MCIS Yearbook 2012

MCIS

Mediterranean Council for Intelligence Studies

Conclusions or opinion expressed are those of the authors and do not necessarily reflect the views of the MCIS.

EDITORIAL TEAM

EDITORIAL BOARD

EDITORIAL BOARD ADDRESS

Mediterranean Council for Intelligence Studies

c/o Research Institute for European and American Studies (RIEAS)

Kalavriton 1 Str.

Alimos, Athens 17456

Attiki

Greece

Web: www.rieas.gr, www.mcisitalia.net
Email: rieasinfo@gmail.com, coordinatore@mcisitalia.net
Tel/Fax**:** +30 210 9911214

YEARBOOK DESIGN

Dr. Stefania Ducci – MCIS Deputy Chair

CONTENTS

EDITORIAL STATEMENT

We are pleased to launch the first issue of our Yearbook, the MCIS 2012 Yearbook, which is the result of an extended engagement of Mediterranean countries and international scholars in a joint effort to advance graduate and postgraduate education and research in the field of Intelligence and Security studies, and to develop regional academic networking.

The Yearbook reflects diverse theoretical approaches towards intelligence and security studies. The first issue contains scientific contributions in the following two areas of study: A) for the section on "Intelligence in action" we have decided for this year to focus it on cyber security and cyber defence, with interventions by Prof. Joseph Fitsanakis & Dr. Micah-Sage Bolden, Dr. Andrew Liaropoulos, and Mr. Anthimos Alexandros Tsirigotis; B) for the part on "Intelligence studies in the Mediterranean region", we have chosen an interesting analysis on the development of intelligence studies in France, by Dr. Eric Denécé.

Besides the focus of its contents, the MCIS Yearbook is fully electronic in format. In fact, we intend to exploit the electronic medium to its fullest degree. Moreover, by not maintaining a print version, we are able to avoid some of the costs that confront other journals. Indeed, another highly unusual feature of MCIS Yearbook is that the journal is completely free and accessible world-wide. Subscriptions are intended for those readers who wish to be notified each time a new issue is published. However, the journal can be read without a subscription, and we invite all readers to contribute articles for publication.

In all these ways, the MCIS Yearbook is filling a gap in our current resources. At the same time, like other top publications, we are committed to upholding the highest academic standards and to providing informative and critical analysis of topical issues accessible to all those interested in intelligence and security studies. All submissions go through a process of anonymous peer review. We are proud to have an outstanding editorial board which works with us to ensure that only research of the highest calibre is published.

The Editorial Team

Prof. John M. Nomikos – MCIS Chairman

Dr. Stefania Ducci – MCIS Deputy Chair

INTELLIGENCE IN ACTION

CYBER SECURITY & CYBER DEFENCE

INTRODUCTION

LIVING IN THE CYBER ERA: REFLECTIONS ON SECURITY IN A HYBRID WORLD

Prof. Maria Luisa Maniscalco
Full Professor of Sociology, Department of International Studies, 'Roma Tre' University, Italy.

1. A HYBRID WORLD

We are living in a hybrid world in which human beings and technology are strictly intertwined. Material and virtual worlds are not opposite realities and our daily life follows two different logics and codes: that of the tangible reality of bodies, nature and things, and that of the intangible that characterizes the web. Individuals, groups, communities, organizations and institutions are now the 'hubs' that connect and compose these two worlds.

What happens in the material world has an immediate repercussion on the web and vice-versa: we celebrate our birthday on the web, we meet people on social networks, and then we weave not only virtual relationships with them. On the Internet we buy clothes we wear every day to get to work and we look for information for health, holidays, leisure time, and investments, and from the cyber space even new religious movements emerge. The network leads and colonizes most of our social life and affects the way of experiencing two fundamental dimensions of life associated with time and space.

Time and space, as pointed out by Emile Durkheim in the early twentieth century, are two fundamental dimensions of social life. They are tools used by players in social practices and structures and they are categories through which to understand and organize experience. As such, they are closely connected with a society's structural and organizational characteristics and they change depending on these. With the emergence of cyber space, the space-time paradigm that governed relationships and communications in modern society has progressively given out. 'Space' has been transformed into a space of flows, a network of interactions and almost simultaneous exchanges among people that are physically displaced, while 'time' is reset to zero (the real time) and has become irrelevant since the social actors may communicate synchronously or asynchronously using the various tools provided by technological innovation. Thus, the relevance of distances and time in individuals and populations' lives has been dissolved. What makes these changes worthy of being defined as a true 'revolution' is their high degree of social penetration that makes our society a 'network society' (Castells, 1996, 1997, 1998) in which the structure of the economy changes and new practices, new cultures, and new expressions of imaginary and social ties emerge.

'Web society' is a global network which revolves around the innovations dictated by technological developments. Organizations,

institutions, individuals, and groups 'should' be connected, otherwise this would lead to marginalization. For this reason, one's existence is two-folded, being lived in both real and virtual worlds. *Homo sociologicus* is nowadays a *homo cyborg*, equipped with technological tentacles with which he/she manages and experiences his/her own life. In turn, collective representations and social, economic, and cultural models of organization and functioning are focused on web's paradigm and new symbolic order. In addition, security must be sought in a manner that takes into account the hybridization of the two worlds: from the virtual one there come risks and threats that impact slightly on real life.

2.NETPOLITIK

At the political level we talk about *netpolitik* (Bollier, 2003; Maniscalco, 2006) as a new way to influence and shape politics and identity, culture and values, as well as practices and cognitive maps by using the power of the web. *Netpolitik* makes it possible a fragmentation of the forms of mediation in place of the one-tier model, which has long been dominant, acting at the level of soft issues such as moral legitimacy, cultural identity, social values, and collective perceptions. Thus, it creates a global political space with new logics, new languages, and especially new players. The horizontality of the web alters the traditional hierarchical relationships among sources. New communication flows emerge, which cross cultures moving in an extraterritorial area that goes beyond the conventional political governance and jurisdiction. The globalization of information leads to extend beyond borders the national public spheres in a complex network of interconnections articulated at different levels, in which States' communications accompany, are combined, and compared with those from organised civil society – which works both at national and transnational level –, mass media and even individuals, networked in a complex interplay of relationships and references. The domino effect triggered by the Tunisian revolt throughout the Maghreb and beyond is a significant example of the amplification and speed up of emulation and 'contagion' dynamics implemented by web-enabled connections.

The political space created by the *netpolitik* changes the usual way to act by traditional media, which confront themselves with the possibilities inherent to new technologies, taking up and amplifying the news circulating on the Internet. Many political or politically relevant news, from softest to most tragic ones, circulate firstly on the web and then are echoed by other media: this was the case, just to name few examples, of Clinton-Lewinsky scandal (Maniscalco, 2002), of the terrifying killings of hostages by terrorist groups, as well as of the 2010 *Cablogate* affair. WikiLeaks has entrusted the selection and dissemination of information to five major newspapers (The Guardian, The New York Times, *Le Monde*, *El País* and the weekly *Der Spiegel*), whose journalists were engaged in the task of preventing that the publication of documents would lay it on the line human life, journalistic sources, and materials, the revelation of which would

compromise ongoing operations. Traditional media have staked their credibility by offering a sort of 'certification of trust' to information and documents whose content's origin and authenticity might seem questionable.

The advent of new information technologies has also changed the forms of protest. Going back in the past, among the various complaints against globalization, a major role is played by the boycotts that are based on the so-called 'naming and shaming' strategy, with the aim of raising public awareness through the web-dissemination of accurate information on sensational cases of special concern, often urging the public not to buy the products of certain corporations. The 'Clean Clothes Campaign', promoted in 1993 by a union of student groups, religious associations and trade unionists, was directed at department stores like M&Mode, Perk&Cloppenburg, C&A, blamed of gaining profits from products made by exploited workers, with poor security and low wages, in different world countries (Honduras, Guatemala, Mexico, Hong Kong, Bangladesh and South Korea). Later examples of boycotts against multinational companies affected McDonald's, Del Monte, Nestlé, Montesanto, Nike, Shell, Pfizer and other big corporations. Another form of boycott that uses Internet as a direct tool is *netstrike*, which consists of simultaneous connection by a high number of users to the same web address on a given day and at a predetermined time. The aim is to cripple a site considered as a symbolic target and to hinder access to its contents. *Netstrike* is a real rally on the web, a mobilization similar to that of a parade that occupies a road until it becomes inaccessible. For example, a 'virtual march' on Washington was organized in February 2003 by the site *moveon.org*. Two hundred thousand people have registered to the initiative by committing themselves to 'bombard' of e-mail messages the electronic addresses of the U.S. administration. Significant most recent events, as recalled by Joseph Fitsanakis and Micah Sage-Bolden in their essay that follows, were, for example, operations on Facebook directed against NATO and the initiative of the group "One Million Voices Against FARC" in opposition to the guerrilla carried out in Colombia by the *Fuerzas Armadas Revolucionarias de Colombia*.

Mobilization potentials have been amplified with web 2.0 applications. Online interactivity allows multiple participants to communicate in a multi-dimensional way, to circulate information, desires, and moods, then dumping them in the high-density symbolic and emotional urban spaces. It is well known that Facebook, Twitter, YouTube, BlogTalkRadio and so on, have been used to plan and organize protests in all Arab countries affected by the so-called 'spring'. The electronic platforms of expression intensified, starting from the immaterial, the flow – from one node to the other – of opinions, aspirations, and dreams. By coagulating moods and corroborating vocations they have outlined forms of sociability and subjectivity not exclusively reducible to the sole web-space, and for which the degree of freedom of action and expression established by the institutionalized powers appeared too much limited compared to the 'game'

played in electronic environments.

3. CYBER SECURITY: OLD AND NEW SECURITY ISSUES

In a world where reality and virtuality are strictly intertwined, cyber security plays an important role. We cannot forget, for instance, that cyber space has long been the new frontier of transnational terrorism. The web has opened up new unthinkable possibilities that move from cyber-terrorism to propaganda, recruitment, and training, including new organizational forms more extensive, flexible and efficient than mass political actions, as shown by the so-called 'Black Bloc' movement that acted in different situations of urban warfare during the last decade.

Terrorism is a phenomenon deeply rooted to advertising and to the effects that it generates both in the population at large and in social areas that constitute a natural recruitment pool. Communication is the first and perhaps the most important weapon used by all contemporary terrorist groups since mass media are the ideal medium for disseminating news and images related to them. Television represents an effective means to disseminate widely and in real-time events that mobilize public opinion's attention and move the collective emotion. More than television, the web has structural features that make it the medium of choice for all types of terrorism. The global coverage, the almost total lack of control, and the possibility to rapidly open and close web-sites, facilitate the diffusion of any type of message, even the most subversive one. Internet has represented the largest investment for Islamist groups. Young people are recruited online and addressed toward the theatres of conflict. In November 2003, Al Ahmad Wasiq Billah, one of Bin Laden's spokesperson, announced the inauguration of Al-Qaeda online university of Jihad, with courses on 'electronic jihad', 'psychological Jihad', 'explosives' technology', and 'car bomb's technology'. The would-be terrorists can find online military training – as that of Al-Battar – that remain active only for a few hours, enough to download the program but too few to allow the source location. Counter-terrorism forces are almost unable to neutralize a cyber training camp that can be practically anywhere. Moreover, on the web there are photos, videos, and information such as the claims of the attacks in Iraq, the instructions for September 11 hijackers, and details on how to attack European cities.

The web grants transnational visibility to every subversive movement, in a way that organizations active in the past decades have ever had. Thus, left-wing extremists, as well as anarcho-insurrectionalism European groups, find in the cyber space a place in which to spread their anti-establishment themes, to keep in touch across borders, and to proselytize.

Also the military strategy changes in cyber era, as illustrated in the essays of Anthimos Alexandros Tsirigotis and Andrew Liaropoulos. We can already mention significant cases of cyber space exploitation for war purposes: for example, the 2008 Russian armed attack against Georgia to gain control of South Ossetia and

Abkhazia was accompanied by cyber attacks that crippled enemy's systems.

In the new scenario, the strategic approach of the control of violence through space-time fixity has been replaced by an approach based on space-time fluidity, ubiquity, and virtuality (Arquilla and Ronfeldt, 2001). The so-called doctrine of 'Revolution in Military Affairs' (RMA) – under which in the U.S. has been synthesized a doctrinal and organizational change in the way of waging war – emphasizes the importance of satellite observation, stealth aircrafts, electronic management of information, and logistics, to achieve the two-fold objective of military supremacy and zero losses. The point of force of this new approach is represented mainly by the domain of information (information dominance), resulting from the interconnection on the web of all the units in the field, to allow a continuous information flow. The 'infodominance' has assumed the role of a strategic metaparadigm that consecrating the real-time as a deletion of the adversary's spatial depth, should provide significant benefits to decision making. The Revolution in Military Affairs continues to be enriched by new military methodologies related to the power of information – such as the network-centric warfare, which foresees the digitization of the space of manoeuvre. Also the new U.S. military policy introduced by President Barack Obama on the 5th of January, 2012 (Obama, 2012), gives a central role to the cyberspace domain and to the use of information technology. Given the risks to states and networked societies' security generated by cyber conflicts, what is still lacking, as pointed out in the Liaropoulos' essay, is the development of adequate capabilities, of an international legal framework, and of strategies to address deterrence in cyberspace.

