In Defense of Stuxnet

James A. Lewis

Revelations about Stuxnet and Flame have provoked a chorus of dire warnings on the dangers of cyber warfare and the need for action. Yet the most troubling question to emerge from these revelations is why, if cyber warfare is such a critical issue, are so many people so badly informed about it? Suggestions that Stuxnet or Flame have increased risk are based on a faulty understanding of how much risk already exists in cyberspace, the already high frequency of state-sponsored malicious cyber action,[1] and the rapid growth in many countries' military capabilities. It is, rather, more accurate to see Stuxnet and Flame as episodes in the ongoing contests between the US, Iran, and Russia.

The belief that Stuxnet increases risk to the US or its allies is based on a number of erroneous assumptions. Notions of blowback, collateral damage, or opening a Pandora's Box do not make sense in the context of how cyber attack techniques have been used and have evolved over the last three decades. Stuxnet did not reveal a new military capability that others will be quick to copy. Cyber attack is a recognized military and intelligence capability that has been in use for years. Perhaps forty states are acquiring or have already acquired military cyber capabilities,[2] including the ability to launch cyber attacks. Most of these national programs are shrouded in secrecy, and there is disagreement on how existing international law that governs armed conflict should apply to the new mode of attack. However, every advanced military already has a cyber attack capability and many other nations wish to acquire it.

The allegation about the US role in Stuxnet was not much of a surprise; most nations had already concluded that the US was responsible, and they were not astonished to see software become a tool of coercion and attack.

Dr. James A. Lewis is a senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies (CSIS).

The use of cyber techniques as intelligence tools dates back to the 1980s; cyber attack by militaries dates back to the 1990s.[3] The development of offensive cyber techniques has accelerated in this century, when high speed global networks became widely available and the internet moved from being an accessory to being the central infrastructure for economic and governmental activity. Whether it is "network-centric" warfare or "warfare in informatized conditions" (as China puts it), cyber attack is not new to military planners.

From Espionage to Attack

Although Stuxnet and Flame have been hailed as the dawn of cyber war, this is mistaken on several counts. Cyber attack is not new, and while sabotage may involve the use of force, not all acts of sabotage count as an act of war. Calling Stuxnet and Flame cyber war perpetuates the exaggeration and imprecise reasoning by analogy that has dogged inquiry into cyber security from the start. Cyber "attack" offers new tools for coercion, espionage, and attack rather than an unprecedented and unique category of conflict.

The line between espionage and attack in cyberspace is very thin. The network penetration and control necessary for espionage could be used to disrupt critical services. An opponent who can gain controlling access to a network can also disrupt and perhaps destroy. One way to think of cyber attack is as the "weaponization" of signals intelligence, transforming the passive collection of information into active disruption. This means, to put "cyber disarmament" in context, that to ban cyber attack we would also need to ban espionage, an activity that no nation will agree to abandon.

Flame was one of the many intelligence collection programs that are found on the internet. There is public knowledge of a dozen programs like Flame used for cyber espionage. Technology has changed how nations spy on each other and cyber espionage has become a central element of national collection programs. The internet has created what some intelligence officials call a "golden age" for espionage.

This golden age is entering its third decade. In the early 1980s, Russian intelligence services used West German hackers to penetrate US military and research networks and exfiltrate information. Chinese security services have waged a long and successful campaign against the networks of the US and its allies, and have engaged in massive state-sponsored industrial espionage. If Stuxnet pointed towards the US and Israel as the nations with the most to gain from disrupting Iran's nuclear effort, what nation would gain the most from spending immense resources to track Tibetan human rights activists? In the last fifteen years, many collection programs like Flame have become public; presumably there are others that are better hidden. For espionage, cyber techniques are in good measure an extension of traditional signals intelligence capabilities, and for China, an extension of the distributed approach using multiple civilian agents seen in Chinese human collection programs.

Both China and Russia use cyber exploits in ways that differ from the cyber activities of Western services in important and potentially destabilizing ways. Both rely on proxies – private hackers acting at the direction of the state for government purposes. Proxies provide an increasingly feeble degree of deniability – does any serious observer believe that China and Russia do not control what happens on their networks – and an advance line of attackers that can shield state actions and, if necessary, be sacrificed to placate other nations. Russian proxies have focused on financial crimes, Chinese proxies on industrial espionage. Both nations provide a degree of training and support to their proxies and insist on one cardinal rule – no hacking against domestic targets. If this rule is observed and if the proxies cooperate in tasks assigned by the state, they are free to act against targets in other nations. Russian proxies were responsible for the exploits against Estonia and Georgia (the latter were precisely coordinated with Russian military plans);[4] Chinese proxies were responsible for the exfiltration of data from many economic and military targets in the US and other nations.

