Stuxnet

CSS CYBER DEFENSE HOTSPOT ANALYSIS

Stuxnet

Zürich, October 2017

Version 1

Cyber Defense Project (CDP)
Center for Security Studies (CSS), ETH Zürich

CSS ETH Zurich

ETH zürich

Author: Marie Baezner, Patrice Robin

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zürich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group; Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Andreas Wenger, Director of the CSS

Please cite as: Baezner, Marie; Robin, Patrice (2017): Hotspot Analysis: Stuxnet, October 2017, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

Executive Summary

Target:	Centrifuges[1] used in the uranium enrichment process in Nuclear plant at Natanz in Iran.
Tool:	Stuxnet: a worm using four zero-day vulnerabilities and infecting computer networks through USB-flash drives.
Effects:	Damage to the centrifuges; modification or/and creation of cyber strategies in the world; increase in awareness of cybersecurity issues.
Timeframe	2009 - 2011

The discovery of Stuxnet raised awareness of cybersecurity issues all around the world. With this piece of malware, States realized that critical infrastructures were vulnerable to cyberattacks and that the potential consequences could be disastrous. The aim of this hotspot analysis is to better understand the case of the Stuxnet worm and its effects. The objective is also to comprehend how Iran managed the situation and how it reacted.

This analysis focuses on the specific case of the Stuxnet worm and the effects of its discovery in Iran and the international community. In this report, a hotspot is defined as a precise event that occurred in cyberspace and had effects in the physical world.

Description

In 2010, the Stuxnet worm was discovered in an Iranian computer. The piece of malware surprised computer experts due to its sophistication and the use of four zero-day exploits. It was later discovered that the malware was not designed to spy, but to sabotage centrifuges in the power facilities of Natanz in Iran. It is believed that the USA built Stuxnet with the support of Israel with the goal of stopping or delaying the Iranian nuclear program. The worm was probably implanted in the Natanz power plant's network with the use of a compromised USB-drive. This technique enabled the worm to penetrate a network that is normally separated from other networks.

Effects

The Hotspot analysis shows that Stuxnet had an impact on Iranian society and politics by making it look weak for not securing properly its critical infrastructures. The effects were also felt in the Iranian economy as the state had to spend money to replace the broken centrifuges and needed to create a new cybersecurity unit. The technological results of this case study showed that malware could be designed specifically to sabotage a very precise piece of industrial equipment. It also revealed new zero-day vulnerabilities and that driver certificates could be stolen and used for malicious intents.

At the international level, Stuxnet had the effect of being a wakeup call for states. They suddenly realized that they needed to develop their cybersecurity policies and/or strategies. They also recognized that they required a comprehensive cybersecurity strategy that includes critical infrastructures and private actors that manage them. Stuxnet also had the effect of decreasing tensions in the Middle East as the Iranian nuclear program did not seem as threatening as before. There was also a fear among the international community to see new versions of Stuxnet appearing in the wild and in cybercrime circles. However, no transformed versions of Stuxnet have come into existence since 2010.

Consequences

Various consequences can be derived from the discovery of Stuxnet and its effects. First, states could work on their cybersecurity by raising awareness of the fact that air gapped networks are also at risk. States also need to integrate private actors who manage critical infrastructures in their cybersecurity processes. Second, states should develop a plan or process on their way to respond to cyberattacks such as Stuxnet. The plan should include infrastructure resilience, but also a way to respond to state actors behind the attacks. Third, states could develop cybersecurity norms and standards for industrial goods to ensure a minimum level of security in networked equipment. Fourth, at the international level, states should try to promote international cooperation on cybersecurity and norms on states' behavior in cyberspace. This could help to reduce mistrust and the risks of misinterpretation among states in regard to cyberspace.

[1] Technical words are explained in a glossary in Section 7 at the end of the document.

1 Introduction

Stuxnet is a computer worm[2] discovered in 2010, which affected nuclear installations in Iran. This cyber-incident provoked a vast change in states' cyber policies and strategies.

This hotspot analysis examining Stuxnet is relevant because the discovery of the worm brings a real change on how states perceive cyberthreats. There is a clear distinction in cyber strategies before and after Stuxnet. The literature on the worm is extensive. However, the time which passed since Stuxnet occurred enabled the research to investigate the events from a different perspective, and with a more conscious approach removing opportunistic and unfounded comments that came out directly after the discovery of the worm.

The analysis of hotspots helps to understand theoretical and abstract concepts of cybersecurity by bringing clear examples. The aim of the hotspot analysis is to examine how victims of cyberattacks were impacted and how they responded to them. This report will also be used as a basis for a broader analysis that will compare various hotspots. This broader document will also provide advice on how states can revise their policies and actions if faced with similar situations.

The document can be updated to ensure the accuracy of the events. This would happen when new elements on the events are disclosed or when important changes occur.