Another issue that shall be considered is the relationship among Internet, privacy, and transparency. Each online behaviour can be 'traced': from cookies – perfectly legal software that store information on our Internet-surfing preferences to make it closer to our needs – to spybots – viruses that keep track of all our activities on Internet. Web 2.0 and social networks have questioned the very concept of confidentiality. The word 'publicly' expresses the idea that our privacy has become public once our profile has been put online, that our intimacy is externalized through Facebook, and that our privacy is available to everybody.

Several controversial issues have called the attention of the privacy trustees and legislators about the new services offered by search engines and web operators (think about, for example, 'street view' or facial recognition software so-called 'second look'). In general, a new chain of activities has been flourished: from profiling for advertising purposes, to recruiting and head hunting by human resource managers. Not to mention the many illegal and even criminal activities that privacy's threshold lowering allows. In 2010 alone, more than thirty of most important American companies have been affected by damage or theft of significant size over Internet. Main oil companies, for example, have been stolen of confidential data relating to the exploration of new oil and gas fields.

High web transparency not only threatens to overwhelm

ordinary people's privacy and companies' confidential information, but also undermines the necessary confidentiality for a good government action. After WikiLeaks the line between transparency and State's secrecy will no longer be the same. In general, secrecy is considered a feature typical of authoritarian states, while transparency is considered a democratic value. However, it should be considered that even democracies have – and must have – areas of secrecy that have to be protected as a public interest.

Like any technological innovation cyber space's power offers both chances and risks: the increase of available information can produce an overload, but it also offers to security and intelligence agencies resources that were unthinkable a few decades ago, increasing the potential of open source intelligence (OSINT). According to Fitsanakis & Bolden, through social networks is possible to analyse public opinion's trends and they provide actionable tactical intelligence in many situations where other information-collection techniques are not feasible.

In conclusion, cyber security has many fields of application and research that will increasingly involve security practitioners and scholars.

BIBLIOGRAPHY OF REFERENCES CITED

Arquilla, J., Ronfeldt, D. (eds.) (2001) Networks and Netwars: the Future of Terror, Crime and Militancy (Santa Monica: RAND).

Barack, O. (2012) Defense Strategy: Sustaining US Global Leadership-Priorities for 21st Century Defense, available online at: http://www.defense.gov

Bollier, D. (2003) The Rise of Netpolitik: How the Internet Is Changing International Politics and Diplomacy (Washington D.C.: The Aspen Institute).

Castells, M. (1996) The Information Age: Economy, Society and Culture, vol. 1: The Rise of the Network Society (Oxford, UK: Blackwell).

Castells, M. (1997) The Information Age: Economy, Society and Culture, vol. 2: The Power of Identity (Oxford, UK: Blackwell, Malden, Mass).

Castells, M. (1998) The Information Age: Economy, Society and Culture, vol. 3: End of Millennium (Oxford, UK: Blackwell, Malden, Mass).

Maniscalco, M.L. (2002) Come una soap opera. L'*affaire* Clinton-Lewinsky, in E. Tedeschi (eds), Il potere dell'audience, pp. 107-132 (Roma: Meltemi).

Maniscalco, M.L. (2006) Netpolitik. Internet e il nuovo spazio politico internazionale, in B. Consarelli (eds), Spazi e politica nella modernità tecnologica, pp. 23-58 (Firenze: Firenze Univ. Press).

MILITARY STRATEGY IN THE CYBER ERA: CONTINUITY AND CHANGES

Anthimos Alexandros Tsirigotis
M.Sc International and European Studies, University of Piraeus, Greece.
Phd Candidate, Reading University, UK.

ABSTRACT

Cyber seems to have created a frenzy of reactions around the world for the last five years. Digital attacks against the networks of states have been proven to be potent enough to provoke considerable harm to the security of information-dependent societies. Threats stemming not from traditional military actions (i.e. bombardment, troop invasion) but instead from malicious computer programs can kneel down the Critical Infrastructures and degrade backbone networks of states. The exposure of contemporary states to the cyberspace is considered to be Achilles' heel vulnerable to any malevolent actor whose identity is difficult to be revealed. Military strategy in the cyber era is undergoing the strenuous process of being revised mainly because of the new profile that foes within the cyber dimension have. However, no matter how profound the changes are, the nature of the strategy will remain untouched. Its function for bridging military and political effects will continue to be necessary in the cyber era even though strategists should find new guiding paths among ends, means and ways.

1. INTRODUCTION

In every era the use of pioneering military technologies fuels the debate about sea changes to the nature of war. Throughout military history, those cases in which the mutations had been as profound as to end up in a new war paradigm are denominated as Revolutions in Military Affairs (RMA). The introduction of railway, telegraph, radar and jet aircraft to mention just few of them, have for sure changed once and for ever the conduct of war (Boot, 2006). Nevertheless, not every single RMA is susceptible to permeate the whole societal body and to provoke far-reaching changes affecting its structure or, much more, its culture. Among the numerous RMAs that one could enlist only few of them are to be considered as milestones that heralded profound changes with far reaching societal repercussions. This is the case of the Military Revolutions (MRs) as the Napoleonic "levée en masse" had been which definitely figures among the most prominent.

As diverse as the opinions may be about the identification of technological breakthroughs whether as RMAs or MRs, the underlying meaning of the Military Revolution Debate (Rogers, 1995) is that war is primarily a political praxis of humans, using the term in its Aristotelian context. The changes in war paradigm and the way society is structured are in absolute concordance (Gray, 1999, p.186). Alvin Toffler has perfectly shaped this notion by classifying war into three separate models taking each time into account the economic mechanism of wealth production. He distinguishes between the

agricultural, industrial and informational war paradigm. The way societies are getting involved in belligerent actions is impossible to be in stark contrast neither to their system of values nor to the way they are structured during peacetime.[1] War has always been and it will continue to be a means of communication among societies.

To that point it is essential for the purposes of this article to clarify what is implied by the dictum that war changes over time. Is that to say that as societies and technology evolve so does war in reference solely to the weapons used? Or, instead, that what really alters is the way people conceive war as a means for succumbing their opponent's will? For instance, if we take a look at the battlefield of the Peloponnesian war in comparison to that of the First World War, obviously there are structural differences as far as the weapons or the tactics used are concerned. However, in both instances there is an element that remains invariable in the course of history; the "essence" of war. Thus, it is of crucial importance to delineate between the nature and the character of war. What really changes under the influence of arms technology is the character of war while its nature remains always untouched.

The "essence" of war or its nature is crystal clear and has come down to us by three of the most prominent war historians as Thucydides (460 - 395BC), Clausewitz (1780 - 1831), and Sun-Tzu (544 – 496BC). The unchanged nature of war is blatantly distilled in just few simple yet insightful and all embracing sentences. For the Greek Thucydides the origins of war can always be found to the "fear, honour, and interest" while the Prussian Clausewitz[2] defined the Trinitarian nature of war as a mixture of passion, chance and rationality (Clausewitz, 1976).[3] The work of Sun-Tzu as instructional as it may sound (full of do's and don'ts) offers to us the "pinnacle of excellence" of war to be "subjugating the enemy's army without fighting" (Sun Tzu, 1994, p.177); a view of war that during our post heroic times[4] is increasingly gaining value.

It is evident that every time a pioneering technological advance introduces significant changes to the war paradigm, as for instance the steam power, the air jet, the radar and nuclear energy have been, writers are inclined to support that the relevant breakthrough of their era is so fundamental as to alter once and forever the nature of war and so potent as to defy its basic grammar.[5] This is also the case with the so called "cyberwarfare" the dynamics of which have made some pundits to believe that future wars will seem as an effort of each part to «gain access to the electronic files of its opponent (financial, governmental, military) while digitally controlling its critical Infrastructure (electricity, water supply, telecommunications etc)» (Nugent & Raisinghani, 2008, p.31).[6] Warfare in the cyber era[7] constitutes, certainly, a new point of concern for the contemporary, Internet dependent and densely networked states. However, what needs to be further examined is the extent to which warfare in the cyberspace adheres to the basic grammar (or as above mentioned to the "essence") of war. Does the cyber dimension of modern communities constitute a profound organisational societal reordering capable of instigating sea changes to the nature of war itself? If that is

the case, then military strategy should be thoroughly redesigned so as to intercept the new threats within the cyber dimension.

2. THE CYBER DIMENSION OF THE MODERN WORLD

For each community wishing to secure its welfare and prosperity, it is of crucial importance to be aware of the primary tendencies that will play a decisive role into shaping the future. Amongst a series of global trends such as terrorism, climate change or energy problems the emergence of every kind of computer networks is a determining factor as well. The rapid emergence of Information Technology (IT) has disproportionally amplified the strength of ordinary people to be expressed and in some instances to exert directly his political power without the intermediary role of the sovereign state (i.e. the Arab upheaval). People seem to be continuously interconnected to an invisible societal body wherever they may be on earth[8] and this is accentuated by the growing tendency towards mobile digital applications (as for instance smart phones) (The Economist, 2011a).

The Internet offers a supreme opportunity for people to self-organize by means of the Internet and to create "virtual communities". Their dynamic is as noticeable as Slaughter equates their strength to «The American social revolution that Alexis de Tocqueville observed in the early 19th century» and she notes that it is this field from where the great future changes will stem because networks are «[...] forever changing the relationship between citizens and their governments, and governments with each other» (2011). However, in contrast to the social revolution of the 19th century, this revolutionary change is not taking place in the physical three-dimensional world. Instead, it is materialized within the infinite limits of cyberspace. Its power to instigate wide repercussions to the societal body is considered pivotal. Karatzogianni developed a thorough theory of this new organisational scheme in world politics following the Deleuzian and Guattarian philosophical school of thinking. She insightfully supports that the theory of Rhizomatic politics fully encompasses the modern societal tendencies worldwide and can explain the modern epistemology. The power of networked organisational schemes, which constitute the salient feature of the cyberspace, empower «[...] socio-political movements to set in motion centrifugal forces which could ultimately render the world system not viable» (Karatzogianni, 2010, p.266).[9]

Thus, it would be insufficient to consider cyberspace to be only «the fusion of all communication networks, databases and information sources into a global virtual system» (Liaropoulos, 2011, p.2). The revolutionary potential of this new medium should be attributed to three of its salient features: i) the priority of networks as organisational schemes in contrast to hierarchies (Ottis, 2010, pp.97-110; Libicki, 2009, pp.11-23; Karatzogianni, 2006; Slaughter, 2004; Castells, 2001; Arquilla, Ronfeldt, 2001, 1997, pp.23-60); ii) the diffusion of power into smaller and non-state actors

(Nye, 2010; Arquilla, Ronfeldt, 1997); and iii) the strategic dimension of cyberspace (Sheldon, 2011; Geers, 2010; Owens, 2008).

Cyberspace has come to change once and for ever the political communication in world politics. It does not only constitute a pioneering technological breakthrough. It is not just an agglomeration of some IT infrastructures that facilitates our everyday lives. Instead, it offers a brand new way for perceiving the three-dimensional reality and far and foremost it offers new political means available to everyone willing to manifest their political existence and to try to meet their political objectives. As the political communication of contemporary societies changes, so does warfare as according to the Clausewitz's dictum, it constitutes the continuation of politics by other means.

3. MILITARY STRATEGY IN CYBER ERA

It would be difficult to deny that the frequency of cyber incidents grows exponentially.[10] In cyberspace, attacks which target networks of every kind (civil or military) have transcended the realm of fiction and constitute a real life attack scenario to which each Internet dependent state is extremely vulnerable. What took place in Estonia as early as in 2007 is considered the first incident of warfare in the cyberspace and has also been denominated as "Web War I" (Blank, 2008). One year later, cyber attacks formed part of the Russian military operations (kinetic operations) of land and air forces against Georgia.[11] Recently the Stuxnet attack against an Iranian nuclear plant has revealed an aspect of the operational dynamic of cyber attacks for succumbing the opponent's will (Milevksi, 2011; Zetter, 2011). To try to give a list of every cyber attack seems to be unproductive and strenuous as every single network (either connected or not to the Internet) is under continuous attack[12] on a 24/7 basis. Military networks are not exempted from the target lists and one recent example is the case of the USA Unmanned Aerial Vehicle that flew over Afghanistan which became infected by virus.[13]

Cyber attacks do constitute a menace for every society that relies, to a higher or lesser degree, on networked organisational schemes. However, what is still unclear and open to further discussion is whether cyber attacks constitute weapons in the hands of perpetrators to meet their political objectives. That is to say that it is still obscure if cyber attacks, even if they were launched against every single network of a society (financial, governmental, military, social) and in the absence of any other traditional military operation, would compel sovereign states to change their political will. For instance, no matter how severe the above mentioned cyber attack against the Iranian nuclear plant may have been; did it finally result in Iran abandoning its nuclear ambitions for developing nuclear weapons? If that was the case then it would indicate that attacks of this kind can meet the political objectives of their perpetrators without the need to resort to military operations.

Possibly, neither nation states nor any other non-state actor have elaborated up to now a complete strategy for what Rattray calls strategic information warfare. Nevertheless, he argues that «The use of non-violent digital attacks to achieve political objectives must be understood as part of a new form of warfare» (Rattray, 2001, p.20). Sovereign states are reluctant to rely on offensive cyber attacks as a means of coercion. They show a preference towards defensive cyber weapons by incorporating into their military organisations some divisions for the vigilance of their networks and the immediate response whenever needed. Their stance towards the cyberspace could be considered a phobic one. This assertion can be inferred by whenever states such as the USA declare that they would treat a significant cyber attack on the nation in the same way they would an attack on the land, sea, air, or in space, and that proportional military force would be an option. They are ready to oil their tanks, airplanes and all their kinetic war machines in order to respond to cyber attacks that stem from groups whose identity is not easily tracked back, they may not even be attributed to sovereign states but rather to non-state actors (terrorist groups, patriotic groups) and which possibly do not result in life losses.

