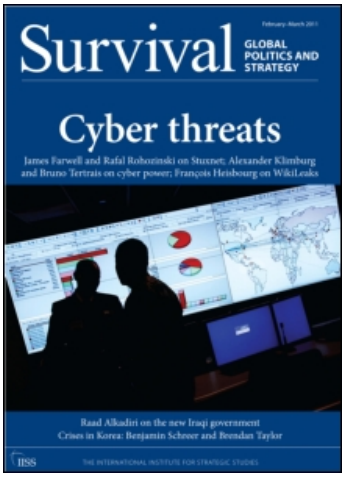

Survival
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t713659919

Stuxnet and the Future of Cyber War

James P. Farwell; Rafal Rohozinski

Online publication date: 28 January 2011

To cite this Article Farwell, James P. and Rohozinski, Rafal(2011) 'Stuxnet and the Future of Cyber War', Survival, 53: 1, 23 — 40
To link to this Article: DOI: 10.1080/00396338.2011.555586
URL: http://dx.doi.org/10.1080/00396338.2011.555586

Stuxnet and the Future of Cyber War

James P. Farwell and Rafal Rohozinski

The discovery in June 2010 that a cyber worm dubbed 'Stuxnet' had struck the Iranian nuclear facility at Natanz suggested that, for cyber war, the future is now. Stuxnet has apparently infected over 60,000 computers, more than half of them in Iran; other countries affected include India, Indonesia, China, Azerbaijan, South Korea, Malaysia, the United States, the United Kingdom, Australia, Finland and Germany. The virus continues to spread and infect computer systems via the Internet, although its power to do damage is now limited by the availability of effective antidotes, and a built-in expiration date of 24 June 2012.[1]

German expert Ralph Lagner describes Stuxnet as a military-grade cyber missile that was used to launch an 'all-out cyber strike against the Iranian nuclear program'.[2] Symantec Security Response Supervisor Liam O Murchu, whose company reverse-engineered the worm and issued a detailed report on its operation, declared: 'We've definitely never seen anything like this before'.[3] *Computer World* calls it 'one of the most sophisticated and unusual pieces of software ever created'.[4]

James P. Farwell is an expert in strategic communication and information strategy who has served as a consultant to the US Department of Defense, the US Strategic Command and the US Special Operations Command. He has three decades' experience as a political consultant in US presidential, senate, congressional and other campaigns. He has published numerous articles and his book *The Pakistan Cauldron: Conspiracy, Assassination and Instability* is forthcoming from Potomac Books in 2011. **Rafal Rohozinski** is the CEO of The SecDev Group and a Senior Scholar at the Canada Centre for Global Security, Munk School of Global Affairs, University of Toronto. He is the co-founder and Principal Investigator of the OpenNet Initiative and Information Warfare Monitor. He is a co-author of the *Ghostnet*, *Shadows in the Cloud* and *Koobface* investigations examining advanced cyber-espionage and cyber-crime networks; and contributing author and editor of *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (MIT Press, 2010).

Survival | vol. 53 no. 1 | February–March 2011 | pp. 23–40 DOI 10.1080/00396338.2011.555586

These claims are compelling. Stuxnet has strong technical characteristics. Yet more important is the political and strategic context in which new cyber threats are emerging, and the effects the worm has generated in this respect. Perhaps most striking is the confluence between cyber crime and state action. States are capitalising on technology whose development is driven by cyber crime, and perhaps outsourcing cyber attacks to non-attributable third parties, including criminal organisations (see essay by Alexander Klimburg in this issue).

Worms as weapons

Stuxnet is a sophisticated computer program designed to penetrate and establish control over remote systems in a quasi-autonomous fashion. It represents a new generation of 'fire-and-forget' malware that can be aimed in cyberspace against selected targets. Those that Stuxnet targeted were 'air-gapped'; in other words, they were not connected to the public Internet and penetration required the use of intermediary devices such as USB sticks to gain access and establish control. Using four 'zero-day vulnerabilities' (vulnerabilities previously unknown, so that there has been no time to develop and distribute patches), the Stuxnet worm employs Siemens' default passwords to access Windows operating systems that run the WinCC and PCS 7 programs.[5] These are programmable logic controller (PLC) programs that manage industrial plants. The genius of the worm is that it can strike and reprogram a computer target.[6]

First Stuxnet hunted down frequency-converter drives made by Fararo Paya in Iran and Vacon in Finland. These each respond to the PLC computer commands that control the speed of a motor by regulating how much power is fed to it. These drives are set at the very high speeds required by centrifuges to separate and concentrate the uranium-235 isotope for use in light-water reactors and, at higher levels of enrichment, for use as fissile material for nuclear weapons.[7]

Then Stuxnet alternated the frequency of the electrical current that powers the centrifuges, causing them to switch back and forth between high and low speeds at intervals for which the machines were not designed. Symantec researcher Eric Chien put it this way: 'Stuxnet changes the output

frequencies and thus the speed of the motors for short intervals over a period of months. Interfering with the speed of the motors sabotages the normal operation of the industrial control process.'[8] In a devious touch, the worm contains a rootkit that conceals commands downloaded from the Siemens systems.