The analysis is organized as follows. Section 2 describes the historical background and chronology of the events that lead to the discovery of Stuxnet and its investigation. It also looks at the events that shaped the specific context of the tensions between Iran and the USA.

In Section 3, the analysis details the technical specificities of the Stuxnet worm, what it was targeting and who might have developed it. It shows that the piece of malware was only targeting a specific type of centrifuge that was located in the Iranian nuclear facility of Natanz and how it was affecting them. It looks at who might have been able to develop a tool such as Stuxnet and why.

Section 4, examines the effects of Stuxnet on Iranian politics and society, on its economy, on the technological field and at the international level. The impact of the Stuxnet worm on Iranian society and politics was characterized by a feeling of insecurity and an indecisive stance from the Iranian government. A state that was a victim of such an intrusion would feel insecure and fear other similar attacks. This was the case in Iran and the Iranian government also seemed unsure how to respond to the attack. The economic impacts were mostly marked by the material costs of replacing the broken centrifuges and building new cyberdefense capabilities.

Stuxnet also had some repercussions in the technological field, as it was the first time that such malware would be designed to target such specific object. The discovery of Stuxnet also brought to light new zero-day vulnerabilities and the fact that driver certificates could be stolen and used in a malware.

At the international level, the discovery of Stuxnet provoked a wave of new national cybersecurity strategies as states realized that cybertools could be used against critical infrastructures. Also States feared to see transformed versions of Stuxnet flourish among cybercriminals. Nevertheless, the delays caused by the worm in the Iranian nuclear program managed to decrease the regional tensions among neighbors.

In conclusion, Section 5 brings recommendations based on the effects of Stuxnet. It shows how states can improve their cybersecurity with awareness campaigns and comprehensive cyber strategies integrating private partners in charge of critical infrastructures. States could also ameliorate their cybersecurity by producing cybersecurity guidelines or standards for networked industrial equipment. They can also contribute to reduce mistrust and risks of misperceptions in cyberspace on the international level by promoting confidence building measures (CBM)[3].

[2] Technical words written in italics are explained in a glossary in Section 7 at the end of the document.

[3] Abbreviations are listed in Section 8 at the end of the document.

2 Background and chronology

This section explores the historical background and the chronology of the events that lead to the discovery of the Stuxnet worm and subsequent investigations. This analysis of events is important for understanding the context in which Stuxnet was developed and used against the Iranian nuclear program and why it was used at that particular moment.

The discovery of Stuxnet took place in the difficult context of the tensions between Iran and the USA. The situation was strained by Iran trying to develop nuclear energy and possibly nuclear weapons. The condition even deteriorated to the point that Israel was ready to physically intervene to stop the Iranian nuclear program.

Date	Events
29.01.2002	George Bush gives his famous state-of-the-union speech to US Congress describing North Korea, Iran and Iraq as an "Axis of evil" for seeking to develop weapons of mass destruction (The Economist, 2002).
08.2002	An Iranian dissident group exposes that their government is enriching uranium in its nuclear facility at Natanz. The USA reacts by asserting that Iran is trying to develop nuclear weapons.
02.2003	Iran acknowledges that they are enriching uranium at Natanz and the international inspectors of the International Atomic Energy Agency (IAEA) visit the nuclear plant for the first time and will continue to visit it on a regular basis afterwards.
2006	The international community begins diplomatic discussions to encourage Iran to stop its nuclear program. However the latter does not want to halt and is subjected to new international sanctions. These exacerbate the existing tensions between the USA and Iran (Davenport, 2016).
06.2010	VirusBlockAda, an antivirus company based in Belarus discovers the Stuxnet worm. They received a sample of malware causing a computer in Iran to continually reboot itself. This malicious software surprises the specialists because of its use of a zero-day exploit, which is unusual for a computer worm (Zetter, 2011a). Normally worms would exploit flaws in webpages, or bugs in genuine software to infect a computer (Barwise, 2010).
12.07.2010	The news of the discovery of a computer worm using a zero-day exploit goes public and the antivirus and technology communities start to reverse-engineer and investigate this peculiar malware. At this time, it is believed that Stuxnet is an industrial spying-tool. Its sophistication suggests that significant resources were invested in its development (Zetter, 2011a).
08.2010	The antivirus firm, Symantec, reveals that the purpose of the worm is to sabotage and not to spy (Zetter, 2011a). They also notice that about 60% of the infected computers in the world are located in Iran, which lead them to think that the worm's spread may originate from there (Matrosov et al., 2010, p. 15). Indeed, experts retraced the start of the spread to five organizations in Iran, confirming that it is the starting point of the infections and probably the target (Lindsay, 2013, p. 380). During the same period it is also noticed that Stuxnet's Command and Control (C&C) servers lose connection with the infected computers in Iran. The experts think that this disconnection means that Iran is trying to deal with the worm and to contain its spread (Zetter, 2011b). The Bushehr power plant in Iran is supposed to launch its nuclear energy section, but is delayed. According to Iranian officials, an undetermined technical problem is the cause of the delay (Collins and McCombie, 2012, p. 85).
09.2010	Iranian officials admit that some personal computers from employees at the Bushehr nuclear plant are infected by a computer virus. They accuse Western countries of being behind the attack (Farwell and Rohozinski, 2011, p. 25).
11.2010	Iran stops its enrichment of uranium completely in the nuclear plant of Natanz without giving any reason (Farwell and Rohozinski, 2011). It is later assumed that they are trying to purge the power plant of Stuxnet. Later, the head of Iran's Atomic Energy Organization, and acting Foreign Minister at the time, admits that a computer virus has infected Iranian nuclear installations (Albright et al., 2010).

