*Future Internet* **2012**, *4*, 672-687; doi:10.3390/fi4030672

OPEN ACCESS

*future internet*

**ISSN 1999-5903**

www.mdpi.com/journal/futureinternet

*Article*

# Stuxnet: What Has Changed?

**Dorothy E. Denning**

Department of Defense Analysis, Naval Postgraduate School, 589 Dyer Road, Monterey, CA 93943, USA; E-Mail: dedennin@nps.edu; Tel: +1-831-656-3105

*Received: 17 May 2012; in revised form: 25 June 2012 / Accepted: 11 July 2012 / Published: 16 July 2012*

---

**Abstract:** This paper considers the impact of Stuxnet on cyber-attacks and cyber-defense. It first reviews trends in cyber-weapons and how Stuxnet fits into these trends. Because Stuxnet targeted an industrial control system in order to wreak physical damage, the focus is on weapons that target systems of that type and produce physical effects. The paper then examines the impact of Stuxnet on various domains of action where cyber-attacks play a role, including state-level conflict, terrorism, activism, crime, and pranks. For each domain, it considers the potential for new types of cyber-attacks, especially attacks against industrial control systems, and whether such attacks would be consistent with other trends in the domain. Finally, the paper considers the impact of Stuxnet on cyber-defense.

**Keywords:** cyber-attack; cyber-security; cyber-warfare; industrial control systems

---

## 1. Introduction

In fall 2010, not long after initial reports of Stuxnet hit the press, I began seeing headlines and stories declaring Stuxnet a game changer. In an article titled "STUXNET—Game Changer," Kevin Coleman, cyber-warfare correspondent for Defense Tech, said it represented a "threshold level event" and "new model of reality" [1]. The head of the Cybersecurity Center at the US Department of Homeland Security told Congress that it was a "game changer" [2], while the European Network and Information Security Agency characterized it as "a game changer for malware defence" [3].

But if Stuxnet was a game changer, what changed?

Like other computer worms, Stuxnet spread indiscriminately from one vulnerable computer to the next. What set it apart from the thousands of other worms that went before it is that it was designed to unleash its payload only when it entered an industrial control system (ICS) matching the characteristics of Iran's nuclear enrichment facility at Natanz. And when it did, it tampered with the code of the

programmable logic controller (PLC) used to control the centrifuges at Natanz, ultimately destroying about a thousand centrifuges and disrupting Iran's nuclear program [4,5]. No previously reported worm had done anything like that before, either in terms of precision targeting or causing physical damage through ICS manipulation.

Is Stuxnet a forefather of future cyber-weapons? Will we soon see a rash of attacks against ICS components and devices, which include Supervisory Control and Data Acquisition (SCADA) systems, as well as PLCs? These systems are used, for instance, to operate electric power grids, distribute oil and gas, and control water treatment systems and dams. Are they adequately protected against cyber-attacks? Will we witness cyber-attacks that go beyond the usual data theft and service disruption in order to cause serious physical damage against specific targets? Will cyber-terrorists use Stuxnet-like tools to cause nuclear explosions, shut down power grids, blow up gas lines, cause floods, or otherwise wreak havoc?

According to *The New York Times*, Stuxnet was developed and deployed by the United States and Israel [5,6]. Does this mean that cyber-attacks have become an instrument of national power, augmenting other forms of national power, especially military power? Is Stuxnet a sign that cyber-warfare is already here or on the brink? Did Stuxnet's exposure and analysis bring cyber-warfare from the closed world of spies and covert operations into the public sphere?

This article addresses these and other questions in order to determine how Stuxnet has changed the ongoing game of cyber-attack *vs.* cyber-defense. The approach is contextual, taking into account how Stuxnet fits into or alters cyber-related trends.

The paper first reviews trends in cyber-weapons. Because Stuxnet targeted an ICS in order to wreak physical damage, focus is on weapons that manipulate systems of that type and produce physical effects. The paper then examines how Stuxnet impacts various domains of action where cyber-attacks play a role, including state-level conflict, terrorism, activism, crime, and pranks. For each domain, it considers the potential for new types of cyber-attacks, especially attacks against an ICS, and whether such attacks would be consistent with other trends in the domain. Finally, the paper considers the effect of Stuxnet on cyber-defense.

## 2. Cyber-Weapons

To appreciate the impact of Stuxnet on the development of destructive ICS cyber-weapons, it is necessary to look at what ICS weapons had already been developed and deployed. If Stuxnet were merely an incremental improvement over previous weapons, it would not qualify as a game changer in this area.

Prior to Stuxnet, the most sophisticated and damaging cyber-attack against an ICS was commonly regarded as the months-long attack launched by Vitek Boden against the Maroochy Shire Council sewerage control system in Queensland, Australia in 2000. A former employee of the contracting company that developed the system, the 48-year-old Australian used equipment and software he had taken from the company in order access the ICS network and alter data. His attack caused pumps to malfunction and alarms to turn off, resulting in raw sewage overflows that killed marine life and harmed the environment [7].

While not to diminish the seriousness of Boden's attack, it was nonetheless considerably less sophisticated than Stuxnet in at least three areas: access, command and control, and stealth. With respect to access, because the network controlling the centrifuges at Natanz was not remotely accessible or even connected to the Internet, Stuxnet was deployed in the form of a complex computer worm that spread across Microsoft Windows machines via USB memory sticks and local network links, exploiting several unknown ("zero-day") vulnerabilities in the systems it hit and using fraudulent digital certificates to trick the systems into running its code [4]. As it spread, it had to examine the hardware, software, and settings of each system to determine if they matched those at Natanz, unleashing its payload only when they did. By contrast, Boden's equipment gave him immediate and direct access to his target.

