The New Reality of Cyber War
James P. Farwell & Rafal Rohozinski

To cite this article: James P. Farwell & Rafal Rohozinski (2012): The New Reality of Cyber War, Survival: Global Politics and Strategy, 54:4, 107-120
To link to this article: http://dx.doi.org/10.1080/00396338.2012.709391

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: http://www.tandfonline.com/page/terms-and-conditions

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae, and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand, or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.
The June 2012 report by New York Times chief Washington correspondent David Sanger that the Stuxnet cyber worm was only part of a broader operation, Olympic Games, launched against Iran by the United States and Israel affirmed what many suspected: cyber attack is not a distant theoretical probability.¹

Stuxnet was the first alleged identified instance of weaponised computer code or malware employed as a ‘use of force’. But it was not alone. Two other targeted computer viruses for espionage have surfaced: Duqu in September 2011, followed by Flame in May 2012. Media reports allege that both also targeted Iran.² As tools of espionage, use of neither would qualify as a use of force, but reflect new emphasis on cyber tools. Of the two, Flame drew wider attention. Apparently 20 times more complex than Stuxnet, Flame affected computers in Lebanon, the United Arab Emirates, the West Bank and Iran. It is said to have gathered intelligence by logging keyboard strokes, recording conversations by activating microphones, and taking screen shots. At Iran’s oil ministry and oil-export terminal, the virus also erased information on hard discs while gathering information.³ Many attribute it to the United States and Israel. These allegations remained unconfirmed by either government.
A new era

These developments put the spotlight on a new era of international engagement. Israeli sources have long boasted about Israel’s involvement in Stuxnet. The US/Israeli use of Stuxnet as reported in detail by Sanger has arguably created a new de facto norm for the conduct of cyber engagements other nations can follow or imitate. Previously, a key constraint on the use of software as a weapon has been the potential for legal liability arising out of collateral damage inflicted upon innocent parties not targeted. In practice, software can be narrowly targeted to surmount that challenge.

What Stuxnet shows is that it is possible to have the specific intended effect while avoiding or minimising unplanned side effects by clearly differentiating between the propagator, or boost-phase code that disseminates the program, and the actual payload code that creates the physical effect on a target (the distinction between the gift wrapping and the gift). The reported operation did apparently limit the scope of damage. Stuxnet shows that one can surmount concerns that malware would take down the global network, not just a specific target. The lesson is that cyber weapons are in a different category from nuclear devices, which have little practical use except as a deterrent.

The rules of conduct for the use of code are evolving. As parties develop more sophisticated capabilities and acquire experience in their use, the picture will grow more complicated and nuanced. The strategic situation contains echoes of the period between the two world wars, when rapid developments in new technologies and domains of war-fighting preceded an understanding of how effectively to employ them operationally. Tanks changed the way armies engaged in battle. But despite British and German experimentation with armour in the inter-war period, armoured tactics could only be proven and fully developed on the battlefield from 1939 onwards. There are, moreover, significant differences of view about whether the Germans, renowned for their blitzkrieg tactics, properly understood the strategic use of armour for manoeuvre warfare.

Reports that two states have employed code against another state against which war has not been declared undercuts the common view that risks of escalation render state-to-state cyber war implausible. Sanger reported
that President George W. Bush, under whom *Olympic Games* was apparently initiated, desired that use of Stuxnet not violate the rules of armed conflict. The Law of Armed Conflict does not prohibit damage to such critical infrastructure. But a strength of using code is that the targeting process can manage the risks.

Stuxnet may appear as embryonic as the British Mk.1 tanks that made their debut at the Battle of the Somme in 1916. But technology moves quickly. Modern states rightly fear cyber war. Evolving technology is accelerating the flow of information, placing unique pressures on decision-making. Responding to cyber attack may require making decisions at network speed using systems that are themselves targeted. The potential for cascading effects is amplified by the interconnectedness of cyberspace. Stuxnet worked leisurely. Future combat in cyberspace may be more akin to the global trading system than existing forms of kinetic engagement, and present a different strategic calculus.

**Active defence versus first strike**

As described by Sanger, *Olympic Games* puts into question the existing discourse over US doctrines of active defence versus offensive use of malware and the strategic communication employed to explain US actions. Nations have been rightfully unwilling to disclose their doctrines for the offensive use of cyber weapons. Open-source discourse has centred on delineating passive and active defence. No nation has been willing to declare its intent to use cyber weapons offensively for a first strike. But Stuxnet blurs the lines between what might constitute active defence and offense. It also moves the impact from the strictly cyber realm to one that may entail mechanical or physical damage.