For every state to elaborate its military strategy in the cyber era, it is a strenuous process. Deep rooted values and ideas that date back to the 19th century have to be conceptualized from scratch. For instance, how powerful the nation-state is so as to assert its sovereignty in the cyber era? Since its monopoly over the means of war is not anymore taken for granted, its longevity in the cyber era is debatable. What does constitute an act of war in cyberspace? In the contemporary reality, networks, even civil or military, should be considered centres of gravity of equal value to physical installations. A well-orchestrated digital attack against them could be an act of war. Who can launch cyber attacks? The comparably low cost for waging digital attacks and the anonymity that reigns to cyberspace enable everyone willing to cause harm. Perpetrators of the attacks can vary amongst terrorist groups, patriotic hackers, criminal groups or even some juveniles eager to gain just the admiration of their peers. In this context, what is the role for military organisations? In the cyber era the border lines between civil and military or private and public seem to become continuously more oblique. The degree to which the private, the public and the military sectors of the states succeed in exchanging information about cyber incidents will finally define their cyber security and resilience. To put it differently, the security manager in charge of the vigilance of the network of his company is as crucial for the cyber security of the state as does an army officer responsible for the security of his or her regiment. In the cyber era, everyone could be a wannabe cyber warrior. For that reason, military organisations should reform their professional model.

In the cyber era, no matter how profound the changes are, the strategy, in its essence, remains always the guiding road among ends, means and ways. As Gray argues, strategy constitutes the bridge between two different sides: on one side lays the military effect while on the opposite one there is the political effect (2010). Thus, strategy «turns one currency

– military (or economic, or diplomatic) power – into quite another (desired political consequences)» (2010, p.7). This "currency" converting function of the strategy will continue to be valid even in the era of digital attacks and of networks prevalence over every social function. Nevertheless, it is high time that states revised their grand strategy for securing their citizens. Thus, they need to show agility and dexterity for quickly adapting to the abruptly altering political map of the new century. Within a "more complex and volatile environment" (Hoskins and O'Loughlin, 2009, p.33) as a result of the reforming effects of the Internet, states do not any more possess the centre of the political system (Dartnell, 2009). Military strategy in cyber era needs to be creative, inspiring and to alienate itself away from all those forces that make it remaining stuck in anachronistic *modi operandi*.

❀❀❀

ENDNOTES

1 The First World War was the war of the first industrial revolution and of nationalized masses while the following World War was characterized by the second industrial revolution and was the first massively mechanized war.

2 Clausewitz was the only one among the three writers who had participated in some of the bloodiest battlefields of the 19th century as those of Napoleonic warfare had been.

3 The passion is related with people and concerns the sentiments of violence, hatred and enmity, while the chance refers to the play of chance and probabilities which are mainly the commander's concern. Finally, the rationality is associated with the government. As Gray pinpoints, Clausewitz does not put barriers among those three aspects. Instead, they «[...] interpenetrate each other and cannot have fixed relationships» (Gray, 1999, p.92).

4 Western societies show a clear aversion towards bloodshed and «[...] a cumulatively radical decline in the willingness to [...] resort to force» (Gray, 1999, p.191).

5 This is what Gray describes as the failure of partial theory to become general theory (Gray 1999, p.125).

6 Arquilla and Ronfeldt share the same point of view and reiterate that: «[...] Institutions can be defeated by networks. It may take networks to counter networks. The future may belong to whoever masters the network form» (1997, p. 40).

7 The term "cyberwarfare" that is always more frequent in newspapers headlines or even in some scientific journals, is not considered to be an appropriate one as it defies the basic idea of war theory that the nature of war remains intact by the elapse of time. Other terms such as war or conflict in the cyberspace are more accurate.

8 The following extract is taken from a group on Facebook and it expresses in the clearest way the core ideology of virtual

societies: «Sit comfortably in your desk chair, your sofa, your bed or even your local café and follow our game while you are updating your Twitter, chatting on your Skype, spying your friends on Facebook, or just searching something on Google […]».

9 Moreover, Stiglitz, in his recent published article, accentuates the considerable changes in world politics as «Globalization and modern technology now enables social movements to transcend borders as rapidly as ideas can» (2011).

10 Eric Sterner gives a concise review of cyber incidents in critical infrastructures and in military sector as well (SSI Quarterly, 2011, pp. 62-64).

11 Cyber attacks against Estonia were first launched on the 27th of April, 2007, after the government's decision to remove a statue of Stalin from the central square of Tallinn, and stopped on the 18th of May, 2007. In Georgia cyber attacks took place from the 8th until the 28th of August, 2008, and they were part of the Russian's military operations against Georgia. For further analysis see Tikk, E., Kaska, K., and Vihul, L. (2010) International Cyber Incidents, Legal Considerations, CCDCOE, Tallinn.

12 The Centre for Strategic and International Studies (CSIS) keeps and regularly updates an inventory of cyber incidents since 2006: <http://csis.org/files/publication/110309_Significant_Cyber_Incidents_Since_2006.pdf> [Last access: 14 October 2011].

13 It is not yet officially admitted whether this incident was an intended attack or an accidental infection. For more details: <http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/> [Last access: 14 October 2011].

❀ ❀ ❀

BIBLIOGRAFY OF REFERENCES CITED

Arquilla, J., Ronfeldt, D. (2001) Networks and Netwars: The Future of Terror, Crime and Militancy (California: RAND).

Arquilla, J., Ronfeldt, D. (1997) In Athena's Camp: Preparing for Conflict in the Information Age (Washington, D.C.: RAND).

Blank, S. (2008) Web War I: Is Europe's First Information War a New Kind of War?, Comparative Strategy, 27: 3, pp.227-247.

Boot, M. (2006) War Made New. Technology, Warfare, and the Course of History. 1500 to Today (Penguin Group, New York).

Sterner, E. (2011) Retaliatory Deterrence in Cyberspace, Strategic Studies Institute Quarterly, Spring Issue, vol.5,
no.1, pp. 62-64.

Castells, M. (2001) The Internet Galaxy. Reflections on the Internet, Business and

Society, (UK: Oxford University Press).

Clausewitz, C. (1976) On War, trans. M. Howard and P. Paret (Princeton, NJ).

Dartnell, M. (2009) Web Activism as an element of global security, in A., Karatzogianni (ed), Cyber Conflict and Global Politics, pp.61-78.

Geers, K. (2010) The Challenge of Cyber Attack Deterrence, Computer Law and Security Review, vol. 26, no. 3, May, pp.249-340.

Gray, S. C. (2010) The Strategy Bridge: Theory for practice (UK: Oxford University Press).

Gray, S. C. (1999) Modern Strategy (UK: Oxford University Press).

Hoskins, A., O'Loughlin, B. (2009) The Internet as a Weapon of War?, in A., Karatzogianni (ed), Cyber Conflict and Global Politics, pp.31-46.

Karatzogianni, A. (2010) Power, Resistance and Conflict in the Contemporary World (UK: Routledge).

Karatzogianni, A. (2006) Broadening the New Security Agenda, Journal of Cyber Conflict Studies, vol. 1, no. 1, pp.12-21.

Liaropoulos, A. (2011) Cyber-Security and the Law of War: The Legal and Ethical Aspects of Cyber-Conflict, Political Studies Association, [on line]. Available at: <http://www.gpsg.org.uk/workingpapers.html> [Last access: 14 October 2011].

Libicki, M.C. (2009) Cyberdeterrence and Cyberwar (California: RAND).

Milevski, L. (2011) Stuxnet and Strategy: A Space Operation in Cyberspace, Joint Force Quarterly, [on line]. Available at: <http://www.ndu.edu/press/stuxnet-and-strategy.html> [Last access: 14 October 2011].

National Intelligence Council (NIC) (2008) Global Trends 2025: A transformed World, [on line]. Available at: <www.dni.gov/nic/NIC_2025_project.html > [Last access: 14 October 2011].

Nugent, H.J., Raisinghani, M. (2008) Bits and Bytes vs. Bullets and Bombs: A New Form of Warfare, in L., Janczewski, A., Colarik (eds), Cyber Warfare and Cyber Terrorism, Information Science Reference, pp.35-42 (New York: Hershey).

Nye, J. (2010) Cyber Power, Belfer Center for Science and International Affairs, [on line]. Available at: <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf> [Last access: 14 October 2011].

Ottis, R. (2010) "From Pitchforks to Laptops:

Volunteers in Cyber Conflicts", Conference on Cyber Conflict 2010, Tallinn: Cooperative Cyber Defence Centre of Excellence, pp.97-109.

Owen, R.S. (2008) Infrastructures of Cyber Warfare, in L., Janczewski, A., Colarik (eds), Cyber Warfare and Cyber Terrorism, Information Science Reference, pp.35-42 (New York: Hershey).

Rattray, J.G. (2001) Strategic Warfare in Cyberspace (London: MIT Press).

Rogers, C.J. (ed) (1995) The Military Revolution Debate: Readings On The Military Transformation Of Early Modern Europe (USA: Westview Press).

Sheldon, J.B. (2011) Deciphering Cyber Power. Strategic Purpose in Peace and War, Strategic Studies Quarterly, [on line]. Available at: <http://www.au.af.mil/au/ssq/2011/summer/Sheldon.pdf> [Last access: 14 October 2011].

Slaughter, A.M. (2011) Problems will be global – And solutions will be, too, Foreign Policy, [on line]. Available at: <http://www.foreignpolicy.com/articles/2011/08/15/problems_will_be_global_and_solutions_will_be_too> [Last access: 14 October 2011].

Slaughter, A.M. (2004) A New World Order (New Jersey: Princeton University Press).

Stiglitz, J. (2001) The Globalization of Protest, Project Syndicate, [on line]. Available at: <http://www.project-syndicate.org/commentary/stiglitz144/English> [Last access: 14 October 2011].

Sun Tzu (1994) The Art of War, trans. R.D. Sawyer (Boulder, Colo.).

The Economist (2011a) [on line] Available at: <http://www.economist.com/node/21531109> [Last access: 14 October 2011].

Zetter, K. (2011) How Digital Detectives Deciphered Stuxnet, Wired, [on line] Available at: <http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/> [Last access: 14 October 2011].

SOCIAL NETWORKING AS A PARADIGM SHIFT IN TACTICAL INTELLIGENCE COLLECTION

Joseph Fitsanakis
Coordinator, Intelligence and Security Studies program, King College, USA.
Senior Editor, intelNews.org.

Micah-Sage Bolden
Communications Director, Security and Intelligence Studies Group, King College, USA.

ABSTRACT

Recent events occurring in the Mediterranean region form the geopolitical backdrop to what may be seen as the cutting edge in tactical intelligence collection — namely open-source information gathered from online social networking media. Facebook, Twitter, YouTube, and a host of other social networking platforms are increasingly viewed by intelligence agencies as invaluable sources of information acquisition. In this paper, we consider three recent case studies that occurred in the Mediterranean region, which we believe highlight the intelligence function of social networking: events associated with the Arab Spring; NATO's operations in the context of the 2011 Libyan civil war; and Israel's sabotage of the 2011 "Welcome to Palestine Air Flotilla" initiative. Examined collectively, these case studies underscore the powerful — yet inevitably controversial — ability of social networking to: (a) reflect opinion trends and channel mass political action; (b) provide actionable tactical intelligence; and (c) serve as a model for resourceful, economical, and highly effective security operations against targeted groups.

1. THE EMERGENCE OF SOCIAL NETWORKING

The emergence of interconnected computer networks arguably represents the biggest post-Cold War paradigm shift in tactical intelligence collection. Its broad and often unpredictable consequences include information overload (MacDonald & Oettinger, 2006), namely the over-exposure of intelligence collectors to information, and — more recently — the so-called "Google effect", which has raised the «threshold for producing [...] genuinely secret intelligence» due to «so much information being readily available online» (Pepper, 2010). But the cutting edge of this broad transformation is undoubtedly embodied in the rapidly escalating phenomenon of social networking. The term encompasses all online applications that spontaneously and interactively connect Internet users, through searchable directories (Facebook, LinkedIn), text- or audio-based blogs (WordPress, BlogTalkRadio), microblogs (Twitter, Tumblr), video-sharing (YouTube,

DailyMotion), collaborative tools (GoogleDocs), and wikis (Twiki, SharePoint) (Rohan, 2011).

After the demise of MySpace, around 2007, the realm of social networking has been dominated by Facebook and — to a lesser extent — Twitter, both of which have successfully utilized globally emerging mobile technologies (Boyd & Ellison, 2007; Nagesh, 2011; Grossman, 2010; Picard, 2011). Facebook, in particular, introduced numerous innovations now considered mainstays of social networking, including the newsfeed, «perhaps the most important [...] feature of social networking» (Ostrow, 2010) and applications, which allowed for the personalization of profiles and the organization of online social activity (Boyd & Ellison, 2007). Observers suggest that Facebook shifted the focus of online activity from the individual to the network, to the extent that one's Facebook profile is now considered one's identity on the Web, a type of Internet passport (Ostrow, 2010; Grossman, 2010). Today it is estimated that four in five Internet users regularly utilize social media, while social networking is overtaking email as the preferred method of online communication among young people (Putnam et al., 2011; Lee, 2011).