Second, with respect to command and control, Stuxnet needed to operate autonomously, with its commands and data wired into the code, although it also had the capability to receive new code over the Internet if so connected. Boden, on the other hand, was able to issue commands directly from a laptop, without the need to preprogram his entire operation. Thus, while Stuxnet's authors needed to get it right the first time, Boden had the opportunity to try things out and adjust his tactics. Further, whereas much of Stuxnet's code had to be developed from scratch and carefully crafted so as to recognize its intended target, Boden was able to use code he had taken from the contracting company and apply it directly against his target.

Third, with respect to stealth, Stuxnet needed to conceal its presence long enough to cause the desired damage. It did this by hiding its code and effects, leading network operators at Natanz to believe that the centrifuges were operating normally, even as they were being manipulated in harmful ways. Boden, by contrast, did little to hide his actions. Operators monitoring the network were aware of the problems he was causing, but initially did not know their source.

There have been reports of cyber-attacks affecting other ICS devices, including those operating electric power grids, but I have not seen any information suggesting that any of these attacks was at the level of Stuxnet. At Idaho National Labs, researchers demonstrated how a cyber-attack could cause a power generator to self-destruct [8], but neither code nor details were released, making it difficult to compare with Stuxnet. Nevertheless, it seems unlikely that the code would have been as complex as Stuxnet, as it did not have to spread, recognize its target, or hide its presence and effects over an extended period of time. Thus, it seems reasonable to say that Stuxnet represented a considerable advance over previous cyber-attacks or demonstrations against ICSs. As a cyber-weapon, it was a major innovation.

Still, for Stuxnet to be a game changer, it has to make a noticeable mark on the future. This might happen through two avenues. First, the authors of Stuxnet, seeing its success and having developed knowledge, skills, and tools for attacking a complex ICS, could build on their work in order to develop and deploy new cyber-weapons against control systems. Indeed, this outcome seems likely. Stuxnet provided not only a means of disrupting Iran's nuclear program, but an investment in the future and building block for future cyber-attacks against ICS devices. Moreover, Stuxnet seems to be but one of several tools developed by the United States and Israel. Another computer worm, nicknamed Flame, reportedly contains some of Stuxnet's code, although it was used to secretly map and monitor Iranian networks rather than cause damage [9]. A third worm, Duqu, which was also used for information

collection rather than sabotage, was said to be "nearly identical to Stuxnet, but with a completely different purpose" [10] and possibly built on the same platform [11].

Second, observers of Stuxnet's success could be inspired to develop similar cyber-weapons of their own. They might do this in order to attack a particular ICS device in support of a specific goal, or simply to keep up with what they see is a "cyber-arms race." This avenue also seems likely, in part because humans are naturally competitive and inclined to borrow useful ideas and techniques from others, but also because Stuxnet is now "out there"—at least its object code is available. Although its source code was not released, analysts have been able to decompile or reverse engineer the object code to discern Stuxnet's functionality, making it easier to develop new cyber-attack tools against control systems. Code developers need not start from scratch.

Besides studying Stuxnet, security researchers have been independently examining ICS security, the objective being to identify vulnerabilities that could be exploited. Ideally, product manufacturers would release patches (fixes) for the vulnerabilities, which customers would then install, rendering any cyber-weapons that attempted to exploit them ineffective. In practice, however, vulnerabilities are not always fixed or patches installed, and exploit software is developed to take advantage of them. Researchers often develop these exploits to underscore the seriousness of the problem, push vendors into fixing them, and provide a mechanism for testing whether a particular system is vulnerable. But once published, the exploit code can also be used to facilitate harmful cyber-attacks.

I started seeing reports of ICS vulnerabilities in 2007 and the release of exploits a few years later. In March 2011, the Moscow security firm Gleg announced the availability of Agora SCADA+, a package with 22 exploits, including exploits for 11 "zero-day" vulnerabilities. Six days later, security researcher Luigi Auriemma released proof-of-concept exploit code against 34 SCADA vulnerabilities in software from four vendors [12]. Then in January 2012, researchers released information describing security flaws in widely-used PLCs from five vendors [13]. They provided exploit code for some of the flaws in the popular Metasploit framework, making it easier for security professionals to test their systems for the vulnerabilities—or their adversaries to attack them. Additional tools can be used to find Internet-connected ICS devices, which might then be attacked. Using the Shodan search facility, for example, Éireann Leveritt found 7500 such devices. By fusing this data with exploit information from Metasploit and ExploitDB plus geolocation data, he showed how someone could identify ICS devices vulnerable to a cyber-attack [14].

Software developers often build on the work of others, and this general principle applies to the development of cyber-attack code. Most viruses, worms, Trojans, and other types of malware are not developed from scratch. Rather, existing code is modified and extended in order to produce a new version that evades detection, takes advantage of new vulnerabilities, produces a different effect, uses a different command and control channel, or puts the author's personal touch on the code. The emergence of cyber-weapons and exploits against ICS devices is thus likely to lead to the development of further cyber weapons against such targets, with Stuxnet offering one example. In this sense, Stuxnet might be regarded as just another data point on an ICS cyber-weapons curve that plots weapons capabilities over time. However, it likely accelerated the curve's rise, as it is more complex than other available ICS tools, and it drew considerable interest and study.

If, as I have conjectured, Stuxnet influences the development of ICS cyber-weapons, how might those weapons be used? The next five sections each examine a domain of action where cyber-attacks

play a role: state-level conflict, terrorism, activism, crime, and pranks. For each domain, Stuxnet's impact is examined in the context of existing trends in the domain.

