group not only committed targeted acts of violence, but it did so in ways designed to make a public statement (e.g., , dismembered or mutilated bodies, sometimes dozens at a time, accompanied by banners listing warnings or demands). These tactics have been used to send information to an organization's own members, to rivals, and to third parties. They have granted DTOs powerful capacities for affecting the IE, despite a lack of formal DTO-run media apparatuses or, in some instances, a reluctance among leadership to make public addresses.

DTOs are highly effective at influencing domestic audiences. Despite the violence and disorder they wreak on Mexican communities, many DTOs are quite popular in their home territory and are sometimes even more trusted than legitimate governmental authorities.

To build and wield influence, DTOs undertake a range of activities with consequences in the IE, including posting narcobanners and using social media to both self-promote and target their enemies. In their favored territories, these tactics have helped them build strong networks of loyal supporters and accomplices while intimidating critics and public officials.

DTOs also show excellence at leveraging narrative, especially with their strategic interactions with the media and their embrace of powerful cultural iconography and traditions. Many DTOs have adopted narcosaints as spiritual icons, such as Jesus Malverde and Santa Muerte, whose continued popularity in Mexico suggests a powerful resonance. Other myth-making efforts have been more ambitious, particularly those of the Templarios, who ultimately failed to attract a steady audience of observant and loyal members from the broader population. Despite inconsistent success, other examples of excellence abound, including La Tuta's viral social media videos, in which he directly addresses the audience to speak about his experiences as a rural teacher and his political ambitions.

Less consistently, DTOs have demonstrated excellence in the censorship and control of information. DTOs maintain wide networks of accomplices within government, civil society, and sometimes even rival organizations, and the use of threats and intimidation has been critical to preventing leaks and defections, as well as to ensuring the secrecy of members' and enablers' identities. In DTO-controlled areas, during periods of conflict, many newspaper and television reporters have stopped or slowed their reporting on crimes related to narco-trafficking, fearful of retribution. On the other hand, DTOs have been less able to silence or manipulate reporting on social media, where narco-related information is frequently reported on Twitter and curated news sites powered by anonymous submissions, and they have even struggled with threats from the online vigilante group Anonymous.[63]

Efforts of Others to Counter DTOs in the IE and Their Effectiveness

There remains an epidemic of drug-related violence in Mexico and many organizations have persisted despite years of law enforcement crackdowns. Nonetheless, some efforts to combat DTO information efforts have proven effective.

Vigilante Social Media Reporting

DTOs' ability to suppress reporting by traditional media has been foundational to their efforts to capture and control territory. In Ciudad Juarez, for instance, reporters cover murders in detail but limit the depth of their investigations. But where traditional media outlets have been silenced, citizens look to social media instead.[64] It has become common for citizens to tweet or post about narco-related activity, such as active shootouts, kidnappings, or other crimes that traditional news outlets sometimes refuse to publish. Many residents rely on social media to help them safely conduct their daily lives, avoiding shootouts and other dangers. And because social media activity can be conducted quasi-anonymously, citizens can feel safe reporting on events that would make television reporters uncomfortable.[65]

Even a single tweet can have real consequences, however: In Veracruz, two people were charged with sabotage and terrorism for tweeting a false report of an active kidnapping at a local school that caused public panic and car accidents.[66]

[63] Bunker, 2011.

[64] Jo Tuckman, "Twitter Feeds and Blogs Tell Hidden Story of Mexico's Drug Wars," *The Guardian*, September 26, 2010.

[65] Cave, 2011.

[66] Cave, 2011.

Websites, such as *El Blog del Narco*, act as clearinghouses for anonymous tips. At its peak, *El Blog del Narco*'s combination of photos, videos, and written reports attracted 4 million weekly visitors. Submissions included interrogation and execution videos; photographs of dead victims' bodies, often mutilated or shown in incriminating poses; and descriptions of law enforcement actions, such as discoveries of weapons, drugs, or safe houses.[67] Other posts reported the identities of gang members, sometimes with pictures of their houses or cars.

Websites and social media handles often emerge in areas experiencing DTO-related conflict, with posts tagged with #ReynosaFollow, #FreeAcuna, #ValorPorTamaulipas, or another location-specific hashtag.[68]

Still, DTO members can turn such platforms into a battleground. Such websites echo the information effects of DTO killings, threats, and narcobanners. Additionally, many social media reports are themselves authored by DTOs, perhaps looking to post a bounty, spread a dangerous rumor, or advertise their own actions.

Successful informal media outlets also attract retaliation. Like journalists, bloggers and social media vigilantes have found themselves targets of DTO violence.[69] Despite operating under a 600,000-peso bounty, the Facebook group "Valor por Tamaulipas" ("Courage for Tamaulipas") persisted even after the 2014 assassination of a primary contributor. (The killers broke the news by posting photos of her body to her Twitter account.) In another case, in 2011, DTO-affiliated killers (possibly Zetas) left two bodies hanging from a highway overpass alongside a narcobanner stating, "This will happen to all Internet snitches."[70] Perhaps the most notable assassination of a blogger occurred just days later, when the severed head of the "girl from Laredo" was found wearing headphones near a computer keyboard.[71] The victim was tortured and murdered by Los Zetas for using her blog to encourage citizens to provide information on drug traffickers to the authorities so that they could be arrested.

Vulnerabilities in DTO Information Efforts

A small Anonymous chapter in Zeta-controlled Veracruz turned the tables on the DTO in 2011 with an act of extortion. In retaliation for the alleged kidnapping of one of its members by Los Zetas, Anonymous posted a YouTube video featuring a Guy Fawkes mask–wearing speaker demanding the captive's release and threatening to dox (release identifying information on) Zeta members and supporters. Anonymous claimed to have acquired this information by hacking into the email systems of Mexican police

[67] Tuckman, 2010.

[68] J. David Goodman, "In Mexico, Social Media Become a Battleground in the Drug War," *New York Times*, Lede Blog, September 15, 2011.

[69] Flock, 2011; McGahon, 2014; Bunker, 2011.

[70] Goodman, 2011; McGahon, 2014.

[71] Bunker, 2011.

agencies over a period of six months. Legitimizing the threat, Anonymous members defaced the website of Gustavo Rosario Torres, a former state prosecutor alleged to have ties to Los Zetas.[72] Anonymous eventually backed off after reporting that the kidnapped member had been released with a note from the abductors threatening to kill ten people for each exposed Zeta identity, a message interpreted as a face-saving gesture.[73]

This episode highlights how the DTO model of influence breaks down when an act in the IE cannot be attributed to a specific actor. However, it also highlights the danger of engaging an organization that kills with impunity: Any blogger, social media vigilante, or innocent bystander could have become collateral damage in an attempt to deter an amorphous enemy.

The informality of DTO quasi-IRCs comes with the downside of vulnerability to false-flag operations. Narcobanners and social media posts can be attributed to anyone, and news reports can be submitted anonymously. DTOs and their rivals frequently take advantage of that vulnerability, working to create the impression of weakness in their opponents' ranks or tarnish their reputation.

Lessons from Mexican DTO Operations in and Through the IE

This review of information-related efforts of Mexican DTOs provides some clear lessons for U.S. operations.

Mexican DTO Information Efforts in Contrast with U.S. IO

Mexican DTOs are fundamentally different from the U.S. military: DTOs are informal and often transient groups, they exist in contravention of the law, they seek to maximize profits, they have no public constituency to which they are accountable, and they are often assembled loosely out of the fabric of smaller, semi-independent "cells" or subcontracted street gangs. These organizations' use of information reflects these differences. Their tactics involve morally repugnant actions, including excessive and gruesome violence, extortion, and misrepresentation. Many of their activities effectively amount to terrorism.

But despite the magnitude of differences, similarities allow some possible points of comparison. First, like the U.S. military, Mexican DTOs expend considerable effort to inculcate loyalty and obedience in their ranks. Recruitment methods and training

[72] Geoffrey Ramsey and Christian Science Monitor, "Showdown Looms Between 'Anonymous' Hackers and Mexico's Zeta Cartel," ABC News, November 5, 2011.

[73] Bunker, 2011; Paul Rexton Kan, "Anonymous vs. Los Zetas: The Revenge of the Hacktivists," *Small Wars Journal*, June 27, 2013. Some media outlets alleged that the kidnapping had not occurred at all and that the hostage's release was fabricated to help Anonymous save face in withdrawing from the fight, fearing potential harm to anti-DTO bloggers and commenters unaffiliated with the operation.

camps can be selective and extreme, designed to push recruits out of their comfort zones and to forge strong familial bonds with their peers and the organization itself. But DTOs are even more aggressive in this realm than the U.S. Army, since they have no compunction about constructing entire quasi-religious belief systems, sometimes resembling death cults, and even deifying their own leaders.

Second, the majority of DTO members deal primarily in violence. DTOs are primarily organizations of soldiers, although beneath them is a wide network of lookouts, frontmen, and other accomplices who are kept at the organizations' periphery.

Third, the outcomes of operations undertaken by both the DTOs and the U.S. military depend, in part, on effects in and through the IE. Without effective information activities, DTOs face restive populations, defection within their ranks and among their collaborators, and more consistent and coordinated opposition from government forces. Similarly, without effective IO and IRC employment, U.S. military operations would face adversaries with better C2 capabilities and risk winning all the battles while losing the war for a lack of international legitimacy and support and acceptance from relevant foreign populations.

Key Takeaways

Despite the massive differences between Mexican DTOs and the U.S. Army, they nonetheless operate in similar environments and face some similar problems.

Capabilities or Practices That the U.S. Army Might Want to Replicate (or Access Through Joint, Interagency, International, or Multinational Efforts)

Social media has become an important source of security-related news in Mexico, often to the disadvantage of DTOs, but DTOs have also been adept at manipulating that public resource. By submitting some news stories that are false and others that are true, DTOs benefit by both amplifying their own actions in the IE and undermining the reliability of sources of news that they cannot fully control.

When combating their rivals, DTOs frequently spread rumors about internal splits brewing within their rivals' ranks or misdeeds they have committed. These rumors are frequently believed, remarkably, despite extraordinarily low levels of public trust. DTOs can appear credible in contrast to the Mexican government, law enforcement, and media, which are often perceived as impotent or corrupt. Thus, competing narratives and information are shared by other actors, including social media users, armed vigilante groups, and rival DTOs. In that vacuum of trust, even the favored DTO may not be considered very credible by local residents, but it is only necessary that it appear more credible than the alternatives.

One of the most salient narratives pushed by DTOs is that they offer order and justice in an environment that is otherwise chaotic and unjust. These are not merely slogans. DTOs prove their commitment to maintaining order by hunting down robbers, rapists, and kidnappers and displaying them in public (alive or dead). In this way, DTOs manage to send a credible—albeit absurd—message that they are the local population's best ally in the cause to restore order and safety to the community.

Other DTO Capabilities or Practices with Which the U.S. Army Must Be Prepared to Contend

Other tactics are essentially acts of terrorism designed to sow chaos, despair, and mistrust. A key tactic is to destroy the reputation of law enforcement and government by spreading (possibly true) rumors of abuses by police and corruption of government officials. In similar circumstances, the U.S. Army should be able to defend itself against such rumors, baseless or otherwise.

The popular DTO claim to protect the safety and security of citizens in controlled territories is, objectively, absurd and paradoxical. That anyone believes it is a testament to DTOs' ability to direct fires in the IE. The Army should prepare to highlight those contradictions by facilitating accurate reporting on adversary activities.

In their adoption of local cultural and religious symbols, DTOs effectively tailor their message in a way with which residents are comfortable. Folk figures, such as Santa Muerte and Jesus Malverde, predate the DTOs, but the past decade has seen them embraced and updated, as exemplified by the deification of "San Nazario." DTOs have sponsored these activities knowing that they carry latent cultural meaning, they have strong appeal to a public that is both highly religious and impoverished, and they are highly visible symbols of authority and trust.

A key aspect of the cultural appeal of DTOs is that their leaders can reputably claim to come from the same geographic area, the same culture, and the same depressed economic conditions as the publics they seek to influence. This fits the narrative of economic empowerment, in which taking up work for a DTO might be a youth's best chance at a middle-class lifestyle. It also fits narratives of cultural solidarity, which DTOs use to convince local residents to take their side rather than support a rival from an adjacent territory or cooperate with federal law enforcement. By integrating their organization into a community's socio-economic fabric, DTOs can secure the support of local communities, but this requires closely tying perceptions of economic performance and identity to illicit activities.

References

Aaron, David, *In Their Own Words: Voices of Jihad*, Santa Monica, Calif.: RAND Corporation, MG-602-RC, 2008. As of January 30, 2018:
https://www.rand.org/pubs/monographs/MG602.html

"About Lawfare: A Brief History of the Term and the Site," *Lawfare Blog*, undated. As of January 30, 2018:
https://www.lawfareblog.com/about-lawfare-brief-history-term-and-site

Alfoneh, Ali, *Indoctrination of the Revolutionary Guards*, Middle Eastern Outlook No.2, American Enterprise Institute, February 2009.

Alkhouri, Laith, and Alex Kassirer, *Tech for Jihad: Dissecting Jihadists' Digital Toolbox*, New York: Flashpoint, July 2016. As of January 30, 2018:
https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf

Al-Rawi, Ahmed, "Video Games, Terrorism and ISIS's Jihad 3.0," *Terrorism and Political Violence*, August 5, 2016.

Al-Tamimi, Aymenn Jawad, "Archive of Islamic State's Administrative Documents," *Pundicity*, January 11, 2016.

Amarasingam, Amarnath, "What Twitter Really Means for Islamic State Supporters," *War on the Rocks*, December 30, 2015. As of January 30, 2018:
https://warontherocks.com/2015/12/what-twitter-really-means-for-islamic-state-supporters

Anderson, Brian, "The Drug Cartels' IT Guy," *Motherboard*, March 3, 2015. As of January 30, 2018:
https://motherboard.vice.com/en_us/article/9akgj8/radio-silence

Applebaum, Anne, and Edward Lucas, "The Danger of Russian Disinformation," *Washington Post*, May 6, 2016.

Arango, Tim, "Uneasy Alliance Gives Insurgents an Edge in Iraq," *New York Times*, June 18, 2014.

Army Recognition, "New Dingo 2 A3 Armoured Vehicle PSYOPS: Psychological Operations of German Army," web page, March 26, 2012. No longer available online.

Ash, Lucy, "How Russia Outfoxes Its Enemies," *BBC News Magazine*, January 29, 2015. As of January 30, 2018:
http://www.bbc.com/news/magazine-31020283

Åslund, Anders, "Why Has Russia's Economic Transformation Been So Arduous?" paper prepared for the Annual World Bank Conference on Development Economics, Washington, D.C., April 28–30, 1999.

Asser, Martin, "Qana Makes Grim History Again," BBC News, July 31, 2006. As of January 30, 2018:
http://news.bbc.co.uk/2/hi/middle_east/5228554.stm

Associated Press, "Official Suicide Bomb Attack Kills 30 Afghan Trainee Police," NBC 26 (Green Bay, Wisc.), June 30, 2016. As of January 30, 2018:
http://www.nbc26.com/news/world/official-suicide-bomb-attack-kills-30-afghan-trainee-police

Bailey, Tracy A., "Ranger Graduates Kaibil School," *ShadowSpear Special Operations*, December 18, 2012. As of January 30, 2018:
http://www.shadowspear.com/2012/12/army-ranger-graduates-kaibil-school

Baranovsky, Alexei, "The Information War Over the Conflict in South Ossetia: The Analysis and Conclusions," osetinfo.ru, November 11, 2008. No longer available online.

Barnes, Julian E., "NATO Moving to Create New Intelligence Chief Post," *Wall Street Journal*, June 3, 2016.

Barry, Ellen, "Abkhazia Is Recognized—by Nauru," *New York Times*, December 15, 2009.

Basile, Mark, "Going to the Source: Why Al Qaeda's Financial Network Is Likely to Withstand the Current War on Terrorist Financing," *Studies in Conflict and Terrorism*, Vol. 27, No. 3, 2004, pp. 169–185.

Bearak, Max, "When ISIS Claims Terrorist Attacks, It's Worth Reading Closely," *Washington Post*, July 26, 2016.

Becerra-Acosta, Juan Pablo, "GATES, Policías de Élite que Combaten Narcos en Coahuila, Bajan la Delincuencia" ["GATES, Elite Police That Combat Narcos in Coahuila, Lower Crime"] *El Milenio*, May 30, 2015. As of January 30, 2018:
http://www.milenio.com/policia/gates_fuerza_especial_coahuila-baja_delincuencia_coahuila-gates_0_526747678.html

Bell, Stewart, "The Propaganda Wing of ISIL Has Recruited Several Canadians, Former CSIS Official Says," *National Post*, April 27, 2016. As of January 30, 2018:
http://nationalpost.com/news/canada/the-propaganda-wing-of-isil-has-recruited-several-canadians-former-csis-official-says

Bergamin, Oscar A. M., "Miss Kosovo als 'operative Waffe'" [Miss Kosovo as an 'Operational Weapon'"], *Allgemeine schweizerische Militärzeitschrift* [*General Swiss Military Magazine*], Vol. 170, No. 1, January 2004, pp. 40–41. As of January 30, 2018:
http://dx.doi.org/10.5169/seals-69205

Berger, J. M., "The Enduring Appeal of Al-Awlaqi's 'Constants on the Path of Jihad,'" *CTC Sentinel*, Vol. 4, No. 10, October 2011, pp. 12–15.

———, "The Decapitation Will Not Be Televised," *Foreign Policy*, July 3, 2016.