Some media reports mistakenly thought the Iranian light-water power reactor at Bushehr was also a target. Iran confirmed that Stuxnet infected personal computers there while denying that much damage was inflicted.[9] But Bushehr seems an unlikely target, because the plutonium produced by such light-water reactors is not well suited for weapons purposes. The more likely target is Iran's uranium-enrichment programme. Although most of the 4,000–5,000 centrifuges operating to date at the pilot and industrial-scale fuel-enrichment facilities at Natanz have been producing only low-enriched uranium, the same centrifuges could be put to use to produce highly enriched uranium for weapons. Alternatively, and in a more likely scenario, it is feared that Iran could be operating secret centrifuge facilities to produce highly enriched uranium. The key to the Stuxnet worm is that it can attack both known and unknown centrifuges.

Emerging modes of cyber war

Understanding Stuxnet's strategic importance requires appreciating what it is not. Forget the media hype. Stuxnet is less sophisticated or advanced than billed. Some of its core technical characteristics, including the use of a DNS-based command-and-control network, make it less stealthy than much of the more advanced malware that criminals use. Stuxnet's 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'. Nor is Stuxnet particularly innovative. The ability to ability to jump air-gap systems is old news. Hackers had already used that technique to steal classified documents from US CENTCOM.

Stuxnet's real strategic importance lies in the insight it offers into the evolution of computer warfare that is occurring far away from Washington's

beltway. The driver for this evolution is industrial cyber crime. Nearly every significant cyber event reported since 2005 involves tradecraft, techniques and code tied to the cyber-crime community. Critics charge that China has outsourced cyber piracy against the United States to third parties acting outside the law, or at least capitalised on their activities.[10] 'Botnets' harnessed by Russian criminal operators effected the denial of service that disrupted Estonia's national networks in May 2007. These botnets are part of an underground economy of crimeware kits and resources that are bought, sold and traded, and typically used for corporate warfare to knock political and business competitors off line.

Botnets played a key role during the 2008 Russia–Georgia war, serving Moscow as a strategic multiplier for its military campaign through distributed denial of service (DDoS) attacks. Commercial-grade botnets originating from Russian cyberspace silenced Georgian government websites and independent media, and disabled the government's ability to communicate to its population. The DDoS attacks helped create an information vacuum that paralysed Georgia's civil administration. In each case, Russia denied official involvement. Yet the botnet attacks directly supported Russian state policy. A genius of the strategy was that no one could link the Russian government and the cyber attackers, protecting the Russian state from political or legal culpability.[11]

Georgia and Estonia epitomise the emerging model. Investigations by the Information Warfare Monitor of the Chinese-based *Ghostnet* and *Shadows* attacks documented how well-known crimeware kits penetrated and extracted confidential material from the Tibetan community in exile in India, as well as the highest reaches of the Indian Ministry of Defense, Foreign Ministry, and its defense research establishment.[12] The recent wide-scale breach of classified systems at CENTCOM that resulted in the loss of thousands of classified documents occurred when a USB stick infected with a well-documented virus was inadvertently used by someone on a laptop connected to a classified network.

The prevalence of crime in cyberspace provides a haystack to conceal cyber espionage. For Stuxnet, a significant body of circumstantial evidence – fragments of code, relationships between individuals, correlations in

cyberspace – suggests a link between the code used by the worm and the burgeoning Russian offshore programming community, where talented programmers work in the grey market of code. In this community, there is no neat division between programmers working one day with Siemens SCADA equipment for an industrial client in Saratov and the next programming online gaming software for the Israeli-owned offshore gaming services in Ireland and the UK. The connections are murky, but digital trails in cyberspace inhibit the complete anonymity of code or locale. Often these fragments can be assembled into a circumstantial picture, although it is complex and frustrating for those seeking clear answers.

Stuxnet used off-the-shelf code and tradecraft. That served two ends. Firstly, it saved money by capitalising upon code expertise already proven effective. As the Information Warfare Monitor documented in its *Ghostnet* and *Shadows* reports, the same target can often be breached by several independent attackers simply because technology is cheap and effective to design and deploy and, more importantly, it works.

