STUXNET AND STRATEGY

A Special Operation in Cyberspace?

By LUKAS MILEVSKI

Cyberpower has posed a challenge for strategists since its advent, and the questions have only grown more pressing with the revelation of the Stuxnet malware attacks on Iranian nuclear sites. Many interpretations currently abound in an attempt to provide a framework within which to think about Stuxnet and about cyberpower more generally. Stuxnet has been described as the digital equivalent of "fire and forget" missiles, and it has caused concerns that cyber war may achieve the same catastrophic results in the highly networked 21st century that superpower nuclear war would have had in the 20th.[1] Neither comparison is particularly apt. Instead, the most constructive way of thinking about Stuxnet is to conceive of it as a special operation in cyberspace. The strengths and weaknesses of Stuxnet correspond to the strengths and

Satellite image of Natanz nuclear facility in Isfahan Province, Iran

Space Imaging Middle East

weaknesses of special operations. Although Stuxnet may be judged a tactical success but a strategic failure, it serves a pioneering purpose and holds the door open for the serious consideration of cyber attack as an instrument of strategy and policy.

Cyberpower and Stuxnet

Cyberpower has been steadily growing in prominence over the past decade, but for the most part it seemed to offer only a limited toolset to strategists. Danny Steed in a recent article suggests that it can be used as a tool or otherwise elicit effects in five different ways. First, it can be a potent tool of intelligence, affecting the scope of and speed with which information can be gathered. Second, it greatly optimizes the use of one's own hard power—the foundation of Western military prowess. Conversely, the third use of cyberpower can disrupt the network that underpins the enemy's hard power. Fourth is a greatly expanded conception of the third use: direct cyber attack on national infrastructure, as seen in Estonia in 2007 and Georgia a year later. Finally, it may have significant impact on morale, particularly on the home front, as casualties and accidents are typically made known, either by the media or the government, with a celerity that far outstrips the achievement of tactical success, let alone strategic success. However, there are two important military applications that the Steed analysis claims that cyberpower *cannot* do. First, it cannot directly cause corporeal harm, either to human beings or to their physical creations. Second, it cannot occupy actual terrain. Ultimately, the analysis concludes that "cyberpower will never coerce in the way that sheer physical force can do."[2]

This pertains to conventional cyberpower. These are the tactical limits within which the vast majority of cyberpower will fall. Strictly speaking, Stuxnet also belongs within these limits, despite purportedly resulting in the destruction of 1,000 Iranian centrifuges at the Natanz enrichment plant. This destruction was a second-order effect of the malware; it created the context within which the destruction occurred but did not directly inflict it. The first-order effect remained at the eternal limit of cyber assault: digital infection. However, Stuxnet is exceptional despite staying within the limits of what is tactically possible for cyberpower because through manipulation within those limits, it was able to reach beyond them. It broke previous patterns of political uses of cyberpower by spreading indiscriminately, while only activating on very particular machines. It exploited four vulnerabilities, including two zero-day vulnerabilities, in Microsoft operating systems to gain access to Siemens programmable logic controllers and control of the operation of centrifuge-operating computers, at which point it displayed decoy signals to indicate normal operation even as it followed instructions that broke those centrifuges.[3] It was the first time that such a comprehensive package—one common in the criminal cyber underworld, capable of spreading by itself, hiding itself, and attacking by itself—was employed against a specific target to achieve, or at least facilitate, a particular strategic or political effect.

