

Nation-State Cyber Surveillance Options: The role of suppliers

Eirik Bae



Master's Thesis

Master of Science in Information Security

30 ECTS

Department of Computer Science and Media Technology

Gjøvik University College, 2014

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Abstract

When Edward Snowden in 2013 leaked documents about U.S. surveillance, the focus shifted to how nation-states perform surveillance of Internet and telecom communications, and it was then a need for educated information about the topic. In this master thesis we investigate how nation-states can perform their cyber surveillance, how suppliers of products or services can support the nation-states' cyber surveillance, and how we can protect ourselves against it. We found that the most prominent way consists of collecting data from central points of communication, e.g. Internet and telecom providers. In some cases, it is necessary for the nation-state to perform targeted surveillance by installing surveillance software onto their suspects' devices. The information they collect from centralized and targeted surveillance can lead to big data issues that relate to collecting, storing, and processing the massive amounts of data. A supplier can decide to help nation-states in their cyber surveillance, and by exploiting the trust we lay in the supplier it would result in that we would face a completely different threat landscape, where we find it difficult to protect our privacy and security.

Sammendrag

Da Edward Snowden i 2013, lekket dokumenter om hvordan USA utfører digital overvåkning, ble fokuset rettet mot hvordan nasjonalstater kan utføre overvåkning av internett- og telekommunikasjon. Det resulterte i at det ble nødvendig med kvalifisert informasjon om temaet. I denne masteroppgaven utforsker vi hvordan nasjonalstater kan utføre overvåkning i cyberspace, hvordan leverandører av produkter eller tjenester kan hjelpe nasjonalstatenes cyber overvåkning, og hvordan vi kan beskytte oss mot dette. Vi fant ut at den mest fremtredende måten for å samle inn data foregår fra sentrale kommunikasjonspunkter hos leverandører av, f.eks. internett- og telekommunikasjon. I noen tilfeller er det nødvendig for nasjonalstaten å utføre målrettet overvåkning ved å installere overvåkningsprogramvare på de mistenktes enheter. Informasjonen de samler inn fra sentrale kommunikasjonspunkter og målrettede overvåkning kan føre til problemer med "Big Data" som er relatert til innsamling, lagring og prosessering av omfattende mengder data. En leverandør kan bestemme seg for å hjelpe en nasjonalstat i å utføre cyber overvåkning, og ved å utnytte tilliten vi har til leverandøren fører det til at vi står ovenfor et helt annet trussellandskap der vi får det vanskelig med å beskytte personvernet og sikkerheten vår.

Preface

The six months of fulltime research of how nation-states can perform their cyber-surveillance have given myself a more comprehensive view on what we are facing today. We are quite vulnerable today in terms of privacy and confidentiality. Although it has not always been easy to find reliable information, I still do believe that the thesis will be informative and useful for individuals of all levels of technology knowledge, who want to be better able to protect their privacy while using communication in cyber-space. Cyber surveillance can be used for both good and bad, depending on who are watching. Now it is up to ourselves how we handle it.

For experienced information security staff I would advise them to look at the the newest contribution in Chapter 6 which explores how the suppliers can support the nation-state in their work of performing cyber surveillance.

Acknowledgements

I would like to thank Prof. Dr. Bernhard M. Hämmerli for his ideas, supervision, and for always being available for interesting and constructive discussions.

Ola Kjelsrud should also have gratitude as he simplified the outdated and unnecessary complicated \LaTeX template, that we hope Gjøvik University College will adapt and thereby improve the master theses by students in the years to follow.

Thank you all that were a part of our student group consisting of André J. Waltoft-Olsen, Espen Didriksen, Ola Kjelsrud and Kjetil Gardåsen as you contributed to the research through daily motivational and theoretical discussions.

I would like to give special thanks to my family for always being there for me. My final gratitude goes to my beloved girlfriend Fenghua Wang, for her support throughout the studies.