Stuxnet was quickly disarmed

Secondly, Stuxnet's amalgam of components helped conceal its etiology. The central challenge in attempting to identify cyber attackers underscores the dark ecology of cyberspace. Culpability is difficult to prove. Is the responsible party a Russian hacker living in New Zealand who may have contributed part of the code used for the rootkit? Or is it an intermediary that may have passed the code onto a state-based military intelligence actor? Deliberate ambiguity is an effective shield against retribution.

This approach comes at a cost. Despite its relative sophistication, Stuxnet was quickly and effectively disarmed. Within months its technical characteristics and components were well known. Iran was able to quickly harness the intellectual capital of the global computer security community through effectively crowdsourcing solutions to the worm, casting some doubt on the conventional wisdom and hype surrounding the efficacy of computer network attacks. Stuxnet's rapid neutralisation also raises the question of why this approach, rather than a more stealthy or direct one, was chosen to target Tehran's nuclear programme. The answer depends

upon the strategic and political goals the Stuxnet attackers aimed to achieve.

There has been much speculation that Israel or possibly the United States may launch air strikes to retard Iran's nuclear programme during 2011, although it seems unlikely that President Barack Obama would consent to US strikes.[13] The costs and benefits of such action have been widely debated.[14] Recent statements by Arab leaders expressing concern about the Iranian nuclear threat have given Israel's rationale for action new credibility and a stronger claim to legitimacy. The WikiLeaks disclosure of confidential US diplomatic cables in December 2010 has strengthened Tel Aviv's hand. The cables confirm that leaders of Israel's Arab neighbours concur with Prime Minister Benjamin Netanyahu's longstanding alarm about Iran's growing nuclear capabilities.[15] Saudi Arabian King Abdullah bin Abdulaziz has told the United States it must 'cut off the head of the snake'. Egyptian President Hosni Mubarak has called the Iranians 'big, fat liars'. The United Arab Emirates defence chief has compared Iranian President Mahmoud Ahmadinejad to Adolf Hitler. King Hamad Bin Isa Al Khalifa of Bahrain has opined that Iran's nuclear programme 'must be stopped'.[16] King Abdullah II of Jordan had gone public as early as 2004, warning against the emergence of an Iranian-backed 'Shia crescent' that might de-stabilise the Middle East.[17] He didn't call for an attack on Iran, but the sentiment for foiling Iran was plain.

Would air strikes against Iran's nuclear programme succeed? Israeli strikes against Iraq's Osirak nuclear reactor in 1981 and a Syrian installation in 2007 did, but they entailed single above-ground, poorly defended sites located closer to Israel. Targets in Iran are much further away. The WikiLeaks disclosures indicate that Saudi Arabia might allow over-flight of its territory. The United States would also, apparently, allow Israel to over-fly Iraq.[18] Israeli bunker-busters could penetrate underground facilities like Natanz. Although refuelling limitations would probably prevent Israel from hitting all of Iran's nuclear facilities in a single strike, its planes could hit the key sites that are critical to fissile-material production. Despite boasts, Iran's air defences seem questionable. Success would achieve critical Israeli security goals and help prevent a nuclear arms race in the region.

But a strike poses risks. A single strike might not succeed, and it is not clear how many over-flights Saudi Arabia or the United States might permit. Israel could sustain significant losses. Iran would hold the United States responsible, and could attack US installations and troops in Iraq, Afghanistan or elsewhere. It might disrupt the flow of oil out of the Gulf and oil prices could escalate. Air strikes might unite a currently divided Iran and enable Ahmadinejad and his allies to consolidate power.

Does cyber attack offer a better risk–benefit trade-off to achieve the goal of stopping or slowing Iran's nuclear programme? How well did Stuxnet perform? At first, Iranian Communications Minister Reza Taghipour was dismissive. He claimed that 'the effect and damage of this spy worm in government systems is not serious', and that 'almost all areas of infection have been identified and dealt with'.[19] Later, Ahmadinejad admitted that Stuxnet had set back the programme but that it affected only a 'limited number of centrifuges'.[20] Siemens acknowledges that Stuxnet struck 14 industrial plants, both in and out of Iran. Tehran has insisted that no Iranian plant operations have been severely affected.[21]

Nevertheless, International Atomic Energy Agency inspectors reported that Iran had stopped feeding uranium into the Natanz centrifuges for one week in late November, which could be an indication of a major breakdown.[22] A 23% decline in the number of operating centrifuges from mid-2009 to mid-2010 may have been due to the Stuxnet attack.[23] The full extent of the damage remains to be seen, but the Iranians were apparently caught off guard and surprised by the degree to which their defences could be penetrated, even against highly protected air-gap systems. And even if the damage was limited and repaired quickly, Stuxnet points to a new way forward. A future attack, using more sophisticated worms or malware, may inflict more serious, longer-lasting damage.