12.2010	The Institute for Science and International Security (ISIS), a US-based non-profit institution following the evolution of the Iranian nuclear program since the 1990s, confirms that the Stuxnet worm is programmed to target elements set in the same configuration as the Natanz's centrifuges.

3 Description

This Section first describes the specificities and features of the Stuxnet worm. It looks into the technical details that make this piece of malware so special. Second, it describes the particularities of Stuxnet's target and how it infected it. Finally, it looks at the identity and origin of the possible developers of Stuxnet and why they could have created such tool.

3.1 Tool

Stuxnet is the name of a specific worm, a piece of computer malware, which targets supervisory control and data acquisition (SCADA) systems in industrial controllers. It is difficult if not impossible to know exactly how the malware was developed, but it is certain that it required considerable resources in manpower, time and finance. Specialists evaluating the development of the worm estimate it must have required a team of five to ten programmers working full-time for at least six months (Chen and Abu-Nimeh, 2011, p. 92).

Stuxnet's size, bigger than comparable worms, was written in several different programming languages with some encrypted components[4] (Chen, 2010, p. 3). It used not one but four zero-day vulnerabilities to infect computers: An automatic process from connected USB-drives, a connection with shared printers and two other vulnerabilities concerning privilege escalation. The latter is a computer process that allowed the worm to execute software in computers even when they were on lock-down (Naraine, 2010). Stuxnet looked to infect computers working on the Microsoft Windows operating system through one of these vectors. When it found one, it used valid, but stolen, driver certificates from RealTek and JMicron to download its rootkit. Using these driver certificates the worm could then search for the Siemens Simatic WinCC/Step-7 software, a program used to control industrial equipment (Falliere et al., 2011, p. 33; Matrosov et al., 2010, p. 68). By infecting files used by this software, the worm was able to access and control the Programmable Logic Controllers (PLCs), small computers use to regulate the power in industrial devices (De Falco, 2012, p. 6). Furthermore the worm was also able to communicate with other infected machines and C&C servers in Denmark and Malaysia in order to update itself and send information about what it had found (Chen and Abu-Nimeh, 2011, p. 93).

When all these requirements were met, Stuxnet would launch its attack by changing the speed of the centrifuges' rotors and cause irreparable damage (Langner, 2013, p. 5).

3.2 Target

The target of Stuxnet appears to have been the Iranian nuclear plant and uranium enrichment site in Natanz. The fact that Stuxnet was programmed to target devices organized in groups of 164 objects and Natanz's cascades were arranged in 164 centrifuges was probably not a coincidence (Albright et al., 2010; Broad and Sanger, 2010). The power plant in Bushehr could also have been a main target, but it enriches plutonium and therefore requires a different configuration of centrifuges (Farwell and Rohozinski, 2011, p. 25). Iran uses IR-1 centrifuges, a European model from the late 1960s and early 1970s, which are both inefficient and now obsolete (Langner, 2013, pp. 5–6). These centrifuges are also fragile and an abrupt change of speed could cause damage or even breakage. The creators of Stuxnet were aware of this flaw and exploited it.

The nuclear plant of Natanz has an air gapped and closed computer network, which means that it does not have a connection to the Internet or other networks. Therefore, it is highly probable that Stuxnet infected the network through the vector of a removable USB-drive (De Falco, 2012, p. 3). This means that the creators of the worm required a person to deliver the worm and infect the network.

3.3 Attribution and actors

Several antivirus experts asserted that only a state could have developed Stuxnet because of its level of complexity, resource investment, and the fact it seemed to be specifically designed to target the centrifuges of Natanz (De Falco, 2012, p. 26). What is certain is that the creators of the worm had extensive knowledge about the Iranian facilities, machines and computer programs. They also needed a testing ground to be able to verify that their target-oriented malware was doing what it was expected to do (Langner, 2013, p. 20).

The Iranians accused the West and more precisely NATO of being behind the attack (Collins and McCombie, 2012, p. 87). Nevertheless experts claimed that the evidence, and the motive pointed to the USA and Israel as the perpetrators (Lindsay, 2013, p. 366; Nakashima and Warrick, 2012; Rosenbaum, 2012; Zetter, 2011a). There is speculation as to whether Israel was involved in the development of the malware, with experts from Symantec claiming they saw some evidence of its involvement in the coding lines (Zetter, 2011a). For example, one sign could be the presence of the word

[4] See the annex 1 in Section 6 for a comparison table between the technical nature of a normal worm and Stuxnet's.