## 3. State-Level Cyber Conflict

As already noted, Stuxnet was reportedly developed and deployed by the United States and Israel [5,6]. The apparent objective was to do more than just destroy some centrifuges. It was to slow down Iran's nuclear program. In that regard, Stuxnet achieved a national security goal that might otherwise have been met with a kinetic attack such as bombing the Natanz facility. But it did so without killing or injuring anyone, destroying anything other than centrifuges, or risking the lives of military personnel delivering bombs. By causing less harm to its target and incurring less risk for its perpetrators, it may have provided a morally better approach than its kinetic alternative, although its collateral effect of infecting about a hundred thousand computers worldwide would also need to be considered. In any case, I am not arguing that the operation was ethical, only that it may have been a more ethical means of destroying centrifuges than bombs would have been [15].

Only a handful of cyber-attacks have been publicly attributed to nation-states. In 1982, the United States is said to have planted a Trojan horse in Canadian software that was used by the Soviets to control their Trans-Siberian gas pipeline. The effect was a massive explosion on a remote area of the pipeline [16]. Then in 2003, just before Operation Iraqi Freedom, the US penetrated the Iraqi Defense Ministry e-mail system, injecting messages telling Iraqi officials that the US did not wish to harm them and asking them to not resist the coming invasion ([17], pp. 9–10).

Israel is said to have used cyber-weapons to blind Syria's air defenses at the time of its airstrike against a Syrian nuclear weapons facility in 2007. Nothing was damaged or destroyed, but the cyber-attack had the effect of hiding the Israeli aircraft from Syrians who were monitoring their airspace ([17], pp. 1–8). Like Stuxnet, the cyber-attack offered a morally better choice than, say, a kinetic attack that physically damaged Syrian's air defenses.

When at war, nations often launch destructive military strikes, including strikes against the critical infrastructures of their adversary. During the opening moments of Operation Desert Storm in 1991, a US fighter plane directed a precision-guided bomb straight down the air-conditioning shaft of the Iraqi telephone system in downtown Bagdad, taking out the entire underground coaxial cable system and the primary means of communicating between the Iraqi high command in Baghdad and subordinates in the field [18]. What Stuxnet and the above instances of nation-state cyber-attacks illustrate is the possibility of meeting national security objectives with bits rather than bombs. In so doing, operations may be less expensive, less deadly, less destructive, and less risky to their perpetrators. Instead of dropping a bomb into a Baghdad communication facility, the US might have been able to temporarily disable Iraqi military communications with a well-crafted cyber-weapon. Stuxnet showed just how sophisticated and precise such cyber-weapons can be. It was dramatically different from the weapons used in the other instances, offering new possibilities for achieving military objectives.

To the extent that cyber-weapons offer a less costly but morally preferred means of achieving national objectives over kinetic strikes, nation-states may find them an attractive alternative. Cyber weapons might be used to disrupt activity at other facilities believed to be involved in the production of weapons of mass destruction. During military operations, they might be deployed to temporarily

disable power, communications, transportation, or other services, allowing the rapid restoration of such services once hostilities end, and thereby avoiding the costs and problems associated with post-conflict reconstruction. Stuxnet showed what is possible against an ICS, while providing a blueprint for attacks against nuclear enrichment facilities. Of course, just because a cyber-weapon employs bits rather than bombs does not mean that it cannot cause serious damage, including deadly explosions. In determining whether a particular cyber-weapon offers a moral advantage over a kinetic one, all effects must be considered.

Although reports of state-level cyber-attacks have been few and far between, states are frequently accused of penetrating each other's networks in order to steal government and commercial secrets. State-level espionage has always been considered fair game, even during peacetime, and cyberspace has proven to be an easy and effective means for collecting information. China alone has been blamed for numerous instances of snooping against US and international targets since 2003, including incidents dubbed Titan Rain, Byzantine Hades, GhostNet, Shadows, Aurora, Night Dragon, Shady RAT, and Nitro. According to US intelligence agencies, most of the spying from China traces back to groups associated with China's People's Liberation Army [19]. Even earlier, Russia reportedly stole information from US Department of Defense networks beginning in the late 1990s in an incident named Moonlight Maze.

Although cyber-espionage is not the same as cyber-attack, their technologies are not all that different, as both require mechanisms to penetrate systems, access information, control operations, and conceal activity and effects. Thus, any country with a cyber-espionage capability is likely to also have a cyber-attack capability. According to Admiral Mike McConnell, former Director of National Intelligence, most industrialized countries in the world today have these capabilities, at least to some degree. Other intelligence officials have suggested that the number of militaries with a "respectable cyber war capability" is around twenty to thirty. Besides those I have already mentioned in this article, namely the US, Israel, China, and Russia, the list includes Taiwan, Iran, Australia, South Korea, India, Pakistan, and several NATO states, to include France [17, p. 64].

Whether Stuxnet has affected these cyber-warfare capabilities is hard to say. Governments had been developing them independent of Stuxnet. Still, Stuxnet represented an advanced cyber-attack against the ICS of another state. Given its exposure, it may influence the types of cyber-weapons that states develop and accelerate a state-level cyber-arms race. It is not surprising that Iran was reportedly investing $1 billion to boost its offensive and defensive cyber-warfare capabilities after it had been hit by Stuxnet [20].

Stuxnet is frequently mentioned in academic and policy discussions about cyber-warfare and security, at both domestic and international levels. It that regard, it may have helped bring cyber-warfare from "the shadows of the clandestine world into the limelight," as Coleman opined [1]. Although cyber-warfare had been the subject of discussion well-before the Stuxnet attack, Stuxnet provided an actual incident, allowing the discussions to move beyond the hypothetical scenarios normally employed to a concrete example that had been experienced and documented. In so doing, it could help advance our understanding of how the law of armed conflict (LOAC) applies to cyberspace. While some might argue that Stuxnet represents a "use of force" in violation of Article 2(4) of the United Nations Charter, others might view Stuxnet as something less than force or as a reasonable use of force against the threat posed by Iran's nuclear program under Article 51. For those in the latter camp,

Stuxnet becomes not only permissible under LOAC, but morally preferred over a kinetic strike, at least if its collateral effects are ignored. By providing a specific cyber-weapon and context for its deployment, Stuxnet lets us not only examine the application of LOAC, but also see how a cyber-attack can potentially offer a kinder and gentler means of achieving a just objective than through the application of traditional force.