Emerging norms

Iran has downplayed Stuxnet as a failure. There is no proof of who mounted the attempted penetration and disruption and, if one accepts the Iranians' account of the damage, only weak grounds for arguing that it represented the use of force, armed attack or aggression under the UN Charter.[24] A 1974

General Assembly Resolution defined 'aggression' as including 'bombardment by the armed forces of a State against the territory of another state or *the use of any weapons by a State against the territory of another* State'.[25] But the resolution preceded the advent of cyber war. Whether industrial facilities qualify as 'territory' is unresolved, but one can reasonably argue that aggression embraces the use of cyber weapons that cause damage to property or injury to human beings. The US Air Force defines weapons as 'devices designed to kill, injure, or disable people or to damage or destroy property'.[26]

But when does cyber attack qualify as use of force or armed attack? Most agree that it depends upon the circumstances and the consequences. Cyber attacks that cause physical damage or injury to people akin to damage or casualties in traditional war qualify as use of force and armed attack.[27] Cutting power from an air-traffic-control facility and causing a plane to crash would qualify as use of force, whether the attack was a denial of service to facility computer systems, disrupting their function, or insertion of viruses, worms or other malware to achieve the same result.

Cyber attacks that cause repairable physical damage with no long-term consequences and no injury to humans have not been treated as use of force or armed attacks. That has been the response, for example, to the thousands of incidents of network probes and penetrations against the US Department of Defense.[28] But would taking down critical infrastructure such as a nation's financial system, and causing serious disruption to commerce, the economy, jobs and lives, qualify as use of force? As a matter of practical politics, how would citizens or governments of Western countries respond were their financial institutions to be taken down? How does taking down those institutions through cyber attack differ from doing so through missile strikes? The answers to many such questions, for better or worse, will be driven by political, diplomatic and strategic considerations, rather than abstract debates about rules of international law.

The United States views cyberspace as a war-fighting domain that favours offense. Its policy explicitly seeks superiority in that domain. It has no declaratory policy for cyber weapons,[29] but the newly nominated commander of US Cyber Command, Lieutenant-General Keith Alexander, made clear that

the United States reserves the right to respond in cyberspace to a cyber attack launched against Department of Defense systems.[30] The Obama administration's approach is multilateral; a policy review stated that 'only by working with international partners can the United States best address these [cyber-security] challenges'.[31] Britain has called for international coordination on cyber-security strategy while securing advantage in cyberspace.[32]

Stuxnet may represent a new twist: first use of a cyber weapon, hidden within a shroud of ambiguity by the use of off-the-shelf and deniable resources drawn from the global cyber-crime community to help avoid attribution. But attribution is a matter of interpretation. The present de facto application of an onerous standard of evidence means states can sidestep culpability even for an event occurring in a segment of cyberspace over which they exert sovereign regulatory authority and jurisdiction. The traditional Law of Armed Conflict requires that one identify an attacker. In cyber war, that is difficult to do. Where attacks emanate externally, outside a targeted nation, there are huge questions about the responsibility of the victim to identify the physical location of a computer or network. As Herbert Lin, chief scientist at the Computer Science and Telecommunications Board of the US National Research Council, points out,

> you may have only an IP address, not a physical location that you can attack in response. Assume a computer controls an adversary's air defense network and you cannot physically locate it. If you go after it with a cyber attack, what if it's located in a neutral nation? Or on your own territory? Cyber war complicates matters and challenges traditional notions of neutrality and sovereignty.[33]

It should matter less, moreover, that a botnet used to attack Estonia and Georgia may have consisted of computers located in Europe and the United States than the fact that their controllers, or instructions for their command-and-control networks originated from IP addresses within the Russian Federation.

Changing the standards for attribution would shift the boundaries currently placing cyber outside of the laws of armed conflict and international

law and back under the UN Charter. It would also make cyber consistent with the US National Security Strategy, which since 9/11 holds nations responsible for harbouring a party that has launched an attack, and reserves the right to pre-emptive action to prevent, deter or interdict attack. Such a shift would also cast into high relief the issue of whether a response through cyber represents the option of first or last resort and meets the tests of necessity and proportionality under international law. As Lin points out, these issues as they apply to cyber remain untested: 'This is new territory and mandates new thinking as states develop policies for the future to counter and protect against cyber attack'.[34]