"myrtus" in the code, which was the name of the file where the worm was stored when it was being developed. This word is believed to be a reference to Queen Esther who saved the Jews from a massacre from the Persians in the Bible and whose name in Hebrew refers to the word "myrtle" (Zetter, 2011a). The involvement of Israel in the development of Stuxnet remains an uncertainty and the evidence pointing in that direction may also have been planted to mask the identity of the real perpetrator. However, Richard Clarke, former US National Coordinator for Security, Infrastructure Protection and Counter-terrorism, argued that if the USA had developed Stuxnet, Israel might have helped in the project by providing a testing site with a similar sample to the IR-1 centrifuge (De Falco, 2012, p. 26; Rosenbaum, 2012).

The New York Times journalist, David E. Sanger, reported in his book that the USA had conducted a covert cyber-campaign, named Operation Olympic Games, against Iranian nuclear facilities. It is said that Stuxnet would have been one piece of malware developed and launched in the context of this operation. The campaign would have begun in 2006 under the Bush administration and would have been intensified by US President Obama (Zetter, 2011a). The operation was unlikely to have been limited to cyberspace. The assassinations of Iranian scientists in 2010 and 2011 that were attributed to the USA and Israel suggest that Stuxnet was only one piece in a larger operation aimed at slowing down or stopping Iran developing nuclear technology (De Falco, 2012). It is also believed that the covert cyber-operation was an agreed concession to avoid an Israeli airstrike on Iranian nuclear facilities. Previously, President Bush had refused to allow Israeli jets to cross the Iraqi border to strike Iranian nuclear installations (De Falco, 2012, p. 54; Lindsay, 2013, p. 366).

Alternatively, Farwell and Rohozinski (2011) argue that Stuxnet's patchwork-design indicates that Stuxnet could have been developed, for some part, by the cybercrime sector, specifically the Russian offshore programming community. They explain that some elements of the worm's codes have the same design as codes written by the cybercrime community. They assert that the USA was still the main developer, but that it could have outsourced the development of certain parts of Stuxnet to these groups.

It would also have been possible for Russia to be the perpetrator of the attack. Russian workers had access to nuclear facilities in Iran as they were working with them on the nuclear site of Bushehr. Apart from the fact that Russia has the capabilities to develop such malware, its motive might have been to prevent Iran from enriching its own uranium by damaging the nuclear sites with Stuxnet. In consequence, Iran would have had no other choice than to buy enriched uranium from Russia (De Falco, 2012, p. 28).

There will always be uncertainties when it comes to attribution in cyberspace. Attribution would normally the "*cui bono*" (to whose benefit) logic. However it remains uncertain that a particular actor that seems to be the perpetrator is indeed the perpetrator. In the case of Stuxnet most evidence tends to show the USA as the main instigator of the development and release of Stuxnet. Indeed, with Stuxnet, the USA would have delayed the uranium-enriching program and avoided a war between Iran and Israel. Even so, the involvement of Israel or Russia remains uncertain and, as is often the case in covert operations and cyberattacks, nothing can be confirmed entirely.

4 Effects

First, this Section analyzes the social and domestic political effects resulting from the attack of Stuxnet on the power plant of Natanz. Second, it examines how the malware impacted the Iranian economy. Third, it studies the effects of the worm on the technological field. Finally, it looks into the impacts of the discovery of the Stuxnet at the international level.

4.1 Social and political effects

On the internal political level, the cyberattack discredited the Iranian government. The Iranian authorities were not able to protect their nuclear facilities from a foreign cyberattack. The Iranian government seemed indecisive on how to officially react to the news that a computer worm might have infected their nuclear facilities. In September 2010, the Iranian authorities first minimized the impact of the attack in their discourse, probably to avoid too much blame from the population, by stating that only personal computers without connections to the nuclear facility of Bushehr were infected and by designating the West and NATO as perpetrators. Two months later, they admitted that the worm had been active in their nuclear plants for more than a year. However, they did not stay inactive and worked intensively to contain and remove the worm, and to identify the attackers (Zetter, 2011b). Iranian authorities did not retaliate to the cyberattacks because the identity of the perpetrators was unknown or unclear and because there was no precedent on how a state should respond to such attack. This inaction made the Iranian government look weak and appear as an easy target.