Berger, J. M., and Jonathan Morgan, *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*, Washington, D.C.: Brookings Project on U.S. Relations with the Islamic World, March 2015. As of January 30, 2018:
https://www.brookings.edu/research/the-isis-twitter-census-defining-and-describing-the-population-of-isis-supporters-on-twitter

Berman, Ilan, vice president, American Foreign Policy Council, "The Iranian Cyber Threat, Revisited," statement before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, March 20, 2013. As of January 30, 2018:
http://docs.house.gov/meetings/HM/HM08/20130320/100523/HHRG-113-HM08-Wstate-BermanI-20130320.pdf

Bershidsky, Leonid, "No Illusions Left, I'm Leaving Russia," *Moscow Times*, June 18, 2014. As of January 30, 2018:
https://themoscowtimes.com/articles/no-illusions-left-im-leaving-russia-36537

Bertrand, Natasha, "How 34 Commandos Created Mexico's Most Brutal Drug Cartel," *Business Insider*, March 5, 2015. As of January 30, 2018:
http://www.businessinsider.com/how-34-commandos-created-mexicos-most-brutal-drug-cartel-2015-3

———, "The U.S.-Led Coalition Is Dropping These Leaflets on ISIS' Capital in Syria to 'Mess with Them,'" *Business Insider*, May 21, 2016. As of January 30, 2018:
http://www.businessinsider.com/leaflets-isis-capital-raqqa-syria-2016-5

Blanford, Nicholas, "Hezbollah Applies New Training Practices in Syria," *Daily Star (Lebanon)*, June 8, 2013. As of January 30, 2018:
http://www.dailystar.com.lb/News/Politics/2013/Jun-08/219769-hezbollah-applies-new-training-practices-in-syria.ashx

Bodine-Baron, Elizabeth, Todd Helmus, Madeline Magnuson, and Zev Winkelman, *Examining ISIS Support and Opposition Networks on Twitter*, Santa Monica, Calif.: RAND Corporation, RR-1328-RC, 2016. As of January 30, 2018:
http://www.rand.org/pubs/research_reports/RR1328.html

Boltenkov, Dmitry, Aleksey Gayday, Anton Karnaukhov, Anton Lavrov, and Vyacheslav Tseluiko, *Russia's New Army*, Moscow: Centre for Analysis of Strategies and Technologies, 2011. As of January 30, 2018:
http://www.cast.ru/files/book/NewArmy_sm.pdf

Bower, Eve, "Germany's Libya Policy Reveals a Nation in Transition," *Deutsche Welle*, December 9, 2011. As of January 30, 2018:
http://www.dw.com/en/germanys-libya-policy-reveals-a-nation-in-transition/a-15367751

Brachman, Jarret, "The Next Osama," *Foreign Policy*, September 10, 2009.

———, "The Worst of the Worst," *Foreign Policy*, January 22, 2010.

Brachman, Jarret M., and William F. McCants, "Stealing Al Qaeda's Playbook," *Studies in Conflict and Terrorism*, Vol. 29, No. 2, 2006, pp. 309–321.

Brady, Anne-Marie, "China's Foreign Propaganda Machine," *Journal of Democracy*, Vol. 26, No. 4, October 2015, pp. 51–59.

Brewster, Murray, "Former CSIS Head Says Canada Should Have Its Own Cyber-Warriors," CBC News, June 22, 2016. As of January 30, 2018:
http://www.cbc.ca/beta/news/politics/military-cyber-wars-fadden-1.3648214

Brittingham, Angela, and G. Patricia de la Cruz, *Ancestry: 2000, Census 2000 Brief*, Washington, D.C.: U.S. Census Bureau, June 2004. As of January 30, 2018:
https://www.census.gov/prod/2004pubs/c2kbr-35.pdf

Brooking, Emerson T., and P. W. Singer, "War Goes Viral," *The Atlantic*, November 2016. As of January 30, 2018:
https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125

Browne, Ryan, and Barbara Starr, "U.S. Military Official: 50 ISIS Foreign Fighters Captured Since November," CNN, December 12, 2017. As of January 30, 2018:
https://www.cnn.com/2017/12/12/politics/isis-foreign-fighters-captured-syria-iraq

Brühl, Jannis, "Why NSA Snooping Is Bigger Deal in Germany," ProPublica, August 23, 2013. As of January 30, 2018:
https://www.propublica.org/article/why-nsa-snooping-is-bigger-deal-in-germany

Brun, Itai, "The Second Lebanon War, 2006," in John Andreas Olsen, ed., *A History of Air Warfare*, Washington D.C.: Potomac Books, 2010, pp. 297–323.

Bruno, Greg, "Al-Qaeda's Financial Pressures," backgrounder, Council on Foreign Relations, February 1, 2010. As of January 30, 2018:
https://www.cfr.org/backgrounder/al-qaedas-financial-pressures

Bump, Philip, "Donald Trump Is Just About Over This Whole NATO Thing," *Washington Post*, March 21, 2016.

Bundeswehr, Twitter account, undated. As of October 2017:
https://twitter.com/bundeswehrinfo

———, YouTube account, undated. As of October 2017:
https://www.youtube.com/user/Bundeswehr/videos

———, Facebook post on Naval Squadron 5 humanitarian assistance/disaster relief operations, March 22, 2016. As of January 30, 2018:
https://www.facebook.com/Bundeswehr/photos/a.234673006597299.61167.122840837780517/1103606059703985/?type=3&theater

———, "Der Einsatz im Kosovo" ["Deployment to Kosovo"], web page, last updated May 24, 2017. As of May 24, 2017:
http://www.einsatz.bundeswehr.de/portal/a/einsatzbw/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pPKU1PjUzLzixJIqIDcxu6Q0NScHKpRaUpWql51fnF-

Bundeswehr Joint Support Service, "Zentrum Operative Kommunikation der Bundeswehr" ["Center for Operational Communication of the Bundeswehr"], web page, last updated January 10, 2014. As of May 24, 2017:
http://www.kommando.streitkraeftebasis.de/portal/poc/kdoskb?uri=ci:bw.skb_kdo.terraufg.zopinfo

———, "Bataillon Elektronische Kampfführung 911: Über uns" ["Electronic Warfare Battalion 911: About Us"], web page, last updated June 1, 2016a. As of May 22, 2017:
http://www.kommando.streitkraeftebasis.de/portal/poc/kdoskb?uri=ci:bw.skb_kdo.ksa.elokabtl911.ueberuns

———, "Kommando Strategische Aufklärung" ["Strategic Reconnaissance Command"], web page, last updated June 1, 2016b. As of May 24, 2017:
http://www.kommando.streitkraeftebasis.de/portal/poc/kdoskb?uri=ci:bw.skb_kdo.ksa

———, "Zentrum Zivil-Militärische Zusammenarbeit der Bundeswehr" ["Center for Civil-Military Cooperation of the Bundeswehr"], web page, last updated June 3, 2016c. As of May 24, 2017:
http://www.kommando.streitkraeftebasis.de/portal/poc/kdoskb?uri=ci:bw.skb_kdo.terraufg.zentrzmzbw.ueberuns

———, "Operative Kommunikation—Die Medienmacher" ["Operational Communication: The Media Managers"], web page, last updated July 1, 2016d. As of May 24, 2016:
http://www.streitkraeftebasis.de/portal/a/streitkraeftebasis/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK94uyk-ILMKr3SnNTM4hK9_ILMvLR8_YJsR0UANB0R0Q!!/

———, "Organisation," web page, last updated February 1, 2017a. As of May 24, 2017:
http://www.streitkraeftebasis.de/portal/poc/streitkraeftebasis?uri=ci:bw.skb_piz.uberun.organi

———, “Zentrum Informationsarbeit Bundeswehr: Über uns” [“Center for Information Work of the Bundeswehr: About Us”], web page, last updated May 11, 2017b. As of May 24, 2017: http://www.kommando.streitkraeftebasis.de/portal/poc/kdoskb?uri=ci:bw.skb_kdo.ska.zinfoabw.ueberuns

———, “Bataillon Elektronische Kampfführung 912: Über uns” [“Electronic Warfare Battalion 912: About Us”], web page, last updated July 28, 2017c. As of August 31, 2017: http://cir.bundeswehr.de/portal/a/cir/start/dienststellen/ksa/elokabtl912/ueberuns

Bundeswehr Planning Office, *Defense Policy Guidelines*, Berlin, May 27, 2011. As of May 24, 2017: http://www.planungsamt.bundeswehr.de/portal/a/plgabw/!ut/p/c4/FYw7DoAwDMVuRHY2TsFnQaFE6ZNCqNpSrk-RB3sybdRxblCuuJ2NFloDxuMdkil3aX78NFbxoUmughP6uJZ0GypKiLJnhFgNDnGa_6Eprb3TdU0firMuqg!!

Bunker, Robert, “The Growing Mexican Cartel and Vigilante War in Cyberspace: Information Offensives and Counter-Offensives,” *Small Wars Journal*, November 3, 2011.

Burenok, Vasily Mikhailovich, Базис сетецентрических войн—опережение, интеллект, инновации . . . [“The Basis of Network-Centric Warfare Is Proactive, Intelligence, Innovation . . . ”], *Independent Newspaper (Russia)*, February 4, 2010. As of January 30, 2018: http://nvo.ng.ru/concepts/2010-04-02/1_bazis.html

Buyny, Lothar, “Implementing STRATCOM,” *Three Swords Magazine*, No. 28, May 2015, pp. 39–44.

Byman, Daniel, *A High Price: The Triumphs and Failures of Israeli Counterterrorism*, New York: Oxford University Press, 2011.

———, *Al Qaeda, The Islamic State and the Global Jihadist Movement: What Everyone Needs to Know*, New York: Oxford University Press, 2015.

Byman, Daniel, Shahram Chubin, Anoushiravan Ehteshami, and Jerrold D. Green, *Iran’s Security Policy in the Post-Revolutionary Era*, Santa Monica, Calif.: RAND Corporation, MR-1320-OSD, 2001. As of January 30, 2018:
http://www.rand.org/pubs/monograph_reports/MR1320.html

Caldwell, William B. IV, Dennis M. Murphy, and Anton Menning, “Learning to Leverage New Media: The Israeli Defense Forces in Recent Conflicts,” *Military Review*, May–June 2009, pp. 2–10.

Callimachi, Rukmini, “A News Agency with Scoops Directly from ISIS, and a Veneer of Objectivity,” *New York Times*, January 14, 2016a.

———, “How a Secretive Branch of ISIS Built a Global Network of Killers,” *New York Times*, August 3, 2016b.

Campion-Smith, Bruce, “Liberals Consider Peacekeeping Mission to Africa,” *Toronto Star*, July 14, 2016. As of January 30, 2018:
https://www.thestar.com/news/canada/2016/07/14/liberals-consider-peacekeeping-mission-to-africa.html

Canadian Armed Forces, *CF Information Operations*, B-GG-005-004/AF-010, April 15, 1998.

———, *Psychological Operations*, Ottawa, Ont., B-GJ-005-313/FP-001, January 15, 2004.

———, *Land Operations*, Ottawa, Ont., B-GL-300-001/FP-00, January 1, 2008.

Canadian Army, “Army Lessons Learned Centre (ALLC),” web page, undated. As of January 30, 2018:
http://www.army-armee.forces.gc.ca/en/lessons-learned-centre/lessons-learned-index.page

———, “21 Electronic Warfare Regiment,” web page, last updated June 23, 2016. As of May 22, 2017:
http://www.army-armee.forces.gc.ca/en/21-electronic-warfare-regiment/index.page

———, “Psychological Operations,” web page, last updated May 6, 2017. As of May 22, 2017:
http://www.army-armee.forces.gc.ca/en/5-cdn-div-ia/psyops.page

Canadian Department of National Defence, *Canada First Defence Strategy*, Ottawa, Ont., June 2008. As of May 24, 2017:
http://www.forces.gc.ca/assets/FORCES_Internet/docs/en/about/CFDS-SDCD-eng.pdf

———, *Strong, Secure, Engaged: Canada’s Defence Policy*, Ottawa, Ont., 2017. As of October 5, 2017:
http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf

Canadian Department of National Defence and Canadian Armed Forces, *A Role of Pride and Influence in the World: Canada’s International Policy Statement*, Ottawa, Ont., April 2005. As of January 30, 2018:
http://publications.gc.ca/site/eng/9.687487/publication.html

———, *2015–16 Report on Plans and Priorities*, Ottawa, Ont., 2015a. As of January 30, 2018:
http://www.forces.gc.ca/assets/FORCES_Internet/docs/en/dnd-rpp-2015-16_eng.pdf

———, “Organization—Communications and Electronic Branch,” web page, last updated July 28, 2015b. As of May 24, 2017:
http://www.forces.gc.ca/en/caf-community-branches-comm-elec/org.page

———, “Communications and Electronic Branch: About Us,” web page, last updated July 29, 2015c. As of May 22, 2017:
http://www.forces.gc.ca/en/caf-community-branches-comm-elec/org-about.page

———, “Courses at the Peace Support Training Centre,” web page, last updated February 24, 2016a. As of May 22, 2017:
http://www.forces.gc.ca/en/training-establishments/peace-support-courses.page

———, “Canadian Army,” web page, last updated August 3, 2016b. As of May 24, 2017:
http://www.forces.gc.ca/en/about-org-structure/canadian-army.page

———, “Peace Support Training Centre (PSTC),” web page, last updated August 22, 2016c. As of May 24, 2017:
http://www.forces.gc.ca/en/training-establishments/peace-support-index.page

———, “Defence Policy Review,” web page, last updated November 16, 2016d. As of May 24, 2017:
http://dgpaapp.forces.gc.ca/en/defence-policy-review/index.asp

———, “Assistant Deputy Prime Minister (Public Affairs),” web page, last updated December 8, 2016e. As of May 24, 2017:
http://www.forces.gc.ca/en/about-org-structure/assistant-deputy-minister-public-affairs.page

———, “Canadian Joint Operations Command,” web page, last updated December 8, 2016f. As of May 24, 2017:
http://www.forces.gc.ca/en/about-org-structure/canadian-joint-operations-command.page

———, “Organizational Structure,” web page, last updated May 1, 2017a. As of May 24, 2017:
http://www.forces.gc.ca/en/about-org-structure/index.page

———, “The Disaster Assistance Response Team,” web page, last updated May 19, 2017b. As of May 24, 2017:
http://www.forces.gc.ca/en/operations-abroad-recurring/dart.page

———, "Frequently Asked Questions," web page, last updated October 27, 2017. As of November 17, 2017:
http://www.forces.gc.ca/en/about/faq.page

Casebeer, William D., and James A. Russell, "Storytelling and Terrorism: Towards a Comprehensive 'Counter-Narrative Strategy,'" *Strategic Insights*, Vol. 4, No. 3, March 2005.

Cavelty, Myriam Dunn, "Cyber-Allies: Strengths and Weaknesses of NATO's Cyberdefense Posture," *IP Global Edition*, Vol. 12, No. 3, 2011, pp. 11–15.

Cave, Damien, "Mexico Turns to Social Media for Information and Survival," *New York Times*, September 24, 2011.

Central Intelligence Agency, "Iran," *World Factbook*, undated(a). As of May 22, 2017:
https://www.cia.gov/library/publications/the-world-factbook/geos/ir.html

———, "Korea, North," *World Factbook*, undated(b). As of May 22, 2017:
https://www.cia.gov/library/publications/the-world-factbook/geos/kn.html

Chen, Adrian, "The Agency," *New York Times Magazine*, June 2, 2015.

Cheng, Dean, "Winning Without Fighting: The Chinese Psychological Warfare Challenge," Washington, D.C.: Heritage Foundation, Backgrounder No. 2821, July 11, 2013. As of January 30, 2018:
http://www.heritage.org/global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge

China State Council Information Office, *China's Peaceful Development Road*, Beijing, 2005. As of January 30, 2018:
http://www.chinadaily.com.cn/english/doc/2005-12/22/content_505678.htm

Ci Weixu, ed., *100 Questions About Psychological Warfare*, Beijing: Liberation Army Press, 2004.

Clarke, Colin P., and Chad C. Serena, "To Defeat ISIL's Brand, Its Territory Must Be Reclaimed," *National Interest*, July 8, 2016a. As of January 30, 2018:
http://nationalinterest.org/blog/the-buzz/defeat-isils-brand-its-territory-must-be-reclaimed-16890

———, "This Is the Problem with Trying to Destroy the Islamic State," *Washington Post Monkey Cage Blog*, July 12, 2016b.

Clarke, Colin P., and Daveed Gartenstein-Ross, "How Will Jihadist Strategy Evolve as the Islamic State Declines?" *War on the Rocks*, November 10, 2016. As of January 30, 2018:
https://warontherocks.com/2016/11/how-will-jihadist-strategy-evolve-as-the-islamic-state-declines

Clarke, Colin P., and Isaac R. Porche III, "The Online Fight Against ISIS," *Project Syndicate*, April 1, 2016. As of January 30, 2018:
https://www.project-syndicate.org/commentary/the-online-fight-against-isis-by-colin-p--clarke-and-isaac-r--porche-iii-2016-04

Coalson, Robert, "Twelve Who Left: A New Wave of Russian Emigration," Radio Free Europe/Radio Liberty, May 21, 2015. As of January 30, 2018:
http://www.rferl.org/content/russia-emigration-emigrants/26970465.html

Cockburn, Patrick, *The Rise of Islamic State: ISIS and the New Sunni Revolution*, London: Verso Books, 2015.

Cohen, Stuart A., "The Israel Defense Forces (IDF): From a 'People's Army' to a 'Professional Military'—Causes and Implications," *Armed Forces and Society*, Vol. 21, No. 2, Winter 1995, pp. 237–254.

Collins, Steven, "Army PSYOP in Bosnia: Capabilities and Constraints," *Parameters*, Summer 1999, pp. 57–73.

———, "Mind Games," NATO Review, No. 2, 2003. As of January 30, 2018:
http://www.nato.int/docu/review/2003/Wake-Iraq/Mind-games/EN/index.htm

Committee to Protect Journalists, "Journalists Killed in Russia Since 1992," web page, undated. As of January 30, 2018:
https://cpj.org/europe/russia

Comras, Victor, "Al Qaeda Finances and Funding to Affiliated Groups," in Jeanne K. Giraldo and Harold A. Trinkunas, eds., *Terrorism Financing and State Responses: A Comparative Perspective*, Stanford, Calif.: Stanford University Press, 2007, pp. 115–133.