Passive cyber defence is easiest to grasp. The notion includes firewalls, cyber ‘hygiene’ that trains an educated workforce to guard against errors or transgressions that can lead to cyber intrusion, detection technology, ‘honey pots’ or decoys that serve as diversions, and managing cyberspace risk through collective defence, smart partnerships, information training, greater situation awareness, and establishing secure, resilient network environments.
Active cyber defence is a more elusive notion. Industry operates under different legal constraints than the military and they view the notion of active defence differently. For industry, the notion includes working actively with private-sector partners to identify and interdict cyber intrusions. Action beyond that raises real concerns. Under US law causing more than $5,000 of damage to another computer is a felony.\textsuperscript{7} US anti-trust\textsuperscript{8} and privacy laws\textsuperscript{9} raise other concerns. Yet private industry owns and operates 90\% of US civilian critical infrastructure. Its concerns will grow as future malware come into play, for current laws and operational capabilities provide inadequate defences.

The public sector operates under different rules. While private parties can take action unless prohibited by law, the military can act only within its prescribed authority. As a result, the military’s notion of active defence remains unformed: no one is certain what it means or how to apply it. The Pentagon has made clear it would employ force to defend against cyber attacks.\textsuperscript{10} But who has the authority to launch what actions, and under what circumstances? If a hostile force targets a naval cruiser for imminent attack, does the captain hold the authority to launch a pre-emptive attack? If he doesn’t, who does? Should he try to move his vessel out of danger? What if he cannot? How can he ‘actively’ mount a defence?

US Cyber Command Chief General Keith Alexander has declared that ‘a Commander’s right to self-defence is clearly established in both U.S. and international law’.\textsuperscript{11} He did not define what that entails. Would it include hot pursuit? Former US Air Force Secretary Michael Wynne has stated that US law allows ‘hot pursuit’ of criminals, enabling law enforcement to track and address cyber crime through the digital world.\textsuperscript{12} That doctrine is well accepted in crime fighting,\textsuperscript{13} but where it applies may hang on the status of an attacker. What rules govern may depend upon the status of an event as criminal activity, a military attack or a terrorist action.

Hot pursuit may well apply in cyberspace. Many concur that the law of the sea sanctions the use of the doctrine in the maritime domain,\textsuperscript{14} which along with air, land, and space is viewed as a global commons. President Barack Obama has declared that cyberspace is also a ‘recognized strategic commons’.\textsuperscript{15}
A use of force?

For the most part, the US discussion on cyber war has revolved around these notions of defence. But *Olympic Games* has apparently shown that the United States and Israel will use cyber weapons offensively.

The United States has previously said that its cyber strategies would respect international law. The key normative standards nest in United Nations Charter articles 2(4) and 51. Article 2(4) prohibits the ‘threat or use of force against the territorial integrity or independence of any state’. Article 51 states that nothing ‘in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations’.

But ‘force’ is not defined. There is no international convention that defines whether the use of software code should be deemed equivalent to the use of force. Cyber expert Herbert Lin has argued that the term almost certainly covers conventional-weapon attacks that injuring persons or irreparably damage property, but excludes economic or political acts (such as sanctions) that do not. In that view, Stuxnet would have constituted a use of force only if it had inflicted damage comparable to a kinetic attack, but it injured no one and the Iranians make no claim of irreparable physical damage.

But the US government apparently did view *Olympic Games* as a use of force. The strategic objective was not only to retard Iran’s progress in developing nuclear weapons but to persuade Israel that using cyber weapons mooted the need for a kinetic attack on Tehran’s nuclear institutions. Both the G.W. Bush and Obama administrations strongly believed that Iran’s nuclear-weapons programme had to be stopped. The United States has clearly felt a need to communicate that it would not tolerate Iranian intransigence. Former CIA Director Michael Hayden stated that:

> This is the first attack of a major nature in which a cyberattack was used to effect physical destruction. And no matter what you think of the effects – and I think destroying a cascade of Iranian centrifuges is an unalloyed good – you can’t help but describe it as an attack on critical infrastructure.
This implies that the Obama administration was willing in this case to affirm G.W. Bush’s policy of pre-emption to deal with a threat deemed vital to national security interests, was willing to act in concert with a ‘coalition of the willing’ (even if the United States and Israel were the sole partners) to keep weapons of mass destruction out of the hands of rogue states,\(^{18}\) and that this concern trumps commitments – including those expressed in the US 2011 Cyber Strategy,\(^ {19}\) to embrace multilateralism and partnership for cyber strategy.