2. INTELLIGENCE RESPONSES TO SOCIAL NETWORKING

As social networking spreads, it encompasses and mirrors a broad spectrum of social activity, to the extent that the latter can often be «directly observable from publicly available data» on the Internet (Matheny, 2011). This, in turn, has prompted varied responses by intelligence professionals (Ashford, 2009). On the counterintelligence side, observers point to an upward trend in incidents of espionage targeted at socially networked individuals holding sensitive positions in government and industry. Known operations on Facebook have been directed against North Atlantic Treaty Organization (NATO) troops, members of the Israel Defence Forces, and employees of Canada's Department of National Defence, to name only a few recent instances (Svantesson, 2009; Stricker, 2010; Pilieci, 2011). There is also considerable apprehension about the extent to which past activity on Facebook and other social networking sites could visually identify case officers deployed in field operations. In the words of Mick Keelty, former Australian Federal Police Commissioner, «how can you turn up at the Australian embassy in Jakarta and say that you're the trade commissioner for education when you've got a photograph [online] of your graduation from [Royal Military College] Duntroon in 2006 and an unexplained absence from the world in the interim years?» (ctd in Stilgherrian, 2011).

On the intelligence collection side, however, analysts appear to be gradually warming up to relatively secure and cost-effective methods of utilizing the "gold mine of intelligence that comes out of" social networking (Stilgherrian, 2011). In some cases, intelligence analysts are even utilizing Wiki- or Facebook-inspired models of online organization to build retrievable indexes of intelligence targets (Vogel, 2009; Connor, 2009). There are reported instances of law enforcement and intelligence agencies utilizing social

networks against individual targets (Chesler, 2011; Lynch, 2010). Primarily, however, intelligence agencies are interested in harnessing the ability of social networks to broadly reflect the political temper of large groups, as well as their power to incite effective political action by quickly building a critical mass of like-minded individuals.

Early examples that attracted the attention of intelligence analysts include the 2008 Facebook group “One Million Voices Against FARC”, which sparked demonstrations by an estimated one million people in over 40 countries, in opposition to the *Fuerzas Armadas Revolucionarias de Colombia* (Drapeau & Wells, 2009). A similar case was later reported in Moldova, where Twitter was used to channel popular discontent sparked by widespread allegations of vote fraud in the April 2009 parliamentary election (Morozov, 2009). This trend appeared to culminate in June of that year, when Twitter and other social networking sites were employed by protesters in Iran to kindle the so-called Green Revolution, following the highly disputed presidential election (Keller, 2010). Twitter quickly became an organizational battleground, as Iranian intelligence forces utilized the service to launch sabotage and psychological operations directed at the protesters (Carafano, 2009:4).

3. THE SIGNIFICANCE OF THE MEDITERRANEAN REGION

The United States Central Intelligence Agency (CIA) has admitted that the 2009 Green Revolution in Iran prompted it to initiate systematic monitoring of social networking media (Anon., 2011a). In the interim, the increasing utilization of social networking tools by drug cartels (Okeowo, 2010), militant groups (Anon., 2011b; Bright, 2011), and flash mobs — as in during the 2011 England riots (Serrao, 2011; Bright, 2011; Best, 2011; Sapsted, 2011) — has sustained intense interest by intelligence agencies in monitoring social networking activity. But it is recent developments in the Mediterranean region, notably in the context of the Arab Spring, that have captured the attention of intelligence planners in America, Europe, Israel, Russia, and elsewhere (Ferris-Rotman & Kalmykov, 2011; Anon., 2009; Anon., 2011b).

The Arab Spring, a multifaceted wave of popular protests and revolutions, can be traced to the October 2010 protest camp that was set up in Gdeim Izik, Western Sahara, to oppose the territory’s ongoing occupation by Morocco (García, 2011; Corbyn & Simanowitz, 2011). It eventually engulfed virtually the entire Arab world, resulting in the direct overthrow of three governments — in Tunisia, Egypt, and Libya — and the destabilization of several others, including in Yemen and Syria. These uprisings did not mark the first-ever instances of using social networking media to spark political protest in the Arab world; prior cases were reported in Egypt in as early as 2008 (Drapeau & Wells, 2009). But the astonishing degree to which online social networks reflected and channelled popular discontent during the Arab Spring «shocked [intelligence] officials into attention» (Banda, 2011).

Doug Naquin, who heads the Open Source Centre at the US Office of the Director of National Intelligence (ODNI), alleges that his analysts had essentially «predicted that social media in places like Egypt could be a game-changer and a threat to the regime» (Anon., 2011a). At the same time, according to Caryn Wagner, Undersecretary of the US Department of Homeland Security, the unprecedented wave of social network-based popular uprisings in the Arab world «prompted the US government to begin developing guidelines for culling intelligence from social media networks» (Banda, 2011).

Recent developments in the Mediterranean region have also demonstrated the critical link between online social networks and actionable intelligence, most notably during NATO's Operation UNIFIED PROTECTOR. The operation was intended to enforce United Nations Security Council resolutions 1970 and 1973, in the context of the 2011 Libyan civil war. However, although it authorized NATO to use aircraft, the UN mandate barred the Organization from deploying ground forces in the North African country. Therefore, during the eight-month engagement, and in the absence of physical ground forces, NATO systematically resorted to social networking media to gather actionable intelligence (Smith, 2011; Ackerman, 2011). It did so by utilizing open sources like Twitter to pinpoint targets for attack (Bradshaw & Blitz, 2011). NATO officials recognized information streaming from Twitter as "a source of tactical intelligence" (Ackerman, 2011), which provided a channel of strategic insight into enemy movement and public opinion on the ground. According to press reports, intelligence harnessed from social networking media was processed through NATO's "fusion centre", where it was combined with and corroborated against intelligence collected from both open and closed sources "ranging from unmanned aerial drones to television news channels" (Smith, 2011; Bradshaw & Blitz, 2011). During the operation, social media accounts unofficially connected to NATO, such as Twitter hash tag "SMS Nonsuch", siphoned intelligence tips by online users (Smith, 2011; Gabbatt, 2011). In some cases, NATO directly solicited online activists with the opposition National Transitional Council, encouraging them to act as «volunteer intelligence analysts [...] discuss[ing] satellite images, vessel tracking, and the latest gossip from their sources inside the country» (Smith, 2011). In short, by partially relying on open source-intelligence collection, including social networking media, NATO was able to weave a web of intelligence in Libya that included sources located outside traditional military or political channels.

A separate conflict in the Mediterranean region, that taking place between Israel and the Palestinians, has served as the geopolitical backdrop to yet another demonstration of the undeniable effectiveness of social networking media as a source of intelligence. The information blackout imposed by the Israeli government on the Occupied Territories has prompted Palestinian activists to resort to online social networking as a primary tool for affecting public opinion (Ward, 2009). Israel, which claims that «the Internet is a war zone between [it] and its enemies, including Hamas, Hezbollah, and Iranian groups» (Budeiri,

2009), has organized its own «social media unit, tasked with monitoring the various social networks in the Arab world» (Segev, 2011). The new unit is viewed by Israel's intelligence planners as a tool against the country's "delegitimization" in global public opinion (Graham, 2009; Shayshon, 2010), which it tries to combat through what its analysts call "the branding of the state of Israel in the world" (Vronsky, 2010). As part of this wider effort, the government of Israel has authorized a host of psychological operations utilizing social media, including the "Is.Real 2010" campaign, and launching an official Israel Defence Forces channel on YouTube (Kilroy, 2011; Ward, 2009). There are also reports that Israeli intelligence is using Facebook and other social networking sites to gather personal information about Palestinians and to recruit assets in the Gaza Strip. Veteran Israeli intelligence correspondent Ronen Bergman alleges that «Israel is using the personal information that is put in massive amounts on the Internet to identify the people who can maybe help Israel» (ctd. in Donnison, 2010).

A revealing case study that epitomizes Israel's systematic utilization of social networking media to gather intelligence was the disruption of the 2011 "Welcome to Palestine Air Flotilla" initiative. The campaign was organized by several European pro-Palestinian groups aiming to draw worldwide attention to the travel restrictions imposed by Israeli authorities on the Occupied Territories (Last, 2011). The plan was for between 600 and 1,000 activists from Belgium, Britain, France, Germany, Japan, Spain, Sweden, the Netherlands, and several other countries, to fly independently to Tel Aviv, before collectively congregating at Israeli-controlled crossings into the West Bank (Bahour, 2011; Lappin & Lazaroff, 2011). However, Israeli intelligence agencies were aware of the campaign, which was heavily promoted on Facebook, had monitored the participants' online activities on social networks, and had compiled extensive lists of their names (Last, 2011). Israeli authorities then communicated the lists' contents to European airline carriers, advising them that the identified passengers would be refused entry into Israel, and that it would be the carriers' responsibility to return stranded passengers to their destinations. Consequently, at least 200 "Air Flotilla" activists were turned away at check-in counters at airports in Paris, Geneva, Athens, and Rome (Flower, 2011; Lappin & Lazaroff, 2011). Upon landing in Tel Aviv, the 310 activists who managed to fly into the Ben-Gurion International Airport, which had been "heavily fortified" (Last, 2011), were immediately singled out and detained by police. Eventually, most of the activists were either placed on return flights to Europe or transported to Israeli jails before being deported (Anon., 2011c; Potalinski, 2011; Lappin & Lazaroff, 2011). The organizers of the initiative condemned the actions by the Israeli authorities as "provocative, blackmailing and illegal" (Last, 2011). They may well be justified; but while the legality of Israel's actions is debatable, the effect of the operation is undisputed: out of as many as 1,000 activists that were expected to enter the West Bank as part of the "Air Flotilla", perhaps fewer than a dozen managed to achieve their goal (Anon., 2011d; Knell, 2011).

Israel’s systematic monitoring of social networking activities allowed it to economically, resourcefully and effectively sabotage an extensive multinational campaign in support of the Palestinian cause. In the aftermath of that success for the Jewish state, defence officials in Tel Aviv vowed to continue to «closely follow organizer activities online» (Last, 2011).

4. FROM THE FIELD TO THE ANALYSIS DESK

There is clear evidence that Western intelligence agencies — particularly in the US — were monitoring social networking outlets up to several years before the case studies described above (Stokes, 2009). Moreover, dependable reports from America suggest that government agencies routinely rely on online social networks as sources of intelligence in both the military and civilian — federal and local — realms (Dinzeo, 2009; Anon., 2011a; Parascandola, 2011). But recent developments in the Mediterranean region, described above, have prompted more intelligence planners to recognize online social networks as “a great source” (Anon., 2011e), and appear to be speeding up the development of intelligence collection protocols relating to social networking sources (Banda, 2011). Their authors are already grappling with issues of reliability, as well as privacy, particularly in complying with already established distinctions between domestic and external intelligence (Dinzeo, 2009; Anon., 2011e). In the case of the United States, much of the government’s intelligence from social networks is collected by the Department of State, the Department of Homeland Security’s Social Networking/Media Capability unit, and the CIA’s Open Source Centre (OSC) (Mayfield, 2011; Various, 2010). The latter monitors «anything overseas that people can access and contribute to openly», including up to «5 million tweets a day» (Anon., 2011a). Despite the infancy stage of this new intelligence source, it reportedly often helps US intelligence agencies «build a picture sought by the highest levels at the White House», which often ends up in the *President’s Daily Brief* (Anon., 2011a).

The use of social networking in the Arab Spring has also triggered calls in the US for the development of automated analytics models focusing on topic trend analysis, online sentiment detection, and opinion mining (Waltzman, 2011). The latter are spearheaded by the Defence Advanced Research Projects Agency (DARPA) and the Intelligence Advanced Research Projects Activity (IARPA), whose Open Source Indicators (OSI) program is currently in the works (Weinberger, 2011; Matheny, 2011). The nature of OSI appears to be predictive, namely it is intended to forecast major events or upheavals, by fusing various early indicators drawn from publicly available data on social networks (Weinberger, 2011). These indicators will then be filtered through several modes of automated, continuous analysis in order to «anticipate and/or detect significant societal events, such as political crises, humanitarian crises, mass violence, riots, mass migrations, disease outbreaks, economic instability, resource shortages, and responses to natural disasters» (Matheny, 2011).

The US Department of Defence, on the other hand, which views «sites like Facebook and Twitter as both a resource and a weapon in future conflicts» (Streitfeld, 2011), is developing offensive methods of harnessing the intelligence aspect of social networking. These methods, which aim to proactively «influence Internet conversations and spread pro-American propaganda» (Fielding & Cobain, 2011), are based on the concept of "socialbots" — armies of fictitious socially networked profiles controlled by a central source (Goodin, 2011). In one recent case, the US Central Command (CENTCOM), which operates as Pentagon's rapid deployment task force in the Middle East and Central Asia, awarded California-based software developer Ntrepid a $2.76 million contract to create an "online persona management service" (Fielding & Cobain, 2011). The service will reportedly enable US military officers to generate and operate thousands of "induced identities", allowing them to "respond to emerging online conversations" on social networking websites "with any number of coordinated messages" (Fielding & Cobain, 2011). The contract was awarded under Operation EARNEST VOICE, a $200 million program developed as "a psychological warfare weapon" and «seen by senior US commanders as a vital counterterrorism and counter-radicalization program» (Fielding & Cobain, 2011).

5. CONCLUSION: THE MEDITERRANEAN REGION AS AN EXPERIMENTATION HOTBED IN INTELLIGENCE COLLECTION

The widening interface between online social networking and tactical intelligence collection is still in its infancy. Yet there is a major sense in which tactical intelligence collection may never be the same following the onset of social networking media. Moreover, events around the Mediterranean region appear to be driving and intensifying the preoccupation of several international intelligence agencies with online social networks. Events associated with the Arab Spring, particularly in Tunisia and Egypt, have prompted intelligence agencies to develop broad legal and methodological protocols of intelligence collection from social networks. They have also helped intensify and systematize efforts to mine and automate trend analysis on social networks, in an effort to forecast major social events. The experience of NATO in utilizing social media during the 2011 Libyan civil war, solidified the critical link between actionable intelligence and information collected from social networking sources. Finally, it is likely that the controversial Israeli operation that sabotaged the "Welcome to Palestine Air Flotilla" initiative last year, will serve as a textbook model of harnessing the power of social network channels to develop resourceful, economical and effective intelligence operations.