Coombs, Howard G., "Afghanistan 2010–2011: Counterinsurgency Through Whole of Government," *Canadian Military Journal*, Vol. 13, No. 3, Summer 2013, pp. 16–24. As of January 30, 2018:
http://www.journal.forces.gc.ca/vol13/no3/doc/Coombs-Pages1624-eng.pdf

———, "North Atlantic Treaty Organization System Analysis and Studies 117," Human Behaviour Representation Research Task Group Symposium, Kingston, Ont., November 17–19, 2015.

Cooper, Helene, "U.S. Drops Snark in Favor of Emotion to Undercut Extremists," *New York Times*, July 28, 2016.

Corcoran, Patrick, "Inside the Moral Code of the Caballeros Drug Gang," Insight Crime, July 20, 2011. As of January 30, 2018:
http://www.insightcrime.org/news-analysis/inside-the-moral-code-of-the-caballeros-drug-gang

———, "Revelations of Mexico's Knights Templar Indoctrination Manual," Insight Crime, December 17, 2013. No longer available online.

Cordesman, Anthony H., "The Real Center of Gravity in the War Against the Islamic State," Washington, D.C.: Center for Strategic and International Studies, September 30, 2014. As of January 30, 2018:
https://www.csis.org/analysis/real-center-gravity-war-against-islamic-state

———, "Paris, ISIS, and the Long War Against Extremism," Washington, D.C.: Center for Strategic and International Studies, November 14, 2015. As of January 30, 2018:
https://www.csis.org/analysis/paris-isis-and-long-war-against-extremism

Cordesman, Anthony H., Steven Colley, and Michael Wang, *Chinese Strategy and Military Modernization in 2015: A Comparative Analysis*, Washington, D.C.: Center for Strategic and International Studies, updated October 10, 2015.

Coren, Courtney, "General Hayden: Panetta Right, Fighting ISIS Will Take 'Generation Plus,'" *Newsmax*, October 6, 2014. As of January 30, 2018:
http://www.newsmax.com/Newsmax-Tv/Leon-Panetta-ISIS-30-year-war/2014/10/06/id/598880

Cottee, Simon, "The Challenge of Jihadi Cool: Why ISIS Propaganda Is So Popular," *The Atlantic*, December 24, 2015. As of January 30, 2018:
https://www.theatlantic.com/international/archive/2015/12/isis-jihadi-cool/421776

Council of the European Union Military Staff, *EU Concept for Civil-Military Co-Operation (CIMIC) for EU-Led Military Operations*, Brussels, July 11, 2008. As of January 30, 2018:
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede260410euconceptcimic_/sede260410euconceptcimic_en.pdf

Council on Foreign Relations, *Winograd Commission Final Report*, Washington, D.C., January 30, 2008.

Counter Extremism Project, *Anwar al-Awlaki's Ties to Extremists*, New York, September 2016. As of January 30, 2018:
https://www.counterextremism.com/anwar-al-awlaki

Cox, Joseph, "Mexico's Drug Cartels Love Social Media," *Vice*, November 4, 2013. As of January 30, 2018:
https://www.vice.com/en_us/article/znwv8w/
mexicos-drug-cartels-are-using-the-internet-to-get-up-to-mischief

Cragin, R. Kim, "Early History of Al-Qa'ida," *Historical Journal*, Vol. 51, No. 4, December 2008, pp. 1047–1067.

Cruickshank, Paul, and Mohannad Hage Ali, "Abu Musab al-Suri: Architect of the New Al Qaeda," *Studies in Conflict and Terrorism*, Vol. 30, No. 1, 2007, pp. 1–14.

Cudmore, James, "Canadian Military Ponders Integrated Force with U.S. to Respond to Hotspots," CBC News, September 28, 2015. As of January 30, 2018:
http://www.cbc.ca/news/politics/canada-election-2015-canadian-us-integrated-force-1.3247362

Czech Ministry of Defense, "103. centrum CIMIC/PSYOPS: O nás" ["103rd CIMIC/PSYOPS Center: About Us"], web page, undated(a). As of May 24, 2017:
http://www.103cp.army.cz/o-nas

———, "Když se řekne psychologické operace" ["About Psychological Operations"], web page, undated(b). As of May 24, 2017:
http://www.army.cz/scripts/detail.php?id=1923

Czech Security Information Service, *Annual Report of the Security Information Service for 2015*, Prague, January 9, 2016. As of January 30, 2018:
https://www.bis.cz/vyrocni-zpravaEN890a.html?ArticleID=1104

Dai Qingmin, *Lun Wangdian Yiti Zhan* [*On Integrating Network Warfare and Electronic Warfare*], Beijing: PLA Press, 2002a.

———, "Lun Duoqu Zhi Xinxi Quan" ["On Seizing Information Supremacy"], *China Military Science*, Vol. 16, No. 2, April 2002b, pp. 11–13.

Dallal, A. J., "Hezbollah's Virtual Civil Society," Television and New Media, Vol. 2, No. 4, 2001, pp. 367–371.

Darczewska, Jolanta, *The Anatomy of Russian Information Warfare: The Crimean Operation, a Case Study*, Warsaw, Poland: Centre for Eastern Studies, May 2014. As of January 30, 2018:
https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf

Dauber, Cori E., and Mark Robinson, "ISIS and the Hollywood Visual Style," *Jihadology*, July 6, 2015. As of January 30, 2018:
http://jihadology.net/2015/07/06/guest-post-isis-and-the-hollywood-visual-style

Dausend, Peter, "Ethnologen in Flecktarn" ["Ethnologists in Flecktarn"], *Zeit Online*, August 6, 2015. As of January 30, 2018:
http://www.zeit.de/2015/30/bundeswehr-propaganda-medien

Dearden, Lizzie, "NATO Accuses Sputnik News of Distributing Misinformation as Part of 'Kremlin Propaganda Machine,'" *The Independent*, February 11, 2017. As of January 30, 2018:
http://www.independent.co.uk/news/world/europe/sputnik-news-russian-government-owned-controlled-nato-accuses-kremlin-propaganda-machine-a7574721.html

Delfs, Arne, and Henry Meyer, "Putin's Propaganda Machine Is Meddling with European Elections," Bloomberg, April 19, 2016.

De Luce, Dan, "Is the U.S. Ready for Endless War Against the Islamic State?" *Foreign Policy*, August 27, 2015.

Denning, Dorothy, "Information Operations and Terrorism," in Lars Nicander and Magnus Ranstorp, eds., *Innovative Terrorism in the Information Age: Understanding the Threat of Cyber-Warfare*, London: Hurst, unpublished, 2005.

Dettmer, Jamie, "Hezbollah Develops New Skills in Syria, Posing Challenges for Israel," Voice of America, April 27, 2016. As of January 30, 2018:
http://www.voanews.com/a/hezbollah-develops-new-skills-in-syria-posing-challenges-for-israel/3304664.html

Dimitriu, G. R., "Winning the Story War: Strategic Communication and the Conflict in Afghanistan," *Public Relations Review*, Vol. 38, No. 2, June 2012, pp. 195–207.

Drews, Dirk, *Die Psychologische Kampfführung/Psychologische Verteidigung der Bundeswehr—eine erziehungswissenschaftliche und publizistikwissenschaftliche Untersuchung* [*The Psychological Battlespace/Psychological Defense of the Bundeswehr—An Educational and Journalistic Examination*], dissertation, Mainz, Germany: Johannes Gutenberg-Universität Mainz, 2006. As of January 30, 2018:
https://publications.ub.uni-mainz.de/theses/volltexte/2006/981/pdf/981.pdf

Dunlap, Charles J., Jr., "Will 'Lawfare' Define Palestinian-Israeli Conflict?" *Al-Monitor*, July 30, 2014. As of January 30, 2018:
https://www.al-monitor.com/pulse/originals/2014/07/lawfare-palestine-israel-gaza-conflict-dunlap.html

Dyer, Geoff, "FT Explainer: Can the U.S. Election be Hacked?" *Financial Times*, August 30, 2016.

Efremov, Steven M., *The Role of Inflation in Soviet History: Prices, Living Standards, and Political Change*, thesis, Johnson City, Tenn.: East Tennessee State University, August 2012. As of January 30, 2018:
http://dc.etsu.edu/etd/1474

Egleder, Julia, *Peace Through Peace Media? The Media Activities of the International Missions (KFOR and UNMIK) and Their Contribution to Peacebuilding in Kosovo from 1999 Till 2008*, dissertation, Regensberg and Münster, Germany: University of Regensburg, and LIT Verlag, 2013.

Eisenstadt, Michael, "The Missing Lever: Information Activities Against Iran," Washington, D.C.: Washington Institute for Near East Policy, Policy Notes No. 1, March 2010. As of January 30, 2018:
http://www.washingtoninstitute.org/policy-analysis/view/the-missing-lever-information-activities-against-iran

Eisenstadt, Michael, Michael Knights, and Ahmed Ali, *Iran's Influence in Iraq: Countering Tehran's Whole-of-Government Approach*, Washington, D.C.: Washington Institute for Near East Policy, Policy Focus No. 111, April 2011.

Eiss, Paul K., "The Narcomedia: A Reader's Guide," *Latin American Perspectives*, Vol. 41, No. 2, March 2014, pp. 78–98.

"Ejecutan a Tres los Mata Zetas" ["Zeta Killers Execute Three"], *El Universal*, June 19, 2009. As of January 30, 2018:
http://archivo.eluniversal.com.mx/nacion/169098.html

Elliot, Chris, "The Readers' Editor on . . . Pro-Russia Trolling Below the Line on Ukraine Stories," *The Guardian*, May 4, 2014. As of January 30, 2018:
http://www.theguardian.com/commentisfree/2014/may/04/pro-russia-trolls-ukraine-guardian-online

Elson, Sara Beth, Douglas Yeung, Parisa Roshan, S. R. Bohandy, and Alireza Nader, *Using Social Media to Gauge Iranian Public Opinion and Mood After the 2009 Election*, Santa Monica, Calif.: RAND Corporation, TR-1161-RC, 2012. As of January 30, 2018:
http://www.rand.org/pubs/technical_reports/TR1161.html

Engel, Pamela, "How ISIS Monitors and Restricts Internet Access in the ISIS 'Caliphate,'" *Business Insider*, November 7, 2015. As of January 30, 2018:
http://www.businessinsider.com/how-isis-governs-its-caliphate-2015-11

Engelbrekt, Kjell, Marcus Mohlin, and Charlotte Wagnsson, eds., *The NATO Intervention in Libya: Lessons Learned from the Campaign*, New York: Routledge, 2013.

Ennis, Stephen, "Russia Brain Drain After Putin Crackdown," BBC News, October 2, 2014. As of January 30, 2018:
http://www.bbc.com/news/world-europe-29450930

"Era un Secreto a Voces que 'El Chayo' Estaba Vivo: Castillo" ["It Was an Open Secret That 'El Chayo' Was Alive: Castillo"], *El Milenio*, March 10, 2014. As of January 30, 2018:
http://www.milenio.com/policia/muere_Nazario_Moreno-confirman_muerte_de_El_Chayo-templarios-Michoacan-Castillo_0_259774086.html

Ernst, Falko A., "Seeking a Place in History—Nazario Moreno's Narco Messiah," Insight Crime, March 12, 2014. As of January 30, 2018:
http://www.insightcrime.org/news-analysis/seeking-a-place-in-history-narazio-moreno-narco-messiah

Esfandiary, Dina, and Ariane Tabatabai, "Iran's Cyberattacks Are Likely to Increase. Here's Why," *Washington Post Monkey Cage Blog*, November 18, 2015. As of January 30, 2018:
https://www.washingtonpost.com/news/monkey-cage/wp/2015/11/18/irans-cyberattacks-are-likely-to-increase-heres-why/?utm_term=.01e4c4bb16a0

Estes, Adam Clark, "Mexico's Tales of Bus Passengers Forced to Fight to the Death," *The Atlantic*, June 14, 2011. As of January 30, 2018:
https://www.theatlantic.com/international/archive/2011/06/gladiator-death-fights-mexico-drug-war/351738

"Excerpts of the 'Code of the Knights Templar' Cartel," Associated Press, July 20, 2011.

Faiola, Anthony, and Souad Mekhennet, "What's Happening to Our Children?" *Washington Post*, February 11, 2017.

Feickert, Andrew, *U.S. Special Operations Forces (SOF): Background and Issues for Congress*, Washington, D.C.: Congressional Research Service, April 8, 2016.

Ferland, Elisabeth, "Hezbollah and the Internet," Washington, D.C.: Center for Strategic and International Studies, March 4, 2010.

Fernandez, Alberto M., *Here to Stay and Growing: Combating ISIS Propaganda Networks*, Washington, D.C.: Brookings Project on U.S. Relations with the Islamic World, October 2015. As of January 30, 2018:
https://www.brookings.edu/wp-content/uploads/2016/06/IS-Propaganda_Web_English.pdf

Fifiled, Anna, "Punishing North Korea: A Rundown on Current Sanctions," *Washington Post*, February 22, 2016.

Filkins, Dexter, "The Shadow Commander," *New Yorker*, September 30, 2013.

Fincham, Christopher, "U.S. Army Medics Train German Psyops Soldiers," U.S. Army, June 29, 2011. As of January 30, 2018:
http://www.army.mil/article/60788/U_S__Army_Medics_train_German_Psyops_Soldiers

Fisher, Matthew, “Route Hyena a Canadian-Built ‘Dagger Through the Heart of the Taliban,’” Postmedia News, April 13, 2011. As of January 30, 2018:
http://www.canada.com/news/route+hyena+canadian+built+dagger+through+heart+taliban/4584232/story.html

Fisk, Robert, “Television News Is Secret Weapon of the Intifada,” *The Independent*, December 2, 2000.

Fitzpatrick, Catherine A., “Russia This Week: Here Comes the Kremlin’s Troll Army (2–7 June),” *The Interpreter*, June 6, 2014. As of January 30, 2018:
http://www.interpretermag.com/14302

Flock, Elizabeth, “Mexican Cartel Decapitates Web Commenter in Latest String of Internet Attacks,” *Washington Post*, September 26, 2011.

Forsythe, Michael, and Andew Jacobs, “In China, Books That Make Money, and Enemies,” *New York Times*, February 4, 2016.

Foster, Peter, and Matthew Holehouse, “Russia Accused of Clandestine Funding of European Parties as U.S. Conducts Major Review of Vladimir Putin’s Strategy,” *The Telegraph*, January 16, 2016. As of January 30, 2018:
http://www.telegraph.co.uk/news/worldnews/europe/russia/12103602/America-to-investigate-Russian-meddling-in-EU.html

Fox, Edward, “Knights Templar Leader Makes Rare Video Appearance,” Insight Crime, August 31, 2012. As of January 30, 2018:
http://www.insightcrime.org/news-analysis/knights-templar-leader-appears-in-video

Fuchs, Christian, “Bundeswehr will soziale Netzwerke überwachen” [“Bundeswehr Wants to Monitor Social Networks”], *Zeit Online*, June 2, 2014. As of January 30, 2018:
http://www.zeit.de/politik/deutschland/2014-06/ueberwachung-bundeswehr-facebook-twitter-social-media

Fuller, Graham E., “The Hezbollah-Iran Connection: Model for Sunni Resistance,” *Washington Quarterly*, Vol. 30, No. 1, Winter 2006–2007, pp. 139–150.

Galeotti, Mark, “The ‘Gerasimov Doctrine’ and Russian Non-Linear War,” *In Moscow’s Shadows*, July 6, 2014. As of January 30, 2018:
https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war

Galloway, Chris, “Media Jihad: What PR Can Learn in Islamic State’s Public Relations Masterclass,” *Public Relations Review*, Vol. 42, No. 4, November 2016, pp. 582–590.

Gartenstein-Ross, Daveed, Nathaniel Barr, and Bridget Moreng, *The Islamic State’s Global Propaganda Strategy*, The Hague, Netherlands: International Center for Counter Terrorism, March 2016a.

———, “How the Islamic State’s Propaganda Feeds into Its Global Expansion Efforts,” *War on the Rocks*, April 28, 2016b. As of January 30, 2018:
https://warontherocks.com/2016/04/how-islamic-states-propaganda-feeds-into-its-global-expansion-efforts

Geers, Kenneth, ed., *Cyber War in Perspective: Russian Aggression Against Ukraine*, Talinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015. As of January 30, 2018:
https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf

George, Alexander L., *The Chinese Communist Army in Action: The Korean War and Its Aftermath*, New York: Columbia University Press, 1967.

German Federal Constitutional Court, *Judgment of the First Senate of 27 February 2008*, Berlin, February 27, 2008. As of January 30, 2018:
http://www.bverfg.de/e/rs20080227_1bvr037007en.html

German Federal Foreign Office, "Kosovo," web page, last updated April 2017. As of May 24, 2017:
http://www.auswaertiges-amt.de/EN/Aussenpolitik/Laender/Laenderinfos/01-Nodes/Kosovo_node.html

German Federal Ministry of Defence, *White Paper 2006 on German Security Policy and the Future of the Bundeswehr*, Berlin, 2006. As of January 30, 2018:
https://www.files.ethz.ch/isn/156941/Germany%202006%20white%20paper.pdf

———, *The Bundeswehr on Operations: Publication to Mark the 15th Anniversary of the First Parliamentary Mandate for Armed Bundeswehr Missions Abroad*, 2nd ed., Berlin, June 2009.

———, "Journalismus über Militär und Krieg im digitalen Zeitalter" ["Journalism on Military and War in the Digital Age"], web page, last updated January 7, 2015. No longer available online.

German Federal Ministry of the Interior, *Cyber Security Strategy for Germany*, Berlin, February 2011. As of January 30, 2018:
https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

Gertz, Bill, "China Using Retired U.S. Officers to Influence Policy," *Washington Times*, February 7, 2012.