It seems evident that the intent of *Olympic Games* was to irreparably damage critical infrastructure. The tenor of the operation and strategic intent – and Hayden’s words – strongly imply that White House and Department of Defense lawyers considered the operation a use of force. The issue must have been considered. One can presume the answer the lawyers provided was affirmative.

Legally, did the White House exceed its jurisdiction either under the Constitution, which reserves to Congress the right to declare war, or under the War Powers Resolution of 1973?\(^ {20}\) It is hard to qualify *Olympic Games* as an act of war. US statute defines that as armed conflict, whether or not war has been declared, between two more nations or between military forces of any origin.\(^ {21}\) It is significant that Iran has not suggested the use of Stuxnet constituted an act of war.

The War Powers Resolution offers a more nuanced issue. The resolution applies to the introduction of ‘United States Armed Forces into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances’.\(^ {22}\) How does a nation use force except through military means? One can debate whether non-uniformed Stuxnet operations personnel qualify under the notion of distinction as combatants, but one can make a strong argument that *Olympic Games* fell under the ambit of the resolution. Presumably the response is that it constituted a covert action that did not trigger the operation of the law.

Given that the objective was to destroy an enemy’s critical war-fighting capacity, though, one might wonder whether the logic in avoiding the jurisdiction of the resolution – or Congress’s power to declare war – would apply to a modern Pearl Harbor. The air war in Libya may offer a clue to policy mindsets. Denying any obligation to ask Congress for authorisation to act,
the Obama administration argued that ‘U.S. operations do not involve sustained fighting or active exchanges of fire with hostile forces, nor do they involve ground troops’. Similarly, Stuxnet did not involve armed fighting or exchanges of fire with hostile forces, although future engagements may focus debate on what constitutes armed forces. That cyber weapons often do not entail uniformed individuals firing rockets, dropping bombs, or firing guns does not, looking over the horizon, inherently render its users non-combatants.

What if Iran decided to respond kinetically? How does that alter the authority of the White House to continue a programme? Stuxnet was a fire-and-forget weapon. Although code can be designed to hit a specific target, in practice, once launched, there was no control over the consequences it inflicted – or upon whom. Indeed, Sanger reported that American officials were quite unhappy when Stuxnet got loose on the Internet. The operational environment in war is random. The collateral effects of a cyber weapon add a new dimension to that challenge. One must think beyond the Iranian situation. What if Congress wanted a president to cease an operation that could not be terminated? Olympic Games side-stepped the problem, but hardly obscures the need for future strategic thinking.

Whether there was use of force raises other issues. Olympic Games involved a pattern of engagements. One must consider the larger implications of an individual event. Does a pattern convert employment of cyber weapons into a use of force? The answer isn’t clear. The unpredictable nature of damage that cyber attack can inflict may require a new definition of war.

Intent may also matter in determining whether an engagement constituted a use of force. Open-source reporting indicates that any damage inflicted on the Natanz uranium-enrichment facility was temporary and reparable. But that was not the intent. What if someone dropped a bomb on London or New York that failed to detonate? Isn’t that a use of force – or possibly, depending on the facts, an act of war? Deciphering intent may pose a challenge, but in law it may be objectively inferred. The case of unexploded ordnance seems easier to grasp, but how deep is the distinction between that and a cyber worm that fails? This issue needs debate and should enter future strategic calculations.
Finally, did Article 51 of the UN Charter justify *Olympic Games*? Like ‘force’, ‘armed attack’ remains undefined, even where force is clearly employed. Certainly the implications of new technologies for Article 51 or other international conventions remain unclear. This consideration matters enormously to Israel, which contends that a nuclear first strike would destroy the nation, preventing or mooting a response. Washington worries about Israeli security, but also a potential and de-stabilising Middle East arms race should Iran acquire a nuclear weapon.

**Strategic implications**

The use of malware by state actors has altered the realities of cyber attack. History teaches that once weapons technology becomes feasible, states deploy it. Today the world may confront a dangerous technology race characterised by rapidly evolving and lethal weapons.

