CSS CYBER DEFENSE PROJECT

Hotspot Analysis:

Stuxnet

Zürich, October 2017

Version 1

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zurich

ETH zürich

Authors: 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

1 Introduction 5

2 Background and chronology 6

3 Description 7
3.1 Tool 7
3.2 Target 8
3.3 Attribution and actors 8

4 Effects 9
4.1 Social and political effects 9
4.2 Economic effects 10
4.3 Technological effects 10
4.4 International effects 11

5 Policy Consequences 11
5.1 Improving Cybersecurity 11
5.2 Integration of critical infrastructures in cyber strategy 11
5.3 Establishment of cybersecurity standards for industrial equipment 12
5.4 Promotion of international Confidence Building Measures (CBMs) 12

6 Annex 1 13

7 Glossary 13

8 Abbreviations 14

9 Bibliography 14

Executive Summary

Target:	Centrifuges[1] used in the uranium enrichment process in a nuclear plant in 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. Through 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 understand 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 among the international community. In this report, a hotspot is defined as a precise event that occurs in cyberspace and impacts on the physical world.

Description

The Stuxnet worm was discovered in an Iranian computer in 2010. This piece of malware surprised computer experts due to its sophistication and the use of four zero-day exploits. It was later found that the malware was not designed to spy, but rather 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 by using a compromised USB drive. This technique enabled the worm to penetrate a network that is normally isolated 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 its critical infrastructures properly. 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 findings of this case study show that malware can be designed specifically to sabotage a very precise piece of industrial equipment. They also reveal new zero-day vulnerabilities and that driver certificates can be stolen and used for malicious intents.

At the international level, Stuxnet had the effect of being a wakeup call for states, which suddenly realized that they needed to enhance their cybersecurity policies and/or strategies. They also recognized that they required a comprehensive cybersecurity strategy that extends to critical infrastructures and the private actors that manage them. Stuxnet also had the effect of decreasing tensions in the Middle East, as the Iranian nuclear program was no longer perceived as an immediate threat. There was also concern among the international community that new versions of Stuxnet might appear in the wild and in cybercrime circles. However, no modified versions of Stuxnet have been found since 2010.

Consequences

Various consequences can be derived from the discovery of Stuxnet and its effects. First, states may wish to enhance their cybersecurity by raising awareness of the fact that even air-gapped networks are at risk. States also need to integrate private actors managing critical infrastructures in their cybersecurity processes. Second, states should develop plans or processes for responding to cyberattacks such as Stuxnet. Relevant plans should include infrastructure resilience as well as ways to respond to state actors behind the attacks. Third, states could develop cybersecurity norms and standards for industrial assets 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 international norms on states' conduct in cyberspace. This could help to reduce both mistrust and the risk of misinterpretation among states in regard to cyberspace.

[1] Technical terms 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 sweeping changes in states' cyber policies and strategies.

This hotspot analysis of Stuxnet is relevant because the discovery of the worm constituted a watershed in terms of how states perceive cyberthreats. There is a clear distinction in cyber strategies before and after Stuxnet. There is a wealth of literature on the worm, but the time that has elapsed since the Stuxnet incident has allowed researchers to investigate the events from a different perspective and with a more deliberate approach, eliminating opportunistic and unfounded comments made in the immediate aftermath of the discovery of the worm.

The analysis of hotspots helps to understand theoretical and abstract cybersecurity concepts by using clear examples. The aim of this hotspot analysis is to examine how victims of cyberattacks were impacted and how they responded to attacks. This report also serves as a basis for a broader comparative analysis of various hotspots. This broader document will also provide suggestions on how states may wish to revise their policies and responses if faced with similar situations.

This document may be updated in the future to accurately reflect any new developments. This may occur if and when new aspects of relevant events are disclosed or important changes occur.

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

Section 3 of the analysis details the technical specificities of the Stuxnet worm, what it was targeting and who may have developed it. It shows that this particular piece of malware only targeted a specific type of centrifuge located in the Iranian nuclear facility of Natanz and describes its effects. It additionally looks at who may have been capable of developing a tool such as Stuxnet and possible reasons for its creation.