Giles, Keir, *Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, London: Chatham House, March 2016. As of January 30, 2018:
https://www.chathamhouse.org/publication/russias-new-tools-confronting-west

Gillespie, R. D., "German Psychological Warfare," *British Medical Journal*, Vol. 1, No. 4239, April 4, 1942, pp. 445–448. As of January 30, 2018:
http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2164895

Glasser, Susan B., and Steve Coll, "The Web as Weapon," *Washington Post*, August 9, 2005.

Glasser, Susan B., and Walter Pincus, "Seized Letter Outlines Al Qaeda Goals in Iraq," *Washington Post*, October 12, 2005.

Glenn, Russell W., *All Glory Is Fleeting: Insights from the Second Lebanon War*, Santa Monica, Calif.: RAND Corporation, MG-708-1-JFCOM, 2012. As of January 30, 2018:
https://www.rand.org/pubs/monographs/MG708-1.html

GlobalSecurity.org, "Sweden: Defense Policy," web page, last updated July 5, 2016. As of May 24, 2017:
http://www.globalsecurity.org/military/world/europe/se-policy.htm

Gómez, Juan Miguel del Cid, "A Financial Profile of the Terrorism of Al-Qaeda and Its Affiliates," *Perspectives on Terrorism*, Vol. 4, No. 4, October 2010.

Goodman, J. David, "In Mexico, Social Media Become a Battleground in the Drug War," *New York Times Lede Blog*, September 15, 2011. As of January 30, 2018:
https://thelede.blogs.nytimes.com/2011/09/15/in-mexico-social-media-becomes-a-battleground-in-the-drug-war/?_r=0

Gould, Joe, "Electronic Warfare: What US Army Can Learn from Ukraine," *Defense News*, August 2, 2015. As of January 30, 2018:
http://www.defensenews.com/story/defense/policy-budget/warfare/2015/08/02/us-army-ukraine-russia-electronic-warfare/30913397

Grace, Robert, and Andrew Mandelbaum, *Understanding the Iran-Hezbollah Connection*, Washington, D.C.: United States Institute of Peace, September 2006. As of January 30, 2018: https://www.usip.org/publications/2006/09/understanding-iran-hezbollah-connection

Grant, Will, "Mexico Violence: Fear and Intimidation," BBC News, May 15, 2012. As of January 30, 2018: http://www.bbc.com/news/world-latin-america-18063328

Grayson, George W., *La Familia Drug Cartel: Implications for U.S.-Mexican Security*, Carlisle Barracks, Pa.: U.S. Army War College, Strategic Studies Institute, December 2010.

———, *The Evolution of Los Zetas in Mexico and Central America: Sadism as an Instrument of Cartel Warfare*, Carlisle Barracks, Pa.: U.S. Army War College, Strategic Studies Institute, April 2014.

Green, Jerrold D., Frederic Wehrey, and Charles Wolf, Jr., *Understanding Iran*, Santa Monica, Calif.: RAND Corporation, MG-771-SRF, 2009. As of January 30, 2018: http://www.rand.org/pubs/monographs/MG771.html

Greenhill, Robert, and Megan McQuillan, *Assessing Canada's Global Engagement Gap*, OpenCanada, October 6, 2015. As of January 30, 2018: https://www.opencanada.org/features/canadas-global-engagement-gap

Griffis, William Elliot, *Corea: The Hermit Nation*, New York: Charles Scribner's Sons, 1894.

Grillo, Ioan, "Behind Mexico's Wave of Beheadings," *Time*, September 8, 2008. As of January 30, 2018: http://content.time.com/time/world/article/0,8599,1839576,00.html

Groisman, Maayan, "ISIS Destroys Syrian Satellite Dishes in Bid to Ban 'Un-Islamic' TV During Ramadan," *Jerusalem Post*, June 2, 2016.

Grytsenko, Oksana, "Ukrainian Protesters Flood Kiev After President Pulls Out of EU Deal," *The Guardian*, November 24, 2013. As of January 30, 2018: https://www.theguardian.com/world/2013/nov/24/ukraine-protesters-yanukovych-aborts-eu-deal-russia

Guevara, America Y., "Propaganda in Mexico's Drug War," *Journal of Strategic Security*, Vol. 6, No. 3, Suppl., 2013, pp. 131–151.

Guo Yanhua, *Psychological Warfare Knowledge*, Beijing: People's Liberation Army National Defense University, 2005.

Guo Yuandan, "PLA Sets Up Overseas Operations Office to Strengthen Overseas Rapid Reaction," *China Military Online*, March 25, 2016. As of January 30, 2018: http://english.chinamil.com.cn/news-channels/pla-daily-commentary/2016-03/25/content_6977517.htm

Gustin, Sam, "The War Will Be Gamified: Israel, Hamas in Social Media Struggle," *Time*, November 16, 2012. As of January 30, 2018: http://newsfeed.time.com/2012/11/16/the-war-will-be-gamified-israel-hamas-in-social-media-struggle

Hallow, Ralph Z., "Republicans Fear Exchange Program Put National Security at Risk," *Washington Times*, April 19, 2012. As of January 30, 2018: http://www.washingtontimes.com/news/2012/apr/19/republicans-fear-exchange-program-put-national-sec

Hamzeh, Ahmad Nizar, *In the Path of Hizbullah*, Syracuse, N.Y.: Syracuse University Press, 2004.

Harding, Joel, “Russian News, Russian Proxy News Sites and Conspiracy Theory Sites,” *To Inform Is to Influence*, November 15, 2015. As of January 30, 2018:
https://toinformistoinfluence.com/2015/11/15/russian-news-and-russian-proxy-news-sites

Harding, Luke, “Enemy of the State: How Luke Harding Became the Reporter Russia Hated,” *The Guardian*, September 23, 2011. As of January 30, 2018:
https://www.theguardian.com/world/2011/sep/23/luke-harding-russia

Harold, Scott Warren, Martin C. Libicki, and Astrid Cevallos, *Getting to Yes with China in Cyberspace*, Santa Monica, Calif.: RAND Corporation, RR-1335-RC, 2016. As of January 30, 2018:
http://www.rand.org/pubs/research_reports/RR1335.html

Hassan, Hassan, “Threats from Two Fronts: Al-Qaeda and IS Define Their Strategies,” Washington, D.C.: Tahrir Institute for Middle East Policy, May 25, 2016.

Hassan, Hassan, and Michael Weiss, *ISIS: Inside the Army of Terror*, New York: Simon and Schuster, 2015.

Headquarters, U.S. Department of the Army, *Insurgencies and Countering Insurgencies*, Field Manual 3-24/Marine Corps Warfighting Publication 3-33.5, Washington, D.C., May 2014.

Heemsbergen, Luke Justin, and Simon Lindgren, “The Power of Precision Airstrikes and Social Media Feeds in the 2012 Israel-Hamas Conflict: ‘Targeting Transparency,’” *Australian Journal of International Affairs*, Vol. 68, No. 5, 2014, pp. 569–591.

Heilig, René, “BND ausgebremst? Irrtum!” [“German Federal Intelligence Service Blocked? Error!”], *Neues Deutschland*, June 11, 2014. As of January 30, 2018:
https://www.neues-deutschland.de/artikel/935480.bnd-ausgebremst-irrtum.html

Heinle, Kimberly, Cory Molzahn, and David A. Shirk, *Drug Violence in Mexico: Data and Analysis Through 2014*, San Diego, Calif.: Justice in Mexico Project, University of San Diego, April 2015. As of January 30, 2018:
https://justiceinmexico.org/wp-content/uploads/2015/04/2015-Drug-Violence-in-Mexico-final.pdf

Herd, Graeme P., “The ‘Counter-Terrorist Operation’ in Chechnya: ‘Information Warfare’ Aspects,” *Journal of Slavic Military Studies*, Vol. 13, No. 4, 2000, pp. 57–83.

Herman, Steve, “Secret Manual Gives Glimpse of North Korean Military Tactics,” Voice of America, September 18, 2010. As of January 30, 2018:
http://www.voanews.com/a/secret-manual-gives-glimpse-of-north-korean-military-tactics-103253534/126266.html

Hernandez, Kristian, “Cartel Boss States ‘We Are Not Terrorists’ Using Narco Banners Throughout Reynosa,” *The Monitor (McAllen, Texas)*, November 3, 2015. As of January 30, 2018:
http://www.themonitor.com/premium/article_0ce5ba30-8291-11e5-8c6d-37ce662d4531.html

“Hezbollah: Rebel Without a Cause?” Brussels: International Crisis Group, Middle East Briefing Paper, July 30, 2003.

Hewlett Packard Enterprise, “HP Security Briefing, Episode 16—Profiling an Enigma: North Korea’s Cyber Threat Landscape,” August 27, 2014. As of January 30, 2018:
https://community.hpe.com/t5/Security-Research/HP-Security-Briefing-episode-16-Profiling-an-enigma-North-Korea/ba-p/6588592#.V-VlLGf2aWg

Higgins, Andrew, “Effort to Expose Russia’s ‘Troll Army’ Draws Vicious Retaliation,” *New York Times*, May 30, 2016.

Hiro, Dilip, *Lebanon Fire and Embers: A History of the Lebanese Civil War*, New York: St. Martin’s Press, 1992.

Hoffman, Bruce, "Al Qaeda Trends in Terrorism and Future Potentialities: An Assessment," paper presented at a meeting of the Council on Foreign Relations, Washington D.C., May 8, 2003.

———, "The Changing Face of Al Qaeda and the Global War on Terrorism," *Studies in Conflict and Terrorism*, Vol. 27, No. 6, 2004, pp. 549–560.

———, "Combating Al Qaeda and the Militant Islamic Threat," testimony before the U.S. House of Representatives Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats, and Capabilities, February 16, 2006. As of January 30, 2018:
https://www.rand.org/pubs/testimonies/CT255.html

———, "Al Qaeda's Uncertain Future," *Studies in Conflict and Terrorism*, Vol. 36, No. 8, 2013, pp. 635–653.

———, "Al Qaeda's Master Plan," *Cipher Brief*, November 18, 2015. As of January 30, 2018:
https://www.thecipherbrief.com/article/al-qaedas-master-plan

Hubbard, Ben, "ISIS Uses Ramadan as Call for New Terrorist Attacks," *New York Times*, July 3, 2016.

Huggler, Justin, "Germany Expands Its Army for First Time Since Cold War in Response to Threat of Isil," *The Telegraph*, May 10, 2016. As of January 30, 2018:
http://www.telegraph.co.uk/news/2016/05/10/
germany-expands-its-army-for-first-time-since-cold-war-in-respon

Hylton, Hilary, "How Hezbollah Hijacks the Internet," *Time*, August 8, 2006. As of January 30, 2018:
http://content.time.com/time/world/article/0,8599,1224273,00.html

Ingram, Haroro J., "Three Traits of the Islamic State's Information Warfare," *RUSI Journal*, Vol. 159, No. 6, December 2014, pp. 4–11.

———, "The Strategic Logic of Islamic State Information Operations," *Australian Journal of International Affairs*, Vol. 69, No. 6, 2015, pp. 729–752.

———, "How to Beat Back ISIS Propaganda," *National Interest*, June 15, 2016a. As of January 30, 2018:
http://nationalinterest.org/feature/how-beat-back-isis-propaganda-16598

———, *Deciphering the Siren Call of Militant Islamist Propaganda: Meaning, Credibility and Behavioural Change*, The Hague, Netherlands: International Centre for Counter-Terrorism, September 2016b. As of January 30, 2018:
https://icct.nl/wp-content/uploads/2016/09/ICCT-Ingram-Deciphering-the-Siren-Call-of-Militant-Islamist-Propaganda-September2016.pdf

Ingram, Haroro J., and Craig Whiteside, "The Yemen Raid and the Ghost of Anwar al-Awlaki," *The Atlantic*, February 9, 2017. As of January 30, 2018:
https://www.theatlantic.com/international/archive/2017/02/
yemen-raid-trump-awlaki-al-qaeda-isis/516180

"Internet Censorship in Iran," University of Pennsylvania, Annenberg School of Communications, Iran Media Program, March 13, 2013.

Iqbal, Muzaffar, *Definitive Encounters: Islam, Muslims, and the West*, Dehli, India: Al-Qalam Publishing, 2008.

"Islamic State Finds Diminishing Returns on Twitter: Report," Reuters, February 18, 2016. As of January 30, 2018:
http://www.reuters.com/article/idIN115455213120160218

"Islamic State: The Propaganda War," *The Economist*, April 15, 2015.

"Israelis Trust the IDF, Are Skeptical of Politicians—Survey," *Times of Israel*, July 10, 2016. As of January 30, 2018:
https://www.timesofisrael.com/israelis-trust-the-idf-are-skeptical-of-politicians-survey

Jacoby, Lowell E., "Five Years After 9/11: What Needs to Be Done?" Philadelphia, Pa.: Foreign Policy Research Institute, February 2007.

Jaitner, Margarita, "Russian Information Warfare: Lessons from Ukraine," in Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression Against Ukraine*, Talinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015. As of January 30, 2018:
https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Jaitner_10.pdf

Janda, Jakub, and Veronika Víchová, *Fungování českých dezinformačních webů* [*The Function of Czech Disinformation Sites*], Prague: Evropske Hodnoty, July 26, 2016. As of May 24, 2017:
http://www.evropskehodnoty.cz/fungovani-ceskych-dezinformacnich-webu/fungovani-ceskych-dezinformacnich-webu-2/

Jane's Sentinel Security Assessment, "Korea, North—Armed Forces," July 2, 2014a.

———, "North Korea—Strategic Weapons Systems," July 23, 2014b.

———, "Korea, North—Army," August 28, 2016a.

———, "Korea, North—External Affairs," August 28, 2016b.

———, "China: Armed Forces," May 15, 2017.

Jane's World Armies, "Israel," May 16, 2016.

———, "North Korea—Army," March 27, 2017.

Janssen, Ulrich M., *Psychological Operations: NATO Psychological Operations Within the Context of Strategic Communications*, Oberammergau, Germany: NATO School Oberammergau, Intelligence, Surveillance, Target Acquisition, and Reconnaissance Department, 2012.

Jenkins, Brian Michael, *Would-Be Warriors: Incidents of Jihadist Radicalization in the United States Since September 11, 2001*, Santa Monica, Calif.: RAND Corporation, OP-292-RC, 2010. As of January 30, 2018:
https://www.rand.org/pubs/occasional_papers/OP292.html

Jenkins, Brian Michael, and Colin P. Clarke, "In the Event of the Islamic State's Unlikely Demise," *Foreign Policy*, May 11, 2016.

Johnson, David E., *Hard Fighting: Israel in Lebanon and Gaza*, Santa Monica, Calif.: RAND Corporation, MG-1085-A/AF, 2011. As of January 30, 2018:
https://www.rand.org/pubs/monographs/MG1085.html

Johnson, James, "South Korea Claims North Korea Is Jamming GPS Signals on Planes," *The Inquisitr*, May 2, 2012. As of January 30, 2018:
http://www.inquisitr.com/228848/south-korea-claims-north-korea-is-jamming-gps-signals-on-planes

Johnson, Toni, "Threat of Homegrown Islamist Terrorism," backgrounder, Council on Foreign Relations, last updated September 30, 2011. As of January 30, 2018:
https://www.cfr.org/backgrounder/threat-homegrown-islamist-terrorism

Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*, Washington, D.C., August 2017. As of August 31, 2017:
http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf

Jones, Sam, "Ukraine: Russia's New Art of War," *Financial Times*, August 28, 2014.

———, "Cyber Warfare: Iran Opens a New Front," *Financial Times*, April 26, 2016.

Jordan, Mary, and Robin Wright, "Iran Seizes 15 British Seamen," *Washington Post*, March 24, 2007.

Jorisch, Avi, "Al-Manar: Hezbollah TV, 24/7," *Middle East Quarterly*, Vol. 11, No. 1, Winter 2004a, pp. 17–31.

———, *Beacon of Hatred: Inside Hezbollah's Al-Manar Television*, Washington, D.C.: Washington Institute for Near East Policy, October 2004b. As of January 30, 2018:
http://www.washingtoninstitute.org/policy-analysis/view/beacon-of-hatred-inside-hizballahs-al-manar-television

Joscelyn, Thomas, "Zawahiri Calls on Muslims to Support Taliban, Reject Islamic State," *Long War Journal*, August 21, 2016. As of January 30, 2018:
http://www.longwarjournal.org/archives/2016/08/zawahiri-calls-on-muslims-to-support-taliban-reject-islamic-state.php

Jun, Jenny, Scott LaFoy, and Ethan Sohn, "What Do We Know About Past North Korean Cyber Attacks and Their Capabilities?" Washington, D.C.: Center for Strategic and International Studies, December 12, 2014. As of January 30, 2018:
http://csis.org/files/publication/141212_Past_North_Korean_Cyber_Attacks_Capability.pdf

Kagan, Frederick W., and Tommy Stiansen, *The Growing Cyberthreat from Iran: The Initial Report of Project Pistachio Harvest*, Washington, D.C.: American Enterprise Institute and Norse Corporation, April 2015. As of January 30, 2018:
https://www.aei.org/wp-content/uploads/2015/04/Growing-Cyberthreat-From-Iran-final.pdf

Kan, Paul Rexton, "Anonymous vs. Los Zetas: The Revenge of the Hacktivists," *Small Wars Journal*, June 27, 2013.

Kavanaugh, Shane Dixon, and Gilad Shiloach, "ISIS Latest Recruiting Film Targets Sensitive Milennials," *Vocativ*, July 12, 2016. As of January 30, 2018:
http://www.vocativ.com/339471/isis-millennial-propaganda-raqqa-video

Khalidi, Walid, *Conflict and Violence in Lebanon: Confrontation in the Middle East*, Cambridge, Mass.: Harvard University, Center for International Affairs, 1979.

Kifner, John, "In Long Fight with Israel, Hezbollah Tactics Evolved," *New York Times*, July 19, 2000.

Kilcullen, David, "Countering Global Insurgency," *Journal of Strategic Studies*, Vol. 28, No. 4, 2005, pp. 597–617.

Kim, Duk-Ki, "The Republic of Korea's Counter-Asymmetric Strategy: Lessons from ROKS Cheonan and Yeonpyeong Island," *Naval War College Review*, Vol. 65, No. 1, Winter 2012, pp. 55–74.

