Unraveling the Stuxnet Effect:
Of Much Persistence and Little Change in the Cyber Threats Debate

Myriam Dunn Cavelty

Cyber threats have been on the security political agenda for a number of years. Since RAND researchers John Arquilla and David Ronfeldt suggested in 1993 that "cyberwar is coming!"[1] cyberwar has become the most prominent buzzword in the debate surrounding computers, national security, and cyberspace. Being at the mercy of well-publicized events and occurrences, interest in the topic used to flare up whenever anything involving the aggressive use of computers hit the news, only to disappear again when other issues took over the limelight.

This changed in 2010. In particular, it was Stuxnet, the sophisticated computer worm written to sabotage systems that control and monitor industrial processes, that stirred up the international community in major ways and catapulted the cyber topic into the sphere of public fears and to the top of everybody's threat list. As a result, more and more countries consider cyber attacks to be one, if not *the* major future security threat.

But how justified is this assumption? And what has Stxunet really changed in the debate?

This article aims to provide a balanced picture of the phenomenon of cyberwar. It will show how and why the meaning of "cyberwar" has evolved from the narrow conception referring exclusively to military interaction to its broad meaning, which has become detached from "war" and encompasses almost every activity linked to the aggressive use of computers. In particular, it will distinguish between different forms of cyber conflict in order to lay the ground for a levelheaded threat assessment.

Dr. Myriam Dunn Cavelty is head of the New Risk Research Unit at the Center for Security Studies in Zurich, Switzerland.

It further shows that there is probably less change and more persistence in the cyber threat debate at large than is currently acknowledged. The threat image has been quite solid since the late 1990s, and Stuxnet has not changed this to any substantial degree. The same can be said for the countermeasures that are planned or envisaged.

Contexts and Meanings of Cyberwar

The importance and emergence of the concept of cyberwar can best be understood in the larger context of the information revolution, which has shaped – and is still shaping – perceptions of opportunities and dangers. In particular, the technologies of the information revolution and related organizational innovations in the 1980s and 1990s seemed to alter the nature of conflict and the kinds of military structures, doctrines, and strategies needed. Thus, it seemed to imply the rise of a "new" kind of warfare in which the factor of information was to grow more and more important. This development was facilitated (if not driven) by the end of the Cold War and the ensuing reorientation in terms of enemies, strategic thought, and defense spending.

It was the second Persian Gulf war of 1991 that created a watershed in military thinking about cyberwar. That conflict was seen by military strategists (mainly American) as the first of a new generation of conflicts where victory is no longer ensured only by physical force, but also by the ability to win the information war and to secure "information dominance." As a result of the conflict, strategists began to publish scores of books on the topic.[2] The reaction to the technological developments after the Gulf War also manifested itself in the publication of new doctrinal papers that institutionalized the information component.

The debate was initially characterized by a great deal of euphoria. Soon after, however, more attention was given to the risks associated with this development. Specifically, the formulation of strategies that no longer aimed at enemy capabilities but directly targeted the opponents' flow of information highlighted the relatively high vulnerability of networked US troops. As the debate over attacks on potential hostile information systems progressed, the possible dangers to civilian data networks were also increasingly discussed. The US as the only remaining superpower was seen as predestined to become the target of asymmetric warfare. Widespread fear took root in the strategic community that those likely to fail against the US war machine might instead plan to bring the US to its knees by striking against vital points at home, namely, critical infrastructures.[3] The concept of critical infrastructure includes sectors such as information and telecommunications, financial services, energy and utilities, and transport and distribution. It also includes a list of additional elements that vary across countries and over time.[4] Most of these sectors rely on a spectrum of software-based control systems for their smooth, reliable, and continuous operation.

With the growth and spread of computer networks into more and more aspects of everyday life, the object of protection moved from being perceived to be limited proprietary (governmental, mainly military) networks to encompass the whole of society – or rather, its way of life provided by the uninterrupted sub-structure of technology.[5] On this basis, a comprehensive threat image with two interrelated sides evolved. First, an inward-looking perspective sees the very connectedness of infrastructure systems as posing dangers, because perturbations within them can cascade into major disasters with immense speed and beyond our control. Advances in information and communication technology have thus augmented the potential for major disaster in critical infrastructures by vastly increasing the possibility for local risks to mutate into systemic risks. Second, an outward-looking perspective focuses on the increasing willingness of malicious actors to exploit vulnerabilities without hesitation or restraint. Because critical infrastructure systems combine symbolic and instrumental values, attacking them becomes integral to a modern logic of destruction that seeks maximum impact.

In addition, the cyber dimension reformulates space into something no longer embedded in place or presence. The "enemy" becomes a faceless and remote entity, a great unknown that is almost impossible to track. This results in two significant characteristics of the threat representation. First, the protective capacity of space is obliterated; there is no place that is safe from an attack or from catastrophic breakdown in general. Second, the threat becomes quasi universal because it is now everywhere.

A Cyber Phenomenology

It comes as little surprise, then, that cyber threats are feared the way they are. Nonetheless, every observer cannot help but notice how unspecified the threats actually are. By leaving its military confines, the concept became greatly blurred: cyberwar has come to refer to basically any phenomenon involving a deliberate disruptive or destructive use of computers.