BIBLIOGRAFY OF REFERENCES CITED

Ackerman, S. (2011) NATO's newest bombing tool: Twitter, Wired, 10 June, available online at: http://www.wired.com/dangerroom/2011/06/natos-newest-bombing-tool-twitter/

Anonymous (2009) Israel uses Facebook to spy on Arabs and Muslims Al Arabiya, 09 November, available online at: http://www.alarabiya.net/articles/2009/11/09/90711.html

Anonymous (2011a) CIA analysts comb social media for trouble spots, The Associated Press, 4 November, available online at: http://www.npr.org/2011/11/04/142029141/cia-analysts-comb-social-media-for-trouble-spots

Anonymous (2011b) Facebook and other social media 'used for cyber-jihad', British Broadcasting Corporation, 12 July, available online at: http://www.bbc.co.uk/news/uk-politics-14126514

Anonymous (2011c) 120 foreign activists detained by Israel, USA Today, 10 July, available online at: http://www.usatoday.com/cleanprint/?unique=1322099661140

Anonymous (2011d) Israel uses Facebook to stymie 'flytilla', The Associated Press, 8 July, available online at: http://www.cbc.ca/news/world/story/2011/07/08/activist-palestine-fly-israel.html

Anonymous (2011e) Tweets tip off NATO on potential Libya air raids , Agence France Presse, 10 June, available online at: http://www.france24.com/en/20110610-tweets-tip-off-nato-potential-libya-air-raids#

Ashford, W. (2009) Social media is ruining spy industry, says NCC group, Computer Weekly, 06 July, available online at: http://www.computerweekly.com/Articles/2009/07/06/236776/social-media-is-ruining-spy-industry-says-ncc-group.htm

Bahour, S. (2011) Welcome to Palestine, if you can get in, The Guardian, 5 July, available online at: http://www.guardian.co.uk/commentisfree/2011/jul/05/welcome-to-palestine-israel

Banda, S. (2011) Homeland Security reviews social media guidelines, The Associated Press, 31 October, available online at: http://www.google.com/hostednews/ap/article/ALeqM5j2QncVujJYeKvVMAwzSqq5eSaSLA

Best, J. (2011) 'Twitter and BBM gave us riot intelligence; we decided against pulling plug': Met Police, Silicon.com, 16 August, available online at: http://www.silicon.com/management/public-sector/2011/08/16/twitter-and-bbm-gave-us-riot-intelligence-we-decided-against-pulling-plug-met-police-39747818/

Boyd, D. M., and Ellison, N. B. (2007) Social network sites: Definition, history, and scholarship, Journal of Computer-Mediated Communication, 13(1).

Bradshaw, T. and Blitz, J. (2011) NATO draws on Twitter for Libya strikes, The Washington Post, 15 June, available online at: http://www.washingtonpost.com/world/nato-draws-on-

twitter-for-libya-strikes/2011/06/15/AGLJpTWH_story.html

Bright, P. (2011) How the London riots showed us two sides of social networking, Ars Technica, 11 August, available online at: http://arstechnica.com/tech-policy/news/2011/08/the-two-sides-of-social-networking-on-display-in-the-london-riots.ars

Budeiri, A. (2009) Israel and foes in internet War, BBC, 15 June, available online at: http://news.bbc.co.uk/2/hi/middle_east/8079774.stm

Carafano, J.J. (2011) Mastering the art of Wiki: Understanding social networking and national security, Joint Forces Quarterly, 60, January, pp.73-78, available online at: http://www.ndu.edu/press/social-networking-national-security.html

Chesler, C. (2011) How cops are casing social networks for crooks, Popular Mechanics, 14 April, available online at: http://www.popularmechanics.com/technology/how-to/computer-security/how-cops-are-casing-social-networks-for-crooks

Connor, S. (2009) Terrorist Facebook: The new weapon against al-Qa'ida, The Independent, 19 August, available online at: http://www.independent.co.uk/news/world/politics/terrorist-facebook-ndash-the-new-weapon-against-alqaida-1774041.html

Corbyn, J., and Simanowitz, S. (2011) A new dawn: Western Sahara and the Arab Spring, The New Internationalist, 14 September, available online at: http://www.newint.org/features/web-exclusive/2011/09/14/western-sahara-independence-resistance/

Dinzeo, M. (2009) Are CIA and Pentagon your friends on Facebook?, Courthouse News Service, 3 December.

Donnison, J. (2010) Israel 'using Facebook to recruit Gaza collaborators', BBC, 5 April, available online at: http://news.bbc.co.uk/2/hi/8585775.stm

Drapeau, M., and Wells, L. (2009) Social software and national security: An initial net assessment, Centre for Technology and National Security Policy, National Defence University, Washington, DC, April.

Ferris-Rotman, A., and Kalmykov, A. (2011) KGB successor blamed in Russian site attacks Reuters, 05 December, available online at: http://www.itnews.com.au/News/282203,kgb-successor-blamed-in-russian-site-attacks.aspx

Fielding, N., and Cobain, I. (2011) Revealed: US spy operation that manipulates social media, The Guardian, 17 March, available online at: http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks

Flower, K. (2011) Israeli officials detain pro-Palestinian protesters at airport, Cable News Network, 8 July, available online at: http://articles.cnn.com/2011-07-08/world/israel.aerial.flotilla_1_pro-palestinian-ben-gurion-airport-micky-rosenfeld

Gabbatt, A. (2011) NATO, Twitter and air strikes in

Libya, The Guardian, 15 June, available online at: http://www.guardian.co.uk/help/insideguardian/2011/jun/15/nato-twitter-libya

García, B.L. (2011) Las barbas en remojo, El País, 07 February, available online at: http://www.elpais.com/articulo/opinion/barbas/remojo/elpepiopi/20110207elpepiopi_4/Tes

Goodin, D. (2011) Army of 'socialbots' steal gigabytes of Facebook user data, The Register, 1 November, available online at: http://www.theregister.co.uk/2011/11/01/facebook_infiltration_bots/

Graham, F. (2009) Gaza crisis spills onto the Web, BBC, 14 January, available online at: http://news.bbc.co.uk/2/hi/technology/7827293.stm

Grossman, L. (2010) The Connector: How Facebook's Mark Zuckerberg Rewired Our World and Changed the Way We Live (New York: Time Books).

Keller, J. (2010) Evaluating Iran's Twitter revolution, The Atlantic, 18 June, available online at: http://www.theatlantic.com/technology/archive/2010/06/evaluating-irans-twitter-revolution/58337/

Kilroy, E. (2011) Israeli foreign ministry launches social media campaign, Mondoweiss, 27 July, available online at: http://mondoweiss.net/2011/07/israeli-ministry-of-foreign-affairs-behind-docu-reality-series-is-real-2011.html

Knell, Y. (2011) Israel blocks pro-Palestinian 'flytilla' activists, British Broadcasting Corporation, 8 July, available online at: http://www.bbc.co.uk/news/world-middle-east-14084547

Lappin, Y., and Lazaroff, T. (2011) Pro-Palestinian activists plan week of protests in W. Bank, The Jerusalem Post, 10 July, available online at: http://www.jpost.com/LandedPages/PrintArticle.aspx?id=228627

Last, J. (2011) Israel blocks airborne protest, questions dozens, The Associated Press, 8 July, available online at: http://www.google.com/hostednews/ap/article/ALeqM5glrdg_c6lwx69-q_kxRP4tTyOq9Q

Lee, A. (2011) Email use plummets among teens, The Huffington Post, 8 February, available online at: http://www.huffingtonpost.com/2011/02/08/email-use-teens_n_820121.html

Lynch, J. (2010) New FOIA documents reveal DHS social media monitoring during Obama inauguration, The Electronic Frontier Foundation, Washington, DC, 13 October, available online at: https://www.eff.org/deeplinks/2010/10/new-foia-documents-reveal-dhs-social-media

MacDonald, M.S., and Oettinger, A.G. (2006) Managing intelligence technologies, Harvard International Review, 24(3), May, available online at: http://hir.harvard.edu/print/intelligence/information-overload

Matheny, J. (2011) Open source indicators (OSI) Program Broad Agency Announcement, United States Intelligence Advanced Research Projects Activity, Office of the Director of

National Intelligence, Washington, DC, 23 August, available online at: https://www.fbo.gov/notices/cf2e4528d4cbe25b31855a3aa3e1e7c9

Mayfield, T.D. (2011) A commander's strategy for social media, Joint Forces Quarterly, 60, pp.79-83.

Morozov, E. (2009) Moldova's Twitter revolution, Foreign Policy, 07 April, available online at: http://neteffect.foreignpolicy.com/posts/2009/04/07/moldovas_twitter_revolution

Nagesh, G. (2011) Facebook raises its game in Washington by forming its own PAC, The Hill, 26 September, available online at: http://thehill.com/homenews/campaign/184041-facebook-raises-its-game-in-washington-with-pac

Okeowo, A. (2010) To battle cartels, Mexico weighs Twitter crackdown, Time, 14 April, available online at: http://www.time.com/time/world/article/0,8599,1981607,00.html

Ostrow, A. (2010) A Look back at the last 5 Years in social media, Mashable, 20 July, available online at: http://mashable.com/2010/07/20/last-5-years-social-media/

Parascandola, R. (2011) NYPD forms new social media unit to mine Facebook and Twitter for mayhem, The New York Daily News, 10 August, available online at: http://www.nydailynews.com/ny_local/2011/08/10/2011-08-10_nypd_forms_new_social_media_unit_to_mine_facebook_and_twitter_for_mayhem.html

Pepper, D. (2010) Intelligence and security in the cyber age, Mountbatten Memorial Lecture, The Institution of Engineering and Technology, London, 10 November.

Picard, A. (2011) The history of Twitter, 140 characters at a time, The Globe and Mail, 20 March, available online at: http://www.theglobeandmail.com/news/technology/tech-news/the-history-of-twitter-140-characters-at-a-time/article1949299/

Pilieci, V. (2011) That Facebook 'friend' could be a foreign spy, The Ottawa Citizen, 15 November, available online at: http://www.vancouversun.com/story_print.html?id=5715652

Potalinski, E. (2011) Israel uses Facebook to blacklist pro-Palestinian protesters, ZDNet, 10 July, available online at: http://www.zdnet.com/blog/facebook/israel-uses-facebook-to-blacklist-pro-palestinian-protesters/2113

Putnam, T., Whitney, M., Sullivan, M., Posey, B., and Smith, G. (2011) The social commerce opportunity, MoonToast, New York, NY.

Rohan, R.J. (2011) Social Networking, Counterintelligence, and Cyber Counterintelligence, unpublished Master Thesis, Utica College, New York, NY, 18 June.

Sapsted, D. (2011) UK spy agency hunts for 'BlackBerry Riot' leaders, 11 August, available online at: http://www.thenational.ae/featured-content/channel-page/news/worldwide/uk-spy-agency-hunts-for-blackberry-riot-leaders

Segev, S. (2011) Israel watches social media, The

Winnipeg Free Press, 23 February, available online at: http://www.winnipegfreepress.com/opinion/westview/israel-watches-social-media-116719244.html

Serrao, S. (2011) Analysis of social media becomes critical, Security Debrief, Homeland Security Policy Institute, The George Washington University, Washington, DC, 25 July, available online at: http://securitydebrief.com/2011/07/25/analysis-of-social-media-becomes-critical/

Shayshon, E. (2010) The Gaza Flotilla: A collapse of Israel's political firewall, The Reut Institute, available online at: http://info.publicintelligence.net/ReutGazaFlotilla.pdf

Smith, G. (2011) How social media users are helping NATO fight Gadhafi in Libya, The Globe and Mail, 14 June, available online at: http://www.theglobeandmail.com/news/world/africa-mideast/how-social-media-users-are-helping-nato-fight-gadhafi-in-libya/article2060965/

Stilgherrian (2011) Has Facebook killed the undercover cop?, CSO, 25 August, available online at: http://www.cso.com.au/article/398581/has_facebook_killed_undercover_cop_/

Stokes, J. (2009) EFF's new lawsuit, and how the NSA is into social networking, Ars Technica, 23 July, available online at: http://arstechnica.com/tech-policy/news/2009/07/effs-new-lawsuit-and-how-the-nsa-is-into-social-networking.ars

Streitfeld, D. (2011) Pentagon seeks a few good social networkers, The New York Times, 2 August, available online at: http://bits.blogs.nytimes.com/2011/08/02/pentagon-seeks-social-networking-experts/?pagemode=print

Stricker, S. (2010) Die schöne Facebook-Freundin der Elitesoldaten, Der Spiegel , 17 May.

Svantesson, E. (2009) Utlandsstyrkan Utsatt För Luskande På Facebook, Dagens Nyheter, 18 April.

Various (2010) Privacy Compliance review of the 2010 Winter Olympics social media event monitoring initiative, United States Department of Homeland Security, Washington, DC, 23 August.