Kimmage, Daniel, *The Al-Qaeda Media Nexus: The Virtual Network Behind the Global Message*, Washington, D.C.: Radio Free Europe/Radio Liberty, March 2008. As of January 30, 2018:
http://docs.rferl.org/en-US/AQ_Media_Nexus.pdf

Kincaid, Cliff, "Bombing Terror Television," *Accuracy in Media*, August 4, 2006. As of May 24, 2017:
http://www.aim.org/media-monitor/bombing-terror-television

Kirsch, Martin, *Die Psychologische Verteidigung der Bundeswehr bis 1990* [*The Psychological Operations of the Bundeswehr to 1990*], Tübington, Germany: Informationsstelle Militarisierung, December 3, 2014. As of January 30, 2018:
http://www.imi-online.de/download/2014_07_kirsch_web.pdf

Kitchen, Philip, and Jeff Newell, "Communicator Research Operator," video transcript, undated. As of January 30, 2018:
http://cdn.forces.ca/_CAPTIONS/00120_communicatorresearchoperator_en.html

Klug, Foster, "North Korea Threatens Strikes Over S. Korean Propaganda Broadcasts, Denies Role in Mine Blasts," Associated Press (*U.S. News and World Report*), August 14, 2015. As of January 30, 2018:
http://www.usnews.com/news/world/articles/2015/08/14/n-korea-threatens-strikes-over-skorea-propaganda-broadcasts

Koerner, Brendan I., "#Jihad: Why ISIS Is Winning the Social Media War," *Wired*, March 30, 2016. As of January 30, 2018:
https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat

Kohlmann, Evan F., "The Real Online Terrorist Threat," *Foreign Affairs*, Vol. 85, No. 5, September–October 2006. As of January 30, 2018:
https://www.foreignaffairs.com/articles/2006-09-01/real-online-terrorist-threat

Kohn, Ayelet, "Instagram as a Naturalized Propaganda Tool: The Israel Defense Forces Web Site and the Phenomenon of Shared Values," *Convergence: The International Journal of Research into New Media Technologies*, Vol. 23, No. 2, 2015, pp. 197–213.

Kondapalli, Srikanth, *China's Political Commissars and Commanders: Trends and Dynamics*, Singapore: Institute of Defense and Strategic Studies, October 2005. As of January 30, 2018:
https://www.rsis.edu.sg/wp-content/uploads/rsis-pubs/WP88.pdf

Koontz, Joshua, "Iran's Growing Casualty Count in Yemen," *War on the Rocks*, June 1, 2017. As of January 30, 2018:
https://warontherocks.com/2017/06/irans-growing-casualty-count-in-yemen

Koplow, Michael, "How Not to Wage War on the Internet," *Foreign Policy*, November 16, 2012.

Kostelnik, James, and David Skarbek, "The Governance Institutions of a Drug Trafficking Organization," *Public Choice*, Vol. 156, No. 1, July 2013, pp. 95–103.

Kovensky, Josh, "ISIS's New Mag Looks Like a New York Glossy—with Pictures of Mutilated Bodies," *New Republic*, August 25, 2014. As of January 30, 2018:
https://newrepublic.com/article/119203/isiss-dabiq-vs-al-qaedas-inspire-comparing-two-extremist-magazines

Kramer, Andrew E., "Ukraine's Opposition Says Government Stirs Violence," *New York Times*, January 21, 2014.

———, "More of Kremlin's Opponents Are Ending Up Dead," *New York Times*, August 20, 2016.

Krasnoboka, Natalya, "Russia," Maastricht, Netherlands: European Journalism Centre, undated. As of January 30, 2018:
http://ejc.net/media_landscapes/russia

Kruglov, V. V., "О вооруженной борьбе будущего" ["On Future Armed Conflict"], Военная мысль [*Military Thought*], No. 4, September–October 1998, pp. 54–58. As of January 30, 2018:
http://militaryarticle.ru/voennaya-mysl/1998-vm/8941-o-vooruzhennoj-borbe-budushhego

Kydd, Andrew H., and Barbara F. Walter, "The Strategies of Terrorism," *International Security*, Vol. 31, No. 1, Summer 2006, pp. 49–80.

Labi, Naya, "Jihad 2.0," *Atlantic Monthly*, July–August 2006. As of January 30, 2018:
https://www.theatlantic.com/magazine/archive/2006/07/jihad-20/304980

Labott, Elise, and Ryan Browne, "U.S. Sanctions North Korean Leader for First Time over Human Rights Abuses," CNN, July 7, 2016. As of January 30, 2018:
http://www.cnn.com/2016/07/06/politics/north-korea-kim-jong-un-human-rights

Laity, Mark, "Rising to the Challenge as Information Takes Centre Stage," *Three Swords Magazine*, No. 28, May 2015a, pp. 58–63. As of January 30, 2018:
http://www.jwc.nato.int/images/stories/threeswords/INFORMATION_CENTRE_STAGE.pdf

———, "NATO and the Power of Narrative," *Information at War: From China's Three Warfares to NATO's Narratives*, London: Legatum Institute, September 2015b, pp. 22–28. As of January 30, 2018:
http://www.li.com/activities/publications/information-at-war-from-china-s-three-warfares-to-nato-s-narratives

Large, David Clay, *Germans to the Front: West German Rearmament in the Adenauer Era*, Chapel Hill, N.C.: University of North Carolina Press, 1996.

Larson, Erik, Patricia Hurtado, and Chris Strohm, "Iranians Hacked from Wall Street to New York Dam, U.S. Says," Bloomberg (*Business Times*), March 24, 2016. As of January 30, 2018:
http://www.businesstimes.com.sg/government-economy/iranians-hacked-from-wall-street-to-new-york-dam-us-says

Laub, Zachary, and Rukmini Callimachi, "The Islamic State's Bloody Summer," Council on Foreign Relations, August 3, 2016. As of January 30, 2018:
https://www.cfr.org/interview/islamic-states-bloody-summer

Lauder, Matthew A., "The Janus Matrix: Lessons Learned and Building an Integrated Influence Activities Capability for the Future Security Environment," *Canadian Army Journal*, Autumn 2013, pp. 33–48. As of January 30, 2018:
http://publications.gc.ca/collections/collection_2014/mdn-dnd/D12-11-15-2-eng.pdf

Laurence, Jeremy, and Danbee Moon, "North Korea Spends About a Third of Income on Military: Group," Reuters, January 18, 2011. As of January 30, 2018:
http://www.reuters.com/article/us-korea-north-military-idUSTRE70H1BW20110118

Lee, Yimou, and Faith Hung, "Special Report: How China's Shadowy Agency Is Working to Absorb Taiwan," Reuters, November 26, 2014. As of January 30, 2018:
http://www.reuters.com/article/us-taiwan-china-special-report/special-report-how-chinas-shadowy-agency-is-working-to-absorb-taiwan-idUSKCN0JB01T20141127

Lennon, Mike, "Hackers Used Sophisticated SMB Worm Tool to Attack Sony," *Security Week*, December 19, 2014. As of January 30, 2018:
http://www.securityweek.com/hackers-used-sophisticated-smb-worm-tool-attack-sony

LePage, Rita, "Understanding Influence Activities," *Vanguard*, February 19, 2013. As of January 30, 2018:
http://www.vanguardcanada.com/2013/02/19/understanding-influence-activities

Li Naiguo, *New Theories of Information War*, Beijing: Academy of Military Science Press, 2004a.

———, *Xinxizhan Xinlun* [*A New Discussion on Information Warfare*], Beijing: National Defense University Press, 2004b.

Lindsay, John, "The Power to React: Review and Discussion of Canada's Emergency Measures Legislation," *International Journal of Human Rights*, Vol. 18, No. 2, 2014, pp. 159–177.

Liska, Michael, Budget Chief, Supreme Headquarters Allied Powers Europe, "NATO Resources: An Overview," briefing sides, undated. As of January 30, 2018:
http://www.asmconline.org/wp-content/uploads/chapters/eruopeanpdi2011/D1_W3_Liska_ASMC_NATO_Resources_Apr%2011.pdf

Lister, Charles, *The Islamic State: A Brief Introduction*, Washington, D.C.: Brookings Institution, 2015.

"Lithuania Says Russia Reopens Soviet Conscript Cases," BBC News, September 8, 2014. As of January 30, 2018:
http://www.bbc.com/news/blogs-news-from-elsewhere-29111188

Liu Zhongshan, "Ziweiquan yu Zhuquan" ["Sovereignty and the Right of Self-Defense"], *Zhanlue yu Guanli* [*Strategy and Management*], No. 1, 2002.

Lohmuller, Michael, "Rumors Fuel the Legend of the 'Narco-Saint,'" Insight Crime, February 6, 2014. As of January 30, 2018:
http://www.insightcrime.org/news-briefs/rumors-fuel-legend-of-narco-saint

Long, Austin G., Stephanie Pezard, Bryce Loidolt, and Todd Helmus, *Locals Rule: Historical Lessons for Creating Local Defense Forces for Afghanistan and Beyond*, Santa Monica, Calif.: RAND Corporation, MG-1232-CFSOCC-A, 2012. As of January 30, 2018:
https://www.rand.org/pubs/monographs/MG1232.html

Longmire, Sylvia, "TCO 101: The Gulf Cartel," *Mexico's Drug War*, 2012. No longer available online.

Lynch, Marc, "Al Qaeda's Media Strategies," *National Interest*, Vol. 83, Spring 2006, pp. 50–52. As of January 30, 2018:
http://nationalinterest.org/article/al-qaedas-media-strategies-883

Lynch, Sarah N., "U.S. Sailors Captured by Iran Were Held at Gunpoint: U.S. Military," Reuters, January 18, 2016. As of January 30, 2018:
http://www.reuters.com/article/us-usa-iran-boats-idUSKCN0UW1Q7

MacFarquhar, Neil, "A Powerful Russian Weapon: The Spread of False Stories," *New York Times*, August 28, 2016.

Majd, Hooman, *The Ayatollah's Democracy: An Iranian Challenge*, New York: W. W. Norton, 2010.

Majidyar, Ahmad, "Celebrations of Iranian Revolution Across Syria Shows [sic] Iran's Soft Power Hegemony," Washington, D.C.: Middle East Institute, February 13, 2017. As of January 30, 2018:
http://www.mideasti.org/content/io/celebrations-iranian-revolution-across-syria-shows-iran-s-soft-power-hegemony

Maldre, Patrik, and Jarno Limnell, "Key Cyber Issues for NATO's Warsaw Summit," *Breaking Defense*, July 5, 2016. As of January 30, 2018:
http://breakingdefense.com/2016/07/key-cyber-issues-for-natos-warsaw-summit

Marret, Jean-Luc, "Al-Qaeda in Islamic Maghreb: A 'Glocal' Organization," *Studies in Conflict and Terrorism*, Vol. 31, No. 6, 2008, pp. 541–552.

Martin, Alexander S., "FSB's Snowden War: Using the American NSA Against Itself," *Modern Diplomacy*, May 24, 2016. As of January 30, 2018:
http://moderndiplomacy.eu/index.php?option=com_k2&view=item&id=1443:fsb-s-snowden-war-using-the-american-nsa-against-itself

McCants, William, *The ISIS Apocalypse: The History, Strategy, and Doomsday Vision of the Islamic State*, New York: St. Martin's Press, 2015

McCants, William, and Clint Watts, "Why the U.S. Can't Make a Magazine Like ISIS," *Daily Beast*, January 11, 2016. As of January 30, 2018:
http://www.thedailybeast.com/articles/2016/01/11/why-the-u-s-can-t-make-a-magazine-like-isis

McConnell, Mike, Michael Chertoff, and William Lynn, "China's Cyber Thievery Is National Policy—and Must Be Challenged," *Wall Street Journal*, January 27, 2012.

McChrystal, Stanley A., *U.S. Forces–Afghanistan/International Security Assistance Force, Afghanistan: Commander's Initial Assessment*, August 30, 2009.

McGahon, Jason, "She Tweeted Against the Mexican Cartels, They Tweeted Her Murder," *Daily Beast*, October 21, 2014. As of January 30, 2018:
https://www.thedailybeast.com/she-tweeted-against-the-mexican-cartels-they-tweeted-her-murder

McLaughlin, Joshua, "The Al Qaeda Franchise Model: An Alternative," *Small Wars Journal*, January 31, 2010.

Meister, Andre, "Wissenserschließung aus offenen Quellen: Wie Bundeswehr und BND die Überwachung sozialer Netzwerke rechtfertigen" ["Knowledge Discovery from Open Sources: How the Bundeswehr and BND Justify Social Network Monitoring"], Neztpolitik.org, June 25, 2014. As of January 30, 2018:
https://netzpolitik.org/2014/wissenserschliessung-aus-offenen-quellen-wie-bundeswehr-und-bnd-die-auswertung-sozialer-netzwerke-rechtfertigen

Menn, Joseph, and Yeganeh Torbati, "Exclusive: Hackers Accessed Telegram Messaging Accounts in Iran—Researchers," Reuters*,* August 2, 2016. As of January 30, 2018:
http://www.reuters.com/article/us-iran-cyber-telegram-exclusive-idUSKCN10D1AM

Mercado, Stephen C., "Hermit Surfers of P'Yongyang: North Korea and the Internet," *Studies in Intelligence*, Vol. 48, No. 1, last updated June 27, 2008. As of January 30, 2018:
https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no1/article04.html

Midgley, Dominic, "What's the Truth About North Korea's Prison Camps?" *Daily Express (UK)*, March 20, 2016. As of January 30, 2018:
http://www.express.co.uk/news/world/654167/North-Korea-prison-camps-American-Otto-Warmbier

Migration Policy Centre, *Russia: The Demographic-Economic Framework of Migration, the Legal Framework of Migration, the Socio-Political Framework of Migration*, Florence, Italy, June 2013. As of January 30, 2018:
http://www.migrationpolicycentre.eu/docs/migration_profiles/Russia.pdf

Milani, Abbas, "The Green Movement," in Robin Wright, ed., *The Iran Primer: Power, Politics and U.S. Policy*, Washington, D.C.: United States Institute of Peace, 2010, pp. 41–44.

Miller, Greg, and Souad Mekhennet, "Inside the Surreal World of the Islamic State's Propaganda Machine," *Washington Post*, November 20, 2015.

Milton, Daniel, "The Islamic State: An Adaptive Organization Facing Increasing Challenges," in Muhammad al-Ubaydi, Nelly Lahoud, Daniel Milton, and Bryan Price, eds., *The Group That Calls Itself a State: Understanding the Evolution and Challenges of the Islamic State*, West Point, N.Y.: United States Military Academy, Combating Terrorism Center, December 2014.

———, *Communication Breakdown: Unraveling the Islamic State's Media Efforts*, West Point, N.Y.: United States Military Academy, Combating Terrorism Center, October 2016.

Minnich, James M., *The North Korean People's Army: Origins and Current Tactics*, Annapolis, Md.: Naval Institute Press, 2005.

Miroff, Nick, and William Booth, “Mexico’s Drug War Intrudes on Monterrey, a Booming Metropolis,” *Washington Post*, March 16, 2011.

Monaghan, Andrew, “Putin’s Way of War: The ‘War’ in Russia’s ‘Hybrid Warfare,’” *Parameters*, Vol. 45, No. 4, Winter 2015–2016, pp. 65–74. As of January 30, 2018:
http://strategicstudiesinstitute.army.mil/pubs/parameters/issues/Winter_2015-16/9_Monaghan.pdf

Moore, Jack, “ISIS’s Twitter Campaign Faltering Amid Crackdown,” *Newsweek*, February 18, 2016a. As January 30, 2018:
http://www.newsweek.com/isiss-english-language-twitter-campaign-faltering-amid-crackdown-428004

———, “ISIS Releases New Video Outlining the Structure of the Caliphate,” *Newsweek*, July 7, 2016b. As of January 30, 2018:
http://www.newsweek.com/isis-releases-new-video-outlining-structure-caliphate-478502

———, “ISIS Confirms Death of Media Emir Abu Mohammed al-Furqan,” *Newsweek*, October 11, 2016c. As of January 30, 2018:
http://www.newsweek.com/isis-confirms-death-media-emir-abu-mohammad-al-furqan-508658

Mörke, Olaf, “Pamphlet und Propaganda, Politische Kommunikation und technische Innovation in Westeuropa in der frühen Neuzeit” [“Pamphlet and Propaganda: Political Communication and Technical Innovation in Western Europe in the Early Modern Period”], in Michael North, ed., *Kommunikationsrevolutionen: die neuen Medien des 16. und 19. Jahrhunderts* [*Communication Revolutions: The New Media in the 16th and 19th Centuries*], Köln, Germany: Böhlau, 1995, pp. 15–32.

Mosso, Rubén, “‘El Tio’ se Escondió en Clóset para Evitar Captura: Rubido” [“‘El Tio’ Hid in the Closet to Avoid Capture: Rubido”], *El Milenio*, January 27, 2014. As of January 30, 2018:
http://www.milenio.com/policia/El_Tio_se_escondio_en_el_closet-detienen_a_lider_templario-capturan_a_Dionisio_Loya_Plancarte_0_234576969.html

Multinational Information Operations Experiment, *Narrative Development in Coalition Operations*, draft, version 0.96, January 10, 2014.

Murphy, David, “Iran Launches ‘Mehr,’ Its Own YouTube-Like Video Hub,” *PCMag*, December 9, 2012. As of January 30, 2018:
http://www.pcmag.com/article2/0,2817,2413014,00.asp

Murphy, Heather, “Ominous Text Message Sent to Protesters in Kiev Sends Chills Around the Internet,” *New York Times*, January 22, 2014.

Nader, Alireza, *Iran’s Role in Iraq: Room for Cooperation?* Santa Monica, Calif., RAND Corporation, PE-151-OSD, 2015. As of January 30, 2018:
https://www.rand.org/pubs/perspectives/PE151.html

Nakashima, Ellen, “To Thwart Hackers, Firms Salting Their Servers with Fake Data,” *Washington Post*, January 2, 2013.