Stuxnet had almost no direct effects on the Iranian population or society itself. The worm was designed to avoid collateral damage (Rosenbaum, 2012). If the attack did have collateral damage or stronger effects that might have caused the loss of human lives, it might have been interpreted as a use of force and might have led to an escalation of violence between Iran and the countries they perceived to have been responsible (Collins and McCombie, 2012, p. 88; Rosenbaum, 2012). The biggest impact of Stuxnet on society was likely a feeling of insecurity. An intrusion into a private domain is never taken lightly. For this reason it can be assumed that Iranians felt betrayed by the country's ineffective cybersecurity measures and its weak stance in regard to the perpetrators. The infection of Iranian networks proved that even though air gapped networks are usually more secure than other networks, it cannot be considered

secure enough (Zetter, 2014). Although the worm only targeted Iranian nuclear facilities the fact that the malware spread to other computers in the world contributes to a global feeling of insecurity.

4.2 Economic effects

This attack also had direct economic effects for Iran. Due to Iran being under international embargoes, it does not have access to the international market to buy nuclear-related materials. In particular they cannot buy centrifuges; therefore they build them themselves, sometimes with foreign components. This patchwork of materials might also be a reason for the quick deterioration of the centrifuges. Being under embargo also means that they have very limited resources and the breakage of almost 1,000 centrifuges added pressure on their material stocks and their budget. From a cost-benefit perspective, the poor returns in terms of productivity of the Natanz nuclear plant might also have added pressure on the finances of the state as it would need to buy enriched uranium from other countries.

The cyberattack also had long-term economic repercussions for Iran as they had to manage the delays in production of low enriched uranium. Establishing new security and cybersecurity measures in nuclear facilities to avoid the reoccurrence of an attack such as Stuxnet would also have meant a significant financial investment. For example, in November 2011 Iran created a new cyberunit in the Revolutionary Guard Corps to address cyberattacks (Fogarty, 2011). This unit is likely to have been behind the cyberattacks of March 2011 in the USA. A US company selling digital authentication certificates, Comodo, accused Iran of attempted cyberattacks on several US companies including Google and Microsoft (Lindsay, 2013, p. 397; Morton, 2013; Peckham, 2011). This attack might have been retaliation for the Stuxnet attack, but even though it seemed to originate from Iran, nothing proved that it was perpetrated by the new cyberunit. According to the NSA, Iran might also have been behind the Shamoon attack which was a worm launched in August 2012 to wipe computers from the Saudi oil-company, Aramco (Zetter, 2015).

4.3 Technological effects

The most direct and only physical effect of Stuxnet was the damage caused to the centrifuges. It was clearly designed to affect the nuclear facility of Natanz. The malware was believed to affect the speed of the centrifuges making them alternate between high and low speed (Farwell and Rohozinski, 2011, pp. 24–25). This change in speed was masked by the worm's rootkit, making the operators think that the centrifuges were going at their normal speed. The change of speed would have caused the centrifuges to wear out faster and to be damaged beyond repair. Natanz had between 6,000 and 9,000 operating centrifuges at the time and about 1,000 of them had to be changed (De Falco, 2012, p. 23; Nakashima and Warrick, 2012). IAEA experts assessing the plants noticed that Iran replaced about 10% of its centrifuges each year due to breakage but between mid-2009 and mid-2010 they removed slightly more centrifuges than usual (Nakashima and Warrick, 2012). ISIS reported that the level of production of low enriched uranium remained steady and even increased during the period of the Stuxnet attack. However, the production levels were not as efficient as they could have been with fully working centrifuges. In other words, the output of low enriched uranium only increased because of an increased working rhythm to compensate for the loss of the damaged centrifuges. In February 2010 the levels were still lower than before the attack in November 2009. It took Iran approximately one year to recover totally from the effects of the Stuxnet attack and return to a level of production similar to November 2009 (Albright et al., 2010).

Taking these observations into account, the physical consequences of Stuxnet were rather limited, but its probable goal would have been to remain hidden for a certain amount of time, damage the centrifuges and disappear (Nakashima and Warrick, 2012). Its discovery probably interrupted the process and put a premature end to the operation. However, the fact that the number of damaged centrifuges was only slightly more than usual adds the possibility that the damage might have been caused by poor manufacturing or normal deterioration (Albright et al., 2010).

The attack of Stuxnet also directly affected the technology sector. Those companies that developed the software with vulnerabilities that were exploited to infect and control the computers in Iran were forced to react in order to contain the malware. Microsoft issued patches to solve the zero-day exploits and Siemens offered patches and removal tools to their customers to remove Stuxnet in the months following the discovery of the malware (Langner, 2011, p. 50; Lindsay, 2013, p. 391). Verisign also reacted within weeks by revoking the stolen certificates from RealTek and JMicron that were used to fool infected computers into making them think that the worm was a legitimate program (Lindsay, 2013, p. 394; Matrosov et al., 2010, p. 19). Inaction by these multinational companies would have led to a loss of confidence from the customers in their ability to produce secure software and technologies. Moreover stricter rules for the management of driver certificates and other digital key systems have been issued to prevent the reoccurrence of a malware using stolen certificates (De Falco, 2012, p. 37).

Long-term technological consequences of Stuxnet can be seen in the Iranians increasing their mistrust of technical malfunctions in their facilities. Every bug or breakdown might trigger a suspicion of another cyberattack on their systems. They later discovered two other malware operating stealthily in their networks: Duqu and Flame.