Section 4 examines the effects of Stuxnet on Iranian politics and society, on the country's economy, in the technological realm and at the international level. The impact of the Stuxnet worm on Iranian society and politics was characterized by a resulting feeling of insecurity and an indecisive stance from the Iranian government. Any state falling victim to such an intrusion would feel insecure and concerned about potential similar attacks. This was also the case in Iran, and the Iranian government also seemed unsure how to respond to the attack. 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 realm, as it was the first time that malware of this type was designed to target a highly specific object. The discovery of Stuxnet also brought to light new zero-day vulnerabilities and the fact that driver certificates can be stolen and used in malware.

At the international level, the discovery of Stuxnet provoked a wave of new national cybersecurity strategies as states realized that cybertools can be used against critical infrastructures. Also, states were gravely concerned that modified versions of Stuxnet might flourish among cybercriminals. At the same time, the delays caused by the worm in the Iranian nuclear program alleviated regional tensions among neighbors.

This hotspot analysis concludes with recommendations derived from the effects of Stuxnet in Section 5. These show how states can improve their cybersecurity through awareness campaigns and comprehensive cyber strategies that integrate private partners in charge of critical infrastructures. States could also enhance their cybersecurity by producing cybersecurity guidelines or standards for networked industrial equipment, and they can work towards reducing mistrust and the risk of misperceptions in cyberspace on the international level by promoting confidence building measures (CBMs)[3].

[2] Technical terms 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 in the lead-up 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.

Stuxnet was discovered in the difficult context of existing tensions between Iran and the USA. The situation was strained by Iran trying to develop nuclear energy and possibly nuclear weapons, with circumstances even deteriorating 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 discloses 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 it is enriching uranium at Natanz. Inspectors from the International Atomic Energy Agency (IAEA) subsequently visit the nuclear plant for the first time and continue to visit the facility on a regular basis afterwards.
2006	The international community launches diplomatic discussions to encourage Iran to stop its nuclear program. However, Iran proves uncooperative and is subjected to new international sanctions as a result. These in turn exacerbate the existing tensions between the USA and Iran (Davenport, 2016).
06.2010	VirusBlockAda, an antivirus company based in Belarus, discovers the Stuxnet worm after the company receives 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 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 a tool for industrial espionage. 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), noting also that about 60% of infected computers worldwide are located in Iran, which leads them to believe that the worm's spread may have originated there (Matrosov et al., 2010, p. 15). Indeed, experts retrace the origin of the spread to five organizations in Iran, confirming that the country was the starting point and probably also the target of the infections (Lindsay, 2013, p. 380). During the same period, it is also found that Stuxnet's Command and Control (C&C) servers lose connection with the infected computers in Iran. Experts believe 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, the delay is caused by an unspecified technical problem (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 in the nuclear plant of Natanz completely without giving any reason (Farwell and Rohozinski, 2011). It is later assumed that this was an attempt 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 that has monitored the evolution of the Iranian nuclear program since the 1990s, confirms that the Stuxnet worm is programmed to target elements configured in the same manner as the Natanz centrifuges.

3 Description

This Section first describes the specificities and features of the Stuxnet worm and 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 was infected. Finally, it looks at the identity and origin of the possible developers of Stuxnet and why they would have created such a tool.

3.1 Tool

Stuxnet is the name of a specific worm, i.e. a piece of computer malware that 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 there can be no doubt that its development 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 is sizeable – larger than comparable worms – and it was written in several different programming languages with some encrypted components[4] (Chen, 2010, p. 3). It exploited 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 running the Microsoft Windows operating system via one of these vectors. When it identified an opening, it used valid, but stolen, driver certificates from RealTek and JMicron to download its rootkit. Using these driver certificates, the worm was then able to 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), i.e. small computers used to regulate 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 transmit information about what it had found (Chen and Abu-Nimeh, 2011, p. 93).