How nations respond – and how much support they can rouse in their defence against an attack – may depend upon their relative power and importance. In 2007, for example, that challenge confronted Estonia, which accused Russia of launching crippling denial-of-service attacks.[35] A NATO member, Estonia sought to invoke collective self-defence under Article V of the North Atlantic Treaty. NATO, however, declined to accuse Russia of armed attack. A frustrated Estonian Defence Minister Jaak Aaviksoo compared the denial of service event to terrorist activity. Tallinn claimed that the denial of service against national networks was coordinated by computers located within Russian cyberspace, and enjoyed at least the tacit concurrence of Russian authorities. In other circumstances, that might satisfy the criteria by which NATO ascertains whether an armed attack has occurred. Significantly, though, no permanent damage to property or injury to people occurred. Aaviksoo conceded that neither the EU nor NATO had defined 'what can be considered a cyber-attack or what are the rights of member states and the obligations of EU and NATO in the event such attacks are launched'.[36] He added: 'NATO does not define cyber-attacks as a clear military action. This means that the provisions of Article V ... will not automatically be extended.'[37]

Recourse to cyber attack is limited

Recourse to cyber attack by states is limited. Inevitably it will give rise, as in the case of Stuxnet, to questions as to whether action is justified under the UN Charter. Was the attack an action of self-defence against a clear and present danger, as those who support stopping Iran's nuclear programme

would probably contend, or was it an unjustified armed attack as well as unwarranted meddling in the internal affairs of another nation, prohibited under Article 2(4) of the charter?

Proportionality imposes another limitation. The right to wage war – *jus ad bellum* – requires proportional response to avoid collateral damage. What constitutes proportional response to an attack is an inherently subjective judgement. It matters to states that care whether their action is seen as legitimate. It may not matter to a nation that does not – or, when attacked, desires to send a strong message of future deterrence to an attacker.

The problem with depending upon the United Nations is that the process for recourse is slow, politically charged and largely useless in dealing with real-time attacks. But it raises an avenue for discussion, exposure and potential action that could prove diplomatically useful for longer-term problems. Iran would find the Security Council of little value in responding to Stuxnet. Its chances of obtaining a resolution supporting its position are zero. The more interesting question is what relief nations that sustain collateral damage might be able to obtain, perhaps in applying pressure to those who employ cyber attack to limit future operations in order to avoid such damage.

Where might debate as to the status of Stuxnet – or a future, more deadly version of it – as a use of force and armed attack lead? Israel and the United States would argue that action to retard or destroy Iranian nuclear facilities constitutes an act of self-defence against an existential threat, is not prohibited, prevents a potentially destructive arms race in the region, and is thus sanctioned by Article 51 of the charter.[38] Iran would argue that this interpretation stretches beyond reason the notion of self-defence and that Stuxnet was a prohibited interference in its internal affairs. While asserting a right to develop peaceful nuclear power, Iran has denied any intention to build nuclear weapons, even though centrifuges at Natanz make little sense except as part of an effort to achieve at least a threshold weapons capability.[39] It contends alternatively that its goals are purely defensive and represent no threat to non-aggressors.

* * *

It is not clear how much physical damage must be sustained to qualify an attack as use of force. In the context of the scale question, Lin asks 'is there (or should there be) a class of cyber attacks whose limited scope makes it a use of force, but nevertheless entitles the target to some action in self-defense that goes beyond protecting the immediate target?'.[40] There is also a corollary issue as to whether an attack that intends but fails to inflict greater harm fits into that category. The implications of these scenarios illustrate the complications that cyber attack holds for the future. Cyber attack is difficult to stop and hackers have proven the Internet is a viable channel through which to insert malware. That is why many argue for detaching critical infrastructure from the Internet or instituting tough security protocols to prevent penetration. Stuxnet adds a particular wrinkle: it appears that some computers were infected by inserting a memory stick. The operation required domain expertise. Media reports have suggested an inside job at an Iraninan nuclear facility, but that may be jumping to a hasty conclusion. Stuxnet infected computers in many countries, and it is not entirely clear how the worm was disseminated.

Cyber attacks carry a risk of collateral damage. As a plant that contains centrifuges that can be used to manufacture weapons-grade uranium, Natanz qualifies as a valid military target. Property in other nations that Stuxnet did not intend to strike does not. It is clear that Stuxnet damaged the property of a number of parties outside Iran, which sustained only 60% of the Stuxnet infections. Some of the damage in countries such as India, which had a satellite affected, may have been potentially serious. That creates a potentially serious risk of political blowback if the attacking parties are identified.

A well-executed cyber attack offers the opportunity for sophisticated targeting. But if damage from cyber attacks can be quickly repaired, careful strategic thought is required in comparing the cost and benefits of cyber versus traditional military attack. One important benefit of cyber attack, to be sure, may be its greater opportunity to achieve goals such as retarding the Iranian nuclear programme without causing the loss of life or injury to innocent civilians that air strikes would seem more likely to inflict.