Nanjing Political Academy, Military News Department Study Group, “Study of the Journalistic Media Warfare in the Iraq War,” *China Military Science*, No. 4, 2003.

Nasr, Vali, *The Shia Revival: How Conflicts Within Islam Will Shape the Future*, New York: W. W. Norton, 2006.

NationMaster, “North Korea Military Stats,” web page, undated. As of January 30, 2018:
http://www.nationmaster.com/country-info/profiles/North-Korea/Military

NATO Communications and Information Agency, “NCI Agency Organisational Overview,” web page, undated. As of January 30, 2018:
https://www.ncia.nato.int/PublishingImages/Organizational%20design.jpg

NATO Joint Electronic Warfare Core Staff, “NATO Joint Electronic Warfare Core Staff (JEWCS): A History of Transformation,” briefing slides, undated. As of January 30, 2018:
http://www2.warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/lectures/gchq/20080904_nr_jewcs_transformation_brief_muxfeldt_unclas_old.pdf

NATO Strategic Communications Centre of Excellence, “About Strategic Communications,” web page, undated(a). As of May 24, 2017:
http://www.stratcomcoe.org/about-strategic-communications

———, “History,” web page, undated(b). As of May 24, 2016:
http://www.stratcomcoe.org/history

———, “Participating Countries,” web page, undated(c). As of May 24, 2017:
http://www.stratcomcoe.org/participating-countries

———, “Publications,” web page, undated(d). As of May 24, 2017:
http://www.stratcomcoe.org/publications

———, “Structure,” web page, undated(e). As of May 24, 2017:
http://www.stratcomcoe.org/structure

———, *Analysis of Russia’s Information Campaign Against Ukraine*, Riga, Latvia, 2015a. As of January 30, 2018:
http://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine-1

———, *Daesh Information Campaign and Its Influence: Results of the Study*, Riga, Latvia, 2015b. As of January 30, 2018:
http://www.stratcomcoe.org/daesh-information-campaign-and-its-influence-1

———, *Mapping of StratCom Practices in NATO Countries*, Riga, Latvia, February 2015–June 2015c. As of January 30, 2018:
http://www.stratcomcoe.org/mapping-stratcom-practices-nato-countries-0

———, *NATO Strategic Communications Centre of Excellence: Report for the Period from 1 October 2014 to 31 December 2014*, Riga, Latvia, March 2015d. As of January 30, 2018:
http://www.stratcomcoe.org/report-period-1-october-2014-31-december-2014

Nicol, Mark, “UK Special Forces Launch ‘Black Ops’ Assault on ISIS Using Electronic Warfare to Cripple Jihadists’ Communications,” *Daily Mail*, May 14, 2016. As of January 30, 2018:
http://www.dailymail.co.uk/news/article-3590890/UK-special-forces-launch-black-ops-assault-ISIS-using-electronic-warfare-cripple-jihadists-communications.html

“N.K. Continues GPS Jamming,” *Korea Herald*, May 7, 2012. As of January 30, 2018:
http://www.koreaherald.com/view.php?ud=20120507000828&cpv=0

North Atlantic Treaty Organization, “What Is NATO?” web page, undated. As of May 24, 2017:
http://www.nato.int/nato-welcome

———, *Allied Joint Doctrine for Information Operations*, Allied Joint Publication 3.10, November 2009.

———, *Bi-SC Information Operations Reference Book*, version 1, March 5, 2010.

———, *NATO Military Public Affairs Policy*, MC 0457/2, February 2011a. As of January 30, 2018:
http://www.nato.int/ims/docu/mil-pol-pub-affairs-en.pdf

———, "Electronic Warfare," web page, last updated November 16, 2011b. As of January 30, 2018: http://www.nato.int/cps/en/natohq/topics_80906.htm

———, *NATO Military Policy on Psychological Operations*, MC 402/2, June 22, 2012a.

———, *NATO's Directory of Public Information and Public Affairs Officers*, November 2012b. As of January 30, 2018:
http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2013_01/20130114_PIO_Directory2012.pdf

———, *Allied Joint Doctrine for Psychological Operations*, Allied Joint Publication 3.10.1, September 2014a.

———, "NATO Launches Industry Cyber Partnership," web page, last updated September 18, 2014b. As of January 30, 2018:
http://www.nato.int/cps/en/natohq/news_113121.htm

———, "Collective Defence—Article 5," web page, last updated March 22, 2016a. As of May 24, 2017:
http://www.nato.int/cps/en/natohq/topics_110496.htm

———, "NATO Communications and Information Agency (NCI Agency)," web page, last updated April 7, 2016b. As of May 24, 2017:
http://www.nato.int/cps/en/natolive/topics_69332.htm

———, "Troop Contributions," web page, last updated June 27, 2016c. As of May 24, 2017: http://www.nato.int/cps/en/natohq/topics_50316.htm

———, "Cyber Defence Pledge," press release, July 8, 2016d. As of May 24, 2017: http://www.nato.int/cps/en/natohq/official_texts_133177.htm

———, "Wales Summit Declaration," press release, last updated September 26, 2016e. As of May 24, 2017:
http://www.nato.int/cps/en/natohq/official_texts_112964.htm

———, "Funding NATO," web page, last updated January 19, 2017a. As of May 24, 2017: http://www.nato.int/cps/en/natohq/topics_67655.htm

———, "Warsaw Summit Communiqué," press release, last updated March 29, 2017b. As of May 24, 2017:
http://www.nato.int/cps/en/natohq/official_texts_133169.htm

———, "Relations with Russia," web page, last updated April 6, 2017c. As of May 24, 2017: http://www.nato.int/cps/en/natohq/topics_50090.htm

———, "Euro-Atlantic Disaster Response Coordination Centre," web page, last updated April 28, 2017d. As of May 24, 2017:
http://www.nato.int/cps/en/natohq/topics_52057.htm

"North Korea—Media Profile," BBC News, August 24, 2017. As of November 8, 2017: http://www.bbc.com/news/world-asia-pacific-15259016

Norton, Augustus Richard, *Hizballah of Lebanon: Extremist Ideals vs. Mundane Politics*, New York: Council on Foreign Relations, 1999.

———, "Hizballah and the Israeli Withdrawal from Southern Lebanon," *Journal of Palestine Studies*, Vol. 30, No. 1, Autumn 2000, pp. 22–35.

———, *Hezbollah: A Short History*, Princeton, N.J.: Princeton University Press, 2007.

Novenario, Celine Marie I., "Differentiating Al Qaeda and the Islamic State Through Strategies Publicized in Jihadist Magazines," *Studies in Conflict and Terrorism*, Vol. 39, No. 11, 2016, pp. 953–967.

Obama White House, "President Obama and Prime Minister Trudeau Hold a Joint Press Conference," video, March 10, 2016. As of January 30, 2018: https://www.youtube.com/watch?v=D5MEX1Yt0Ro

O'Boyle, Michael, "Mexican Cult-Like Drug Gang Says Willing to Disband," Reuters, November 29, 2010. As of January 30, 2018: https://www.reuters.com/article/us-mexico-drugs-truce/mexican-cult-like-drug-gang-says-willing-to-disband-idUSTRE6AS57M20101129

Odling-Smee, John, *The IMF and Russia in the 1990s*, Washington, D.C.: International Monetary Fund, 2004. As of January 30, 2018: https://www.imf.org/external/pubs/ft/wp/2004/wp04155.pdf

Office of Management and Budget, Executive Office of the President of the United States, *Fiscal Year 2014 Budget of the U.S. Government*, Washington, D.C., 2013. As of January 30, 2018: https://www.gpo.gov/fdsys/pkg/BUDGET-2014-BUD/pdf/BUDGET-2014-BUD.pdf

Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2011*, Washington, D.C., March 2011. As of January 30, 2018: https://www.defense.gov/Portals/1/Documents/pubs/2011_CMPR_Final.pdf

Office of the Secretary of Defense, *Military and Security Developments Involving the Democratic People's Republic of Korea: Annual Report to Congress*, Washington, D.C., 2015. As of January 30, 2018: https://www.defense.gov/Portals/1/Documents/pubs/Military_and_Security_Developments_Involving_the_Democratic_Peoples_Republic_of_Korea_2015.PDF

Olson, Eric T., "War of Ideas: From the Taliban to the Islamic State," *War on the Rocks*, January 6, 2016. As of January 30, 2018: https://warontherocks.com/2016/01/wars-of-ideas-from-the-taliban-to-the-islamic-state

Opall-Rome, Barbara, "Israel to Consolidate Cyber Spending, Ops," *DefenseNews*, June 18, 2015. As of January 30, 2018: http://www.defensenews.com/story/breaking-news/2015/06/18/israel-establish-cyber-command-integrate-c4i-defensive-offensive/28916147

Oren, Elizabeth, "A Dilemma of Principles: The Challenges of Hybrid Warfare from a NATO Perspective," *Special Operations Journal*, Vol. 2, No. 1, 2016, pp. 58–69.

O'Shaughnessy, Nicholas J., and Paul R. Baines, "Selling Terror: The Symbolization and Positioning of Jihad," *Marketing Theory*, Vol. 9, No. 2, 2009, pp. 227–241.

Ostovar, Afshon, *Vanguard of the Imam: Religion, Politics and Iran's Revolutionary Guards*, Oxford, UK: Oxford University Press, 2016.

Otero, Silvia, "'La Tuta' y el Síndrome Ahumada" ["'La Tuta' and the Smoke Signal Syndrome"], *El Universal*, February 27, 2015. As of January 30, 2018: http://archivo.eluniversal.com.mx/nacion-mexico/2015/-34la-tuta-34-y-el-sindrome-ahumada-1080566.html

Paganini, Pierluigi, "A High-Profile Defector Warns That North Korea's Cyber Army Has the Capability to Run Cyber Attacks That Could Cause Loss of Human Lives," *Security Affairs*, May 30, 2015. As of January 30, 2018: http://securityaffairs.co/wordpress/37313/intelligence/north-korea-cyber-capabilities.html

Pahlavi, Pierre Cyril, "The 33-Day War: An Example of Psychological Warfare in the Information Age," *Canadian Army Journal*, Volume 10, No. 2, 2007, pp. 13–26.

———, "Understanding Iran's Media Diplomacy," *Israel Journal of Foreign Affairs*, Vol. 6, No. 2, 2012, pp. 21–33.

Palomera, Rocco, "Narcomutilaciones Tienen un Signficado" ["Narco Mutililations Have a Meaning"], *El Occidental*, June 7, 2010.

Panarin, Igor, "Вторая мировая информационная война. Как в ней победить России?" ["The Second World Information War: Can Russia Win?"] *KM Online*, September 28, 2015. As of January 30, 2018:
http://www.km.ru/spetsproekty/2015/09/28/
mirovaya-ekspansiya-ssha/764831-vtoraya-mirovaya-informatsionnaya-voina-kak-

Panda, Ankit, "Russian Emigration Spikes in 2013–2014," *The Diplomat*, July 25, 2014. As of January 30, 2018:
http://thediplomat.com/2014/07/russian-emigration-spikes-in-2013-2014

Panizzi, Massimo, "The Development of NATO Strategic Communications: From Public Affairs to a Broader Communications Policy," *Three Swords Magazine*, No. 21, Autumn–Winter 2011, pp. 9–17. As of January 30, 2018:
http://www.jwc.nato.int/images/stories/threeswords/THREE_SWORDS_21.pdf

Paul, Christopher, Colin P. Clarke, Michael Schwille, Jakub Hlávka, Michael A. Brown, Steven Davenport, Isaac R. Porche III, and Joel Harding, *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment*, Santa Monica, Calif.: RAND Corporation, RR-1925/1-A, 2018. As of April 2018:
https://www.rand.org/pubs/research_reports/RR1925z1.html

Paul, Christopher, and William Courtney, "Russian Propaganda Is Pervasive, and America Is Behind the Power Curve in Countering It," *U.S. News and World Report*, September 12, 2016.

Paul, Christopher, and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016. As of January 30, 2018:
http://www.rand.org/pubs/perspectives/PE198.html

Pauly, Stefan, "Vier Jahrzehnte 'Radio Andernach'" ["Four Decades of 'Radio Andernach'"], *WochenSpiegel*, September 14, 2016. As of January 30, 2018:
http://www.wochenspiegellive.de/eifel/kreis-mayen-koblenz/mayen/artikel/
vier-jahrzehnte-radio-andernach-25664

Pavel, Petr, Chair of the NATO Military Committee, "The Road to Warsaw and Beyond," speech to the NATO Parliamentary Assembly, Defence and Security Committee, last updated October 14, 2015. As of January 30, 2018:
http://www.nato.int/cps/en/natohq/opinions_123879.htm

Paz, Alon, and Naday Pollak, "Operational Wisdom and Strategic Distress," Washington, D.C.: Washington Institute for Near East Policy, PolicyWatch 2289, July 22, 2014. As of January 30, 2018:
http://www.washingtoninstitute.org/policy-analysis/view/operational-wisdom-amid-strategic-distress

Peng Guangqian and Yao Youzhi, eds., *The Science of Military Strategy*, English translation, Beijing: Military Science Publishing House, 2005.

Peri, Yoram, "Intractable Conflict and the Media," *Israel Studies*, Vol. 12, No. 1, Spring 2007, pp. 79–102.

Pfeffer, Anshel, “Psychological Warfare on the Digital Battlefield,” *Haaretz*, November 19, 2012. As of January 30, 2018:
http://www.haaretz.com/israel-news/psychological-warfare-on-the-digital-battlefield.premium-1.478984

Pfeiffer, Ingo, *Gegner wider Willen: Konfrontation von Volksmarine und Bundesmarine auf See* [*Opponents Against Their Will: Confrontation Between the East German Volksmarine and the West German Bundesmarine at Sea*], Norderstedt, Germany: Books on Demand, August 2012.

Phares, Walid, “Hezbollah’s Communication Network Confirms Its Terror Goals,” *World Defense Review*, May 21, 2008.

Polityuk, Pavel, and Jim Finkle, “Ukraine Says Communications Hit, MPs Phones Blocked,” Reuters, March 4, 2014. As of January 30, 2018:
http://www.reuters.com/article/us-ukraine-crisis-cybersecurity-idUSBREA231R220140304

Pollack, Kenneth M., *The Persian Puzzle: The Conflict Between Iran and America*, New York: Random House, 2004.

Pomerantsev, Peter, “Russia and the Menace of Unreality: How Vladimir Putin Is Revolutionizing Information Warfare,” *The Atlantic*, September 9, 2014. As of January 30, 2018:
http://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880

Priest, Dana, and Walter Pincus, “New Target and Tone,” *Washington Post*, April 16, 2004.

Priest, Dana, Ellen Nakashima, and Tom Hamburger, “U.S. Investigating Potential Covert Russian Plan to Disrupt November Elections,” *Washington Post*, September 5, 2016.

“Putin Reveals Secrets of Russia’s Crimea Takeover Plot,” BBC News, March 9, 2015. As of January 30, 2018:
http://www.bbc.com/news/world-europe-31796226

“Que Quieren de Nosotros?” [“What Do You Want from Us?”], *El Diario*, September 19, 2010. As of January 30, 2018:
http://diario.mx/Local/2010-09-19_cfaade06/_que-quieren-de-nosotros/?/

Qing, Koh Gui, “China Budgets 2014 Fiscal Deficit of 2.1 Percent of GDP,” Reuters, March 4, 2014. As of January 30, 2018:
http://www.reuters.com/article/us-china-economy-budget-idUSBREA2402920140305

R., Luis, “Los Rojos–CDG Leave 2 Naked, Chained Kidnappers with Manta Message,” *Borderland Beat*, November 10, 2015. As of January 30, 2018:
http://www.borderlandbeat.com/2015/11/los-rojos-cdg-leaves-2-naked-chained.html

Rabasa, Angel, Peter Chalk, Kim Cragin, Sara A. Daley, Heather S. Gregg, Theodore W. Karasik, Kevin A. O’Brien, and William Rosenau, *Beyond Al-Qaeda: The Global Jihadist Movement, Part I*, Santa Monica, Calif.: RAND Corporation, MG-429-AF, 2006. As of January 30, 2018:
https://www.rand.org/pubs/monographs/MG429.html

Radio Free Europe/Radio Liberty, “Russia Refuses Entry to Armenian Political Analyst,” September 1, 2016. As of January 30, 2018:
http://www.rferl.mobi/a/armenian-analyst-refused-entry-russia/27959629.html

Raghavan, Sudarsan, “Inside the Brutal but Bizarrely Bureaucratic World of the Islamic State in Libya,” *Washington Post*, August 23, 2016.

Ramsey, Geoffrey, and the Christian Science Monitor, “Showdown Looms Between ‘Anonymous’ Hackers and Mexico’s Zeta cartel,” ABC News, November 5, 2011. As of January 30, 2018: http://abcnews.go.com/International/showdown-looms-anonymous-hackers-mexicos-zeta-cartel/story?id=14875273

Raska, Michael, *Confronting Cybersecurity Challenges: Israel’s Evolving Cyber Defence Strategy*, Singapore: Nanyang Technological University, January 2015. As of January 30, 2018: https://www.rsis.edu.sg/rsis-publication/gpo/confronting-cybersecurity-challenges-israels-evolving-cyber-defence-strategy

———, “China and the ‘Three Warfares,’” *The Diplomat*, December 18, 2015. As of January 30, 2018: http://thediplomat.com/2015/12/hybrid-warfare-with-chinese-characteristics-2

Rasmussen, Robert C., “Cutting Through the Fog: Reflexive Control and Russian STRATCOM in Ukraine,” Center for International Maritime Security, November 26, 2015. As of January 30, 2018: http://cimsec.org/cutting-fog-reflexive-control-russian-stratcom-ukraine/20156

Reding, Anais, Kristin Weed, and Jeremy J. Ghez, *NATO’s Strategic Communications Concept and Its Relevance for France*, Santa Monica, Calif.: RAND Corporation TR-855/2-MOD/FR, 2010. As of January 30, 2018: http://www.rand.org/pubs/technical_reports/TR855z2.html

Reed, John, “Unit 8200: Israel’s Cyber Spy Agency,” *Financial Times*, July 10, 2015.