Once all these requirements were met, Stuxnet launched its attack by changing the speed of the

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

centrifuges' rotors, causing 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 may also have been a major 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 can 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, closed computer network, which means that it does not have a connection to the Internet or other networks. It is therefore highly probable that Stuxnet infected the network through the vector of a removable USB drive (De Falco, 2012, p. 3), meaning 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 have 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 in 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 designed 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 both 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 the country's involvement in the coding lines (Zetter, 2011a). This was suggested by the presence of the word "myrtus" in the code, for example, which was the name of the file where the worm was stored while it was being developed. This word is believed to be a reference to Queen Esther, who saved the Jews from a massacre by the Persians according to the Bible and whose name in Hebrew refers to the word "myrtle" (Zetter, 2011a). The involvement of Israel in the development of Stuxnet remains uncertain, and any evidence pointing in that direction may have been planted to mask the identity of the real perpetrator. However, Richard Clarke, the former US National Coordinator for Security, Infrastructure Protection and Counter-terrorism, argued that if the USA had developed Stuxnet, Israel may have assisted in the project by providing a testing site with a sample similar 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 conducted a covert cyber-campaign, named Operation Olympic Games, against Iranian nuclear facilities. It is believed that Stuxnet was one piece of malware developed and launched in the context of this operation. The campaign most likely began in 2006 under the Bush administration and would have been intensified under 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 component of a larger operation aimed at slowing down or stopping Iran's development of 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, at least in part, by the cybercrime sector, specifically the Russian offshore programming community. They explain that some elements of the worm's code feature the same design as code written by the cybercrime community. They assert that the USA still would have been the main developer, but that it could have outsourced the development of certain parts of Stuxnet to these groups.

There is also the possibility that Russia perpetrated the attack. Russian workers had access to nuclear facilities in Iran as part of a Russo-Iranian cooperation at the Bushehr nuclear site. Russia has the capabilities to develop such malware, and its motive may have been to prevent Iran from enriching its own uranium by damaging the country's nuclear sites with Stuxnet. As a consequence, Iran would have had no choice but 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 follow the "*cui bono*" (to whose benefit) logic. However, it is difficult, if not impossible, to prove that a particular

actor that seems to be the perpetrator is indeed the perpetrator. In the case of Stuxnet, most evidence points towards the USA as the main instigator of the development and release of Stuxnet. Indeed, the USA would have delayed the uranium enrichment program and avoided a war between Iran and Israel with Stuxnet. Even so, the involvement of Israel or Russia remains a possibility and, as is often the case in covert operations and cyberattacks, nothing can be confirmed beyond any doubt.

4 Effects

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

4.1 Social and political effects

On the domestic political level, the cyberattack discredited the Iranian government, as the Iranian authorities were not able to protect their nuclear facilities against a foreign cyberattack. The Iranian government seemed indecisive on how to officially react to the news that a computer worm might have infected its nuclear facilities. In September 2010, the Iranian authorities first played down the impact of the attack in their discourse, probably to avoid blame from the Iranian 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 passive and worked intensively to contain and remove the worm, and to identify the attackers (Zetter, 2011b). At the same time, Iranian authorities did not retaliate against 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 an 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 had caused collateral damage or had had more powerful effects, including the potential 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 it believed to be responsible (Collins and McCombie, 2012, p. 88; Rosenbaum, 2012). The biggest impact of Stuxnet on society was likely a feeling of insecurity, as an intrusion into a private domain is never taken lightly, and it can therefore 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, they cannot be considered secure enough (Zetter, 2014). Although the worm only targeted Iranian nuclear facilities the fact that the malware spread to other

computers around the world contributed to a global feeling of insecurity.