Vogel, S. (2009) For intelligence officers, A wiki way to connect dots, The Washington Post, 27 August, available online at: http://www.washingtonpost.com/wp-dyn/content/article/2009/08/26/AR2009082603606_pf.html

Vronsky, H. (2010) We'll take over the world? Ministry of foreign affairs allocates 100 million shekel for state branding, Israeli globes, Pulse Media, 17 August, available online at: http://pulsemedia.org/2010/08/23/we%E2%80%99ll-take-over-the-world-ministry-of-foreign-affairs-allocates-100-million-shekel-for-state-branding/

Waltzman, R. (2011) Social Media in Strategic Communication, United States Defence Advanced Research Projects Agency, Arlington, VA, 14 July, available online at: https://www.fbo.gov/utils/view?id=260a47e592fc4e0bb25207af167c13f3

Ward, W. (2009) Social media

and the Gaza conflict, Arab Media and Society, no. 7, winter, available online at: http://www.arabmediasociety.com/?article=701

Weinberger, S. (2011) The spy who Tweeted me: Intelligence community wants to monitor social media, Wired, 7 September, available online at: http://www.wired.com/dangerroom/2011/09/social-media-spies/

❀❀❀

DETERRENCE IN CYBERSPACE: IMPLICATIONS FOR NATIONAL SECURITY

Dr. Andrew Liaropoulos
Lecturer at the Department of International and European Studies, University of Piraeus, Greece.
Senior Analyst at the Research Institute for European and American Studies (RIEAS), Greece.

ABSTRACT

Security experts argue that cyberspace has added a new strategic environment that requires new approaches to defence and thereby deterrence. The hard reality of cyber-attacks, which can be asymmetric and non-attributable, force states to reconsider their deterrence policy. Security experts need to untie the Gordian knot of cyber-deterrence. Questioning whether states can deter state-executed cyber-attacks against their critical infrastructure and whether that can be achieved by denial or punishment, is the task of this essay. The purpose is to demonstrate that the Cold War model of nuclear deterrence, which involves denial and punishment, seems dysfunctional in cyberspace.

1. INTRODUCTION

Over the past two decades, cyberspace has been one of the most thought-provoking terms in public life and political science. Cyberspace offers a variety of assets, threats and opportunities for state and non-state actors. In the globalized world of digital communications, the way governments, corporations and citizens act, has been radically transformed. The spread of information technologies has increased the volume and range of communication and thereby influenced the way key concepts like power, security and identity are defined (Betz & Stevens, 2011). In the so-called cyber domain, governments try to exercise sovereignty, protect their citizens and deter cyber-attacks. The latter, are one of the most critical security challenges that states face in cyberspace (Libicki, 2009). The purpose of this essay is to provide a conceptual framework for understanding how deterrence can be applied in cyberspace at the state level and examine how states can prevent attacks against their critical infrastructure.

The lack of an international treaty that would clearly define the use of force in cyberspace (Hughes, 2010; Liaropoulos 2011), operational difficulties in attributing cyber-attacks, as well as the asymmetric nature of such attacks, pose without a doubt great pressure on traditional deterrence theory (Sterner, 2011; Geers, 2011). As a preliminary to this discussion, however, some exegesis of the key concepts – cyberspace and cyber-conflict

– is required. This may seem as a semantic exercise, but semantics are important. The way words are understood defines expectations and expectations are vital in shaping action. In a latter phase, we will explore recent cases of cyber-conflict, analyze the complexities of cyber-deterrence and offer some policy recommendations.

2. SECURITY IN CYBERSPACE

Over the years, many different definitions have evolved for cyberspace. Cyberspace refers to the fusion of all communication networks, databases and information sources into a global virtual system and should not be confused with the Internet. Cyberspace is composed of three layers. The first one is the physical layer that consists of electrical energy, integrated circuits, communications infrastructure, fibre optics, transmitters and receivers. The second layer is the software, meaning the computer programmes that process information. The last and least concrete layer is that of data (Tabansky, 2011, p.77).

Over the last years, state and non-state actors have chosen cyberspace as a new battlefield, where conflict is (in)directly carried out. Cyber-conflict is defined as cyberspace-based attacks on critical information infrastructures (transportation, power, communications and financial infrastructures) upon which modern societies increasingly depend. Cyber-conflict involves the conduct of large scale, politically motivated conflict to disrupt digital systems, networks and infrastructures (Carr, 2010).

Cyber-attacks come in many different forms. The cyber-conflict battlefield is comprised of many components that include the Internet and all things that connect a computer to the Internet. This would include: web servers, enterprise information systems, client server systems, communication links, network equipment, and the computers in businesses and homes. The terrain also encompasses information systems like electrical grids, telecommunication systems, and various corporate and military robotics systems. Attacks on computer networks that involve power plants, water supply stations, communications hubs, and commercial infrastructure facilities are high on the security agenda. A few examples of cyber-conflicts vividly illustrate the challenges that network societies face.

In April 2007, the Estonian government's decision to move a Soviet-era war memorial triggered a cyber-conflict in the form of a three-week wave of distributed denial-of-service (DDOS) attacks that crippled the country's information technology infrastructure (Blank, 2008). In particular, the cyber-attacks temporarily disrupted the Estonian communications networks, by targeting the government, newspapers, mobile phones, emergency response systems and commercial banks. In addition, the offices of the president, prime minister, parliament, and the foreign ministry, were also attacked. Although the cyber-attacks cannot be attributed to a specific actor, it is widely believed in Estonia that Moscow was behind these attacks. Russia denied these accusations and claimed that the attacks came from cyber-patriots (Crosston, 2011).

Regardless of the true identity of the attacker, the important issue is that the inability to trace the origin of the attack (the attribution problem) hinders any attempt of retaliation (Clark & Landau, 2011).

Likewise, during the conflict that broke out in August 2008 between Russia and Georgia over South Ossetia, cyber-attacks were launched against Georgian governmental websites (Korns & Kastenberg, 2009). As with the Estonian case, there is no proof of who was behind the attacks. Georgia accused Russia, claiming that the route traffic pointed to the Russian Business Network (RBN). The Georgian case clearly shows that cyber-attacks that take place in a borderless world, where the traditional law of armed conflict cannot be applied, might be a very handy strategy when states choose to exercise coercive diplomacy. The cyber option seems to be a very attractive and less costly one, compared to the use of traditional military means.

Cyber-attacks can take many forms and the examples of Ghost Net and the Google hacking are indicative of the above. Both incidents have been related to China and raise many questions regarding the way the victims could respond. Ghost Net was a massive cyber-espionage operation that was discovered by the Information Warfare Monitor in March 2009. The operation used malware and attacked non-governmental organizations and embassies working on Tibetan issues, in 103 countries. In early January 2010, Google announced that a computer attack originating from China had penetrated its corporate infrastructure and stolen information from its computers, most likely source code. The attacks also targeted Gmail accounts of some human-rights activists and infiltrated the networks of 33 companies (Thomas, 2010; Morozov, 2011). The borderless and complex nature of cyberspace might explain why Beijing regards Google as an element of US power and social networks as a threat to national security (Klimburg, 2011).

The latest known cyber-attack is Stuxnet worm. Stuxnet is a malicious software (malware) that was designed specifically to strike the Iranian nuclear facility at Natanz. It has affected more than 60.000 computer systems, more than half of them in Iran. The value of Stuxnet lays not so much on its technical characteristics, but on the political and strategic context, within which it operated (Farwell & Rohozinski, 2011, p.24). The scenario of launching an air strike to stop or slow down Iran's nuclear programme is still troubling the international community. The outcome of such an operation would be doubtful and the risks for the regional and global security, potentially disastrous. An Israeli or US preventive air strike on Iranian nuclear facilities would most probably start a conflict in the Middle East and would be unlikely to prevent the eventual acquisition of nuclear weapons by Iran (Farwell & Rohozinski, 2011, p.28).

The above brief overview of some recent cyber-conflicts, clearly illustrates the complex nature of cyberspace and how hard it is to apply traditional deterrence models in the cyber-domain. Not only it is difficult to determine the true identity of a cyber-attacker, furthermore the true motives of the attack, but cyberspace seems to favour offense over defence. In addition, cyber-

attackers can easily use inexpensive and off the shelf technologies in order to identify a vulnerability in the system, whereas cyber-defenders must protect the entire critical infrastructure and keep up to date with new technological developments. This asymmetric characteristic of cyber-conflicts raises the cost of defence (Tabansky, 2011, p.88).

3. CYBER-DETERRENCE: UNTYING THE GORDIAN KNOT

Deterrence has been approached by various disciplines: political science, strategic studies, psychology, economics and game theory. Deterrence is defined as the actions taken to convince an enemy not to proceed with a specific action, by threatening it with punishment or failure (Shelling, 1967; Jervis et al., 1985). Deterrence theory comprises two strategies: denial and punishment. The basic requirements in order to exercise a deterrence strategy are capability and credibility (Geers, 2011, p.111). The question that troubles the global security community is whether deterrence – that has been successfully exercised in the conventional and nuclear domain – can also be applied in the cyber domain (Solomon, 2011; Sterner 2011). Deterrence theory is a product of the Cold War and a concept that was developed to prevent a nuclear war. Cyberspace poses a number of challenges for deterrence.

Deterrence by denial means persuading the enemy not to attack, by convincing it that its attack will be defeated and that it will not succeed in its objectives. Deterrence by denial is the strategy where the potential attacker is prevented from using its weapons. Whereas in the case of nuclear weapons it is not only difficult to acquire the necessary material and know-how to develop a nuclear weapons program, in the case of cyber-attacks, the relevant tools and techniques are easily assessable and rather inexpensive. A nuclear weapons program is practically very difficult to hide, but the same does not apply in the case of cyber-capabilities. Furthermore, it is also possible to outsource the creation of malicious code to a criminal party (Geers, 2011, p.114).

The concept of deterrence by denial that characterizes the Non-Proliferation Treaty (NPT) is absent in cyberspace. Establishing a similar international regime, in order to ban the development and use of cyber-weapons, is easier said than done. Most of the technology that is associated with cyber-attacks is dual-use technology that we use in our everyday life. Therefore, a cyber-proliferation treaty would be very difficult to sign and enforce.

A key concept of deterrence is credibility. The potential attacker must believe that the threat of retaliation is real (Sterner, 2011). But how real is the threat or, rather, how disruptive can cyber-threat be? Unless cyber-attacks pose a credible threat and raise the question of survival, deterrence cannot operate effectively. Cyber-attacks are disruptive and can cause great financial cost, but at the same time they do not cause any harm or human casualties. It has been argued that the success of deterrence in the nuclear era originates from the strong memory of the dropping of the atomic

bombs in Hiroshima and Nagasaki. The world has not experienced a similar cyber-bomb. A global cyber-war would probably alter the perception on the disruptive and 'destructive' effects of cyber-conflicts.

When deterrence by denial fails, the last option is deterrence by punishment. In this case two problems occur, regarding deterrence in cyberspace: attribution and credibility (Geers, 2011, p.118). To begin with, in order for punishment to be a vital option, the attacker has to be successfully identified. A major advantage of cyberspace is that it offers its users anonymity. Given the difficulty of assigning attribution, how is it possible for deterrence to work? Even in the case where a cyber-attack is precisely and timely attributed, deterrence is still weak. Even if retaliation is justified, it is still unclear whether retaliation should be (only) in kind or also involve conventional weapons. In both cases, it is difficult to assess the collateral damage of a cyber counter-strike (Liaropoulos, 2011). Nuclear deterrence assumed a rather large degree of collateral damage as acceptable. Could we argue the same for cyber-deterrence? This uncertainty obviously limits the utility of deterrence, since a leader will hesitate to authorize cyber counter-strikes.

Untying the Gordian knot is not an easy task. Some scholars argue that deterrence in cyberspace should depend less on retaliation and more on enhancing the protection of one's network systems. Others estimate that retaliation from a potential cyber-attack should not limit to cyberspace, but instead should also include military deterrence.

4. CONCLUSION

To conclude, the Cold War model of nuclear deterrence seems impracticable in the cyber domain, at least at this point. Given the nature of cyberspace, it is possible to attack remotely critical state infrastructures with little risk to the attacker. As stated above, states have two options: denial and punishment. Denial is problematic, since it is relatively easy for potential cyber-attackers to acquire the necessary know-how and technology. Adding to that, the absence of an international treaty on cyberspace as well as the deficiency of an inspection mechanism further complicates deterrence policies. Deterrence by punishment is also weak because of the attribution problem.

Recent cyber-conflicts demonstrate the security implications of cyber-attacks for states and networked societies. Raising awareness about the need to develop capabilities, an international legal framework and strategies to address deterrence in cyberspace is imperative (Tikk, 2011). There are useful lessons to be learned from taking a broader historical and conceptual look in deterrence theory. In parallel with the nuclear era and the concept of Mutually Assured Destruction (MAD), the information era needs to form an equivalent Cyber MAD policy.

ENDNOTES

1 The prefix cyber actually comes from the Greek verb kyverno (κυβερνώ), which means to steer or govern. Cyber as a prefix refers to electronic and computer-based technology. In recent years the term cyber has been used to describe almost anything that has to do with networks and computers.

2 Note that due to the unique nature of cyberspace, it is very often difficult to discern between various types of cyber-attacks (cyber-war, cyber-terrorism, cyber-espionage, cyber-vandalism, hacktivism, etc.).

3 Note that over thirty countries have officially created cyber units in their militaries. The UK announced the creation of the Office of Cyber-Security (OCS) of the Cabinet Office and the Cyber-Security Operations Centre (CSOC) in 2009, France created the Agency for National Information Security (ANSSI) in 2009 and the US created a Cyber Command in 2010.