Stuxnet broke previous patterns of political uses of cyberpower

Its physical effect was significant: 1,000 centrifuges were destroyed, out of a total of 9,000 at Natanz, but Iran has been estimated to have only stockpiled the material to build 12,000 to 15,000 centrifuges. Nine thousand are deployed at Natanz, and 2,000 are broken either through routine operation or by Stuxnet—and with no easy chance for Iran to avoid international economic sanctions.[4] Institute of Science and International Security experts on the Iranian nuclear program argue that Stuxnet must have had significant implications for Iranian morale as well due to the uncertainty surrounding the attack. Before the discovery of the malware itself, the sudden damage to so many centrifuges must have thrown serious doubt upon the reliability of the quality assurance program necessary to run such a facility and diverted Iranian attention and effort into emergency mitigation. Even Stuxnet's discovery could only have fed Iran's sense of vulnerability, particularly given the immensely detailed specifications Stuxnet would have required to achieve the results it did: information "far beyond what the [International Atomic Energy Agency] knew." This fear could easily impact Iranian decisions concerning secret nuclear facilities, particularly in the additional context of Western discovery of the Qom facility in 2009. Its view of the quality of goods it obtains through smuggling might also have been damaged, and it may assume the task of producing more of the requisite materials and machines domestically despite limited industrial capabilities at the necessary level. Finally, given how widely Stuxnet has proliferated, particularly in Iran, those working in the nuclear program will have to take extra care to prevent reinfection.[5]

Stuxnet as a Special Operation

Special operations expert James Kiras has explored the relationship between special operations and strategy, arguing that "the root of strategically effective special operations is an appreciation for how special operations forces perform in extended campaigns by inflicting moral and material attrition in conjunction with conventional forces." He goes on to define *special operations* as "unconventional actions against enemy vulnerabilities in a sustained campaign, undertaken by specially designated units, to enable conventional operations and/or resolve economically politico-military problems at the operational or strategic level that are difficult or impossible to accomplish with conventional forces alone." As one of his concluding thoughts, he suggests ultimately that "at the strategic level, however, special operations are less about an epic Homeric raid than they are about the combined effects of disparate unorthodox activities in the ebb and flow of a campaign or series of campaigns."[6] That is, if used properly, they are ultimately the best option available to policymakers in those particular situations where more conventional force is unwise. Does Stuxnet meet the requirements of what makes a special operation, albeit in digital form?

Kiras focuses on special operations within the context of a wider war; his examples draw almost entirely from World War II for the good reason that it offers such a wide selection of special operations. Arguably, however, one of the great advantages of special operations is that they are suitable not just to war but also to the murky zone between war and peace. Cyberpower by its very character also occupies this niche area, and anonymity online is one of the Internet's defining features. Additionally, the very construction of Stuxnet was designed to preclude attribution. It has been suggested that "Stuxnet's

Lukas Milevski is a Doctoral Candidate at the University of Reading under Professor Colin Gray and Winner of the 2010 RUSI Trench Gascoigne Essay Competition.

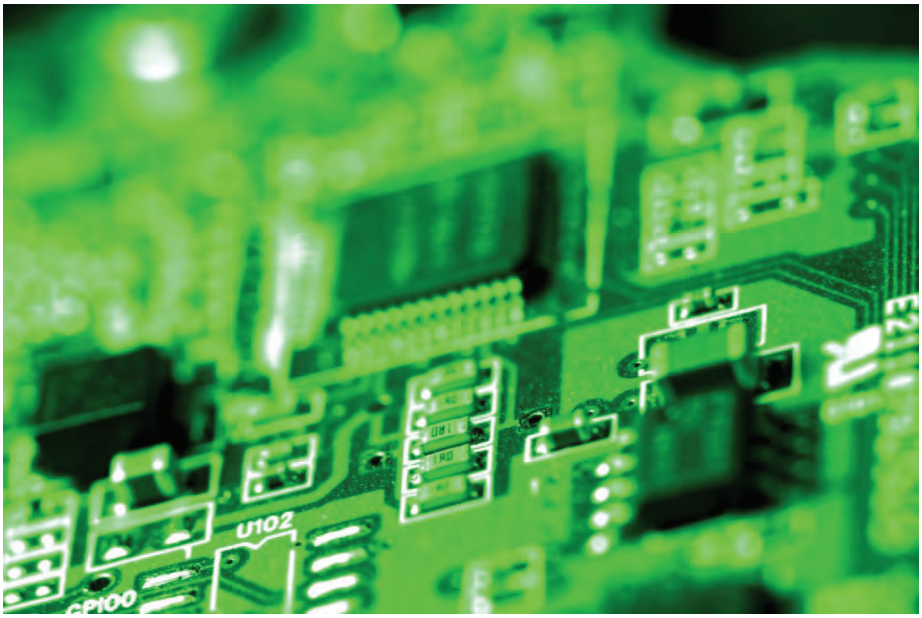
core capabilities and tradecraft, including the use of multiple zero-day exploits, render it more of a Frankenstein patchwork of existing tradecraft, code, and best practices drawn from the global cyber-crime community than the likely product of a dedicated, autonomous, advanced research programme or 'skunk works.'"[7] Whether due to deliberate design or simply the casual practices of veteran cyber criminals, deniability of responsibility for the attack is a byproduct of Stuxnet's design.