4.2 Economic effects

This attack also had direct economic effects for Iran. As Iran is subject to international embargoes, it does not have access to international markets for buying nuclear-related materials. In particular, it cannot buy centrifuges and therefore builds them itself, sometimes with foreign components. The resulting patchwork of materials may be one of the reasons for the quick deterioration of the centrifuges. Being under embargo also means that Iran has very limited resources, and the breakage of almost 1,000 centrifuges added pressure on stocks of materials and budgets. From a cost-benefit perspective, the poor returns in terms of productivity of the Natanz nuclear plant may also have added pressure on government finances, as enriched uranium needed to be purchased from other countries.

The cyberattack also had long-term economic repercussions for Iran as it needed to manage delays in the production of low-enriched uranium. Establishing new security and cybersecurity measures in nuclear facilities to avoid the recurrence of an attack such as Stuxnet would also have required a significant financial investment. For example, Iran created a new cyberunit in the Revolutionary Guard Corps to address cyberattacks in November 2011 (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 may have been in retaliation for the Stuxnet attack, but even though it seemed to originate from Iran, there was nothing to prove that it was perpetrated by the new cyberunit. According to the NSA, Iran may also have been behind the Shamoon attack, which involved a worm launched in August 2012 to wipe computers inside 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. The malware, which was clearly designed to affect the nuclear facility in Natanz, was believed to affect the speed of the centrifuges, causing them to alternate between high and low speeds (Farwell and Rohozinski, 2011, pp. 24–25). This change in speed was masked by the worm's rootkit, making the operators believe that the centrifuges were operating at their normal speed. The change of speed would have caused the centrifuges to wear out faster and suffer damage beyond repair. Natanz had between 6,000 and 9,000 operating centrifuges at the time, about 1,000 of which needed to be replaced (De Falco, 2012, p. 23; Nakashima and Warrick, 2012). IAEA experts assessing the plants noted that Iran replaced about 10% of its centrifuges each year due to breakage, but exchanged slightly more centrifuges than usual between mid-2009 and mid-2010 (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, production levels were less efficient as they could have been with fully working centrifuges. In other words, the output of low enriched uranium only increased because of accelerated working cycles to compensate for the loss of the damaged centrifuges. Even by February 2010, production levels were still lower than before the attack in November 2009. It took Iran approximately one year to recover fully from the effects of the Stuxnet attack and to return to a level of production comparable to November 2009 (Albright et al., 2010).

Taking these observations into account, the physical consequences of Stuxnet were rather limited, but it was probably designed to remain hidden for a certain amount of time, damage the centrifuges and then disappear (Nakashima and Warrick, 2012). Its discovery probably interrupted the process and terminated the operation prematurely. However, the fact that the number of damaged centrifuges was only slightly higher than usual lends strength to the possibility that the damage might have been caused by poor manufacturing or normal wear (Albright et al., 2010).

The Stuxnet attack also directly affected the technology sector. Companies that had developed 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 relevant zero-day exploits, and Siemens offered patches and removal tools to 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 RealTek and JMicron certificates that were used to trick infected computers into accepting the worm as a legitimate program (Lindsay, 2013, p. 394; Matrosov et al., 2010, p. 19). Inaction by these multinational companies would have caused their customers to lose confidence in their ability to produce secure software and technologies. Moreover, stricter rules for the management of driver certificates and other digital key systems have since been issued to prevent the recurrence of malware using stolen certificates (De Falco, 2012, p. 37).

Long-term technological consequences of Stuxnet are evident in Iranians approaching technical malfunctions in their facilities with a greater degree of mistrust, as any bug or breakdown may raise suspicion about another cyberattack on Iranian systems. Iran later

discovered two additional pieces of malware operating stealthily in its networks, namely Duqu and Flame.