In contrast, neither the US nor its allies use proxies to engage in state sponsored financial crime, and the US does not engage in industrial espionage. US doctrine for the use of cyber techniques as an extension of traditional tools of coercion is different, but certainly not unprecedented.

Cyber Attack and the Weaponization of Signals Intelligence

Capabilities like those contained in Stuxnet reflect years of development and experimentation in how to exploit digital networks to gain military power. Stuxnet had advanced destructive capabilities, as it was designed to affect industrial control systems – specialized computers that run machinery – but it was an extension and refinement of existing software attack techniques. The ability to use software to disrupt industrial control systems and cause physical destruction was demonstrated in a 2005 experiment at Idaho National Labs. Perhaps five nations have this capability – the US, the UK, Israel, Russia, and China - and many other nations are trying to acquire it. In this regard, the US may be *primus inter pares*, but it has peers (or near peers) when it comes to cyber attack. Stuxnet may be the most advanced such "weapon" (another hallmark of the US), but it is by no means a unique capability.

Cyber attack is another option for military planners. With Stuxnet, for example, planners could weigh the merits and disadvantages of cyber attack, air strike, special operations teams, saboteurs, or missiles. Existing military doctrines have been extended and adapted to the new mode of attack. Nations have created cyber attack capabilities and have developed doctrine and strategies for their use. These national doctrines are not the same in all countries. We are in a period of experimentation as nations evaluate this new military capability and explore how best to use their new cyber capabilities. In addition to Russia's use of cyber "attack" in Estonia and Georgia and alleged Israeli use in Syria, we have seen Russia and China carry out reconnaissance for attacks on US critical infrastructure (according to the head of the US National Security Agency),[5] and probes by Iran against Israel and Gulf states. The US used cyber attacks in the 1990s during the conflict with Serbia and against Iraqi air defenses between Persian Gulf wars.

The US, Russia, China, and others include attacks on critical infrastructure as part of their doctrine for the military use of cyber attack. Publicly available doctrine suggests that each country makes decisions on the use of cyber attack in a manner consistent with planning for the use of other long range weapons – such as the benefits of a strike, the risk of escalation, and the potential for collateral effect. US doctrine shows some parallels to thinking about strategic bombing and the use of aerial bombing to reduce the will and capacity of an opponent to resist while avoiding a prolonged confrontation with its military forces. Russian doctrine pays greater attention to disrupting political stability and military command systems through cyber techniques, and this resembles Soviet doctrine on crippling first strikes against NATO by attacking critical infrastructure. China's doctrine is more opaque, but public discussion has emphasized attacks on infrastructure to disrupt the US ability to intervene in a regional crisis.[6]

Putting cyber attack in the context of military decision making (and assuming that state and non-state actors overall have similar military planning processes) has implications for use of cyber attacks. Nations are no more likely to launch a cyber attack that causes physical damage against the US or its allies after Stuxnet than they were before its discovery, nor are they likely to stop using cyber techniques for espionage and political coercion. We have not seen physically damaging attacks that could cause damage, destruction, or casualties (as opposed to espionage and crime) against the US and its allies from those countries with this capability because they assess the risk of a violent response as too high. This is the same reasoning that keeps them from launching aircraft or missiles against the US. However, international practice and law do not justify the use of force in response to espionage and crime, making the risk of a violent response small and acceptable.

This reluctance to attack may change as other nations with a different tolerance for risk, such as Iran, acquire advanced cyber attack capabilities, or as actors who overestimate their ability to remain covert gain advanced capabilities. What we do not know is how far non-state actors have advanced in their ability to develop similarly destructive techniques. The only indisputable evidence is that to date, we have not seen non-state actors engage in such attacks. This may reflect an absence of motive or of capability, and we cannot estimate how quickly such actors may gain the ability to carry out Stuxnet-like attacks.