Difficulty in identifying a cyber attacker presents multiple headaches for responding. Nations such as Iran or Israel will act to protect their interests,

but they would prefer the international community recognise the legitimacy of the action they take. The Law of Armed Conflict and Article 51 effectively condition self-defence upon proving the attacker's identity. It is not clear what degree of certainty in identification is required to justify a response. Launching a response against an innocent party would qualify as an act of aggression, not self defence. Stuxnet offered a clear advantage over air strikes where the attackers can be easily identified. In this case, however, Israeli bloggers trumpeted Israeli participation. That helped make it appear culpable, easing Iran's burden should it elect to retaliate.

Although there is no hard evidence that Stuxnet has exposed Ahmadinejad to public criticism that the government failed to competently defend key installations, cyber can nevertheless be a tool to discredit, destabilise and weaken the authority of adversarial regimes. Cyber also offers great potential for striking at enemies with less risk than using traditional military means. For example, North Korea poses threats other than through its nuclear programme. It is involved, for example, in extensive counterfeiting. Cyber attack offers potential options that may prove effective in countering such criminal activity. Cyber is, moreover, less costly than traditional military action. It is unclear how much the Stuxnet program cost, but it was almost certainly less than the cost of single fighter-bomber.

Cyber is less costly than military action

Third parties currently working in concert with a state may or may not be held under tight control. Criminal groups are mercenary. They may well sell their services twice. Outsourcing to the underworld is a slippery slope. On the flip side, however, the evolution of cyber strategies may place the United States, in particular, at some disadvantage compared to other nations that do outsource cyber attacks to third parties or rely on them for help in dealing with cyber threats. The Computer Fraud and Abuse Act[41] imposes strong constraints on the US ability to outsource cyber activities, at least to US citizens.

A key strategic risk in cyber attack, finally, lies in potential escalatory responses. Nations such as Iran and North Korea are presumed to have access to sophisticated cyber capabilities. Effective cyber attacks by such

nations on critical infrastructure could create significant problems. The same issues of attribution that afflict Iran with regard to Stuxnet will afflict other nations' ability to respond, especially in light of the staggering number of cyber attacks to which Western nations are already subject. We may prove more vulnerable than they are. Indeed, a report sent to Congress in mid-December warned that Stuxnet could be adapted into a weapon that could cause widespread damage to critical infrastructure in the United States[42] Strategies for using cyber weapons like Stuxnet need to take into account that adversaries may attempt to turn them back against us.[43]

Notes

1 Symantec says the discovery was in July 2010; other media reports put it in June. *Computer World* reports that researchers at the Belarussian security firm VirusBlokAda found it in July on computers in Iran. See Robert McMillan, 'Siemens: Stuxnet Worm Hit Industrial Systems', *Computerworld,* 14 September 2010, http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems; Mark Clayton, 'Stuxnet Malware is "Weapon" Out to Destroy … Iran's Bushehr Nuclear Plant?', *Christian Science Monitor*, 21 September 2010; Mark Clayton, 'How Stuxnet Cyber Weapon Targeted Iran Nuclear Plant', *Christian Science Monitor*, 16 November 2010; John Makoff, 'A Silent Attack, but not a Subtle One', *New York Times*, 26 September 2010. Symantec reverse-engineered Stuxnet and issued a detailed technical report on its operation: Nicolas Falliere, Liam O Murchu and Eric Chien, 'W32.Stuxnet Dossier', *Symantec Security Response*, Version 1.3, November 2010. In cyber talk, a 'worm' is a malicious program or code inserted into computer systems without user permission or knowledge. They spread automatically from computer to computer and can replicate themselves hundreds of thousands of times. See 'Worms', OnlineCyberSafety, http://www.bsacybersafety.com/threat/worms.cfm.

2 Clayton, 'Stuxnet Malware is "Weapon"'. Langner has written extensively on Stuxnet on his blog at http://www.langner.com/en/. See especially Ralph Langner, 'The Big Picture', 19 November2010, http://www.langner.com/en/2010/11/19/the-big-picture/.

3 McMillan, 'Siemens: Stuxnet Worm Hit Industrial Systems'.

4 *Ibid*.

5 See G. Garza, 'Stuxnet Malware Used 4 Zero-day Exploits', 7-windows.com, 14 September 2010, http://www.7-windows.com/stuxnet-malware-used-4-zero-day-exploits/.

6 McMillan, 'Siemens: Stuxnet Worm Hit Industrial Systems'.

7 Clayton, 'Stuxnet Malware is "Weapon"'; William J. Broad and David E. Sanger, 'Worm was Perfect for Sabotaging Centrifuges', *New York Times*, 18 November 2010.