Such conceptual vagueness is not helpful if we are to understand what goes on in "cybered" conflicts[6] and what kinds of countermeasures are actually needed for what kind of phenomena. Bruce Schneier, an internationally renowned security technologist and author, differentiates between cyber vandalism, which includes the defacing of websites; cyber crime, which includes theft of intellectual property, extortion based on the threat of Distributed Denial of Service attacks (DDoS) attacks, fraud based on identity theft, and so on; cyber terrorism, e.g., hacking into a computer system to cause a nuclear power plant to melt down, a dam to open, or two airplanes to collide; and cyberwar.[7] Schneider uses "cyberwar" to refer to the use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems.

Schneier's classifications construct a cyber threat escalation ladder – from rung to rung, the potential effects as well as the scope and the intensity become more severe. The last few years have shown that cyber espionage and cyber sabotage are missing from this ladder. More important, however, is that the lines of demarcation between the different activities are greatly blurred. When a particular detrimental event occurs, it is often difficult to determine whether it is the result of a malicious attack, a failure of a component, or an accident. And although their goals are different, the tools and tactics used by armies, terrorists, and criminals in cyberspace are very similar, if not the same. This means that knowing who is behind an attack and what kind of phenomenon it constitutes is a major difficulty when it occurs.

Then again, just because it is difficult does not mean that such a differentiation is not necessary: the opposite is true. First, the advantage of a "severity of effects" view is that it helps policymakers prioritize in theory, which is highly needed. Only computer attacks whose effects are sufficiently destructive or disruptive should be regarded as a national security issue – and should therefore earn the attention needed for something existentially threatening. Attacks that disrupt nonessential services or that are mainly a costly nuisance are not.[8] Second, a narrow and precise definition also helps to circumvent other dangers inherent in calling something "war," like exculpating the victims of an attack from their own responsibility for the consequences of their negligence in terms of computer security or creating pressure to retaliate against hackers, real or imagined.[9] Third, it clearly shows where the center of gravity lies: with careful computer forensics. Each and every occurrence must be carefully investigated. As Schneier notes:

> Just as every shooting is not necessarily an act of war, every successful Internet attack, no matter how deadly, is not necessarily an act of cyberwar. A cyberattack that shuts down the power grid might be part of a cyberwar campaign, but it also might be an act of cyberterrorism, cybercrime, or even – if it's done by some fourteen-year-old who doesn't really understand what he's doing – cybervandalism. Which it is will depend on the motivations of the attacker and the circumstances surrounding the attack...just as in the real world.[10]

Threat Assessment

That said, how endangered are we? Conflicts in cyberspace have been a reality for over a decade: elements of any political, economic, and military conflict take place in and around the internet. Furthermore, criminal and espionage activities aided by information and communication technologies take place every day. But in the entire history of computer networks, there have been very few examples of severe attacks that had the potential to disrupt or actually did disrupt the activities of a nation state in a major way. There are even fewer examples of cyber attacks that resulted in physical violence against persons or property. The huge majority of cyber attacks are low level and cause inconvenience rather than serious or long term disruptions. In fact, it has been convincingly shown that a "pure" (or strategic) cyberwar is very unlikely to ever occur, with attacks on computer systems more likely to be used in conjunction with other, physical forms of attack.[11]

Did this estimation change with Stuxnet? Classifying Stuxnet according to the escalation ladder is a challenge. Stories and speculations about the worm, its origins, and its intent exist by the thousands.[12] Well written or less so, they all contain bits and pieces of a puzzle that is inherently unsolvable. The pieces of the puzzle all seem to suggest that only one or several nation states – the usual "cui bono" logic pointing either to the US or Israel – would have the capability and interest to produce and release Stuxnet in order to sabotage the Iranian nuclear program. Though the world will probably never know for certain who is behind this piece of code, the majority of strategic planners out there are willing to believe that a "digital first strike" has occurred and a virtual Pandora's Box has been opened.

However, even if the most extreme case is assumed – that the majority of states in this world have developed effective and powerful cyber weapons or will in the near future (which is very doubtful) – the mere existence and availability of such capabilities does not automatically mean that they will be used. The cyber realm seems to lead people to assume that because they have vulnerabilities they will be exploited. Still, in security and defense matters, careful threat assessments need to be made. Such assessment necessitates the careful deliberation of the following question: "Who has the interest and the capability to attack us, and why would they?" For many democratic states, the risk of war has moved far to the background. The risk of a cyber attack of the severest proportions should be treated the same if there is no natural enemy.

Unraveling the Stuxnet Effect

On the other hand, the publication of Stuxnet's code and many other details has already led to many piggyback attacks. SCADA systems – computer systems that monitor and control industrial, infrastructure, or facility-based processes – are therefore likely going to be the target of choice for any kind of hacker in the near to midterm future. This comes with an inherent danger of intended and unintended (side) effects, of course – but in fact, the critical infrastructure community has been talking about the threat to SCADA systems for over a decade. In addition, experts have been expecting a major occurrence in cyberspace for a long time. Seen this way, Stuxnet is less of a surprise and more of a confirmation of what has been discussed and feared for years. Though it has focused the minds of politicians on the upper two rungs of the ladder, at least temporarily, it does not change the probability of cyber terror or cyberwar occurring.