The essential requirement of special operations, however, is that they augment other, more conventional efforts. Special operations acting entirely on their own rarely achieve a significant level of effect if their target can devote all his resources to countering and mitigating the results of any given special operation. However, working alongside conventional military operations is not the only context in which special operations could have considerable effect; conditions suitable for special operations can be manufactured. Writing about the Arab Revolt of World War I, T.E. Lawrence suggested that "the death of a Turkish bridge or train, machine or gun or charge of high explosive, was more profitable to us than the death of a Turk."[8] What the Turks in Arabia lacked was hardware, not manpower. Special operations can be usefully employed to attrite resources that the other side is short of or reliant upon, whether hardware or manpower. A state of affairs in which materiel is worth more than manpower due to its relative scarcity may sometimes exist of its own accord, or be a product of political neglect, innate lack of resources or industrial capacity, or still other internal factors. It may also be imposed by an outside party, both in war and in peace, through a variety of actions, including the attritional effects of successive military engagements and operations in war. The United States has a method of achieving such material shortage in selected states during times of peace, particularly if it can act in a multilateral context, which multiplies its effectiveness if properly implemented by all involved parties—sanctions.

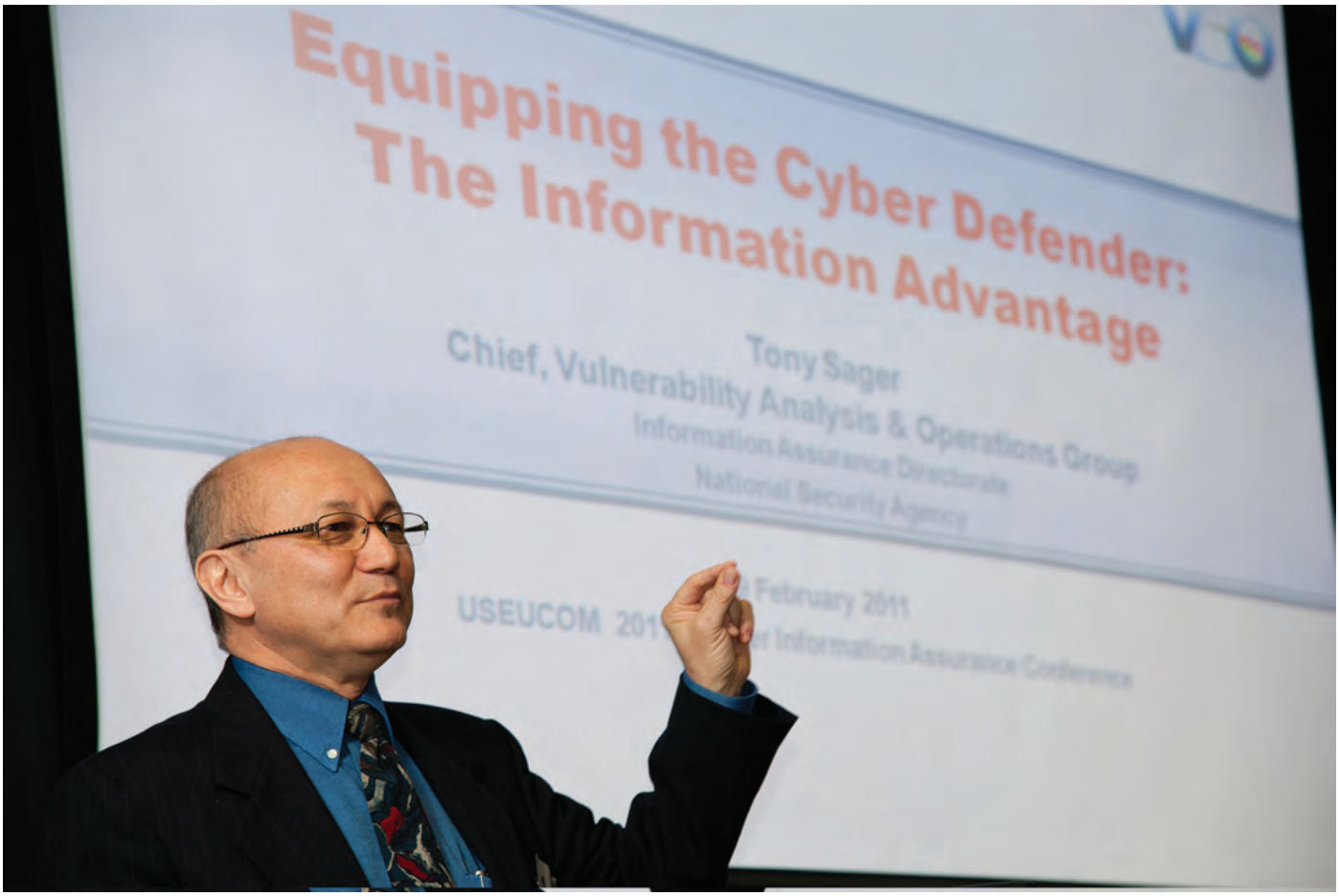
In June 2010, the United Nations Security Council passed Resolution 1929 to adopt a fourth round of sanctions against Iran and the toughest multilateral sanctions yet designed to inhibit the development of the Iranian nuclear program. Beyond this, the United States and the European Union have also imposed further unilateral sanctions. Despite the nay-saying of the Russians, the sanctions are slowly having an effect, both on the Iranian nuclear program and Iranian society at large, although neither is at the breaking point. Resolution 1929 represents the culmination of a long-term sanctioning campaign against Iran, a campaign that has steadily decreased Iran's options for the procurement of necessary materials for its nuclear program and that has also, to varying extents, cut into Iran's ability to function economically, both internally and externally, with other states. For example, IranAir is losing gasoline contracts and finding