4.4 International effects

At the international level, the cyberattack managed to delay the Iranian uranium-enrichment program for a short period of time, which decreased slightly the related international tensions. Indeed, it seemed that the apparent delays in the program had reassured Israel enough that it would not risk launching an airstrike to physically halt enrichment (Lindsay, 2013, p. 385).

At the international level, the developer of Stuxnet, even if its identity remains uncertain, showed that it is possible to build a highly sophisticated, offensive cybertool, and that perpetrators have the resources to accomplish such an attack. Moreover, this case demonstrated that separating a critical infrastructure's network from the internet can no longer be considered a sufficient security measure. States realized that they needed to take action in order to avoid becoming a victim of such attack. Several states, like Iran, invested in cybersecurity, or created military cyberunits and/or centers to build up their capabilities in case of an upcoming cyberwar. Some states also started to review and update their cyber strategies to cover critical infrastructures, and to strengthen their ability to legally respond to cyberattacks (Dunn Cavelty, 2012, pp. 150–151).

Another consequence of the Stuxnet cyberattack was the fact that the worm leaked and spread to other computers outside Iran. Having the malware in the wild meant that anybody with the right competences could reverse-engineer it, modify it to suit other purposes, sell it or use it (Collins and McCombie, 2012, p. 89). The possibility of criminal or terrorist groups starting to use such tools for their own purposes was particularly concerning. As a result, the ability to actively protect systems has also been included in states' defense policies, strategies, expenses and discourses. However, this threat has never materialized. Stuxnet's code has not been transformed and used for other purposes since its discovery in 2010. Modified versions of Stuxnet did not emerged because it is not possible to simply copy a piece of malware. This means that it needs to be reprogrammed to fit its new target and it is not easy to find the necessary resources to do this. Moreover, zero-day exploits used by Stuxnet ceased to be zero-day vulnerabilities the moment they were discovered. In consequence, if perpetrators wanted to reuse Stuxnet's code, they would have to find new zero-day exploits, which would take time and resources.

5 Policy Consequences

This Section examines the consequences that derived from the discovery of Stuxnet. These consequences are presented as recommendations for state actors.

5.1 Improving Cybersecurity

To avoid situations such as Stuxnet reoccurring, states can focus on improving their cybersecurity. The case of the Stuxnet worm showed that infecting computers by means of USB-drive was effective and could affect air gapped networks. Therefore, states should particularly focus on computer users and the issue of using unknown USB-drives. They can organize sensitization campaigns specially oriented on this issue for workers in critical infrastructures. Users would get a better understanding of the risks and possible damage that such behavior could cause. It would hopefully result in more cautious conduct.

States can also improve their cybersecurity by creating a standard operating procedure for a simplified and proper way to respond to a cyberattack. This procedure could be at the technical level with cybersecurity experts acting rapidly to solve the technical problems linked to the attack and to come back to a normal working rhythm after the attack. Also when Iran recognized it had been targeted by a cyberattack, there seemed to have been confusion inside the Iranian authorities on the way to politically respond to the attack. Therefore, a standard operating procedure at the political level could also help provide guidance to the authorities on how to respond to a cyberattack perpetrated by another state if the attribution could be confirmed and within the frame of available resources.

5.2 Integration of critical infrastructures in cyber strategy

The damage caused by Stuxnet to the Iranian centrifuges showed that critical infrastructures could be targeted by cyberthreats. The fact that Natanz's networks were separated from the other networks did not sufficiently protect it against the malware. In consequence, states should take into account that critical infrastructures should be integrated in cybersecurity strategies. Such consideration would imply an increase in protection in regard to cyberthreats, with higher cybersecurity standards. It also signifies more cooperation of the state with the actors, public or private, that manage these infrastructures. The goal would be to increase protection against cyberthreats, but also to increase resilience in case of cyberattacks.

5.3 Establishment of cybersecurity standards for industrial equipment

States could promote international cybersecurity standards for industrial equipment. The incident of the Stuxnet worm showed that industrial equipment such as SCADA systems often had weak cybersecurity standards and were open to attack when connected to the internet. To diminish the risk of these vulnerabilities being exploited, States could promote at the international level technical standards that would indicate the level of cybersecurity of connected equipment. States could then decide to only take connected equipment with the highest standards for critical infrastructures. States could also recommend that operators of critical infrastructures not connect SCADA systems to the internet as air gapped network remain a suitable way to avoid infection.

5.4 Promotion of international Confidence Building Measures (CBM)

States could reduce mistrust and misperceptions in cyberspace by promoting internationally CBM. These could also help to later develop international norms for cyberspace. So far, states have only agreed to apply international law to states' activities in cyberspace, respecting principles such as proportionality or avoiding civilian casualties. However, the difficulties inherent to the attribution of cyber activities increase ambiguities and mistrust among states. CBM could be a first step towards more transparency and better interstate relations. CBM could be developed at the bilateral level or at regional or international level in fora or international organizations. Stauffacher and Kavanagh (2013) suggested a series of such measures for cybersecurity which consist of: transparency measures, compliance indicators and monitoring transparency measures, cooperative measures, communication and collaborative mechanisms and restraint measures. States could then expand such measures into international norms or treaties.