Contents

Abstract	ii
Sammendrag	iii
Preface	iv
Acknowledgements	v
Contents	vi
List of Figures	viii
List of Tables	ix
Glossary	x
1 Introduction	1
1.1 Problem Description	1
1.2 Keywords	1
1.3 Justification, Motivation and Benefits	1
1.4 Research Questions	2
1.5 Claimed Contributions	3
1.6 Thesis Outline	3
2 Choice of Methods	4
3 Background Material	7
3.1 Cyber Surveillance	7
3.2 The Insecurity of Software and Hardware	9
3.2.1 Vulnerabilities and Exploits	10
3.2.2 Software and Hardware Vulnerabilities	11
3.3 Supply Chain Security	15
3.4 Surveillance Software	17
3.4.1 Targeted Malware Distribution and Updates	17
3.4.2 Government Use of Malware for Surveillance	18
4 Nation-state Cyber Surveillance	19
4.1 Information that is Collected	19
4.1.1 Metadata	20
4.1.2 Content Data	21
4.2 Surveillance Categories	23
4.2.1 Data in Transition	24
4.2.2 Data at Rest	27
5 Evaluation of Collected Intelligence Data	31
5.1 Big Data	31
6 Nation-state Surveillance with Supplier Support	33
6.1 Motivation for a Supplier to Support Nation-state Cyber Surveillance	33

6.1.1	Legal Pressure	33
6.1.2	Patriotism	34
6.1.3	Staying in Control	34
6.1.4	Economical	35
6.1.5	Mutual Sharing of Information	35
6.2	How a Supplier Can Support Nation-State Surveillance	36
6.2.1	Disclosing of Requested Intelligence Information	36
6.2.2	Manipulating Their Products and Services	39
7	Discussion of Differences in Mitigation	46
7.1	Without Supplier Support	46
7.2	With Supplier Support	47
8	Discussion of Research Questions and Implications	49
9	Future Work	54
10	Conclusion	56
	Bibliography	58
A	Hacking Team’s Surveillance Software	68
B	Table from the EFF 2014 Report	72

List of Figures

1	The amount of vulnerabilities in software and hardware compared between 2012 and 2013. Most of the vulnerabilities found are related to application software. (For 2013: Application 75%, Operating System 19%, Hardware 6%). [1]	11
2	Hardware can contain additional hardware. The picture shows two x-ray photos of cell phones where the right one contains additional hardware. [2]	15
3	The surveillance software provided by Hacking Team can gather information from personal computers. [3]	22
4	The surveillance software provided by Hacking Team can also gather information from smart phones. [3]	22
5	Infographic map from 2006 on how the ACLU believed the NSA could collect information from different probes.[4]	24
6	An example of how a nation-state handle "Big Data". The information is collected, and then processed, before it is stored. Whenever it is needed, the nation-state can aggregate the data [5].	32
7	Through passive surveillance can the nation-states use the supplier's help to obtain information about their targets.	38
8	An example of a digital software certificate. It contains the name of the supplier and certificate authority, in addition to the time it is valid.	44
9	The RCS supports a wide range of platforms. [6]	68
10	The RCS can gather information from personal computers. [3]	69
11	The RCS can gather information from smart phones as well. [3]	69
12	The RCS can be distributed through masquerading it as a benign pdf-document. [7] 70	
13	Citizenlab suspected that 21 governments use the RCS surveillance software. [8] 71	

List of Tables

1	Outline for the thesis.	3
2	A comparison of the amount of vulnerabilities in operating systems reported in 2012 and 2013. This table is adapted from the original figure by Florian [1]	12
3	A comparison of the amount of vulnerabilities in applications reported in 2012 and 2013. This table is adapted from the original figure by Florian [1]	13
4	Sources for exploits used in exploitation of devices.	28

1 Introduction

1.1 Problem Description

Today, most of us use Internet and communication services for nearly everything. Their popularity therefore makes them a target in the area of surveillance. Suppliers of products and services have a high ability to affect the level of privacy and security, due to our dependency of them. Nation-states could exploit the suppliers' position by using different means to control them, and in that way be better able to perform surveillance of our communications. If a supplier or a nation-state implement cyber surveillance, it can lead to a breach of confidentiality, integrity and availability for their users. In most cases will such surveillance be able to collect massive amounts of information and be difficult to detect. It is possible that suppliers support the cyber surveillance performed by nation-states, something that could affect the users because suppliers of software and hardware are deciding their privacy and security.