Clausewitz believed that in warfare, the advantage rested with the defence. Cyber reverses that equation. It also offers the potential to build the fog of war through the ability to effect disruption, deception, confusion and surprise. We are only beginning to envisage the potential for different forms of malware, or the strategies or tactics employed to use it.

A cyber-security tool may require millions of lines of code and a complex system to track and identify events. Malware requires a lot less. Computer code can be designed to evolve rapidly, mutating faster than defences can be mustered. Code can be highly targeted. It can leverage social and technological vectors. It can render a cyber defence obsolete within seconds. It can overwhelm a system that may have taken years to construct. Clausewitz believed that the advantages enjoyed by defence required that an offense employ greater resources. Cyber reverses that equation. Nations may now shift away from a refusal to use cyber weapons for first strike. That in and of itself complicates both offensive and defensive strategies.

Although some have argued that *Olympic Games* lowered the threshold for the use of cyber weapons, it may in fact actually raise it. States may recognise a higher responsibility to design weapons that offer strong assurance of striking only the intended targets. That was the intent of Stuxnet’s planners and designers. But matters could have worked out much differ-
ently. Robert Burns was right: the best laid plans of mice and men often go awry.

Stuxnet shows that creating effective malware turns on imagination, technical expertise and ingenuity. But to deliver code as a warhead also requires highly specific domain experience and superior intelligence capabilities that often only states possess. Our view is that malware is not a wide-area weapon. As it evolves, it will be used narrowly to attack particular targets and to generate specific shaping effects.

*Olympic Games* raises the veil on key strategic implications. Stuxnet aimed to destroy a specific capability. But it importantly illustrates the political nature of war. Achieving a strategic political objective does not necessarily require destroying an enemy. *Olympic Games* was devised when G.W. Bush pushed for an alternative to the unpleasant choice between allowing Iran to develop a nuclear-weapons capability or halting the programme through kinetic attack. The cyber programme bought time in which to employ punishing sanctions and to signal to Iran that other nations would not tolerate an Iranian nuclear-arms programme. The lesson is that cyber weapons may offer non-kinetic ways to disrupt an operational capability of an adversary.

Future cyber weapons will similarly aim to constrain the ability of an adversary to manoeuvre, coordinate or synchronise, and to divert enemy commanders from focusing on the achievement of their own objectives. Stuxnet succeeded splendidly in creating confusion. Sanger reports that Iranians came to distrust their own instruments. The idea, he quotes one source, ‘was to mess with Iran’s best scientific minds’ and ‘make them feel they were stupid’.25

Conceptually, unsettling the consciousness of an adversarial commander, or a CEO or government official, causing a loss of belief in his ability to control events and depriving him of control, helps disrupt an adversary’s ability to fulfil its objectives. Stuxnet’s creators merit high marks for recognising the value of that goal. While the final result fell short, open-source reporting indicates that Stuxnet did retard Iranian progress.

As reported in open sources, *Olympic Games* exemplified an operation intended to reduce the resistance of a rival system and to inflict attrition upon its resources. Destruction of an asset is one of many potential objec-
tives that cyber weapons can achieve. Future cyber weapons may disrupt communications systems or the ability of adversaries to cohesively operate air, naval or ground forces. They could slow the speed at which an adversary is able to mass forces or deploy assets, destroying precious momentum vital for an adversary’s offense. Indeed, smart strategy is often less about destroying an enemy than paralysing command and control, and neutralising an adversary’s operational ability.

One unfortunate development has been the leaks from Washington and Israel (where sources have long claimed credit for Stuxnet) about Olympic Games. These present a strategic challenge. An obstacle confronting any nation that wishes to retaliate against a cyber intrusion is the need to identify the intruder. The leaks solved that problem for Iran, and opened the United States and Israel to potential counterpunches that would entail far less stigma for Tehran than action against a putative attacker whose guilt could not be confirmed.

Finally, it is worth noting that the weapons employed by Olympic Games are largely indistinguishable from the technology that cyber criminals employ. That will make international treaties and conventions aimed at limiting cyber crime more difficult to secure. The utility and effectiveness of these weapons for national-security interests may trump policy considerations that favour better global policing of cyber crime.