6 Annex 1

Comparison table between Stuxnet and other worms (Chen and Abu-Nimeh, 2011, p. 91):

Features	Stuxnet	Usual worm
Target	Only Siemens Simatic/Step-7 software	Computers Indiscriminately
Size	500 Kilobytes	App. 100 Kilobytes
Infection vectors	USB-removable drives or shared printers	Internet
Exploited vulnerability to infect	Four zero-day exploits	One zero-day exploit
Purpose	Affect Iranian centrifuges	Most of the time spread or install a backdoor

7 Glossary

Air gapped network: A security measure that implies to physically separate a network from the Internet or other unsecure local networks (Zetter, 2014).

Cascade: Centrifuges are organized in groups that are called “cascades” in uranium enrichment process (Langner, 2013).

Centrifuge: a centrifuge is a cylinder with a rotating rotor in which uranium is fed in form of isotopic gas. The goal is to use the centrifugal force to separate the heavier gas for the lighter. The former becomes the depleted uranium and the latter the enriched (Institue for Science and international Security, n.d.).

Command and Control (C&C): A server through which the person controlling a malware communicates with it in order to send commands and retrieve data (QinetiQ Ltd, 2014, p. 2).

Confidence Building Measures (CBM): Various procedures that can be established to build trust and prevent escalation between state-actors (United Nations, n.d.).

Driver certificate: certification issued by firms to authenticate their drivers. Let the computer know that the software is genuine (Matrosov et al., 2010).

Duqu: worm discovered in 2011 which goal was to steal information (Kushner, 2013).

Flame: worm discovered in 2012 used to gather information in countries in the Middle East (Kushner, 2013).

Low enriched uranium: essential element to make nuclear fuel (International Atomic Energy Agency, 2017).

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins and McCombie, 2012).

Patch: An update for software that repairs one or more identified vulnerability(ies) (Ghernaouti-Hélie, 2013, p. 437).

Privilege escalation: function allowing a remote computer user to access another computer’s system by using a Guest account (Matrosov et al., 2010).

Programmable Logic Controllers (PLCs): small computers controlling electrical functions in hardware such as switches (Collins and McCombie, 2012).

Rootkit: program downloading itself in the infected system and taking control of certain functions (Lindsay, 2013).

Shamoon: Computer virus targeting computers from the energy sector in the Middle East. The Saudi Arabia national oil company Aramco was particularly hit by the attack. The virus wipes the files from an infected computer rendering it unusable (BBC News, 2012).

Siemens Simatic WinCC/Step-7 software: industrial software serving as human-machine interface (Lindsay, 2013)

Supervisory Control And Data Acquisition (SCADA): Computer programs used to control industrial processes (Langner, 2013, p. 9)

Worm: standalone, self-replicating program infecting and spreading to other computers through networks (Collins and McCombie, 2012).

Zero-day exploit / vulnerabilities: security vulnerabilities from which software developers are not aware, which could be used to hack a system (Karnouskos, 2011)

8 Abbreviations

C&C	Command and Control
CBM	Confidence Building Measures
IAEA	International Atomic Energy Agency
IP	Internet Protocol
ISIS	Institute for Science and international Security
NATO	North Atlantic Treaty Organization
PLCs	Programmable Logic Controllers
SCADA	Supervisory Control And Data Acquisition

9 Bibliography

Albright, D., Brannan, P., Walrond, C., 2010. Did Stuxnet take out 1,000 Centrifuges at the Natanz Enrichment plant? Institute for Science and International Security.

Barwise, M., 2010. What is an internet worm? [WWW Document]. Webwise. URL http://www.bbc.co.uk/webwise/guides/internet-worms (accessed 20.10.16).

BBC News, 2012. Shamoon virus targets energy sector infrastructure [WWW Document]. BBC News. URL http://www.bbc.com/news/technology-19293797 (accessed 8.11.16).

Broad, W.J., Sanger, D.E., 2010. Worm Was Perfect for Sabotaging Centrifuges [WWW Document]. N. Y. Times. URL http://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html (accessed 20.10.16).

Chen, T., 2010. Stuxnet, the real start of cyber warfare? [Editor's Note. IEEE Netw. 24, 2–3. doi:10.1109/MNET.2010.5634434

Chen, T.M., Abu-Nimeh, S., 2011. Lessons from Stuxnet. Computer 44, 91–93. doi:10.1109/MC.2011.115

Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. doi:10.1080/18335330.2012.653198

Davenport, K., 2016. Timeline of nuclear Diplomacy With Iran [WWW Document]. Arms Control Assoc. URL https://www.armscontrol.org/factsheet/Timeline-of-Nuclear-Diplomacy-With-Iran#2006 (accessed 19.10.16).