Reporters Without Borders, “China,” web page, undated. As of January 30, 2018: https://rsf.org/en/china?nl=ok

Rid, Thomas, and Marc Hecker, *War 2.0: Irregular Warfare in the Information Age*, Westport, Conn.: Praeger Security International, 2009.

Rivera, Jason, “Iran’s Involvement in Bahrain: A Battleground as Part of the Islamic Regime’s Larger Existential Conflict,” *IO Sphere*, Winter 2015, pp. 12–19.

Roggio, Bill, “The Seven Phases of the Base,” *Long War Journal*, August 15, 2005. As of January 30, 2018: http://www.longwarjournal.org/archives/2005/08/the_seven_phase.php

Rothrock, Kevin, “‘Anonymous International’ Leaks Kremlin’s Instructions to Russian TV,” Global Voices, March 28, 2014. As of January 30, 2018: https://globalvoices.org/2014/03/28/anonymous-international-leaks-kremlins-instructions-to-russian-tv

Rowayheb, Marwan George, “Political Change and the Outbreak of Civil War: The Case of Lebanon,” *Civil Wars*, Vol. 13, No. 4, 2011, pp. 414–436.

Royal Canadian Air Force, *Aerospace Electronic Warfare Doctrine*, Ottawa, Ont., B-GA-403-002/FP-001, March 2011.

———, “Chapter 5: The Functions of Canada’s Air Force B-GA-400-000/FP-000, Canadian Forces Aerospace Doctrine,” *Canadian Forces Aerospace Doctrine*, last updated June 20, 2016.

Rubalcava, Iggy, “German, American Soldiers, Polizei Train Together,” U.S. Army, April 7, 2014. As of January 30, 2018: http://www.army.mil/article/123355/German__American_Soldiers__polizei_train_together

Rubin, Barry, *The Tragedy of the Middle East*, Cambridge, UK: Cambridge University Press, 2002.

Runkle, Benjamin, and William Caldwell, "The War of Narratives in Operation Protective Edge," *Jerusalem Post*, March 29, 2015. As of January 30, 2018:
http://www.jpost.com/Opinion/The-war-of-narratives-in-Operation-Protective-Edge-395516

Russia Beyond the Headlines and Russia Today, "Über das Verhältnis von Russen und Deutschen" [On the Relationship Between the Russians and Germans"], *Deutschland und Russland*, April 4, 2012. As of January 30, 2018:
https://de.rbth.com/articles/2012/04/03/ueber_das_verhaeltnis_von_russen_und_deutschen_14371

Russian Federation, *Information Security Doctrine of The Russian Federation*, September 9, 2000. As of May 24, 2017:
https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf

———, *The Military Doctrine of the Russian Federation*, February 5, 2010. As of May 24, 2017:
http://carnegieendowment.org/files/2010russia_military_doctrine.pdf

———, *The Military Doctrine of the Russian Federation*, December 25, 2014. As of May 24, 2017:
http://www.rusemb.org.uk/press/2029

———, *Doctrine of Information Security of the Russian Federation*, December 5, 2016. As of November 17, 2017:
http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

"Russian Khimki Forest Journalist Mikhail Beketov Dies," BBC News, April 9, 2013. As of January 30, 2018:
http://www.bbc.com/news/world-europe-22078842

Russian Ministry of Defence, "Mission and Objectives of the Russian Armed Forces," web page, undated(a). As of May 24, 2017:
http://eng.mil.ru/en/mission/tasks.htm

———, "Russian Federation Armed Forces' Information Space Activities Concept," web page, undated(b). As of May 24, 2017:
http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

Russian Ministry of Foreign Affairs, "National Security Concept of the Russian Federation," decree of the President of the Russian Federation No. 24, January 10, 2000. As of May 24, 2017:
http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768

"Russian Spy Agency Targeting Western Diplomats," *The Guardian*, September 23, 2011. As of January 30, 2018:
https://www.theguardian.com/world/2011/sep/23/russia-targeting-western-diplomats

Ryan, Mark A., David M. Finklestein, and Michael A. McDevitt, eds., *Chinese Warfighting: The Experience of the PLA Since 1949*, Armonk, N.Y.: M. E. Sharpe, 2003.

Ryan, Michael W. S., *Decoding Al-Qaeda's Strategy: The Deep Battle Against America*, New York: Columbia University Press, 2013.

Sadjapour, Karim, "The Islamic Republic Will Never Be the Same," Washington, D.C.: Carnegie Endowment for International Peace, June 26, 2009. As of January 30, 2018:
http://carnegieendowment.org/2009/06/26/islamic-republic-will-never-be-same-pub-23325

Sakwa, Richard, *Russian Politics and Society*, 4th ed., New York: Routledge, 2008.

Salih, Mohammad A., “How Islamic State Is Trying to Lure Kurds into Its Ranks,” *Al-Monitor*, August 12, 2016. As of January 30, 2018:
http://www.al-monitor.com/pulse/originals/2016/08/islamic-state-propaganda-video-kurds-iraq.html

Samaha, Nour, “Hezbollah’s Crucible of War,” *Foreign Policy*, July 17, 2016.

Sanburn, Josh, “Al-Qaeda Group Uses Donald Trump in Recruitment Video,” *Time*, January 2, 2016. As of January 30, 2018:
http://time.com/4165462/donald-trump-al-qaeda-video

Sanger, David E., “U.S. Blames China’s Military Directly for Cyberattacks,” *New York Times*, May 6, 2013.

———, “U.S. Cyberattacks Target ISIS in a New Line of Combat,” *New York Times*, April 24, 2016.

Sanger, David E., David D. Kirkpatrick, and Nicole Perlroth, “The World Once Laughed at North Korean Cyberpower. No More,” *New York Times*, October 15, 2017.

Sang-Hun, Chloe, “Kim Jong-un Takes an Additional Title in North Korea,” *New York Times*, June 29, 2016.

Saunders, Phillip C., and Joel Wuthnow, “China’s Goldwater-Nichols? Assessing PLA Organizational Reforms,” *Strategic Forum*, Washington, D.C.: National Defense University, April 2016.

Scanlon, Charles, “North Korea: Past Lessons Will Affect the Next Move,” BBC News, April 4, 2013. As of January 30, 2018:
http://www.bbc.com/news/world-asia-22032246

Scaparrotti, Curtis M., Commander, United Nations Command, United States–Republic of Korea Combined Forces Command, and U.S. Forces Korea, statement before the U.S. House of Representatives Armed Services Committee, Washington, D.C., April 2, 2014. As of January 30, 2018:
http://docs.house.gov/meetings/AS/AS00/20140402/101985/HHRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf

Schäfer, Christoph, “Propaganda: Die Psychokrieger der Bundeswehr” [“Propaganda: The Psychological Warrior of the Bundeswehr”], *Der Spiegel*, October 24, 2001. As of January 30, 2018:
http://www.spiegel.de/politik/deutschland/propaganda-die-psychokrieger-der-bundeswehr-a-163995.html

Scheuer, Michael, *Imperial Hubris: Why the West Is Losing the War on Terror*, Washington, D.C.: Brassey’s, 2004.

———, “Al Qaeda’s Media Doctrine: Evolution from Cheerleader to Opinion-Shaper,” *Terrorism Focus*, Vol. 4, No. 15, May 30, 2007.

Schleifer, Ron, “Psychological Operations: A New Variation on an Age Old Art: Hezbollah Versus Israel,” *Studies in Conflict and Terrorism*, Vol. 29, No. 1, 2006, pp. 1–19.

———, *Perspectives of Psychological Operations (PSYOP) in Contemporary Conflicts*, Eastbourne, UK: Sussex University Press, 2011.

Schmitt, Eric, “As ISIS Loses Land, It Gains Ground in Overseas Terror,” *New York Times*, July 3, 2016.

Security Council of the Russian Federation, “The National Security of Russia,” September 26, 2016.

Seftel, Bennett, “What Drives ISIS,” *Cipher Brief*, May 5, 2016a. As of January 30, 2018:
https://www.thecipherbrief.com/article/middle-east/what-drives-isis-1089

———, "Hezbollah's Many Faces," *Cipher Brief*, July 14, 2016b. As of January 30, 2018:
https://www.thecipherbrief.com/hezbollahs-many-faces

Seib, Philip, "The Al-Qaeda Media Machine," *Military Review*, May–June 2008, pp. 74–80.

Seldin, Jeff, "U.S. in 'Crisis Mode' in Fight Against IS Online Messaging," Voice of America, July 6, 2016. As of January 30, 2018:
http://www.voanews.com/a/united-states-crisis-mode-fight-islamic-state-online-messaging/3407346.html

Semenova, Janina, "Behind Russia's TV Propaganda Machine," *Deutsche Welle*, September 2, 2015. As of January 30, 2018:
http://www.dw.com/en/behind-russias-tv-propaganda-machine/a-18689297

Semenova, Ksenia, "A New Emigration: The Best Are Leaving, Part 1," New York: Institute of Modern Russia, April 7, 2015. As of January 30, 2018:
http://imrussia.org/en/analysis/nation/2224-a-new-emigration-the-best-are-leaving-part-1

Seper, Jerry, "Ruthless Mexican Drug Cartel Recruiting in U.S.; Los Zetas Looks to Prisons, Street Gangs," *Washington Times*, July 7, 2013. As of January 30, 2018:
https://www.washingtontimes.com/news/2013/jul/7/ruthless-mexican-drug-cartel-recruiting-in-the-us

Shabi, Rachel, "Special Spin Body Gets Media on Message, Says Israel," *The Guardian*, January 1, 2009. As of January 30, 2018:
https://www.theguardian.com/world/2009/jan/02/israel-palestine-pr-spin

Shachtman, Noah, and Robert Beckhusen, "Hamas Shoots Rockets at Tel Aviv, Tweeting Every Barrage," *Wired*, November 15, 2012. As of January 30, 2018:
https://www.wired.com/2012/11/gaza-social-media-war

Shambaugh, David, "China's Soft-Power Push," *Foreign Affairs*, June 16, 2015. As of January 30, 2018:
https://www.foreignaffairs.com/articles/china/2015-06-16/china-s-soft-power-push

Shane, Scott, *Objective Troy: A President, A Terrorist and the Rise of the Drone*, New York: Deckle Edge, 2015.

———, "The Enduring Influence of Anwar al-Awlaki in the Age of the Islamic State," *CTC Sentinel*, Vol. 9, No. 7, July 2016a, pp. 15–19. As of January 30, 2018:
https://www.ctc.usma.edu/posts/the-enduring-influence-of-anwar-al-awlaki-in-the-age-of-the-islamic-state

———, "ISIS Media Output Drops as Military Pressure Rises, Report Says," *New York Times*, October 10, 2016b.

Shane, Scott, Richard Pérez-Peña, and Aurelien Breeden, "'In-Betweeners' Are Part of a Rich Recruiting Pool for Jihadists," *New York Times*, September 22, 2016.

Shatz, Howard J., and Erin-Elizabeth Johnson, *The Islamic State We Knew: Insights Before the Resurgence and Their Implications*, Santa Monica, Calif.: RAND Corporation, RR-1267-OSD, 2015. As of January 30, 2018:
http://www.rand.org/pubs/research_reports/RR1267.html

Shen Weiguang, Jie Xijiang, Ma Ji, and Li Jijun, eds., *Zhongguo Xinxi Zhan* [*China's Information Warfare*], Beijing: Xinhua Press, 2005.

Shiloach, Gilad, "ISIS Hackers Respond to U.S. Cyberattacks with Threats," *Vocativ*, April 27, 2016. As of January 30, 2018:
http://www.vocativ.com/313259/isis-hackers-respond-to-u-s-cyber-attacks-with-threat

Siers, Rhea, “Israel’s Cyber Capabilities,” *Cipher Brief*, December 28, 2015. As of January 30, 2018:
https://www.thecipherbrief.com/article/israel’s-cyber-capabilities

Simmons, Katie, Bruce Stokes, and Jacob Poushter, “NATO Public Opinion: Wary of Russia, Leery of Action on Ukraine,” Washington, D.C.: Pew Research Center, June 10, 2015. As of January 30, 2018:
http://www.pewglobal.org/2015/06/10/1-nato-public-opinion-wary-of-russia-leary-of-action-on-ukraine

Singh-Bartlett, Warren, “Al-Manar Molds Itself to Changing Situation,” *Daily Star (Lebanon)*, January 3, 2001. As of January 30, 2018:
http://www.dailystar.com.lb//Culture/Art/2001/Jan-03/101569-al-manar-molds-itself-to-changing-situation.ashx

Small Media, *Iranian Internet Infrastructure and Policy Report*, London, January 2014. As of January 30, 2018:
https://smallmedia.org.uk/sites/default/files/u8/InternetInfrastructure_Jan14.pdf

Smyth, James, “China’s $10bn Propaganda Push Spreads Down Under,” *Financial Times*, June 9, 2016.

Snegovaya, Maria, *Putin’s Information Warfare in Ukraine: Soviet Origins of Russia’s Hybrid Warfare*, Washington, D.C.: Institute for the Study of War, September 2015. As of January 30, 2018:
http://www.understandingwar.org/report/
putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare

Solomon, Jay, “U.S. Detects Flurry of Iranian Hacking,” *Wall Street Journal*, November 4, 2015.

Solo un Hack, “‘La Tuta’ en su Rancho Envia Mensaje a EPN y al Gobierno de México” [“‘La Tuta’ on His Ranch Sends a Message to EPN and to the Government of Mexico”], video, posted April 27, 2013. As of January 30, 2018:
https://www.youtube.com/watch?v=hsJv43j7o-U

Sommer, Allison Kaplan, “Israel’s Online PR Offensive Sees Blowback,” *Haaretz*, November 18, 2012. As of January 30, 2018:
http://www.haaretz.com/israel-news/israel-s-online-pr-offensive-sees-blowback.premium-1.478639

Spaaij, Ramón, “The Enigma of Lone Wolf Terrorism: An Assessment,” *Studies in Conflict and Terrorism*, Vol. 33, No. 9, September 2010, pp. 854–870.

Spitz, Malte, “Germans Loved Obama. Now We Don’t Trust Him,” *New York Times*, June 29, 2013.

Stavridis, James, NATO Supreme Commander, Twitter post, October 21, 2011. As of January 30, 2018:
https://twitter.com/stavridisj/status/127344566050369536

Stepchenkov, Valeri, Olga Petrova, and Alissa de Carbonnel, “Mikhail Kosenko, Putin Critic, Sentenced to Detention in Psychiatric Ward,” Reuters (*Huffington Post*), updated January 23, 2014. As of May 24, 2017:
http://www.huffingtonpost.com/2013/10/08/mikhail-kosenko-psychiatric-ward_n_4064595.html

Stern, Jessica, and J. M. Berger, *ISIS: The State of Terror*, New York: HarperCollins, 2015a.

———, “A 6-Point Plan to Defeat ISIS in the Propaganda War,” *Time*, March 30, 2015b. As of January 30, 2018:
http://time.com/3751659/a-6-point-plan-to-defeat-isis-in-the-propaganda-war/

Stewart, LtGen. Vincent R., Director, Defense Intelligence Agency, "Statement for the Record: Worldwide Threat Assessment," statement to the U.S. House of Representatives Armed Services Committee, February 3, 2015. As of January 30, 2018:
https://www.armed-services.senate.gov/imo/media/doc/Stewart_02-09-16.pdf

Stokes, Bruce, "Russia, Putin Held in Low Regard Around the World," Washington, D.C.: Pew Research Center, August 5, 2015. As of January 30, 2018:
http://www.pewglobal.org/2015/08/05/russia-putin-held-in-low-regard-around-the-world

Stokes, Mark, "The Chinese Joint Aerospace Campaign: Strategy, Doctrine, and Force Modernization," in James Mulvenon and David Finkelstein, eds., *China's Revolution in Doctrinal Affairs*, Arlington, Va.: Center for Naval Analyses, 2002.

STRATFOR, "Lebanon: Hezbollah's Communication Network," May 9, 2008.

———, "Dispatch: Korea's Refocusing Policy Postures," November 18, 2010.

———, "The Geography of Mexican Drug Cartels," January 25, 2016.

Streibl, Ralf E., "Psychologische Kriegführung und Information Warfare" ["Psychological Warfare and Information Warfare"], in Gert Sommer and Albert Fuchs, eds., *Krieg und Frieden: Handbuch der Konflikt- und Friedenspsychologie* [*War and Peace: A Handbook of Conflict and Peace Psychology*], Weinheim, Germany: Beltz, 2004.

Sullivan, John P., "Criminal Insurgency: Narcocultura, Social Banditry, and Information Operations," *Small Wars Journal*, December 3, 2012.

Sullivan, John P., and Adam Elkus, "Cartel v. Cartel: Mexico's Criminal Insurgency," *Small Wars Journal*, February 1, 2009.

Swanson, Ana, "China's Influence over Hollywood Grows," *Washington Post*, September 24, 2016.

Takeyh, Ray, "Iran's Revolutionary Guards Are Shaping the Future of the Middle East," *Defense One*, June 17, 2016. As of January 30, 2018:
http://www.defenseone.com/ideas/2016/06/irans-revolutionary-guards-are-shaping-future-middle-east/129182

"Taliban Chief: U.S. Forces Must Leave Afghanistan," *Deutsche Welle*, February 7, 2016. As of January 30, 2018:
http://www.dw.com/en/taliban-chief-us-forces-must-leave-afghanistan/a-19373402

Talmadge, Eric, "North Korea Clamps Down on Already Spare Internet Access," *Christian Science Monitor*, July 6, 2015. As of January 30, 2018:
http://www.csmonitor.com/Technology/2015/0706/North-Korea-clamps-down-on-already-spare-Internet-access

Tasker, John Paul, "Top Ranks of Canadian Forces Get Shake-Up with New Army, Navy Commanders," CBC News, January 19, 2016. As of January 30, 2018:
http://www.cbc.ca/news/politics/vance-new-army-navy-commanders-1.3410474

"The Operations Man: Ayman al-Zawahiri," *The Estimate*, Vol. 13, No. 17, September 21, 2001. No longer available online.