It also does not change the methods and tools available to counter cyber threats. This concerns information assurance measures, for example, or the many diverse activities, concepts, and processes subsumed under "critical infrastructure protection" (CIP). CIP is handled similarly in many states:[13] close partnerships with the corporate sector and international partners are sought, mostly in order to exchange information on threats and issues. In addition, more recently, a shift away from the concept of protection towards the concept of "resilience" can be observed.[14] Resilience is not a new concept, of course, but its current rise indicates a significant and crucial shift in thinking. While protective (and defensive) measures aim to prevent disruptions from happening, resilience accepts that certain disruptions are inevitable.

Such thinking is absolutely necessary and needs to become rooted deeply in politicians' minds and subsequently in the minds of the population. Information networks can never be "secure" in the national security sense. In fact, the opposite is true: cyber incidents are fated to happen, because they simply cannot be avoided. In other words, even the most perfect defenses will not be able to guarantee that nothing severe will happen in a networked world.

States have the tendency to react forcefully to such a challenge and try to increase the level of security by all means. But cyberspace should not be mistaken for just another "realm" in which military action can be taken at will. To continue reaping the benefits of the cyber age, it is necessary to learn how to live with insecurity in pragmatic ways. Apart from legal and strategic restraints that will certainly be factored into any consideration of whether to use cyber attacks as weapons or not, the biggest impediment should be fears of uncontrollable blowback. First of all, repercussions could emerge directly through the interdependencies between various critical assets that characterize the environment. Second, blowback may be felt through the more intangible effect of undermined trust in cyberspace, with damaging repercussions for the global economy.[15]

By implicitly or explicitly moving an issue into the realm of national security and military actions, one tends to subject it to the rules of an antagonistic zero sum game, in which one party's gain is another party's loss. The logic of cyberspace, however, is a different one. Like the governance of space and the oceans, its governance requires globally accepted norms. The avenues currently available for arms control in this arena are primarily information exchange and norm building, whereas attempts to prohibit the means of cyberwar altogether or restricting the availability of cyber weapons are likely to fail. However, these difficulties should not prevent the international community from pushing all countries to adopt responsible limits and self-restraint in the use of cyber weapons and from thinking about new and innovative ways to enhance protection of vital computer networks without inhibiting the public's ability to live and work with confidence on the internet.

Notes

1 John Arquilla and David F. Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (1993): 141-65.

2 Greg Rattray, *Strategic Warfare in Cyberspace* (Cambridge: MIT Press, 2001); Michael O'Hanlon, *Technological Change and the Future of Warfare* (Washington: Brookings Institution, 1999).

3 Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge, 2008).

4 Elgin Brunner and Manuel Suter, *International CIIP Handbook 2008/2009* (Zurich: Center for Security Studies, 2009).

5 Myriam Dunn Cavelty, "Cyber-Security," in Peter Burgess, ed., *The Routledge Handbook of New Security Studies* (London: Routledge, 2010), pp. 154-62.

6 Chris Demchak, "Cybered Conflict as a New Frontier," *Atlantic Council*, October 28, 2010, http://www.acus.org/new_atlanticist/cybered-conflict-new-frontier.

7 Bruce Schneier, "Schneier on Security: A Blog Covering Security and Security Technology," Post: "Cyberwar," June 4, 2007, http://www.schneier.com/blog/archives/2007/06/cyberwar.html.

8 Cf. Clay Wilson, *Computer Attack and Cyber-terrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Report for Congress (Washington: Congressional Research Service, 2003) and Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in John Arquilla and David F. Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica: RAND, 2001), pp. 239-88.

9 Martin Libicki, *Defending Cyberspace and Other Metaphors* (Washington: National Defense University, 1997), p. 38.

10 Schneier, http://www.schneier.com/blog/archives/2007/06/cyberwar.html.

11 Peter Sommer and Ian Sommer, *Reducing Systemic Cybersecurity Risk*, OECD/IFP Project on Future Global Shocks, 2011, www.oecd.org/dataoecd/3/42/46894657.pdf.

12 Two prominent examples are: Mark Clayton, "Stuxnet Malware is Weapon out to Destroy Iran's Bushehr Nuclear Plant," *Christian Science Monitor*, September 21, 2010, www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant; and William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

13 Myriam Dunn Cavelty and Manuel Suter, "Public-Private Partnerships are no Silver Bullet: An Expanded Governance Model For Critical Infrastructure Protection," *International Journal of Critical Infrastructure Protection* 2, no. 4 (2009): 179-87.

[14] Christine Pommerening, "Resilience in Organizations and Systems: Background and Trajectories of an Emerging Paradigm," in *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, CIP Program Discussion Paper Series (Washington: George Mason University, 2007), pp. 9-22.

[15] Andrew Rathmell, "Controlling Computer Network Operations," *Information & Security: An International Journal* 7 (2001): 121–44.