## 4. Cyber-Terrorism

I have been writing about the prospects of cyber-terrorism since the late 1990s, always coming to the conclusion that it was not yet here, but leaving open the possibility that we would see it in the future and acknowledging that cyber-threats overall were serious, growing, and in need of being addressed. In my most recent article, a follow-up to one I had written right after al-Qaeda's 11 September 2001 terrorist attacks, I wrote: "Thus, the decade following 9.11 closes in much the same state as it began. Al-Qaeda and other terrorist groups still prefer bombs to bytes, and cyber terrorism remains a hypothetical threat even as the overall threat level in cyberspace has increased" [21].

This does not mean that terrorists and jihadists aligning themselves with al-Qaeda have never conducted a cyber-attack. Indeed, they have defaced and conducted low-level denial-of-service (DOS) attacks against websites they believe are harmful to Islam. But none of these attacks has risen to the level of cyber-terrorism. For a politically-motivated cyber-attack to be considered an act of cyber-terror, it would have to be serious enough to actually incite terror on a par with violent, physical acts of terrorism such as bombings. Attacks that caused major blackouts, gas pipeline explosions, train derailments, plane crashes, large financial losses, and the like would fall in that category. Attacks that merely disrupt access to a public website do not.

In another paper, I offered three indictors that might precede a successful incident of cyber-terrorism [22]:

- Failed cyber-attacks against critical infrastructures, particularly the ICS devices that are used to monitor and control these infrastructures. I thought it unlikely that a first attempt would succeed with the desired effect, given the novelty of such an attack and uncertainty about how it would play out. Stuxnet might be considered an exception to this, but terrorists would not have the capabilities and resources of nation-states such as Israel and the United States, and thus more difficulty getting it right the first time. Even their kinetic attacks frequently fail.
- Research and training labs, where terrorists simulate the effects of cyber-attacks against critical infrastructures, develop methods and tools to attack ICSs, and train people on how to conduct such attacks. I reasoned that it is hard to perform controlled experiments and analyze the consequences without a lab, as Israel appeared to have had for Stuxnet at their Dimona complex. Absent special facilities, I expected to at least see training materials showing terrorists how to conduct damaging attacks against ICSs and software tools designed to facilitate such attacks.
- Extensive discussions and planning relating to acts of cyber-terror against critical infrastructures, not just attacks against websites and attacks aimed at making money.

When Stuxnet came along, at least one jihadist took notice. A posting to the popular al-Shamukh jihadist forum in late 2010 called for attacks against SCADA systems, claiming they could be used to cause a massive explosion in a power plant, even a nuclear one, among other things. However, while giving a broad overview of SCADA systems and pointing to Stuxnet, the Australian sewage overflows, and other incidents affecting critical infrastructures, the posting offered no details for executing such attacks. Further, the premier jihadist English-language publication, *Inspire*, which has published nine issues as of May 2012, has focused exclusively on physical acts of violence. Readers can learn how to "make a bomb in the kitchen of your mom," but not how to conduct even rudimentary cyber-attacks.

Although jihadist websites and forums have offered tutorials and tools for rudimentary hacking, I have not seen jihadist materials for specifically attacking an ICS or any information suggesting that jihadists have access to a lab with ICS equipment and software, or that they have even attempted cyber-attacks against an ICS. The existence of Stuxnet, recognition of the potential damage that cyber-weapons such as Stuxnet could cause, and the availability of exploit tools against ICSs may bring us a bit closer to a cyber-terrorist incident than we were before Stuxnet, but the threat does not seem imminent.

## 5. Cyber-Activism

Cyber-activism refers to the use of cyberspace to promote some cause. It includes the development and use of cyber-tools that that support online actions such as e-petitions and e-mail writing campaigns, facilitate the organization and coordination of offline activities such as street demonstrations and marches, and help persons evade government censorship and surveillance while using the Internet. It also includes the development and use of cyber-attack tools for protesting the actions of governments and corporations. Cyber-activism is sometimes referred to as hacktivism, as it lies at the intersection of hacking (writing software or conducting cyber-attacks) and activism. While most cyber-activists would have no interest in a destructive tool like Stuxnet, a few might find it of value.

To the best of my knowledge, no hacktivist group has conducted a cyber-attack against an ICS. Rather, those who deploy cyber-attacks have resorted primarily to web defacements and DOS attacks. They either post their grievances and demands on the hacked websites of their opponents, or else they bombard the sites with so much network traffic that legitimate access to the sites becomes difficult to impossible. The cyber-attacks launched by patriotic Russian hackers against Estonia in 2007 and Georgia in 2008 illustrate [17, pp. 11–21], as do many of those conducted by the collective named Anonymous.

Some hacktivists have gone beyond web defacements and DOS attacks, however, compromising and disclosing sensitive documents, e-mails, and personal data, including passwords and credit card numbers. For example Anonymous, together with various groups linked to it such as LulzSec, has exposed the poorly secured systems of numerous agencies and corporations, and in so doing released sensitive, embarrassing, and personal information. They have put people at risk of identity theft, fraud, and other criminal acts. They also threatened a DOS attack against the Internet's root name servers, although the attack either did not take place or else had no noticeable effect [23]. According to the National Cybersecurity and Communications Integration Center (NCCIC), Anonymous has expressed an interest in targeting ICSs, but they have not yet demonstrated a capability to inflict damage on such systems [24].