8 Eric Chien, 'Stuxnet: A Breakthrough', Symantec.com, 12 November 2010, http://www.symantec.com/connect/blogs/stuxnet-breakthrough.

9 David E. Sanger, John Markoff and William Young, 'Iran Fights Malware Attacking Computers', *New York Times*, 25 September 2010; William Yong, 'Iran Denies Malware Connection to Nuclear Delay', *New York Times*, 5 October 2010; William Yong, 'Iran Says it Arrested Computer Worm Suspects', *New York Times*, 2 October 2010.

10 See US–China Economic and Security Review Commission, *2009 Report to Congress*, November 2009, http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf; Alexander Klimburg, 'Mobilising Cyber Power', *Survival*, vol. 53, no. 1, February–March 2011, pp. 41–60 (this issue).

11 Ronald Deibert, Rafal Rohozinski and Masashi Crete-Nishihata, 'Cyclones in Cyberspace: Information Shaping and Denial in the 2008 South Ossetia War', unpublished ms, forthcoming 2011.

12 See http://www.infowar-monitor.net/.

13 See, for example, Jeffrey Goldberg, 'The Point of No Return', *Atlantic*, September 2010. Goldberg interviewed a number of insiders and reported on what he perceived as a consensus that Israel would act.

14 See most recently Dana Allin and Steven Simon, *The Sixth Crisis: Iran, Israel, America and the Rumors of War* (New York: Oxford University Press, 2010); Steven Simon and Ray Takeyh, 'If Iran Came Close to Getting a Nuclear Weapon, Would Obama Use Force?', *Washington Post*, 1 August 2010; Kori Schake, 'Foreign Policy: Iran Sanctions Are Not Tough Enough', *Foreign Policy*, 10 June 2010; Trita Parsi, 'Want to Defuse the Iran Crisis?', *Foreign Policy*, 12 November 2010; Goldberg, 'The Point of No Return'; Dan Murphy, 'Could an Israeli Air Strike Stop Iran's Nuclear Program?', *Christian Science Monitor*, 13 October 2009; Scott Peterson, 'Iran War Games Begin with "Ultra Fast" Speed Boats', *Christian Science Monitor*, 22 April 2010; Robert D. Kaplan, 'Living with a Nuclear Iran', *Atlantic*, September 2010; and Sam Gardiner, *The Israeli Threat: An Analysis of the Consequences of an Israeli Air Strike on Iranian Nuclear Facilities* (Stockholm: Swedish Defence Research Agency, March 2010).

15 For Netanyahu's statements see Dan Murphy, 'Repercussions of an Israeli Attack on Iran', *Christian Science Monitor*, 12 August 2010.

16 Ian Black and Simon Tisdall, 'Saudi Arabia Urges US Attack on Iran to Stop Nuclear Programme', *Guardian*, 29 November 2010; 'WikiLeaks and Israel – Quiet Relief, Louder Vindication, for Now', *Los Angeles Times*, 29 November 2010; Andrea Stone, 'WikiLeaks: Arabs Agree that Iran is a Threat', AoLNews.com, 29 November 2010, http://www.aolnews.com/2010/11/29/wikileaks-arabs-agree-with-israel-that-iran-is-a-threat/.

17 Abbas Kadhim, 'Shi'a Perceptions of the Iraq Study Group Report',

Strategic Insights, vol. 6, no. 2, March, 2007; Ian Black, 'Fear of a Shia Full Moon', *Guardian*, 26 January 2007. See also Bob Woodward, *The War Within* (New York: Simon and Schuster, 2008), pp. 258–9, which illustrates that anti-Iranian fears are hardly new. He reported that Gulf Cooperation Council ministers expressed worries to US Secretary of State Condoleezza Rice about the threat they felt Shi'ites posed to Sunni Muslims in the region.

18 Goldberg, 'The Point of No Return'.

19 Scott Lucas, 'Is the Stuxnet Worm a State-directed Cyber-attack on Iran?', *EAWorldView,* 26 September 2010, http://www.enduringamerica.com/home/2010/9/26/is-the-stuxnet-worm-a-state-directed-cyber-attack-on-iran.html, quoting the semi-official Mehr News Agency; 'Iran Identifies Sources of Stuxnet Virus in its Computers', Radio Samaneh/Payvand.com, 21 October 2010, http://www.payvand.com/news/10/oct/1169.html.

20 Gautham Nagesh, 'Iran Says Stuxnet Damaged its Nuclear Program', The Hill, 29 November 2010, http://thehill.com/blogs/hillicon-valley/technology/130965-iran-says-stuxnet-damaged-its-nuclear-program.