Theohary, Catherine A., and John Rollins, *Terrorist Use of the Internet: Information Operations in Cyberspace*, Washington, D.C.: Congressional Research Service, March 8, 2011.

Thomas, Timothy L., "Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations," *Journal of Slavic Military Studies*, Vol. 11, No. 1, March 1998, pp. 40–62.

———, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" *Parameters*, Vol. 33, No. 1, Spring 2003, pp. 112–123.

———, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies*, Vol. 17, 2004, pp. 237–256.

———, *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness*, Fort Leavenworth, Kan.: U.S. Army Foreign Military Studies Office, 2011.

———, "Asia-Pacific: China's Concept of Military Strategy," *Parameters*, Vol. 44, No. 4, Winter 2014–2015, pp. 39–48.

Tidd, Chris, and Amanda Collins, "Army Communication and Information Systems Specialist," video transcript, undated. As of January 30, 2018:
http://cdn.forces.ca/_CAPTIONS/00362_armycommunicationandinformationsystemsspecialist_en.html

Times Wire Services, "Hundreds of Thousands Protest Missiles in Europe: Urge U.S. to Match Soviet Halt," *Los Angeles Times*, April 8, 1985. As of January 30, 2018:
http://articles.latimes.com/1985-04-08/news/mn-18506_1_cruise-missiles

Tinoco, Miguel García, "Criminales del Medievo; Hallan Túnicas de Caballeros Templarios" ["Medieval Criminals: Tunics Found from Knights Templar"], *Excelsior (Mexico)*, July 20, 2011. As of January 30, 2018:
http://www.excelsior.com.mx/2011/07/20/nacional/754520

Torres, Manuel R., Javier Jordán, and Nicola Horsburgh, "Analysis and Evolution of Global Jihadist Media Propaganda," *Terrorism and Political Violence*, Vol. 18, No. 3, 2006, pp. 399–421.

Tribal Analysis Center, *Mexico's Knight Templar and Code of Conduct Implications*, Williamsburg, Va., November 2013. As of January 30, 2018:
http://www.tribalanalysiscenter.com/PDF-TAC/Codigo%20De%20Los%20Caballeros%20Templarios%20De%20Michoacan%20v1.pdf

Tsfati, Yariv, and Gabriel Weimann, "www.terrorism.com: Terror on the Internet," *Studies in Conflict and Terrorism*, Vol. 25, No. 5, 2011, pp. 317–322.

Tucker, Patrick, "Why Ukraine Has Already Lost the Cyberwar, Too," *Defense One*, April 28, 2014. As of January 30, 2018:
http://www.defenseone.com/technology/2014/04/why-ukraine-has-already-lost-cyberwar-too/83350

———, "How to Stop the Next Viral Jihadi Video," *Defense One*, June 17, 2016. As of January 30, 2018:
http://www.defenseone.com/technology/2016/06/how-stop-next-viral-jihadi-video/129210

Tuckman, Jo, "Twitter Feeds and Blogs Tell Hidden Story of Mexico's Drug Wars," *The Guardian*, September 26, 2010. As of January 30, 2018:
https://www.theguardian.com/world/2010/sep/26/twitter-blog-mexico-drug-wars

———, "Mexican Drug Cartel Massacres Have Method in Their Brutal Madness," *The Guardian*, May 14, 2012. As of January 30, 2018:
https://www.theguardian.com/world/2012/may/14/mexico-drug-cartel-massacres-analysis

UK House of Commons Defence Committee, *Towards the Next Defense and Security Review*, Part 2: NATO, London, July 31, 2014. As of January 30, 2018:
https://publications.parliament.uk/pa/cm201415/cmselect/cmdfence/358/35802.htm

"Ukraine Crisis: Russian Troops Crossed Border, NATO Says," BBC News, November 12, 2014. As of January 30, 2018:
http://www.bbc.com/news/world-europe-30025138

"Ukraine Crisis: Timeline," BBC News, November 13, 2014. As of January 30, 2018: http://www.bbc.com/news/world-middle-east-26248275

United Nations General Assembly, *Human Rights in Palestine and Other Occupied Territories: A Report on the United Nations Fact Finding Mission on the Gaza Conflict*, A/HRC/12/48, September 25, 2009. As of January 30, 2018: http://www2.ohchr.org/english/bodies/hrcouncil/docs/12session/A-HRC-12-48.pdf

United Nations Office on Drug and Crime, *World Drug Report 2005*, Vienna, Austria, 2005. As of January 30, 2018: https://www.unodc.org/unodc/en/data-and-analysis/WDR-2005.html

United Nations Office for the Coordination of Humanitarian Affairs, *Ukraine*, Situation Report No. 34, April 3, 2015. As of January 30, 2018: https://www.humanitarianresponse.info/en/operations/ukraine/document/ocha-ukraine-situation-report-number-34-3-april-2015

Unwala, Azhar, and Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict," *Military Cyber Affairs*, Vol. 1, No. 1, Article 7, 2015.

U.S. Army Reserve, "U.S. Army Civil Affairs and Psychological Operations Command (Airborne)," web page, undated. As of May 24, 2017: http://www.usar.army.mil/USACAPOC

U.S. Army Special Operations Command, "Counter-Unconventional Warfare White Paper," September 26, 2014.

Venter, Al J., "South Lebanese Army Combats Internal Disintegration," *Jane's International Defense Review*, Vol. 29, August 1996, pp. 55–58.

Ventre, Daniel, "China's Strategy for Information Warfare: A Focus on Energy," *Journal of Energy Security*, Vol. 18, May 2010. As of January 30, 2018: http://www.ensec.org/index.php?option=com_content&view=article&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361

"Violence in Mexico and Central America: A Lethal Culture," *The Economist*, December 11, 2014. As of January 30, 2018: https://www.economist.com/news/americas/21636052-drugs-and-machismo-are-dangerous-mix-lethal-culture

Votel, Joseph L., Christina Bembenek, Charles Hans, Jeffrey Mouton, and Amanda Spencer, "#Virtual Caliphate: Defeating ISIL on the Physical Battlefield Is Not Enough," Washington, D.C.: Center for a New American Security, January 12, 2017. As of January 30, 2018: https://www.cnas.org/publications/reports/virtual-caliphate

Wainwright, Tom, *Narconomics: How to Run a Drug Cartel*, New York: PublicAffairs, 2016.

Wang Zhengde, ed., *Jiedu Wangluo Zhongxin Zhan* [*Interpretation of Network-Centric Warfare*], Beijing: National Defense Industries Press, 2004.

Wastnidge, Edward, "The Modalities of Iranian Soft Power: From Cultural Diplomacy to Soft War," *Politics*, Vol. 35, Nos. 3–4, November 2015, pp. 364–377.

Watts, Clint, "Inspired, Networked and Directed—The Muddled Jihad of ISIS and Al Qaeda Post Hebdo," *War on the Rocks*, January 12, 2015. As of January 30, 2018: https://warontherocks.com/2015/01/inspired-networked-directed-the-muddled-jihad-of-isis-al-qaeda-post-hebdo

Wege, Carl Anthony, "Hezbollah's Communication System: A Most Important Weapon," *International Journal of Intelligence and Counterintelligence*, Vol. 27, No. 2, 2014, pp. 240–252.

Wehrey, Frederic, "A Clash of Wills: Hezballah's Psychological Campaign Against Israel in South Lebanon," *Small Wars and Insurgencies*, Vol. 13, No. 3, 2002, pp. 53–74.

Wehrey, Frederic, Jerrold D. Green, Brian Nichiporuk, Alireza Nader, Lydia Hansell, Rasool Nafisi, and S. R. Bohandy, *The Rise of the Pasdaran: Assessing the Domestic Roles of Iran's Islamic Revolutionary Guards Corps*, Santa Monica, Calif.: RAND Corporation, MG-821-OSD, 2009. As of January 30, 2018:
http://www.rand.org/pubs/monographs/MG821.html

Wehrey, Frederic, David E. Thaler, Nora Bensahel, Kim Cragin, Jerrold D. Green, Dalia Dassa Kaye, Nadia Oweidat, and Jennifer J. Li, *Dangerous but Not Omnipotent: Exploring the Reach and Limitations of Iranian Power in the Middle East*, Santa Monica, Calif.: RAND Corporation, MG-781-AF, 2009. As of January 30, 2018:
http://www.rand.org/pubs/monographs/MG781.html

Weimann, Gabriel, "Hezbollah Dot Com: Hezbollah's Online Campaign," in Dan Caspi and Tal Samuel-Azran, eds., *New Media and Innovative Technologies*, Tel Aviv, Israel: Ben-Gurion University Press, 2008, pp. 17–38.

Weiss, Caleb, "Islamic State Launches Mobile App for Children," *Threat Matrix*, May 11, 2016. As of January 30, 2018:
http://www.longwarjournal.org/archives/2016/05/islamic-state-launches-mobile-app-for-children.php

Wells, Miriam, "Knights Templar Blame Self-Defense Groups for Violence in Mexico," Insight Crime, April 29, 2013. As of January 30, 2018:
http://www.insightcrime.org/news-briefs/knights-templar-blames-vigilantes-for-violence-in-mexico

———, "Mexico's Knights Templar Love Publicity, but Where Will It Get Them?" Insight Crime, February 18, 2014. As of January 30, 2018:
http://www.insightcrime.org/news-briefs/
mexicos-knights-templar-love-publicity-but-where-will-it-get-them

Welsh, Declan, and Eric Schmitt, "Drone Strike Killed No. 2 in Al Qaeda U.S. Officials Say," *New York Times*, June 5, 2012.

Wharton, Cabel N., and Daniel E. Welsh, *Net-Warlords: An Information Analysis of the Caballeros Templarios in Mexico*, Monterey, Calif.: Naval Postgraduate School, 2014.

"What Makes Hitler Tick? Brain in the Machine," *Journal of Electrical Workers and Operators*, Vol. 40, No. 8, August 1941. As of January 30, 2018:
http://www.ibew.org/Journals/scans/The%20Journal%20of%20Electrical%20Workers%20and%20
Operators/1941-08%20August%20The%20Journal%20of%20Electrical%20Workers%20and%20
Operators.pdf

White House Office of the Press Secretary, "Statement by the President on ISIL," September 10, 2014. As of January 30, 2018:
https://obamawhitehouse.archives.gov/the-press-office/2014/09/10/statement-president-isil-1

———, "Remarks by the President on Progress in the Fight Against ISIL," July 6, 2015. As of January 30, 2018:
https://obamawhitehouse.archives.gov/the-press-office/2015/07/06/
remarks-president-progress-fight-against-isil

Whiteside, Craig, *Lighting the Path: The Evolution of the Islamic State Media Enterprise (2003–2016)*, The Hague, Netherlands: International Centre for Counter-Terrorism, November 2016.

Winter, Charlie, “Islamic State Propaganda: Key Elements of the Group’s Messaging,” *Jamestown Terrorism Monitor*, Vol. 13, No. 12, June 12, 2015a.

———, *The Virtual “Caliphate”: Understanding Islamic State’s Propaganda Strategy*, London: Quilliam Foundation, July 2015b.

———, “ISIS Is Using the Media Against Itself,” *The Atlantic*, March 23, 2016. As of January 30, 2018:
https://www.theatlantic.com/international/archive/2016/03/isis-propaganda-brussels/475002

———, *Media Jihad: The Islamic State’s Doctrine for Information Warfare*, London: International Centre for the Study of Radicalisation and Political Violence, February 2017. As of January 30, 2018:
http://icsr.info/wp-content/uploads/2017/02/Media-jihad_web.pdf

Winter, Charlie, and Jordan Bach-Lombardo, “Why ISIS Propaganda Works,” *The Atlantic*, February 13, 2016. As of January 30, 2018:
https://www.theatlantic.com/international/archive/2016/02/isis-propaganda-war/462702

Winter, Charlie, and Colin P. Clarke, “Is ISIS Breaking Apart? What Its Media Operations Suggest,” *Foreign Affairs*, January 31, 2017. As of January 30, 2018:
https://www.foreignaffairs.com/articles/2017-01-31/isis-breaking-apart

Winter, Charlie, and Haroro J. Ingram, “How ISIS Weaponized the Media After Orlando,” *The Atlantic*, June 17, 2016. As of January 30, 2018:
https://www.theatlantic.com/international/archive/2016/06/isis-orlando-shooting/487574

Wolff, Andrew T., “Crafting a NATO Brand: Bolstering Internal Support for the Alliance Through Image Management,” *Contemporary Security Policy*, Vol. 35, No. 1, 2014, pp. 73–95.

Woody, Christopher, and Mike Nudelman, “Here’s How Many Foreign ISIS Fighters Have Returned Home from the Battlefield,” *Business Insider*, October 26, 2017. As of January 30, 2018:
http://www.businessinsider.com/how-many-foreign-isis-fighters-have-returned-home-from-the-battlefield-2017-10

World Bank, International Bank for Reconstruction and Development, *World Development Indicators 2012*, Washington, D.C., 2012. As of January 30, 2018:
https://openknowledge.worldbank.org/handle/10986/6014

Wortzel, Larry M., Commissioner, U.S.-China Economic and Security Review Commission, “China’s Approach to Cyber Operations: Implications for the United States,” testimony before the U.S. House of Representatives Committee on Foreign Affairs at the hearing “The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security and Trade,” March 10, 2010. As of January 30, 2018:
https://www.uscc.gov/china’s-approach-cyber-operations-implications-united-states

———, *The Chinese People’s Liberation Army and Information Warfare*, Carlisle Barracks, Pa.: U.S. Army War College, Strategic Studies Institute, March 2014.

Wright, Lawrence, “The Master Plan,” *New Yorker*, September 11, 2006.

Wright, Robin, “The Demise of Hezbollah’s Untraceable Ghost,” *New Yorker*, May 13, 2016.

Yaffa, Joshua, “The Insanity of Protesting Against Putin,” *New Yorker*, October 9, 2013.

Ye Zheng, *Xinxihua Zuozhan Gailun* [*An Introduction to Informationalized Operations*], Beijing: Military Science Press, 2007.

Young, Leslie, “Soap Operas and Short-Wave Radio: How North Koreans Learn About the Outside World,” Global News (Canada), September 29, 2017. As of January 30, 2018:
https://globalnews.ca/news/3776420/north-korea-foreign-media-propaganda

Young, William, David Stebbens, Bryan Frederick, and Omar Al-Shahery, *Spillover from the Conflict in Syria: An Assessment of the Factors that Aid and Impede the Spread of Violence*, Santa Monica, Calif.: RAND Corporation, RR-609-OSD, 2014. As of January 30, 2018: https://www.rand.org/pubs/research_reports/RR609.html

Yrayzoz, Javier, "MNB Southwest Distributes 35,000 Magazines," *KFOR Chronicle*, January 31, 2003. As of January 30, 2018: http://www.nato.int/KFOR/chronicle/2003/chronicle_01/10.htm

Zelin, Aaron Y., "The War Between ISIS and al-Qaeda for Supremacy of the Global Jihadist Movement," Washington, D.C.: Washington Institute for Near East Policy, Research Note 20, June 2014. As of January 30, 2018: http://www.washingtoninstitute.org/policy-analysis/view/the-war-between-isis-and-al-qaeda-for-supremacy-of-the-global-jihadist

———, "Picture or It Didn't Happen: A Snapshot of the Islamic State's Official Media Output," *Perspectives on Terrorism*, Vol. 9, No. 4, 2015.

Zetter, Kim, "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits," *Wired*, November 19, 2015. As of January 30, 2018: https://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols

Zhang Yuliang, ed., *Zhanyi Xue* [*The Science of Military Campaigns*], Beijing: National Defense University Press, 2006.

Zhao Erquan, "Lun Xinxihua Zhanzheng dui Wuzhuang Chongtu fa de Shenyaun Sixiang" ["A Discussion of Far-Reaching Thinking on Armed Conflict and Informatized Warfare"], in Liu Jixian and Liu Zheng, eds., *Xin Junshi Geming yu Junshi Fazhi Jianshe* [*The New Revolution in Military Affairs and Building a Military Legal System*], Beijing: PLA Press, 2005.

Zverev, Anton, "Ex-Rebel Leaders Detail Role Played by Putin Aide in East Ukraine," Reuters, May 11, 2017. As of January 30, 2018: https://www.reuters.com/article/us-ukraine-crisis-russia-surkov-insight/ex-rebel-leaders-detail-role-played-by-putin-aide-in-east-ukraine-idUSKBN1870TJ

Harnessing the power of old and new technology, it is easier than ever for U.S. allies and adversaries to reach—and influence—vast and varied audiences to achieve their strategic goals. Modern conflicts are fought as much in the information environment as on the physical battlefield, and the line between these domains is dissolving. Less sophisticated state actors and even nonstate actors have acquired capabilities previously available only to the most advanced nations to use information power in support of their objectives. Adversaries of the United States and its allies do not operate under the same legal and ethical constraints and are free to engage in offensive cyberwarfare, disseminate propaganda, censor traditional and online media, and threaten their detractors. As it prioritizes investments in future capabilities, the U.S. Army stands to benefit from an examination of the evolution of allied and adversary information campaigns, as well as their successes, failures, and potential future directions. This collection of 12 detailed case studies reviews the information-related activities and strategic goals of a range of allies, adversaries, and potential adversaries, highlighting insights for future U.S. Army force planning. A companion volume, *Lessons Others for Future U.S. Army Operations in and Through the Information Environment,* presents a comparative analysis of the cases, highlighting the capability areas in which others excel to guide the Army in either adopting or countering these practices and principles.

RAND ARROYO CENTER

www.rand.org

$56.00

ISBN-10 0-8330-9997-3
ISBN-13 978-0-8330-9997-6

55600

9 780833 099976

RR-1925/2-A