As a countermeasure in order to protect the privacy and security of the users of the users, there are ways to identify what kind of cyber surveillance the users need to protect themselves against. By analyzing the current options for the nation-states to perform cyber surveillance today, it is possible to get a better understanding of what we need to protect ourselves against, and how we can do so.

1.2 Keywords

Nation-state, Cyber surveillance, Data encryption, Invasive software, Vulnerability, Exploit, Motives, Hardware, Software, Digital Signatures, Trust, Suppliers, Firmware, Disclosure protection, Supply chain security, Privacy.

1.3 Justification, Motivation and Benefits

While the issues of cyber surveillance have been relevant for a long time, the issues were renewed in 2013 when Edward Snowden leaked detailed documents which showed that the U.S. were much more able to perform cyber surveillance than what we before had expected.

With such emerging cyber surveillance that is most likely most also performed by other nation-states, there is a need for educated information on how to behave when we use products and services that are connected to cyber space. It is important to identify how cyber surveillance can be done, what the effect is, and how we can protect ourselves against it. As nation-states possibly could use the support from suppliers to be better able to perform their cyber surveillance, it is important to investigate why and how the suppliers could help the nation-states.

It is not a focus to see which nation-states and suppliers that are performing particular actions, but it is necessary to mention origins of currently known tools and mechanisms used. We base our study on the assumption that most nation-states in the world have cyber surveillance capabilities, which then instead enables us to focus on what extent the cyber surveillance can be done. While some nation-states are mentioned in the report, it is important to keep in mind that the list is not comprehensive. However, a lot of effort is given in order to make it as complete as possible. There are no intentions on covering all forms of signal intelligence, and we are therefore focusing on issues that mainly revolves around telecommunications and Internet, as most of our communication revolves around them. Our investigation is as much as possible limited to cyber surveillance performed by nation-states.

One of the goals is to have understandable and informative results, which then will provide information for both highly technical and less technical users. Security personnel and researchers should also to get an idea on alternative ways that attacks can be performed and get to know the insecurity that resides in the steps of the production chain. Guidelines for mitigation of nation-state cyber surveillance should hopefully provide increased levels of security in the users' communication.

1.4 Research Questions

This thesis will attempt to give information and explain on the current threats we face when nation-states want to perform their cyber-surveillance. We have defined questions to better focus on what we want to know. During the work, we found that some of the research questions needed some modifications. We therefore we changed the questions slightly. The new research questions are similar to the original ones, but the changes enabled us to better work along the line we wanted. The research questions are as following:

1. Which options for distribution of surveillance software are available for a nation-state?
2. At which part of the supply chain could software or hardware manufacturers add surveillance to their products?
3. What is the result if a supplier of software or hardware is working together with a nation-state in order to perform cyber surveillance?
4. How can we protect ourselves against cyber surveillance which is a result from a nation-state that has support from suppliers?

1.5 Claimed Contributions

The claimed contributions of the thesis is an overview of current options a nation-state could have today when they want to perform cyber surveillance, how a supplier can help them, and how we can protect ourselves against such surveillance. The thesis work resulted in a report that contains the following:

1. **An overview** of the current options nation-states have to perform surveillance in cyber space, what information is being collected and what the information can be used for.
2. **Information** on how suppliers of products and services can help the nation-states to make it easier for them to perform cyber surveillance.
3. **A comparison and suggestions for mitigations** of conventional and supplier supported nation-state cyber surveillance.

1.6 Thesis Outline

The outline for this thesis is presented in the following Table 1 which shows each chapter and their content.

Table 1: Outline for the thesis.