BIBLIOGRAFY OF REFERENCES CITED

Betz, D.J., Stevens, T. (2011) Cyberspace and the State. Toward a Strategy for Cyber-Power, Adelphi Paper 424 (Oxon: Routlegde, IISS).

Blank, S. (2008) Web War I: Is Europe's First Information War a New Kind of War?, Comparative Strategy, 27(3), pp.227-247.

Carr, J. (2010) Inside Cyber Warfare (Beijing: O'Reilly).

Clark, D., Landau, S. (2011) Untangling Attribution, Harvard National Security Journal, 2.

Crosston, M. (2011) World Gone Cyber MAD. How Mutually Assured Debilitation is the best hope for cyber deterrence, Strategic Studies Quarterly, 5(1), pp.100-116.

Farwell, J., Rohozinski, R. (2011) Stuxnet and the future of Cyber War, Survival, 53(1), pp.23-40.

Geers, K. (2011) Strategic Cyber Security (Estonia: NATO Cooperative Cyber Defence Centre of Excellence).

Hughes, R. (2010) A Treaty for Cyberspace, International Affairs, 86(2), pp.523-541.

Jervis, R. et al. (1985) Psychology and Deterrence (Baltimore: Johns Hopkins University Press).

Klimburg, A. (2011) Mobilizing Cyber Power, Survival, 53(1), pp.41-60.

Korns, S., Kastenberg, J. (2009) Georgia's Cyber Left Hook, Parameters, 38(4), pp.60-76.

Liaropoulos, A. (2011) War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory, in J. Ryan (ed), Leading Issues in Information Warfare & Security Research, Vol.1, pp.118-130 (Reading: Academic Publishing International Ltd).

Libicki, M.C. (2009) Cyberdeterrence & Cyberwar (Santa Monica, CA: RAND).

Morozov, E. (2011) The Net Delusion. The Dark Side of Internet Freedom, Public Affairs, New York.

Schelling, T. (1967) Arms and Influence (New Haven: Yale University Press)

Solomon, J. (2011) Cyberdeterrence Between Nation-States. Plausible Strategy or a Pipe Dream?, Strategic Studies Quarterly, 5(1), pp.1-25.

Sterner, E. (2011) Retaliatory Deterrence in Cyberspace, Strategic Studies Quarterly, 5(1), pp.62-80.

Tabansky, L. (2011), Basic Concepts in Cyber Warfare, Military and Strategic Affairs, 3(1), pp.75-92.

Thomas, T. (2010) Google Confronts China's Three Warfares, Parameters, (Summer), pp.101-113.

Tikk, E. (2011) Ten Rules for Cybersecurity, Survival, 53(3), pp.119-132.

❀❀❀

INTELLIGENCE STUDIES IN THE MEDITERRANEAN REGION

THE DEVELOPMENT OF INTELLIGENCE STUDIES IN FRANCE

Eric Denécé
PhD in Political Science, Director of the Centre Français de Recherche sur le Renseignement (CF2R) (denece@cf2r.org).

Gérald Arboit
PhD in History, Director of Research at the CF2R (arboit@cf2r.org).

❀❀❀

ABSTRACT

From the mid-1990s onwards, the French academic world has expressed a new and significant interest for intelligence. Initially, the latter is linked to the emergence of information society and the realization of the new worldwide economic competition that led, in the first place, economic players to integrate intelligence in their management processes. In order to respond to their new need of specialists, management universities and business schools have developed numerous business intelligence diplomas and other specialized training modules. Simultaneously, researches and publications on the subject have multiplied. At the same time, international relations' evolutions have led political players and public opinion to further realize the role of intelligence in national security. This sense has particularly been reinforced since 9/11 attacks. Jihadist terrorism has thus also been an acceleration factor of the renewed interest for intelligence, hence hitting historians, political scientists and journalists. Thereby, in less than two decades, French studies on intelligence that used to be more than low-key, have dramatically expanded around three main disciplines (management, history, and political science). It translated into numerous works and studies, academic degrees and the creation of first specialized research centre. Thus, it took shape a veritable surge of acknowledging intelligence, a discipline that French elites traditionally lacked of interest for. This article gives an overview over research on intelligence in France and its perspectives for the years to come.

❀❀❀

1. INTRODUCTION

Since the mid 1990s, interest in intelligence studies has grown in France, resulting in a surge of publications, seminars and training sessions on the theme. It is tempting to see in this surge the birth of a "French School of Intelligence Studies". But such a school of thought, if it even exists, is still in its infancy.

Nevertheless, there is a growing awareness of the importance of intelligence as a subject for study, signalling a major shift in the French mentality. This change comes on the heels of the geopolitical upheavals of the post-Cold War era which have made intelligence an essential instrument for an understanding of the new geopolitical landscape and consequently for scoping future threats. France, like other world powers, cannot afford to overlook such a transformation.

Those seeking to promote this sea change in the French

psyche have had to overcome the inherent reticence of the French people and their political leaders to a profession that is still viewed pejoratively, a phenomenon that explains the longstanding contempt shown towards it. Above all, the academic community has come to the study of this 'missing dimension'[1] in French research in a singularly fragmented fashion.

In the present paper we will endeavour to present a concise overview of the state of academic research on the subject in France and outline the conditions for the 'establishment' of a veritable French school of intelligence studies.

2. REASONS FOR THE LATE EMERGENCE OF INTELLIGENCE STUDIES IN FRANCE

There are historic and cultural reasons for the relative disinterest in intelligence studies in France. The absence of an intelligence culture in France is stunning given the role the country has played on the world stage for so long.

The absence of an intelligence culture in France

Intelligence work is a discipline that has never been held in high regard by politicians, the military, academics or economists.

One only has to visit a British or American library to see that France lags far behind its Anglo-American allies on the subject. For each book on intelligence published in France, there are at least ten others published in Britain and the United States. By comparison with these two countries, there is a distinct lack of an intelligence culture in France outside a small coterie of professionals and the few specialists on the subject. Former intelligence professionals, such as Admiral Lacoste, have noted bitterly that «*the intelligence culture of French leaders and of public opinion in France is famously lacking, a result of the vicissitudes of recent history and a reflection of specific characteristics of French society*».

Moreover, the Cartesian heritage has moulded the national psyche forging a tendency towards conceptualisation and abstraction, sometimes leading to a denial of reality, and a tendency to avoid the concrete resolution of problems. As General Mermet, former director of the DGSE (France's foreign intelligence service) has noted, «*we tend to, more than other people, overlook the facts and prefer ideas and subjective judgements to indisputable witness reports, whether it be in politics, where for example we were loath to believe in the changes afoot in Eastern Europe, or in military affairs, as shown by the attitude of the French Military High Command before 1939, despite the fact that the military had in its possession hard intelligence*».

French culture has always maintained a strict distinction between knowledge and intelligence; the former is deemed 'noble' and 'legitimate', the latter 'contemptible' and 'illegitimate'. To prove the point, in France, intelligence is absent from the writing of the greatest French military strategists. The conferences, classes and

[1] Christopher M. Andrew and David N. Dilks, eds., *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century*, MacMillan, London, 1984.

writings of Foch, Castex, Beaufre, Gallois or Poirier hardly mention the subject at all.

We are here faced with a dual problem:

– on one hand, the manner in which intelligence work has been performed in France is traditionally and also of necessity focused on domestic matters. The fight against the enemy within is one of the salient features of the French cultural model.

– on the other hand, since the "Dreyfus Affair" (1894), French intelligence services have been mistrusted by the political class. No one has forgotten the enduring impact that the Dreyfus Affair and its aftermath had on all of French society. Since that traumatic event, government leaders have consistently shackled the intelligence services instead of asking themselves how the services could be best put to use and how the performance of the services might be improved. This means that in France, more than in any other Western country, the work of the intelligence services is subservient to political fluctuations and electoral demands. When we bring Ben Barka (1965) and the *Rainbow Warrior* (1985) into the picture, it is easy to see how the political class have come to view and manage the intelligence services.

Thusly, intelligence work has negative connotations in the French psyche, and is unjustly connected with ideas of espionage, privacy violations and dirty tricks campaigns. On the other hand, counter-espionage, that is to say the effort made to protect French military, industrial and economic interests, is seen in a far better light. In France, all endeavours to defend the nation's interests are more easily accepted and implemented than are offensive measures.

The quasi-inexistence of academic research before the mid-1990s

Though perceptions of the profession were marshalled by an absence of a real intelligence culture in France, intelligence has hardly been ignored or derided. A diverse national intelligence production has long existed, and generally falls into two categories: memoirs and accounts written by former intelligence staff, and writings by journalists. Before the end of the 1980s, academic research on the subject was virtually inexistent.

The history of intelligence as a science in its own right was long the prerogative of foreign researchers. At university level, the Americans were the first to consider intelligence as an academic subject, before going on to establish *Intelligence Studies* courses in the 1980s. The British followed their lead in the 1990s, with several university chairs in intelligence established.

The recognition of intelligence as a subject of study in its own right is a recent phenomenon in contemporary French historiography. Until very recently, historians and political scientists had not considered intelligence as a significant parameter of statecraft, nor did they consider the intelligence services as significant stakeholders in state policy. It cannot be said that the subject was totally ignored, but it is fair to say that its importance was largely underestimated and hardly appears in social and human sciences, with even

military historians giving it short shrift.

It must be admitted that the secret nature of intelligence work did not facilitate the work of researchers and the issue of access to documents was for a long time a brake on historic research. When the rare academics sought to understand the contribution of intelligence to history, their lack of knowledge about the intelligence profession, and their incapability in identifying the characteristic signs of clandestine operations led them to declare that there was no source material on the subject. Before the 1990s, few university writers, compared to their Anglo-American counterparts, worked on the subject of intelligence.

3. THE EMERGENCE OF ACADEMIC INTELLIGENCE STUDIES IN THE 1990s

The emergence of intelligence studies in the world of French academia is firstly a result of the emergence of the society of information and the growing awareness of the reality of global competition, obliging economic stakeholders to integrate intelligence into their management processes. In order to respond to their new demand for specialists, business universities and schools at the beginning of the 1990s began to provide degree courses or other specialised post-graduate courses on 'business intelligence', to instruct economic players on the management of information and disinformation. In parallel, research and publications increased on the subject.

The work performed by the Martre Commission on Competitiveness and Economic Security (Martre Report, 1994) led to a growing awareness of new market entry strategies and the new realities of global competition.

In France, a dynamic and conflictual approach to international commerce and trade has emerged only recently. Elsewhere, the major international powers all understood that to guarantee peace, scope out emerging threats and emerge victorious from global economic rivalries, effective services, drawing from a culture of intelligence disseminated throughout the administration, business and civil society, were key. Though such awareness was slow to arrive in France, at least a demand for corporate information processing specialists had begun.

The second factor that explains the new interest in intelligence is terrorism, in particular the attacks of September 11, 2001. These attacks made French politicians and the general public in France more aware of the role that intelligence plays in national security. Intelligence was rediscovered as an essential information and decision-making instrument for political leaders with regard to foreign policy, defence and domestic security, and as a means of action.

The emergence of education and courses dedicated to intelligence

At the beginning of the 1990s, in response to the demand for specialists, universities and business schools established degree courses and specialised post-graduate courses on business intelligence, to initiate students and employees to the practices of intelligence

as applied to the business world.

In 1995, upon the initiative of Admiral Pierre Lacoste, former director of the DGSE, the CESD *(Centre d'études scientifiques de la Défense)* of the University of Marne-la-Vallée was established. The aim of the CESD is to teach, promote study and research and act as a factory for ideas, with research covering the newly-widened scope of defence and security issues in contemporary society.

In parallel, the University of Marne-la-Vallée established a Master degree course in information and security that covers the work of the intelligence services and intelligence culture in general. Two Master courses in business intelligence and security engineering were also set up to cover a comprehensive range of intelligence issues.

In 1997, the former director of the EIREL (Inter-service School for Intelligence and Linguistic Skills) in Strasbourg, General Jean Pichot-Duclos, and the former leader of NAPAP (French maoïsts), Christian Harbulot, set up the *École de guerre économique* (School of Economic Warfare - EGE). This unique post-graduate academy is supported by the Paris-based ESLSCA School of Business, and aims to fill in the gap in skills training for French business managers, namely the fact that the notion of information warfare is absent from the strategic planning of corporations, administrations and local authorities.

In addition, intelligence has been gradually introduced into the programs of ENA (French National School of Administration), allowing future senior civil servants to learn about the field. One of the missions of the IHEDN (French Institute of National Higher Defence Studies) is to provide in-depth information on the major issues connected with defence, and gives a course on the threats posed by foreign intelligence services, as well as a course on business intelligence. Finally, in 2006, the CID (French National Defence College) inaugurated a seminar on intelligence. Before this date, apart from some one-off conferences, there was no specialised seminar on the subject in the training of senior French military officers.

Also in 2006, the Masters program in International Affairs at Sciences Po Paris set up a seminar entitled "Clandestine Worlds: intelligence in the face of terrorism", led by Stephen Duso-Bauduin, Professor in Sociology of International Relations and Jean-Pierre Pochon, a former top-level officer of the French secret services having worked at the DCRG *(Direction centrale des renseignemetns généraux)*, the DST *(Direction de la surveillance du territoire)*, and the DGSE *(Direction générale de la sécurité extérieure)*. The seminar studies the role of intelligence in the combat against terrorism in different countries, with a primary focus on the United States and the French services, while also covering other major services worldwide.

The following year, the same institute established a new course called "Intelligence Policies", helmed by Philippe Hayez, former deputy director of intelligence at the DGSE. The seminar aims to enable students to better understand this 'special' form of public policy, its ties with other instruments of state (*corps diplomatiques*, military, police, judiciary)

and administrative decision-making.