To the credit of the designers of Stuxnet, it was carefully written to avoid collateral damage. Other attackers may not be so careful, but this has nothing to do with access to the Stuxnet code. Potential opponents still go through the same calculus of benefit and risk in deciding whether to use force against the US, and they are deterred by the likely US military response using all military assets at its disposal, not just cyber attack. They may now cite Stuxnet as part of any public justification of attack, but this will be an excuse, not part of their decision making. Nations are no more likely to launch a cyber attack against the US or its allies after Stuxnet than they were before its discovery.

How militaries will use the potential of cyber attack has important implications that explain why Stuxnet and Flame did not greatly change matters. Like any weapon, cyber attack has its own characteristics. Cyber attacks can be fast, covert, and contain less political risk in some scenarios.

Their drawback is a less destructive payload. An attack planner will consider these aspects, and assess the likelihood of a cyber attack achieving the desired effect at lowest "cost" when compared to other modes of attack. In some scenarios, cyber attack is preferable. The alternatives to Stuxnet included sabotage teams, airs strikes, missile strikes, or even occupation of the territory by conventional forces. Even this short list of potions, all of which pose greater risk of friendly losses, turmoil, and escalation, is enough to indicate why cyber attack was preferable

Nations already routinely use "cyber attacks" in ways that serve their needs. Other nations have the ability to carry out an attack like Stuxnet; but their strategies emphasize other goals, and to date, it has not been in their interest to cause physical damage. Russia and China have demonstrated advanced capabilities and could launch Stuxnet-like attacks should such attacks seem useful to them. That cyber conflict before Stuxnet was largely hidden from public view does not mean it was not taking place.

Another erroneous assumption is that Stuxnet was an event like Hiroshima, unleashing a new and uncontrollably destructive military force. But there is no Oppenheimer to chant of Stuxnet, "'Now I am become Death, the destroyer of worlds."[7] Despite the apparently tempting desire to compare cyber attack to nuclear weapons, this comparison is fallacious. Even small nuclear weapons have immense destructive power. Cyber attacks do not. They are a support weapon, useful to shape the battlefield in advantageous ways, but their effect is neither massively destructive nor fatal, and they do not pose an existential threat to nations. Cyber attack can be best compared to a missile, offering a fast, long range strike, with greater covertness (perhaps) but a smaller destructive payload. This limited destructive capability does not mean we should welcome the disruption of an artificial financial panic or a blackout that could last weeks, but we must also avoid exaggerating the effect of a cyber attack.[8] Stuxnet called attention to the vulnerability of modern software, but the destructive power of cyber attack is nowhere near that of nuclear weapons or even a sustained assault using kinetic weapons.

The Regional Contest

Stuxnet's code is now publicly available and some worry that it could now be reused by others. This ignores one of the primary limitations of cyber attack. They are usually "single-use" exploits. Once the "zero days" and other programming errors in operating systems or industrial control systems are exposed by an attack, they are usually fixed. The publicly available Stuxnet code was part of a larger and more complex exploit that involved a range of espionage techniques. The code was only part of the exploit and by itself insufficient. Stuxnet, if relaunched, would not work. The best evidence of this is that while many systems around the world were infected, only one, in Iran, was damaged.

Iran may seek revenge for Stuxnet, but it was not news to the Iranians that the US and other nations are engaged in covert campaigns aimed at hampering their illicit nuclear weapons program, nor have the Iranians ever been shy about using violence against the US or Israel. Iran is responsible for the deaths of American personnel in Beirut, the Persian Gulf, and Iraq. Stuxnet is another chapter in a covert, sporadic conflict between the US and Iran that has been going on for more then thirty years.

Iran is also not bashful about uttering threats, and makes no secret of its own desire to develop and use cyber attack techniques. Venomous rhetoric against Israel by Iranian leaders may simply be rantings designed for a domestic audience, but this does not excuse them. States bear responsibility for the public remarks of their leaders. Given these threats, and in the context of repeated violations of its international commitments regarding nuclear weapons, to say that a covert action involving the use of software against Iran's nuclear program is inappropriate – an action that produced no casualties or collateral damage – is a strange conclusion.[9]

If we accept that the US was involved in Stuxnet, this is also not a surprise. The US has a history of using covert action against aggressive, non-democratic regimes. The capability was developed in World War II (under the tutelage of the British) and was refined and expanded during the Cold War. But the US has never used covert force against a democratic nation or against a nation that posed no threat to international peace. We can question the US ability to discern threats to peace – there have been many errors, but Iran is not one of them. Covert action is preferable to other military responses in many cases, as it reduces the risk of direct confrontation or expanded conflict. Covert action is a middle ground between acquiescence and open war, another tool for legitimate defense for state use even if it is repugnant to some.