Given the apparent interest of Anonymous (and perhaps other hacktivists), the possibility of hacktivists targeting an ICS cannot be ruled out. Further, a survey of 353 students at a Midwestern university in the United States found that a small percentage would be willing to conduct a cyber-attack that compromised a regional electric power grid, causing a temporary blackout, or a nuclear power plant, causing a release of radioactivity. In particular, 1.68% said they thought it would be appropriate to compromise a regional grid in their own country if their government engaged in harmful and unjust activities, while 3.08% said they would be willing to attack a grid in a foreign country that had harmed their homeland. A smaller percentage said they thought it would be appropriate to compromise a nuclear power plant, with 0.84% willing to attack one in their own country and 0.28% willing to attack one in a foreign country. A much larger percentage supported defacing a politician's or government website in their homeland (25.21%) or foreign country (22.40%), and still larger percentage supported posting something on Facebook (77.31% and 76.19%) [25].

In addition to attacking an ICS to protest the actions of one's own or a foreign government, hacktivists might attack an ICS in order to protest the nature of the facilities using the ICS. A group opposed to the continued use of fossil fuels, for example, might conduct a cyber-attack against an ICS in order to temporarily disrupt the processing or distribution of such fuels. If hacktivists do target ICSs, then Stuxnet, together with other ICS-related exploit tools, might prove to be a game changer in this domain. Still, most hacktivists could stay clear of ICS attacks out of concern for harming people or the environment.

## 6. Cyber-Crime

Cyber-attacks in the criminal domain are generally motivated by money or the desire for revenge. Those motivated by money usually do so through fraud, industrial espionage, and extortion. Fraud-related crimes include financial fraud, identity theft, and theft of services. They are facilitated by cyber-attacks that penetrate systems, steal financial account data such as bank and credit-card numbers, impersonate account holders, and alter accounts and usage information. Because ICSs are not used to control the flow of money or to manage accounts, cyber-attacks are not likely to be conducted against ICSs for the purpose of financial fraud or identity theft. However, they might be used to alter the usage information reported by sensors, for example, in order to hide the consumption of resources such as electricity, gas, or water. According to an FBI cyber intelligence bulletin, one US electric utility lost hundreds of millions of dollars because of cyber-attacks against their smart meters, and low-cost tools and software for tampering with the meters were readily available on the Internet [26]. However, the software bears no resemblance to Stuxnet, so Stuxnet may have little or no impact in this area.

In the area of industrial espionage, criminals might be interested in penetrating ICSs in order to steal their codes and develop competing products. Stuxnet or Duqu would offer a starting point for operations of this type. However, it is probably easier to acquire the codes by hacking the business networks of the vendors or by reverse-engineering their products, so again Stuxnet may have little or no impact here.

With respect to extortion, cyber-criminals frequently use cyber-attacks, especially DOS attacks, in order to extort money from a target, threatening to continue the attacks if the target does not pay up. If they successfully penetrate a target's networks and find sensitive information, they might instead

threaten to expose the information if not paid. The security firm McAfee reported that 25% of the 200 industry executives they surveyed in sectors using ICSs (electricity, oil/gas, and water) had experienced extortion attempts in 2010 [27]. The report does not say whether these involved cyber-attacks against an ICS or, more likely, a company's business network, but the former would be facilitated with a tool like Stuxnet because of its potential to cause considerable physical damage. Still, extortionists are primarily interested in making money, not developing software, so may prefer the simpler methods they have been using than to invest in a Stuxnet-like tool that is more complex and unlikely to work against as many targets.

Some cyber-attacks are simply acts of sabotage, usually motivated by revenge. Typically, these are conducted by "disgruntled" insiders, or former insiders, who are angry about how they have been treated. Boden's attack against the Maroochy Shire Council sewerage control system was of this nature. Like Boden, insiders can sabotage systems with tools considerably less sophisticated than Stuxnet, although a more sophisticated attack cannot be ruled out.

## 7. Cyber-Pranks

The domain I call "pranks" refers to cyber-attacks that are conducted more for personal gratification and amusement than anything else. Unlike the domains of terrorism and activism, which serve some cause, and the domain of crime, which is driven by money and revenge, the domain of pranks is driven by excitement, curiosity, challenge, and ego. Persons who conduct cyber-attacks in this domain want to have fun, experiment, and impress others. Zone-h, which recorded about 1.4 million web defacements in 2010, reported that over half were conducted "just for fun" and over 20% to "be best defacer" [28]. The remaining reasons, which included patriotism, politics, revenge, and challenge, each accounted for less than 10%.

In addition to defacing websites, hackers operating in this domain launch computer viruses and worms, break into systems, and conduct DOS attacks, among other things. Some of their cyber-attacks have affected ICSs, even if they did not attack them directly. The Slammer worm, for example, which infected up to 200,000 computers running unpatched Microsoft SQL software in early 2003, had the side effect of disabling a nuclear power plant's safety monitoring system and disrupting communications on the control networks of several utilities.

Like those who hack for a cause, most of those who hack for fun are probably not interested in shutting off power, causing pipeline explosions, or producing other harmful effects. However, there may be a small percentage with no qualms about such actions, even seeking them out. In 1999, a group calling itself "Realm of Chaos" caused 28 power outages in northeastern Wisconsin [29]. And in 2008, a 14-year-old electronics "genius" built an infrared device that gave him control over the Polish tram system. His actions caused four trains to derail and numerous injuries [30]. Hackers have also intentionally disrupted emergency 911 services, and Slammer had the additional side-effect of doing so as well.