Chapter	Description of content
2	Methods and approaches that have been used in order to get the results in the thesis.
3	Covers necessary terms in order to understand nation-state cyber surveillance and explains the current knowledge in the field.
4	Information about which information the nation-state could collect through cyber surveillance and how they are able to collect it.
5	Challenges and opportunities that arise when data is collected, stored and processed.
6	How a supplier of software or hardware can support the nation-state in performing cyber surveillance.
7	Approaches for mitigation of nation-state cyber surveillance with and without supplier support.
8	Discussion about the results of nation-state cyber surveillance and how suppliers can support them in their work.
9	Future work that would be useful for the research community in the area of nation-state cyber surveillance.
10	The conclusion of the thesis.

2 Choice of Methods

In this section, the various methods used in the work with this thesis are presented. The methods have been chosen to best possibly cover the research questions defined in Section 1.4. Most of the research is based on literature reviews and qualitative research as described by Leedy and Ormod[9, p. 51-70, 139-164].

2.1 Literature review

In order to get the best understanding of the current situation in the field, a literature review is a necessity. We used available literature to better understand the current situation in nation-state cyber surveillance, and in addition provide the readers of this thesis necessary fundament for understanding our research results. Our literature review was based on the approach described by Leedy and Ormod[9][p.51-70], and was carried out in many iterations throughout the research period:

1. Identifying relevant keywords.
2. Search for literature at the library, and in scientific online databases (IEEE Xplore, ACM, ScienceDirect, etc.) and search engines, e.g. Google (Scholar).
3. Identify and read literature that seems relevant.
4. If we find useful literature, we store relevant information, add our comments, and store it together with citation and date of collection.
5. If we find a relevant reference to another information source, we follow it and repeat steps 3, 4 and 5.

2.2 Qualitative Research

The research methodology used in this thesis is based on a qualitative research methodology. As there are inadequate amounts of general and scientific information about how nation-states perform cyber-surveillance today, it is necessary that we look at data from publicly available sources, make observations and ultimately create conclusions if possible. The grounded theory study used in this thesis consists of the following research design presented the Section 2.2.1.

2.2.1 Grounded Theory Study

We chose to use the grounded theory study design as described by Leedy and Ormod [9][p.146-148]. The research design is suited for our study because there are inadequate amounts of information about the current situation in the area of nation-state cyber surveillance. It is therefore

necessary to develop the theories from data collected from various sources, e.g. news articles, videos or other publicly available documents. The data should be linked to scientific sources when possible. The research is performed by having an objective viewpoint from the start and throughout the project. The work is then based on collecting data, while at the same time analyzing and categorizing the collected data. We look at how the nation-state cyber surveillance takes place, when it is used and how it is being done. From the collected data, we intend to create a theory on how the nation-states are performing their surveillance.

Data collection

In order to perform a grounded theory study, it is important to collect relevant data. Throughout the study, the relevant data has been gathered and stored together with notes of important observations. The following paragraphs explain the methods used for data collection.

Observations

This is the main method we used to collect data for the master thesis. By observing cyber-surveillance related scientific articles, news articles, books, and internet sources, it will be possible to acquire information on the situation in the field. We chose to collect data through observations because the data sources are not already known. This method is flexible in that it is also possible to include unforeseen data sources to the research. Our methodology for collecting data through observations is similar to the algorithm used in the literature review in Section 2.1, but the main difference is that observations enables us to be less limited to scientific sources. Some of the data are based on the leaked documents from Edward Snowden. Because the documents still are classified, we decided to adhere to U.S. law and ethical guidelines of research by not republishing them. However, we will discuss some of their content, and we have some citations with links that points to classified documents from publicly available sources on the Internet. We carried out the data collection iteratively as following:

1. Identify relevant keywords.
2. Search for literature at the library, and in scientific online databases (IEEE Xplore, ACM, ScienceDirect, etc.) and search engines, e.g. Google (Scholar). In addition, we use non-scientific sources, e.g. online newspapers, or blogs from well-known security experts.
3. Identify and read relevant information.
4. If we find useful information, we store it, add our comments, and store it together with citation and date of collection.
5. If we find links or references to other sources of, we follow them and repeat steps 3, 4 and 5.