There are now more than forty Masters courses specialised in competitive intelligence in French universities or business schools.

The multiplication of publications

Two factors emerge from an analysis of French and foreign publications in France since 1975. The first factor to be considered is the slow beginnings of intelligence studies as of 1991, followed by a surge as of 1998, with a peak reached in the wake of the 9/11 attacks. From a publishing point of view, it is clear that French production on the subject has grown considerably since 1995.

The second aspect illustrated by the statistics is a fall in the number of foreign books published to the benefit of French-authored books. French publications have been amplified by the surge in interest from publishers on intelligence since the attacks of 9/11. Several publishers launched collections on the subject, with L'Harmattan establishing the collection "*Culture du renseignement*" (Intelligence Culture) in 1999, followed in 2001 by the collection "*Renseignement et guerre secrete*" (Intelligence and Secret Warfare) by Lavauzelle, replaced three years later by "*Renseignement, histoire et géopolitique*" (Intelligence, history and geopolitics). In 2003, Ellipses also published a range of books on the subject.

The rise of academic research

Ten years after Great Britain, French academics began to conduct research on intelligence studies. There has been a high number of doctorates, degree papers, Masters dissertations and IEP diplomas on the subject. Analysis of that academic production reveals the areas of research explored and the progress of the ongoing 'establishment' of specifically a French intelligence school. On account of its multidisciplinary nature, intelligence studies encompass history, political science, law, economic science, information and communications sciences. Its areas of application cover all sectors of national security and economic/corporate security.

Being it a passing fad, or the focus of legitimate attention, the dissertations and official accreditations granted for thesis research since 1996 illustrate a diversity of research not seen in the publishing business. Above all, it shows the primacy of subjects connected to business intelligence (49 %), to the detriment of international relations and warfare (20 %). It means that the university system is adapting to a dual demand, one from the state and the other arising from purely professional requirements.

Paradoxically, practitioners of business intelligence research are loath to recognize its relationship with intelligence work. Business intelligence is considered more as a new form of business management, the result of a cross between open source management and the rigorous and scientific approach employed in marketing and consultancy, despite the fact that, internationally, the relationship between business intelligence and intelligence work in general is taken for granted. Consequently, many academics believe themselves to have 'invented' a new discipline. Accordingly, the information and communications sciences,

whose scope is the widest due perhaps to its lack of definite contours, have quickly gained prominence in the field. Since 1996, information and communications sciences account for one third of thesis papers submitted on the subject of intelligence and two thirds of theses presented on business intelligence. This trend creates a misunderstanding about the reality of economic intelligence and has resulted in the fact that 49 % of thesis papers presented were dedicated to open sources monitoring, i.e. electronic information management processes.

This reductionist approach has since extended beyond the field of information and communications sciences and has been imported to all academic disciplines that treat of economic intelligence. In this way, in business management, 49 % of business intelligence thesis papers presented were on the theme of open source monitoring; 13 % of economics thesis papers also. The interest in business intelligence has also extended beyond the sciences and has spread to the humanities, including law (22 % of thesis papers), political science (15 % of theses) and even history (4 %).

For the last thirteen years sixteen different disciplines have participated in intelligence studies in French universities. Contrary to what occurred in Great Britain, the history of intelligence (16 % of thesis papers) is not the guiding force. Just as with information and communications sciences, the study of the history of intelligence can be said to deform the reality of its object of study. Military intelligence is overrepresented (60 % of historical thesis papers), benefitting from the progress made in military history research over the last twenty years. Though international relations are well represented (28 %), it should be noted that 80 % of the subjects treat modern history only. Unlike military history, disinterest among students for the history of foreign relations has grown, especially in relation to contemporary history. There are no professors working on the history of intelligence who are also foreign relations experts, despite the fact that foreign relations constitute the traditional theatre of operations for the intelligence services.

Bizarrely, political science thesis papers on intelligence (8 %) are not comparable in quality to the efforts of foreign students working in the same field. With 47 % of theses on spy literature and only 38 % on the intelligence agencies and their structures, we can hardly talk about any knock-on effect. The same goes for thesis papers in law (15 %), despite that law constitutes the third reservoir of intelligence studies in France.

The structure of official academic research on the subject of intelligence is still in the development stage, but it is in the area of business intelligence that the most important initiatives are taking place, with, in particular, the establishment in 2003 of the *Laboratoire de recherche en guerre économique* (LAREGE – The Economic Warfare Research Laboratory), by the School of Economic Warfare. Under the direction of professor Philippe Baumard from the University of Aix-Marseille III, his aim is to make up for the time lost in France concerning the field of business intelligence.

Other centres of research are also studying and working on intelligence questions: the *Centre d'études d'histoire de la*

Défense (CEHD – Centre for Historical Study on Defence), established in 1995, set up a History of Intelligence Commission in 2000 chaired by jurist Bertrand Warusfel. The objective of the Commission is to promote research and debate, and to allow the military to contribute to university research in this potentially rich field of historiographic study. However, after eight years work, and one publication presenting the conferences held over its first five years of existence, the Commission was disbanded. The *Centre de recherche des écoles de Coëtquidan* (Coëtquidan Military Schools Research Centre), where Olivier Forcade ran a seminar on intelligence from 1997 to 2002, met a similar fate; the program was ended when its founder left having co-supervised fifty-eight dissertations by junior grade lieutenants on the subject of intelligence.

In parallel, the *Agence nationale de la recherche* (ANR – National Research Agency) supports a four-year program (2006-2009) for young researchers, entitled "*Information ouverte, Information fermée*" (IOIF – Open and closed source information), set up by Sébastien Laurent, Associate Professor at Bordeaux III and Science Po Paris. The program gathers twenty-two researchers and its objective is to be the first multidisciplinary intelligence approach in France (history, political science, law), composed mostly of young academics who work closely with their international counterparts. This interesting initiative is however more of a gathering of researchers interested in intelligence rather than a centre for intelligence experts. Their grasp of intelligence is somewhat limited even though the work produced is of a high quality and the meetings organised do enable many young historians to familiarise themselves with the subject.

The birth of a specialised research centre

Though French universities did not allow for the establishment of a specific research centre on intelligence studies, one striking project has been developed at the margins of university life, around the *Centre Français de Recherche sur le Renseignement* (CF2R – French Centre for Intelligence Studies), founded in 1999. University researchers and former intelligence officers, overcoming ingrained reticence from the academic world, decided to create an independent think tank to foster the development of intelligence studies. With a dual entrepreneurial and academic approach, professionals with backgrounds in the services and a team of researchers, both young and more experienced, have for the last ten years produced more than twelve thousand pages of books, documents, and multidisciplinary articles. They have worked on numerous private university and military academy degree programs, and have addressed conferences in France and abroad. CF2R has established exchanges with international research institutes and with foreign researchers and has set up a university prize that awards the work of students on the subject. In addition, researchers at CF2R have taught a variety of audiences (general public, children and adolescents) and have given orientation sessions and consultancy work to MPs, the media, filmmakers, etc.

Though there existed no specific diploma dedicated exclusively to intelligence studies, CF2R and the *Centre d'analyse politique comparée,*

de géostratégie et de relations internationales (CAPCGRI – Centre for Comparative Political Analysis, Geostrategy and International Relations) of University Montesquieu-Bordeaux IV, established a Master degree in Intelligence Studies in September 2006.

With this diploma program, CF2R and CAPCGRI sought to deepen and disseminate a veritable intelligence culture in France. With this end in mind, the course aimed to teach students the principles governing the actions undertaken by intelligence operatives, enabling students to recognize the traces of such actions in their research. This project is in the process of being relaunched within the framework of the *Groupe de recherche Sécurité et gouvernance* (GRSG – Study Group on Security and Governance) at the University of Social Sciences Toulouse 1.

In addition, despite the fact that the government's *Livre Blanc sur la Défense et la Sécurité* (French government White Paper on Defence and Security, 2008) pilloried the need for an intelligence academy in France, CF2R launched at the beginning of 2009 a diploma for professionals unique in the French-speaking world, entitled "*Management des agences de renseignement et de sécurité*" (Intelligence and Security Agencies Management). The course is aimed at high-ranking civil servants and military officers, as well as deputies who work in or with intelligence and security services and who wish to become proficient in this environment. The objective is to allow participants direct, manage or supervise intelligence services, to integrate such services with success, or to work effectively with them.

4. LIMITS OF AND CHALLENGES FACING ACADEMIC INTELLIGENCE STUDIES IN FRANCE

The main reason for the late emergence of scientific study of intelligence arises from two difficulties.

The first difficulty is simply the secret nature of intelligence work. There is nothing more difficult than an analysis of a field of activity whose main characteristic is the elimination of all trace of its existence or activity. Nevertheless, this difficulty also applies to many other fields of human endeavour and cannot be accepted as a reason for failure. Over time archives have been declassified and former intelligence officials will accept to talk openly about their work. Secondly, the work and professional practices of the intelligence services are wholly misunderstood; it is only with the acquisition of such knowledge that is becomes possible to identify the many traces of intelligence work throughout history and behind current events. Very few university teachers are able to comprehend the range of professional practices employed by intelligence operatives. Such practices are extremely rigorous and codified and have been perfected over centuries. Few researchers are aware of this gap in their knowledge when dealing with the work of the services. This is why academic courses must be developed on the subject.

A subject of research that is ill-defined

When we talk about intelligence, what is referred to exactly? There is much confusion about what

constitutes a piece of intelligence, intelligence work in general and indeed the function of the intelligence services. Such confusion usually stems from problems of vocabulary. Indeed the term ‘intelligence’ refers to the intelligence services, their operations and the results of their work:

– *special services* provide state information to various Departments (Ministries of the Interior, Defence, Foreign Affairs, Economy);

– *professional practices* enable the penetration of the secrets of adversaries using different means. The means employed to penetrate enemy secrets do not consist solely in illegal actions. Such practices are conducted to lend meaning to a mass of different data, both secret and non-secret, and to make such data understandable and actionable for a decision-maker;

– *finished product*, drafted to respond to a given demand. The finished intelligence product arrives directly on the desk of the authorities providing them with information; such information does not originate only from the special services.

When intelligence is studied, a researcher may be led to focus on several areas of expertise:

– the *administrative bodies* in charge of intelligence missions; the position and importance of such bodies within the state defence and security apparatus;

– the *professional clandestine skill-sets* developed to conduct intelligence missions. Such skill-sets are the only parameter by which one can judge the professionalism of an organisation; however, this is an area where archival material is very rare and academics are insufficiently trained;

– *intelligence product*, i.e. the intelligence gathered, the quality of that intelligence and the manner by which such product is taken into account or not by government authorities;

– *the manner by which a power (State) informs itself* about the world around it with a view to safeguarding control over its destiny and for the realisation of political and/or military projects;

– *intelligence culture*, i.e. the relationship between the national community and intelligence work in general.

It is very important to give a detailed explanation of what is commonly referred to as a ‘culture of intelligence’. The term not only covers intelligence work proper. In fact it covers all aspects of ‘secret warfare’, be that intelligence, action or influence: intelligence and counterintelligence, clandestine operations and special operations, interceptions and decoding, psychological warfare and deception. These activities cannot be separated one from another. Only a holistic, global approach allows for an understanding of the impact of such actions and their combined interaction.

An object of research that requires a well-defined discipline

Intelligence study is by its very nature multidisciplinary and incorporates political science, law, history, geopolitics, management sciences, the organisation of information and communications. Intelligence applies to all

areas of national security, and economic security via business intelligence.

In an appendix to the compendium of papers presented at the seminar "French Intelligence Culture" at Marne-la-Vallée, Admiral Lacoste provided eleven themes of research essential to intelligence study. He drew from his experience as director of the DGSE as well as from the advances made in Anglo-American research, as published in British journal *Intelligence and National Security*:

- documentation;

- elaboration and decision-making;

- methodological approach to intelligence;

- internal workings of secret services;

- business intelligence;

- information processing and information warfare;

- criminality and public order;

- ethics and deontology;

- civil liberties;

- investigative journalism;

- culture.

This indicative list constitutes an initial largely multidisciplinary 'road map'. The former director of the DGSE suggested *«a multiplication of complementary approaches from a range of disciplines»*. A non-exhaustive list of specialist subjects indicated could be gleaned by looking at the speakers invited by Admiral Lacoste to the seminar: they included historians, economists, political scientists, sociologists and jurists.

In less than two decades, French intelligence studies have undergone a major transformation, benefiting from the favourable environment born of the information revolution and the attacks of September 11th, 2001. The different government reports on business intelligence have also largely influenced the integration of the subject into university curricula. This has led to the establishment of diploma and degree courses, the first thesis papers and research programs as well as the creation of a specialised research centre (CF2R).

In addition, closer correspondence between the academic world and the publishing business has led to a popularisation of a specifically "French intelligence culture", that differs from the traditional journalistic approach and has resulted in the publication of numerous books that can be qualified as 'scientific' in their treatment of the subject.

Accordingly, and despite the traditional disinterest of political leaders in the subject, intelligence has achieved a level of recognition that hitherto it lacked. The existence of university courses on this subject seemed quite unrealistic only a decade ago. Such progress still requires comprehensive harmonization by the universities in France.

We believe that it is still too early to talk of the emergence of a "French School" of intelligence. As a subject of research, it is still too early to say whether the renewed interest in intelligence is but a passing fad. Research projects, save for CF2R and LAREGE, remain too fragile to constitute a real trend.

❀❀❀