* * *

There has been a widespread view that criminal entrepreneurs or state-sponsored proxies, acting at arm’s length to insulate states from culpability for their policies, would emerge as the real challenges in a cyber era in which one individual can change the way the world does business. But now it seems that state-to-state engagement, whether or not it meets the conventional definitions of the use of force or an act of war, will define a new reality and require new strategic calculations. The discourse arising out of reports about Olympic Games underscores why the United States and other countries should engage in a transparent debate over whether or how cyber weapons should be employed. Every nation – including civilian as
well as government institutions – must develop strategies to address these new realities.

Notes

1 David E. Sanger, ‘Obama Order Sped Up Wave of Cyberattacks Against Iran’, Washington Post, 1 June 2012. Sanger lays out his report in Confront and Conceal: Obama’s Secret Wars and Surprising Use of American Power (New York: Crown, 2012), ch. 8. Although some wondered whether the White House had foolishly leaked the story, Sanger’s book makes clear that he had access to sources with insider knowledge. He makes clear that former CIA Director Michael Hayden refused to discuss what he knew while holding that job and that, far from wanting to leak the secret, President Barack Obama wanted to preserve its secrecy.

2 The Jerusalem Post reported that Israel created both. ‘Israel Admits to Waging Cyber War on Iran’, Fars News Agency, 29 May 2012. See also Ellen Nakashima, Greg Miller and Julie Tate, ‘U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say’, Washington Post, 19 June 2012.

3 Nick Hopkins, ‘Computer Worm that Hit Iran Oil Complex “is Most Complex Yet”’, Guardian, 28 May 2012, http://www.guardian.co.uk/world/2012/may/28/computer-worm-iran-oil-w32flamer.

4 Sanger, Confront and Conceal, Kindle location 3108/7721.

5 Eligible Receiver was a 1997 US operation to test US Department of Defense planning and crisis/action capabilities when faced with attacks on DoD information structure. It revealed significant vulnerabilities to cyber attack and led to a new focus on cyber security. A breach of US military classified systems by the Agent/btz worm led to a Pentagon effort, Operation Buckshot Yankee, to disinfect worms. The operation led the armed forces to revamp information defences and create the US Cyber Command. See Kim Zetter, ‘The Return of the Worm that Age the Pentagon’, Wired, 9 December 2011, http://www.wired.com/dangerroom/tag/operation-buckshot-yankee/.


7 Computer Fraud and Abuse Act, 18 USC 1030.

8 See Sherman Antitrust Act (Sherman Act), 15 USCA 1-7, as amended by the Clayton Anti-Trust Act of 1914, 15 USC 12 et seq, notably Section 1(a); the Federal Trade Commission Act of 1914, 15 USCA 45 et seq, notably Section 5 that applies to unfair methods of competition. The Sherman Act prohibits business activities that reduce competition in the marketplace and requires the federal government
to investigate and pursue trusts, companies and organisations it suspects may violate the act. It makes illegal contracts, combinations in the form of trusts or otherwise, or conspiracy, in restraint of trade or commerce. The FTC Act authorises the commission to enforce the anti-trust laws.

9 18 USC 2510, et seq and 18 USC 2701-12. This legislation deals with protecting the privacy of stored electronic communications. The PATRIOT Act, 18 USCA 1 (Pub. L. 107-56, 107th Congress) et seq. arguably weakened some provisions of the ECPA.


16 See James P. Farwell and Rafal Rohozinski, ‘Stuxnet and the Future of Cyber War’, Survival, vol. 53, no. 1, February–March 2011, pp. 23–40. The article summarises the debate on whether a kinetic strike against Iran made the most sense.

17 Sanger, Confront and Conceal, Kindle location 3215/7721.


19 Department of Defense Strategy for Operating in Cyberspace, July 2011, http://www.defense.gov/news/d20110714cyber.pdf. The 4th Strategic Initiative it sets forth emphasises the need to ‘build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity’ (p. 9). The language is especially relevant as the United States views Iranian acquisition of nuclear weapons as a global threat, not one merely to the United States or Israel.


21 See 18 USC 2331.

22 50 USC 1542.

Sanger, Confront and Conceal, Kindle locations 3279–87/7721.
Ibid., Kindle location 3206/7721.
See Shimon Naveh, In Pursuit of Military Excellence: The Evolution of Operational Theory (New York: Frank Cass Publishers, 1997). A retired Israeli Defense Forces Brigadier, General Naveh is a strong proponent of operational strategies that achieve these objectives in a systematic, cohesive manner. This section of the paper adapts some of his ideas.