itself unable to refuel in certain countries, and ships belonging to the Islamic Republic of Iran Shipping Lines are unwelcome in many ports. It is difficult for Iran to acquire either more uranium or more materials required for its current generation of centrifuges. The major hub of Iranian smuggling is currently Asia, but many of Asia's major ports belong to American allies, adding to Iranian difficulties. As already noted, the Iranians are estimated to have the materials for only about 12,000–15,000 of their IR–1 centrifuges. Eleven thousand have been deployed, of which 2,000 have been broken through routine use or by Stuxnet. Iran's cushion against accident or hostile action is becoming increasingly thin as a result of its inability to procure materials for more IR–1 centrifuges. It is currently developing next-generation centrifuges, the IR–2 and IR–4, the latter of which requires additional material, but these have yet to be deployed beyond limited testing. These new generations are expected to increase enrichment efficiency significantly, allowing for fewer centrifuges to achieve the same enrichment rates as the many thousands Iran currently has deployed. For any actor concerned with delaying the Iranian nuclear program and feeling that sanctions were not taking effect quickly enough, the time to strike covertly had to be before the new centrifuges were introduced en masse.

Conventional means are clearly inadequate against the Iranian nuclear program. The dispersal of existing plants, their locations within mountains and other difficult terrain, and secrecy surrounding planned facilities all prevent an easy military response such as the Israeli attacks on Osirak and the alleged Syrian reactor in 2007. Sanctions have not yet had sufficient effect to dissuade the Iranians, and quite plausibly will not, as long as the Iranian political calculus remains steadfast and finds sufficient attraction to and utility in its chosen course. The Iranians view diplomacy as a method of keeping the international community at bay rather than a way to resolve the situation in an agreeably Western manner. A special operations strike of some sort was clearly necessary if one's goal was the delay of the nuclear program, but the very character of that program also precludes easy destruction by a limited number of operatives. A cyberstrike must have been much more compelling as an option. Stuxnet's abilities to self-replicate, quickly proliferate across systems, and disguise its presence until activated all indicate that it was specifically

newjestic.com



Computer circuit board



U.S. Army (Martin Greeson)