De Falco, M., 2012. Stuxnet Facts Report: A Technical and Strategic Analysis. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.

Dunn Cavelty, M., 2012. The Militarisation of Cyberspace: Why Less may Be Better, in: 2012 4th International Conference on Cyber Conflict (CYCON 2012): Tallinn, Estonia, 5 - 8 June 2012. IEEE, Piscataway, NJ, pp. 141–153.

Falliere, N., O Murchu, L., Chien, E., 2011. W32.Stuxnet Dossier (No. 1.4). Symantec Security Response.

Farwell, J.P., Rohozinski, R., 2011. Stuxnet and the Future of Cyber War. Survival 53, 23–40. doi:10.1080/00396338.2011.555586

Fogarty, K., 2011. Iran responds to Stuxnet by expanding cyberwar militia [WWW Document]. ITworld. URL http://www.itworld.com/article/2746341/security/iran-responds-to-stuxnet-by-expanding-cyberwar-militia.html (accessed 19.10.16).

Ghernaouti-Hélie, S., 2013. Cyberpower: crime, conflict and security in cyberspace, 1. ed. ed, Forensic sciences. EPFL Press, Lausanne.

Institue for Science and international Security, n.d. What is a Gas Centrifuge? [WWW Document]. Inst. Sci. Int. Secur. URL http://exportcontrols.info/centrifuges.html (accessed 20.10.16).

International Atomic Energy Agency, 2017. What is LEU? [WWW Document]. Int. At. Energy Agency. URL https://www.iaea.org/topics/leubank/what-is-leu (accessed 12.7.17).

Karnouskos, S., 2011. Stuxnet worm impact on industrial cyber-physical system security. IEEE, pp. 4490–4494. doi:10.1109/IECON.2011.6120048

Kushner, D., 2013. The Real Story of Stuxnet [WWW Document]. IEEE Spectr. URL http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (accessed 18.10.16).

Langner, R., 2013. To kill a centrifuge: a technical analysis of what Stuxnet's creators tried to achieve.

Langner, R., 2011. Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Secur. Priv. Mag. 9, 49–51. doi:10.1109/MSP.2011.67

Lindsay, J.R., 2013. Stuxnet and the Limits of Cyber Warfare. Secur. Stud. 22, 365–404. doi:10.1080/09636412.2013.816122

Matrosov, A., Rodionov, E., Harley, D., Malcho, J., 2010. Stuxnet Under the Microscope (No. 1.31). ESET LLC.

Morton, C., 2013. Stuxnet, Flame, and Duqu - the OLYMPIC GAMES, in: A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association, Vienna, VA, pp. 212–232.

Nakashima, E., Warrick, J., 2012. Stuxnet was work of U.S. and Israeli experts, officials say [WWW Document]. Wash. Post. URL https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html (accessed 18.10.16).

Naraine, R., 2010. Stuxnet attackers used 4 Windows zero-day exploits [WWW Document]. ZDNet Eur. URL http://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/ (accessed 18.10.16).

Peckham, M., 2011. Iranian Government Accused in Serious Net Attack [WWW Document]. Time. URL http://techland.time.com/2011/03/24/iranian-government-accused-in-serious-net-attack/ (accessed 19.10.16).

QinetiQ Ltd, 2014. Command & Control: Understanding, denying, detecting. QinetiQ Ltd.

Rosenbaum, R., 2012. Richard Clarke on Who Was Behind the Stuxnet Attack [WWW Document]. Smithsonianmag.com. URL http://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/?no-ist (accessed 19.10.16).

Stauffacher, D., Kavanagh, C., 2013. Confidence Building Measures and International Cyber Security. ICT4Peace, Geneva, Switzerland.

The Economist, 2002. George Bush and the axis of evil [WWW Document]. The Economist. URL http://www.economist.com/node/965664 (accessed 18.10.16).

United Nations, n.d. Military Confidence-building [WWW Document]. U. N. Off. Disarm. Aff. URL https://www.un.org/disarmament/cbms/ (accessed 16.3.17).

Zetter, K., 2015. The NSA Acknowledges What We All Feared: Iran Learns From US Cyberattacks [WWW Document]. The Wired. URL https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/ (accessed 19.10.16).

Zetter, K., 2014. Hacker Lexicon: What Is an Air Gap? [WWW Document]. Wired. URL https://www.wired.com/2014/12/hacker-lexicon-air-gap/ (accessed 4.11.16).

Zetter, K., 2011a. How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History [WWW Document]. Wired. URL https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ (accessed 18.10.16).

Zetter, K., 2011b. Stuxnet Timeline Shows Correlation Among Events [WWW Document]. Wired. URL https://www.wired.com/2011/07/stuxnet-timeline/ (accessed 18.10.16).

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.