4.4 International effects

At the international level, the cyberattack succeeded in delaying the Iranian uranium-enrichment program for a short period of time and thus slightly alleviated associated international tensions. Indeed, it seems that the resulting delays in the program reassured Israel sufficiently so 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 demonstrates that separating a critical infrastructure network from the internet can no longer be considered an adequate security measure. States have realized that they need to take action in order to avoid falling victim to attacks of this nature. Several states, including Iran, subsequently 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 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 would be able to 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 has been 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 to date. Stuxnet's code has not been modified and used for other purposes since it was discovered in 2010. Modified versions of Stuxnet have not emerged because it is not possible to simply copy a piece of malware; it rather needs to be reprogrammed to match new targets, and finding the necessary resources to achieve this is a major challenge. Moreover, zero-day exploits used by Stuxnet ceased to be zero-day vulnerabilities the moment they were discovered. As a 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 can be derived from the discovery of Stuxnet. These consequences are presented as recommendations for state actors.

5.1 Improving Cybersecurity

States may wish to focus on improving their cybersecurity to avoid situations such as Stuxnet reoccurring. The case of the Stuxnet worm showed that infecting computers by means of a USB drive is effective as a means of targeting air-gapped networks. Therefore, states should particularly focus on computer users and the issue of using unknown USB drives. States can run specific awareness-building campaigns on this issue for workers in critical infrastructures in order to improve users' understanding of the risks and possible damage that such behavior can cause. This would hopefully promote a more cautious approach to this issue.

States can also improve their cybersecurity by creating a standard operating procedure for a simplified and adequate way to respond to a cyberattack. A relevant procedure could address the technical level with cybersecurity experts acting rapidly to solve technical problems resulting from an attack and to return work cycles to normal as quickly as possible after an attack. Also, when Iran recognized that it had been targeted by a cyberattack, there seemed to have been confusion among the Iranian authorities on how to respond to the attack politically. Therefore, a standard operating procedure at the political level could also provide useful guidance for authorities on how to respond to a cyberattack perpetrated by another state, provided that attribution can be confirmed and the required resources are available.

5.2 Integration of critical infrastructures in cyber strategy

The damage caused by Stuxnet to the Iranian centrifuges showed that critical infrastructures can be targeted by cyberthreats. The fact that the Natanz networks were separated from other networks did not sufficiently protect them against the malware. As a consequence, states should take into account that critical infrastructures should be integrated in cybersecurity strategies. Relevant considerations would result in increased protection against cyberthreats and higher cybersecurity standards and at the same time promote closer cooperation between governments and actors - whether public or private – who manage these infrastructures. The goal would be to increase protection against cyberthreats, while also increasing resilience in case of cyberattacks.

5.3 Establishment of cybersecurity standards for industrial equipment

States may wish to promote international cybersecurity standards for industrial equipment. The incident of the Stuxnet worm has shown that industrial equipment such as SCADA systems often suffers from weak cybersecurity standards and is open to attack when connected to the internet. To diminish the risk of these vulnerabilities being exploited, states could promote technical standards indicating the level of cybersecurity of connected equipment at the international level. States could then decide to only use connected equipment that meets the most stringent standards in critical infrastructures. States could also recommend that operators of critical infrastructures not connect SCADA systems to the internet, as air-gapped networks remain appropriate for avoiding infection.

5.4 Promotion of international Confidence Building Measures (CBMs)

States may wish to reduce mistrust and misperceptions in cyberspace by promoting international CBMs. These measures could subsequently also be used to support the development of 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 in the attribution of cyber activities increase ambiguities and mistrust among states. CBMs could be a first step towards more transparency and better international relations. CBMs could be developed at the bilateral level or at regional or international levels 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 transparency monitoring 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	Approx. 100 kilobytes
Infection vectors	Removable USB 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 physical separation between a network and the Internet or other unsecure local networks (Zetter, 2014).

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

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

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

Confidence Building Measures (CBMs): 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 and let computers know that software is genuine (Matrosov et al., 2010).

Duqu: Worm discovered in 2011, whose 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 an 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 Arabian national oil company Aramco was particularly affected 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 of which software developers are not aware and which can be used to hack a system (Karnouskos, 2011).

8 Abbreviations

C&C	Command and Control
CBMs	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. https://doi.org/10.1109/MNET.2010.5634434

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

Institute 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. https://doi.org/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. https://doi.org/10.1109/MSP.2011.67

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