National Security Agency official discusses cyber ecosystem at U.S. European Command's Cyber Defense/Information Assurance Conference, Stuttgart, Germany

designed to counter the security measures put in place to prevent a conventional or unconventional attack on the Iranian nuclear program. All three characteristics were necessary to approach and infect the relevant computers and damage a portion of the centrifuges at Natanz. There could have been no other sure way for Stuxnet to have jumped the air gap between the wider Internet and computers at Iranian nuclear facilities without self-replicating and proliferating wildly across computers and onto USB sticks and other portable data transfer devices, and hiding its presence until it reached precisely the computers it had been coded to infect and control.

Martin Libicki, an expert on cyberpower, argues that cyber war is ultimately about confidence, particularly confidence in the systems being attacked. He suggests that any cyber attack must of necessity have two fundamental bases: "(1) the exposure of target systems to the rest of the world, coupled with (2) flaws in such systems which are then exploited."[9] By jumping the air gap, Stuxnet surprised the Iranians and weakened their confidence in their ability to preclude cyber attack altogether through disconnection. Even severing a direct connection to the wider Internet does not remove exposure. The further infection of computers in Natanz after the penetration of the air gap only increased the Iranians' realization of their own insecurity despite the measures they had taken. Although the Iranians have now most likely removed all traces of Stuxnet from their systems and may have addressed the software and operating system vulnerabilities that the previous iterations of the malware attacked, they are also assuredly now particularly sensitive to a potential similar attack that would take advantage of different weaknesses.

cyber war is ultimately about confidence, particularly confidence in the systems being attacked

The vulnerabilities that attacks like Stuxnet exploit are one of the major factors that distinguish them from more conventional cyber attacks such as the sustained distributed denial-of-service assault on Estonian cyber infrastructure in 2007. Kiras warns that special operations forces "conduct missions of strategic importance, yet exist in finite quantities, and must therefore be used wisely."[10] Similarly, Libicki has noted that, although cyber vulnerabilities are by their very character unknown until exploited (or discovered and fixed), "cyber attacks are self-depleting."[11] That is, there are only so many vulnerabilities that can be exploited, and to some extent the character of the vulnerability may also define the limits of what the cyber attack may achieve. One would think that this would lead to very selective use of cyber attacks that

rely on exploiting system flaws, in the same way as special operations forces are only used selectively because there are relatively so few of them and they are difficult to replace. This is not necessarily the case, however, as there are other pressures involved.

First, the available vulnerabilities, whether known or unknown, are finite in number, as Libicki implied—to use them is to deplete them, as they will inevitably be corrected. More important, the available vulnerabilities are largely *collective*. That is, whereas any one nation's special operations forces are purely that nation's to use as, when, and how it wishes, this is not the case with cyber vulnerabilities. Such flaws, being a collective pool, are open to anyone and everyone seeking to use or fix them. If one country's hackers discover a new flaw, it is probable that any other country's hackers may already have, or will in the future. Furthermore, while such hackers, depending on their motives, may desire to hold the potential exploit secret for personal, commercial, or national use, there are also firms whose duty is to discover and patch such vulnerabilities out of existence. Stuxnet may no longer find it possible to use the same avenues of exploitation to break into computer systems because Symantec has updated its malware definitions and because Microsoft and other relevant companies may have patched those particular vulnerabilities in their own software. This inherent dynamic in cyberspace concerning system flaws is such that an operator's first instinct is to try immediately to exploit any discovered weaknesses for fear that otherwise someone else will, and that ultimately however the vulnerability is, or is not, used, it will be patched and that avenue of attack will be closed off. For those concerned with national security, this instinct must be balanced by the need to achieve beneficial effect in service of strategy or policy. Is there sense in using a recently discovered, powerful cyber vulnerability on a target of low importance solely to make sure it is not used against oneself or fixed before it can be used?