For those hackers who take pleasure in harming others, a tool derived from Stuxnet or other ICS exploits would offer an attractive possibility. But even those who are not so motivated might experiment with such a tool in order to see what it does and show off to their friends. In the process of fooling around, they could cause more damage than they anticipated or even knew was possible. Over

time, Stuxnet and related ICS cyber-tools could lead to more harmful pranks than we have experienced so far, but it hasn't changed the game yet.

## 8. Cyber-Defense

Stuxnet damaged the centrifuges at Natanz by reprogramming the Siemens PLC that controlled them. To do that, it had to first compromise a Microsoft windows system, and then the Siemens WinCC/PCS 7 SCADA control software running on it. This was accomplished by exploiting several vulnerabilities, one of which was a hardcoded WinCC/SCADA password that had been posted on the Internet. Recently, the Rugged Operating System, which runs RuggedCom switches and servers on the communications networks of power grids and other critical infrastructures, was reported to have a similar backdoor with hardcoded password. In this case, the password used with a particular device was unique. However, if an adversary was able to acquire the device's MAC address, say through the Shodan search facility, then the password could be computed by plugging the MAC address into a Perl script [31].

To defend against the likes of Stuxnet and other ICS cyber-attacks, the operators and vendors of ICSs need to do better. There is no excuse in today's threat environment for posting passwords on the Internet or using ones that an adversary can easily determine.

Given the extensive attention Stuxnet received in the press, including reports of vulnerabilities in the ICSs running critical infrastructures and the harm that could result from ICS cyber-attacks, Stuxnet could serve as a motivator to governments and industry worldwide to initiate or accelerate efforts to enhance infrastructure security. In the remainder of this section, I will focus on US efforts in ICS cyber-security and Stuxnet's impact on these efforts. I make no claims about Stuxnet's impact in other countries, especially Iran, where its effects were much more significant.

Within the United States, the vulnerabilities of ICSs were recognized long before Stuxnet, with efforts to address them dating back to at least 1996 when President Clinton established the President's Commission on Critical Infrastructure Protection (PCCIP). The commission's report, issued in 1997, led to the creation of several government offices and to industry-centered information sharing and analysis centers for promoting cyber and critical infrastructure security [32]. Since then, but also before Stuxnet was reported in the press, the US government took several additional steps to strengthen cyber-defenses, including:

- Creation of the office of Cyber Security and Communications (CS & C) in the National Protection and Programs Directorate (NPPD) of the Department of Homeland Security (DHS). This office also includes the National Cybersecurity and Communications Integration Center (NCCIC) mentioned previously, the National Cyber Security Division, and the US-CERT.
- Appointment of a cyber-security coordinator in the White House.
- Issuance of the National Strategy to Secure Cyberspace (NSSC) [33].
- Issuance of the Comprehensive National Cybersecurity Initiative (CNCI) [34].
- Issuance of the Strategy for Securing Control Systems (SSCS) [35].
- Formation of US Cyber Command.

While most of these initiatives go well beyond ICS security, they also recognize the problems in this area. The NSSC states that the security of digital control systems and SCADA systems is a national priority, and that DHS will work with other concerned agencies and the private sector to increase the security of these systems. The twelfth initiative of the CNCI explicitly addresses cyber-security for critical infrastructures, calling for an approach that "builds on the existing and ongoing partnership between the Federal Government and public and private sector owners and operators of critical infrastructures and key resources." And, of course, the SSCS is devoted entirely to control systems. It includes the establishment of the Industrial Control Systems Joint Working Group and an expanded ICS Cyber Emergency Response Team (ICS-CERT). In addition to these initiatives, several legislative proposals to strengthen cyber-security were introduced prior to Stuxnet's public disclosure.

Since Stuxnet, DHS issued the Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise [36]. Released in November 2011, the Blueprint addresses two areas of concern: protecting critical infrastructures and strengthening cyber-ecosystems. Among its goals are to strengthen cyber-defenses for ICS/SCADA systems in order to protect against attacks that could harm the general public. However, it is difficult to assess the influence, if any, of Stuxnet on the Blueprint given the earlier efforts to strengthen cyber-security. The NSSC was issued in 2003, the CNCI in 2008 (as NSPD-54/HSPD-23 under the Bush administration) and again in 2009 (under the Obama administration), and the Strategy for Securing Control Systems (SSCS) in 2009. These all preceded the public disclosure of Stuxnet in July 2010. However, the case is not so straightforward, as some US government officials would have been aware of Stuxnet as early as 2009 if indeed the US was involved in the operation, as the malware appears to have infected Natanz that year [37]. Indeed, some would have been aware of the effort even earlier, as the impetus behind it reportedly goes back to 2006 [6]. Still, the government's drive for greater ICS security was likely motivated more by a growing awareness of the threats and risks than by Stuxnet specifically. According to Mark Weatherford, deputy undersecretary for cybersecurity at NPPD, they were "seeing a troubling increase in the threats and the vulnerabilities" associated with ICSs [38].

Since Stuxnet, there have also been several new legislative proposals addressing cyber-security. At least one of these, Senate bill S.2015, The Cybersecurity Act of 2012, has several provisions aimed at strengthening the cyber-security of critical infrastructures. But again, it is difficult to assess the influence of Stuxnet on the introduction of this bill, given the earlier attempts at legislation. For example, S.773, the Cybersecurity Act of 2009, also addressed critical infrastructure security. However, the details of the two bills vary, so Stuxnet—along with all the other cyber-security threats that occurred in the interim—may have had some impact on the 2012 bill.

Even if Stuxnet has had little impact on the strategic direction of the US government's cyber-security program, it has impacted day-to-day operations. Testifying before the US House Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies on 16 March 2011, Philip Reitinger, then deputy undersecretary of NPPD, reported that his division had taken several steps to help combat the Stuxnet threat [39]. Among others, the NPPD's ICS-CERT had analyzed the Stuxnet code, briefed government and industry organizations about the threat, and issued several advisories and updates about detecting and mitigating the threat. Companies and individuals in the security field have taken similar steps to understand, publicize, and mitigate the threat.