Interviews

A series of interviews were originally intended to be conducted. However, the sensitive nature of nation-state related material resulted in that no interviews were conducted during this project. We found it infeasible to get better information than what was already available from public sources.

3 Background Material

In this chapter, we provide fundamental knowledge needed to better understand the thesis. In addition, we also provide the state of the art in the area of cyber surveillance performed by nation-states.

3.1 Cyber Surveillance

In order to understand cyber surveillance we need to understand the definitions. First we take a look the definition of *surveillance*, *cyber* and *cyber-surveillance* which are described by Monica Tremblay[10] and presented in the following paragraphs, respectively. A definition for surveillance is as following:

"[...] gathering and analysis of information in the pursuit of various finalities - in particular, preventing certain risks, orienting human behaviors, and in the event of a problem, locating the persons responsible." [10]

Examples of this are suppressing of people, be aware of other countries' behavior, and to prevent terror. The second definition we need to look at is "*cyber*" which basically covers everything that is performed in virtual space using computer systems and telecommunications[10]. Already here we have a broad range of devices and systems that are covered by this definition. Together, *cyber* and *surveillance* combine into *cyber-surveillance* which can be defined as the following:

"Cyber-surveillance is a mechanism for the surveillance of persons, objects or processes that is based on the new technologies and that is operated from and on data networks, such as the Internet. Its purpose is to facilitate surveillance, in keeping the quantity, rapidity or complexity of the data to be processed." [10]

In this thesis, surveillance in Internet and telecommunication networks will be described. It will not be completely technical as surveillance can be achieved through other means where e.g. laws and collaboration could influence. In order to better understand cyber-surveillance, we need to look at some parts of recent surveillance history.

A Look at Recent Surveillance History

With the information revolution, it brought focus to cyber surveillance. The surveillance programs we see today started in the early 1990s and developed from laws of communications surveillance into larger surveillance programs towards the early 2000s, that focused on developing interception capabilities [11][p. 5]. The most recent surveillance programs in the USA are discussed by N. Lee[12]. He describes that after the 9/11 terrorist attack, the U.S. created a

program called *Total Information Awareness (TIA)* which most likely was an earlier version of the *PRISM* [13], which is one of the U.S. surveillance programs we know today, and will be further described in Section 4.1. The TIA was supposedly never put into action due to privacy concerns, but was instead converted into *Terrorism Information Awareness (TIA)* so that they could keep the program running. Such large surveillance programs shows that a national entity is willing to put a lot of money and resources into the goal of achieving information dominance. For example, the USA is stating through their laws, e.g. *Homeland Security Act of 2002* [14], that they are willing to do what is needed to protect their nation, and many countries are most likely doing this as well.

Electronic Frontier Foundation describes the following story on surveillance in the years that were following [15]. The *National Security Agency (NSA)* and their surveillance program got known when *New York Times* in 2005 published a story on it [15]. At that time, the program was thought to be covering only terrorists, but instead everyone, including American citizens. As the surveillance did not comply with the *Foreign Surveillance Act (FISA)*, which enables the government to do a lot of spying, it has supposedly been continued under Bush, and now Obama, thus under different justifications [15].

During spring of 2013, Edward Snowden became a whistleblower by leaking confidential intelligence documents on how NSA and its allied countries perform surveillance [16]. Details from these documents have been published by *The Guardian* and the *New York Times* throughout 2013 and the beginning of 2014. These newspapers were the ones that reported on these leaked documents because they were the ones that received the documents from Snowden. Snowden has appeared via video conference at different conferences, e.g. *SXSW*[17], as he would face legal issues if he were to return to the USA [18].

While many Americans are mostly troubled about that their government would perform warrant-less surveillance of their own citizens, we believe that the insight to the nation-state surveillance is interesting in a research context.