cyber vulnerabilities are by their very character unknown until exploited

Ultimately, the question of when to exploit a cyber vulnerability is answered by human judgment. Judgment is also required concerning when to protect against a known flaw. Other cyber actors may detect one while fixing a previously unknown flaw and decide quickly to exploit the defect before the patch proliferates and destroys their chances of capitalizing on it. A defender may be so confident in his defenses—such as an air gap—that he neglects basic security on the machines behind that gap, with the result that already known and fixed vulnerabilities may yet be available for exploitation. Software firms may also be lazy or duplicitous about addressing vulnerabilities in their own software. An inability to find the flaw allowing cyber attacks or to perceive that a cyber attack is actually under way—as with Stuxnet, which took control of the feedback systems to inform those monitoring the centrifuges that everything was normal even as it was tearing 1,000 of them apart—also allows vulnerabilities to last longer than in ideal theoretical conditions. Some known vulnerabilities have persisted for years, across multiple generations of software, without being addressed. Others are exterminated immediately upon discovery. The individual organizational or communal culture frequently determines the alacrity with which flaws are fixed.

One of the major fears that has yet to be borne out from the Stuxnet attack is the possibility that it could serve as a blueprint for others for their own cyber attacks, potentially including those hostile to the West. This seems unlikely if Stuxnet really is the digital equivalent of a special operation, for special operations are immensely context-dependent. As Colin Gray notes, "Findings on the conditions for the success or failure of special operations cannot sensibly be presented as a formula, a kind of strategist's cookbook."[12] Stuxnet was designed to take advantage of particular flaws of specific operating systems and programmable logic controllers of select nuclear facilities to overwhelm the physical limits of particular centrifuges. This points to an extended period of gestation for Stuxnet simply to discover such a succession of vulnerabilities, flaws, and the breaking point of

Estonia Today

U.S. Department of Homeland Security

Left: National Cybersecurity and Communications Integration Center director speaks to press at Department of Homeland Security, 2010

Left: President George W. Bush visits Estonia, 2006

Right: Secretary of State Condoleezza Rice arrives for meeting with Georgian Minister of Foreign Affairs, August 2008

Embassy of the United States

IR–1 centrifuges. Stuxnet would seem to have little to offer in terms of concrete ability actually to reproduce such an attack against a different facility: vulnerabilities and flaws would necessarily be different and the purpose and aims of the attack would differ as well. What can be extrapolated from Stuxnet is a design philosophy, and perhaps inspiration for further innovation in the creation of serious cyber attacks. Due to the character of Stuxnet alluded to above—the Frankenstein of best practices—all the tools already existed, for the most part. It was just a matter of using them in concert in the specific way in which they were used.

Conclusion

Special forces are "military assets designed and trained to conduct tactical actions delivering strategic outcome out of proportion with their size and that if conducted by conventional units may have disproportionate negative impact on policy."[13] The West, fearing such a disproportionate negative effect, has been shy of the prospect of armed conflict with Iran. The preferred method has been a mixture of sanctions and diplomacy. Given the slow effect of sanctions thus far, employment of Stuxnet to attrite the physical capacity of Iranian nuclear plants, even if the attacks to date have not had a sufficient effect necessary to overwhelm the Iranian ability to replace broken machinery, fits in well with overall policy. Strategically, it makes sense: first, one prevents the importation of necessary materials, and then one takes covert action that forces one's opponent to expend his limited stocks without being able to renew them, as stock limitation on its own is hardly potent without a context that makes those limits meaningfully damaging.