In addition to affecting day-to-day operations, Stuxnet has influenced the cyber-security conversation. It is frequently mentioned in news stories, presentations, reports, and articles relating to cyber-threats, legislation, and developments. I have cited it in other papers and discussed it in classes at NPS and in outside presentations. It has raised awareness of ICS cyber-threats and the dangers of worms and other forms of malware. It could further inspire the development of cyber-security requirements, standards, products, practices, and regulations. But these activities are not indicative of a game change so much as an already growing concern over cyber-threats, not only to control systems, but to all targets.

## 9. Conclusions

The following summarizes the impact of Stuxnet on cyber-attacks and cyber-defenses:

- *Cyber-weapons*: Stuxnet will likely inspire, accelerate, and serve as a building block for the development of new cyber-weapons that target ICS devices. These weapons will also be influenced by the growing interest of the cyber-security research community in ICS security, which has led to recent releases of vulnerability information and exploit tools that can be used against ICS devices, but Stuxnet could push development towards more complex tools and effects. Some of these tools, like Stuxnet, could be precisely targeted.
- *Cyber-warfare*: Stuxnet could be a forbearer of the way nation-states use cyber-warfare, offering militaries a weapon that may be morally superior to a kinetic one, such as a bomb, when it incurs less harm and risk than the kinetic weapon while achieving the same objective. Stuxnet has also influenced academic and policy discussions about cyber-warfare, in part by offering a case study based on an actual incident.
- *Cyber-terrorism*: While terrorists have expressed some interest in Stuxnet-like attacks, they appear to lack the capabilities and resources to conduct them or other devastating cyber-attacks. At least in the near-term, Stuxnet has had little impact on cyber-terrorism, though it has been cited to draw attention to the threat.
- *Cyber-activism*: Some hacktivists might use tools derived from Stuxnet or other ICS weapons to conduct a cyber-attack against an ICS, but most are likely to prefer tools that are simpler and less likely to physically harm persons or the environment.
- *Cyber-crime*: Criminals might use Stuxnet-like weapons against an ICS in order to extort money from the owner or to sabotage it out of revenge, but most are likely to prefer simpler tools that offer a greater financial return on their efforts.
- *Cyber-pranks*: Some hackers like to fool around with cyber-weapons, in some cases deploying them without regard for or an understanding of potential consequences. Weapons derived from Stuxnet or other ICS exploits could attract some of these hackers, who might cause serious harm in the process of trying them out.
- *Cyber-defense*: At least in the US, the response to Stuxnet appears to be following general trends in this area, which include increased attention to ICS security, as well as cyber-security more generally. Stuxnet does not appear to have shifted the US cyber-defense strategy.

Thus, Stuxnet's greatest impact may lie in the domains of cyber-weapons and cyber-warfare. It could be a prelude to a new class of cyber-weapons against ICS devices and to methods of achieving national security objectives that are less damaging and risky than kinetic strikes.

**Acknowledgments**

I am grateful to the referees and editor for constructive comments on a draft of this paper.

**References**

1. Coleman, K. STUXNET—Game Changer. Available online: http://defensetech.org/2010/10/04/stuxnet-game-changer/ (accessed on 13 April 2012).
2. Leyden, J. Stuxnet 'a game changer for malware defense' EU agency warning. *The Register*, 9 October 2010. Available online: http://www.theregister.co.uk/2010/10/09/stuxnet_enisa_response/ (accessed on 13 April 2012).
3. Benson, P. Computer virus Stuxnet a 'game changer' DHS official tells Senate. *CNN*, 17 November 2010. Available online: http://articles.cnn.com/2010-11-17/tech/stuxnet.virus_1_stuxnet-nuclear-power-plants-target?_s=PM:TECH (accessed on 13 April 2012).
4. Falliere, N.; Murchu, L.O.; Chien, E. W32.Stuxnet Dossier. Available online: http://www.symantec.com/connect/blogs/updated-w32stuxnet-dossier-available (accessed on 13 April 2012).
5. Broad, W.J.; Markoff, J.; Sanger, D.E. Israeli test on worm called crucial in Iran nuclear delay. *The New York Times*, 15 January 2011. Available online: http://www.cfr.org/iran/nyt-israeli-test-worm-called-crucial-iran-nuclear-delay/p23850 (accessed on 11 July 2012).
6. Sanger, D.E. Obama order sped up wave of cyberattacks against Iran. *The New York Times*, 1 June 2012. Available online: http://www.huffingtonpost.com/2012/06/01/new-york-times-obama-orde_n_1562102.html (accessed on 11 July 2012).
7. *R v Boden [2002] QCA 164*; Supreme Court of Queensland: Brisbane, Australia, 2002. Available online: http://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf (accessed on 11 July 2012).
8. Meserve, J. Sources: Staged cyber attack reveals vulnerability in power grid. *CNN*, 26 September 2007. Available online: http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US (accessed on 17 April 2012).
9. Nakashima, E.; Miller, G.; Tate, J. U.S. and Israel created 'Flame.' *Washington Post*, 20 June 2012. Available online: http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html (accessed on 12 July 2012).
10. W32.Duqu: The precursor to the next Stuxnet. Available online: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf (accessed on 17 April 2012).
11. Kaspersky lab experts: Duqu and Stuxnet the only malicious programs created by the responsible team. Available online: http://www.kaspersky.com/about/news/virus/2011/Kaspersky_Lab_Experts_Duqu_and_Stuxnet_Not_the_Only_Malicious_Programs_Created_by_the_Responsible_Team (accessed on 17 April 2012).