The US justified these interventions on the grounds that it is leading a coalition of nations in defense of democracy – a role thrust upon it by

World War II and the Cold War. This role was generally accepted by the community of democracies between 1941 and 1990. Even if we do not accept the assertion that the US still leads a coalition of nations in defense of democracy, we can make a strong case that Iran's behavior threatens US security and international peace, justifying active measures in response.

The advantages of Stuxnet are many and the only regret we should feel is that it was discovered prematurely. Launching Stuxnet posed much less political risk than air strikes. There was no collateral damage, no televised images of smoking buildings and weeping civilians, and no downed pilot being marched through the streets of Tehran en route to being tortured. The "weaponized" code cost much less than a single F-16.

The Missing Political Context

The emphasis on cyberwar in the public discussion of Stuxnet and Flame has meant that interesting questions have gone largely unasked. Seeing an opponent "stumble" across a complex, covert operation, especially if this happens more than once, suggests that we should consider explanations other than coincidence. The hypothesis about both Stuxnet and Flame worth exploring is the connection of the revelations to Russia. The revelations about Flame served a larger Russian political agenda on internet governance and cyber security. Putting Stuxnet and Flame in the context of the practice of espionage and covert political action may better explain what occurred than a focus on warfare.

In particular, the way that information about Flame was released is consistent with an effort at political manipulation to win support at upcoming multilateral meetings on internet governance later this year. Russia and others would like the International Telecommunications Union (ITU) to play a larger role in cyber security and internet governance. A greater role for the ITU would undercut any perceived American "hegemony" in cyberspace and perhaps reduce the risk Russia faces from the untrammeled access to information that the internet can provide. Russia may also seek to "stigmatize" the use of cyber attacks and wing support for a treaty banning weapons like Stuxnet in an effort to undermine an area of perceived US military advantage. This is a standard trick in international negotiations, to propose constraints that erode an opponent's capabilities more than your own (similar to the efforts in the 1980s to manipulate nuclear disarmament in Europe to reduce NATO capabilities more than those of the Warsaw Pact).

There are unusual associations in the entire affair. The Chief Executive Officer of the company that found Flame was an unofficial spokesperson for the Russian government at the 2011 London Cyber Conference. In November 2011, his company and the ITU announced they were forming a partnership to promote global cybersecurity.[10] The company says that it found Flame after the ITU asked it, in an unprecedented request, to look at data breaches in the Middle East, on the basis of which the ITU announced a global warning on cyber security, which was also unprecedented.[11] This could be straightforward; an alternate hypothesis which cannot be rejected is that this is a larger political maneuver designed by the Russians to influence opinion in key nations. It is a common intelligence technique to use a proxy to release damaging information about an opponent and Russia relies heavily on proxies in its own cyber espionage practices. These anomalies are suggestive and point to alternative hypotheses, the most plausible being that Western services created Flame to spy on Iran, and that Russia exploited its discovery for political purposes.

In recent years, Russia and China (sometimes acting through the Shanghai Cooperation Organization) have begun to develop an international strategy that would create an internet more accommodating to their interests. They believe that the information dominance of the West is part of a larger strategy of hegemony rather than a reaction to the failure of state-run media. While they can suppress their own citizens, they cannot suppress foreign sources of information. They have invested heavily in censoring technologies but have also sought international agreement to define information as a weapon that must be controlled. The internet creates political pressures not easily controlled by authoritarian regimes that can be a threat to their regimes (how much of a threat is another matter). This larger effort to restrict access to information and undercut the US is the political context for Flame.

At roughly the same time that Flame and Stuxnet were attracting such attention another piece of spyware went largely unremarked. A popular proxy service (which allows internet users to evade government controls) was compromised so that every person who downloaded the proxy program also downloaded malware that provided their user name and machine name and logged all of their keystrokes. The Simurgh malware affected thousands of people. The researchers at the University of Toronto's Munk School who found it believe it was targeted at Iranian and Syrian dissidents.[12] The malware created far greater risk than Flame but was not as loudly trumpeted, nor did the ITU issue a global warning. One possible explanation for this anomaly is that Flame fit a larger political agenda and Simurgh did not.