The disproportionate effect is simultaneously both confirmed and doubtful. Stuxnet destroyed 1,000 centrifuges, but it could not remove from operation the remaining 8,000 at the Natanz facility. For a program, however malicious, ultimately to achieve that level of physical destruction of infrastructure, even if only as a second-order effect, is disproportionate considering how inexpensive such an attack is compared to other, less attractive policy options. Importantly, however, Iranian production of lightly enriched uranium did not drop; it actually increased somewhat during the period it was affected by Stuxnet as the Iranian nuclear facilities improved their efficiency—although clearly it did not increase as much as it could have, had the damage not been done. Furthermore, Iran was able to replace the lost centrifuges, and it still maintains a buffer of materials remaining to build additional IR–1 centrifuges as necessary. This remainder may be sufficient for only 1,000 more, or possibly up to 4,000 more, and Iranian smuggling efforts may increase these numbers. It is unknown whether those responsible for Stuxnet are heartened by their success, or are frustrated by having failed to destroy more, but either reaction may motivate further attacks. Regardless of motive, further attacks would be necessary to affect the Iranian nuclear program significantly; as long as they can replace centrifuges, lost centrifuges only represent relatively minor time lost to the Iranians. Another cyber attack, however, will undoubtedly be expected, and the Iranians are on guard. Surprise, the best ally of special operations, is now missing.

The Stuxnet malware, in the context of international sanctions, ultimately has not affected Iranian political will to a sovereign nuclear program or Iranian capabilities sufficiently that their goal cannot be pursued regardless of intent. What would a strategically successful Stuxnet look like? That sort of attack would have to be destructive enough to at least leave a permanent mark on Iranian capabilities by overwhelming the material redundancy available to their nuclear programs. It would also have to be able to overcome increased Iranian nuclear efficiencies.

Such success may be possible, since malware such as Stuxnet has one significant advantage over physical special operations: unlike actual people, a program can be in multiple places at once—hundreds of thousands, millions, or more—if necessary. It should be possible to attack multiple specified targets with a single virus exploiting a set of vulnerabilities common to all targets—that is, compress a special operations campaign in time to orchestrate a massive attack in parallel, rather than a sequence of missions. Stuxnet may even have been designed to achieve this, too. Iran has admitted that Stuxnet found its way into their Bushehr nuclear power plant and, in early 2011, nearly 170 fuel rods had to be removed from the reactor soon after inserting them—an occurrence not unheard of elsewhere in the world, but hardly frequent. Some have speculated on the existence of a link between Stuxnet's infiltration of the Bushehr facility and its recent troubles. Whether or not Stuxnet had an effect on Bushehr is irrelevant: the potential for attacks in parallel has already been noted.

Yet not having achieved the necessary level of success at Natanz is not surprising. Any sort of friction could have intruded upon Stuxnet's infection and control of Natanz enrichment facilities, and solitary special operations rarely have such decisive effect on their own, although "solitary" may not gel well in possible future cases of a massively parallel assault on multiple facilities. Nonetheless, as the first special operation in the cyber dimension of war, and with the purpose of causing physical damage, Stuxnet was operating entirely in unknown territory. Now, the right lessons need to be learned. **JFQ**

NOTES

[1] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (January 2011), 24. See also the *Economist* cover for July 3–9, 2010: a digitized nuclear explosion.

[2] Danny Steed, "Cyber Power and Strategy: So What?" *Infinity Journal* 2 (Spring 2011), 21–24.

[3] Nicolas Falliere, Liam O. Murchu, and Eric Chien, "W32.Stuxnet Dossier," Symantec, February 2011, available at <www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.

[4] David Albright, Paul Brannan, and Christina Walrond, *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report* (Institute for Science and International Security, February 2011), 4, available at <http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf>.

[5] Ibid., 4–5.

[6] James D. Kiras, *Special Operations and Strategy: From World War II to the War on Terrorism* (New York: Routledge, 2006), 2, 5, 115.

[7] Farwell and Rohozinski, 25.

[8] T.E. Lawrence, *Seven Pillars of Wisdom* (New York: Anchor Books, 1991), 194.

[9] Martin C. Libicki, "Cyberwar as a Confidence Game," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011), 133.

[10] Kiras, 115.

[11] Libicki, 133.

[12] Colin S. Gray, "Handful of Heroes on Desperate Ventures: When Do Special Operations Succeed?" *Parameters* 29, no. 1 (Spring 1999), 3.

[13] Simon Anglim, "Special Forces—Strategic Asset," *Infinity Journal* 2 (Spring 2011), 16.