21 McMillan, 'Siemens: Stuxnet Worm Hit Industrial Systems'.

22 William J. Broad, 'Reports Suggests Problems with Iran's Nuclear Effort', *New York Times*, 23 November 2010.

23 John Markoff and David E. Sanger, 'In a Computer Worm, a Possible Biblical Clue', *New York Times*, 29 September 2010.

24 The notions of 'use of force' under Article 2(4) and 'armed attack' under Article 51 of the UN Charter are linked to one another and to the notion of 'aggression'.

25 UN General Assembly Resolution 3314 (XXIX), , Article 3(b), http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf.

26 US Department of the Air Force, 'Compliance with the Law of Armed Conflict', Policy Directive 51-4, 1993, para. 6.5.

27 See William A. Owens, Kenneth W. Dam and Herbert S. Lin (eds), *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington DC: National Academies Press, 2009), p. 251 and Appendix D, p. 356, summarising Michael Schmitt and Duncan Hollis. Schmitt cited a spectrum of possibilities: shutting down an academic network temporarily, which was not use of force; physical destruction or a pipeline, which qualifies; and causing death by shutting down power to a hospital with no back-up generators, which qualifies. Hollis opposes extending the laws of armed conflict to cyber attack. The consequences of cyber attack, such as against a stock exchange, may or may not cause immediate death or destruction. Should that count as use of force? He finds preserving the distinction between civilian and military entities difficult. He argues that traditional LOAC ignores the issues of states against non-state actors and sub-national entities and that applicable rules are unclear. We agree with Schmitt. Hollis raises interesting points, but in real-world politics, those obstacles are unlikely to deter attacked

states from taking action they believe appropriate, especially where they can sheath them in a cloak of legitimacy.

28 A report submitted to the US Congress in 2009 reported that in 2008, 54,640 cyber attacks were launched against the US Department of Defense, a steep increase from 43,880 attacks in 2007. General John Davis, deputy commander for network operations at the US Cyber Command, has stated that in just the first six months of 2009, the military spent $100 million repairing damage caused to its networks by cyber attacks. Although concerns are growing, no party was accused of conducting armed attack against the United States. See US–China Economic and Security Review Commission, *2009 Report to Congress*, p. 168.

29 See Peter Pace, 'National Military Strategy for Cyber Space Operations', unclassified memo, December 2006, available at http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf; *Cyberspace Operations*, Air Force Doctrine Document 3-12, 15 July 2010, available at http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf.

30 'Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command', http://armed-services.senate.gov/statemnt/2010/04 April/Alexander 04-15-10.pdf, pp. 19, 24.

31 White House, 'Cyberspace Policy Review', May 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, p. 20.

32 'Cyber Security Strategy of the United Kingdom – Safety, Security and Resilience in Cyber Space', UK Cabinet Office, June 2009.

33 Interview with Dr. Herbert Lin.

34 *Ibid.*

35 See Ian Traymor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia', *Guardian*, 17 May 2007; 'NATO Says Urgent Need to Tackle Cyber Attack', Reuters, 21 June 2007; Evgeny Morozov, 'The Fog of Cyberwar', *Newsweek*, 18 April 2009.

36 Traymor, 'Russia Accused of Unleashing Cyberwar'.

37 *Ibid.*

38 See, for example, W. Michael Reisman, 'Criteria for the Lawful Use of Force in International Law', *Yale Journal of International* Law, vol. 10, 1985, pp. 279, 281; W. Michael Reisman, 'The Use of Force in Contemporary International Law', *American Society of International Law Proceedings*, vol. 78–79, 1984–85, pp. 79–84; W. Michael Reisman, 'War Powers: The Operational Code of Competence', *American Journal of International Law*, vol. 83, 1989, p. 777; and Michael N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', *Columbia Journal of Transnational Law*, vol. 37, 1999, p. 885.

39 'Iran's Rights to Nuclear Non-negotiable: Ahmadinejad', *Reuters*, 10 November 2010; 'Ahmadinejad: Iran is Now a "Nuclear State"', Associated Press, 11 February 2010.

40 Interview with Dr Herbert Lin.

41 18 USC 1030, amended in 1988, 1994, 1996, 2001 (by the USA Patriot Act),

2002 and 2008 (by the Identify Theft Enforcement and Restitution Act), places severe penalties upon US parties who cause at least $5,000 of damage to another party's computer.

42 Paul K. Kerr, John Rollins and Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, CRS Report for Congress R41524 (Washington DC: Congressional Research Service, 9 December 2010).

43 Mark Clayton, 'Stuxnet "Virus" Could Be Altered to Attack U.S. Facilities, Report Warns', *Chrisian Science Monitor*, 15 December 2010.