The relation of Flame to international negotiations on cyber security (and internet governance) provides important background on the multilateral efforts to make cyberspace more secure. One unremarked aspect in the recent public commentary is that the new risk from cyber attack became part of the international security agenda several years ago, when the military and security risks of high speed global connectivity became apparent. Cyberspace, weakly governed and poorly secured, is a now a source of international instability. Nations fear inadvertent escalation into a larger kinetic conflict more than the actual effect of cyber attack, given its limited potential for damage. A serious dialogue on how to reduce risk has been underway at least since the Russian effort to coerce Estonia using cyber techniques in 2007. The "attacks" against Estonia in 2007 posed much greater danger to international stability than Stuxnet, as it threatened to trigger armed conflict between NATO and Russia.

As a result, there are discussions in many official forums on how to reduce risk and increase stability. These include the UN's Group of Government Experts, the Organization for Stability and Cooperation in Europe, the Asian Regional Forum and the London Conference Process. The Organization of American States has held meetings on cyber security. The US, Russia, and China are engaged in bilateral discussions on cybersecurity, and the US has engaged in similar discussions with close allies. To portray Stuxnet and Flame as a grave new danger is more of a rhetorical device to gain negotiating advantage than a serious analysis of international security.

Conclusion

Technologically advanced militaries have created cyber techniques and will make use of them to advance their interests. There is conflict (even if it is not "warfare"). If Stuxnet and Flame point to any risk, it is that a lack of knowledge of the military and negotiating terrain for cyber security and a quasi-superstitious understanding of cyber attack will impede efforts to make cyberspace more stable and secure. Stuxnet and Flame were not apocalyptic, not particularly new, and not the dawn of some new era of warfare. Technology has reshaped warfare since the start of the industrial age. We may not like this, but states and armed groups have rarely forsaken a new capability. Nations may reject massively horrific weapons, but everything else will be used. Cyber attack is no different. States will behave as they have always behaved, and simply take advantage of new technologies to achieve their purposes.

Notes

[1] Malicious cyber action can be defined as software sent over digital networks to illicitly access target computers and execute instructions without the owner's permission.

[2] James A. Lewis, Katrina Timlin, "Cybersecurity and Cyberwarfare," UNIDIR Resources, 2001, www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf.

[3] Clifford Stoll's *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (New York: Doubleday, 1989) details Soviet cyber espionage in the 1980s. While there is little public discussion of cyber attacks by the US against Serbia in the 1990s, US officials have provided details in interviews.

[4] US Cyber Consequences Unit, "Overview by the US CCU of the Cyber Campaign against Georgia," August 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

[5] "Militarisation of Cyberspace: How the Global Power Struggle Moved Online," *The Guardian*, April 2012, http://www.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle.

[6] See, for example, Steve DeWeese, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman, October 2009.

[7] Robert Oppenheimer, scientific head of the project to develop an atomic bomb, quoted this statement from the Bhagavad Gita at the first successful test.

[8] "Cyber-like-nuclear" scenarios involve long chains of dubious assumptions about the political effect of attack and the resilience of the target. For a longer discussion, see James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," CSIS, December 2002, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

[9] See, for example, Robert Wright, "How Obama's Cyberweapons Could Boomerang," *The Atlantic*, June 2012; Misha Glenny, "We will Rue Stuxnet's Cavalier Deployment," *Financial Times*, June 2012, http://www.ft.com/cms/s/0/6b674600-afc7-11e1-a025-00144feabdc0.html#axzz25KCLvt33; or

Jason Healy, “Stuxnets are not in the US National Interest: An Arsonist Calling for Better Fire Codes,” Atlantic Council, June 2012. Note that the triggering event for these cries of anguish was not the actual attack, but a news story about the attack, illustrating the media driven nature of much of the discussion. Noise in the press is not a good measure of actual risk.

10 “ITU Teams Up with Kaspersky Lab for ITU Telecom World 2012,” http://www.kaspersky.com/about/news/business/2012/ITU_Teams_Up_with_Kaspersky_Lab_for_ITU_Telecom_World_2012.

11 “Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat,” http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat/.

12 Munk School of Global Affairs, “Iranian Anti-Censorship Software ‘Simurgh’ Circulated with Malicious Backdoor,” May 2012, https://citizenlab.org/2012/05/iranian-anti-censorship-software-simurgh-circulated-with-malicious-backdoor-2/.