12. Goodin, D. Dozens of exploits released for popular SCADA programs. *The Register*, 22 March 2011. Available online: http://www.theregister.co.uk/2011/03/22/scada_exploits_released/ (accessed on 12 July 2012).
13. Zetter, K. Hoping to teach a lesson, researchers release exploits for critical infrastructure software. Available online: http://www.wired.com/threatlevel/2012/01/scada-exploits (accessed on 18 April 2012).
14. Leverett, E.P. Quantitatively Assessing and Visualising Industrial System Attack Surfaces. Ph.D. Thesis, University of Cambridge, Cambridge, UK, June 2011.
15. Denning, D.E.; Strawser, B.J. Moral cyber weapons. Naval Postgraduate School, Monterey, CA, USA. Unpublished work, 2012.
16. Saffire, W. The Farewell Dossier. *The New York Times*, 2 February 2004. Available online: http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html (accessed on 12 July 2012).
17. Clarke, R.A.; Knake, R.K. *Cyber War*; Harper Collins: New York, NY, USA, 2010; pp. 9–10.
18. Denning, D.E. *Information Warfare and Security*; Addison Wesley: Reading, MA, USA, 1999; p. 5.
19. Gorman, S. U.S. homes in on China Spying. *The Wall Street Journal*, 13 December 2011. Available online: http://www.globalvelocity.com/news-media/industry-news/u-s-homes-in-on-china-spying.html (accessed on 16 July 2012).
20. Katz, Y. Iran embarks on $1 billion cyber-warfare program. *Jerusalem Post*, 18 December 2011. Available online: http://www.jpost.com/Defense/Article.aspx?id=249864 (accessed on 12 July 2012).
21. Denning, D.E. Whither cyber terror? 10 years after September 11, A Social Science Research Council Essay Forum. Available online: http://essays.ssrc.org/10yearsafter911/whither-cyber-terror/ (accessed on 23 April 2012).
22. Denning, D.E. A View of Cyberterrorism Five Years Later. In *Readings in Internet Security: Hacking, Counterhacking, and Society*; Himma, K., Ed.; Jones and Bartlett: Boston, MA, USA, 2007; Chapter 7, pp. 123–139.
23. Sengupta, S. After threats, no signs of attack by hackers. *The New York Times*, 31 March 2012. Available online: http://www.nytimes.com/2012/04/01/technology/no-signs-of-attack-on-internet.html (accessed on 12 July 2012).
24. *Assessment of Anonymous Threat to Control Systems. National Cybersecurity and Communications Integration Center Bulletin*; A-0020-NCCIC/ICS-CERT-120020110916; National Cybersecurity and Communications Integration Center: Washington, DC, USA, 2001.
25. Holt, T.J.; Kilger, M. Examining willingness to attack critical infrastructure on and off-line. *Crime Delinq.* **2013**, in press.
26. Krebs, B. FBI: Smart meter hacks likely to spread. Krebs on Security. Available online: http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/ (accessed on 25 April 2012).
27. Baker, S.; Filipiak, N.; Timlin, K. *In the Dark: Crucial Industries Confront Critical Cyberattacks*. McAfee: Santa Clara, CA, USA, 2011.
28. Almeida, M. Defacement statistics 2008–2009–2010. Available online: http://www.zone-h.com (accessed on 26 April 2012).

29. 'Dr. Chaos' Gets seven more years in jail. *SC Magazine*, 1 December 2005. Available online: http://www.scmagazine.com/dr-chaos-gets-seven-more-years-in-jail/article/32757/ (accessed on 12 July 2012).
30. Wilson, T. Teenage hacker takes over Polish tram system. *Dark Reading*, 11 January 2008. Available online: http://www.darkreading.com/security/perimeter-security/208803765/teenage-hacker-takes-over-polish-tram-system.html (accessed on 12 July 2012).
31. Zetter, K. Equipment maker caught installing backdoor account in control system code. *Wired Threat Level*, 25 April 2012. Available online: http://www.wired.com/threatlevel/2012/04/ruggedcom-backdoor/ (accessed on 27 April 2012).
32. Critical Foundations: Protecting America's Infrastructures—Report of the President's Commission on Critical Infrastructure Protection. Available online: http://www.fas.org/sgp/library/pccip.pdf (accessed on 11 July 2012).
33. The National Strategy to Secure Cyberspace. Available online: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (accessed on 3 May 2012).
34. The Comprehensive National Cybersecurity Initiative. National Security Council. Available online: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed on 3 May 2012).
35. Strategy for Securing Control Systems. Department of Homeland Security. Available online: http://www.uscert.gov/control_systems/pdf/Strategy%20for%20Securing%20Control%20Systems.pdf (accessed on 3 May 2012).
36. Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise. Department of Homeland Security. Available online: http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf (accessed on 3 May 2012).
37. Zetter, K. Report strengthens suspicions that Stuxnet sabotaged Iran's nuclear plant. *Wired Threat Level*, 27 December 2010. Available online: http://www.wired.com/threatlevel/2010/12/isis-report-on-stuxnet/ (accessed on 7 May 2012).
38. Sternstein, A. DHS cyber chief: Industrial system threats are growing. *Nextgov*, 2 May 2012. Available online: http://www.nextgov.com/cybersecurity/2012/05/dhs-cyber-chief-industrial-system-threats-are-growing/55541/ (accessed on 3 May 2012).
39. Testimony of Deputy Under Secretary Philip Reitinger, National Protection and Programs Directorate, Before the US House Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Examining the Cyber Threat to Critical Infrastructure and the American Economy. Available online: http://www.dhs.gov/ynews/testimony/testimony_1300283858976.shtm (accessed on 3 May 2012).