Current Knowledge in the Field

While the text in Section 3.1 is just an excerpt of the U.S. surveillance history, it has been well known that e.g. the EU, China, France, Germany, India, Israel, Russia, Switzerland and UK have known intelligence programs[19][20][loc. 2820]. However, they are in different scale as some are more comprehensive than others are. Some perform tight surveillance and packet filtering (*The Great Firewall of China*[21]), or just storing basic communication data for short periods (the EU data retention[22]). Various researches have been conducted in order to gather information on how cyber surveillance is done today; some are generic while others are in most cases quite specific to each nation.

One of the generic analyses are described by Gregory and Glance[23] and covers various inci-

dents of government surveillance and alleged malware distribution. They further describes legal impacts of surveillance, and how it affects data retention in Australia. A second generic analysis is given in by Hosein and Palow[11], where they cover general information about targeted and mass surveillance.

There has also been a series of more nation specific researches. Maria Xynou[24] discussed India's surveillance and has gathered a lot of information on how it is being done there. In relation to the Sochi Olympics 2014 in Russia have Soldatov and Borogan[25] given a general description of how surveillance is done in Russia. For U.S. surveillance, The Guardian and The Washington Post have covered the case of NSA spying in the digital domain [26, 27]. The U.S. surveillance program has been further discussed by Bruce Schneier who has acted as "security guru" for the U.S. surveillance debate, where he has spoken at various conferences and discussed relevant issues in his blog [28, 29, 30].

For the common surveillance problem, the non-profit organization German Informatics Society has published a document on most frequent questions about information surveillance [31]. In the document they state that there is a problem, and cover common questions about perpetrators, what the stolen information is used for and the most relevant technical aspects. However, what it does not cover are details of such attacks, nor does the information explain about collaboration and deeper technical details for the layers in software and hardware.

The Basic Understanding

What the reader should note is that surveillance programs are being used to perform surveillance on foreign and in some cases local citizens, so that the government are in a better situation for decision-making, counter terrorism and in some cases suppression of their people. In order to achieve the nation-states' goals, laws and regulations are created, and in some cases they surpass their legal jurisdiction through presidential orders or breaking the law [15]. Due to the legislation, the citizens and companies residing in the nation-state are in most cases left with no choice and have to cooperate with their government. Collaboration related issues for cyber surveillance will be further described in Chapter 6. The reader should now have an understanding of cyber surveillance and some of its implications. In order to better understand how cyber surveillance affect the security of software and hardware, we first need to see how software and hardware by default are not that secure.

3.2 The Insecurity of Software and Hardware

What is seen today is that in order to stay secure on the Internet, the users need to update their operating systems, anti-virus software, etc. In order to defend ourselves against most malicious computer programs, e.g. worms, trojans and viruses, most computers have updated anti-virus software installed. For most operating systems, security updates needs to be downloaded on a regular basis in order to patch and then protect against flaws in the software, which otherwise

could be used to take control of the computer or steal information. Many resources are used in order to secure the systems we use today. In this setting, we will see that what we use is already susceptible for modification and exploitation. The following first section contains some important terms, while the latter sections provide examples on some flaws that are existing today.

3.2.1 Vulnerabilities and Exploits

Terms like *vulnerability* and *exploit* are common in the information security area. They are described in the following paragraphs in order to give the reader an understanding of these terms.

Vulnerability

Microsoft describes the definition of a security vulnerability [32]:

"A security vulnerability is a weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product." [32]

The definition mentions product, which in this setting can mean software or hardware. Further is an attacker the term for an adversary with malicious intent, e.g. a criminal wanting to steal information, but the attacker could mean a nation-state with the means of getting hold of intelligence data. Note that just because a nation-state could be the attacker, it does not necessarily mean that they have malicious intent, but rather focus on national security.

The weakness can allow integrity, availability and confidentiality of the product to be compromised. By compromising the integrity, it could lead to being less trustworthy as someone would be able to modify the product without permission. Availability can also be compromised. Although the product should be available whenever is needed, it could have consequences if it is not available when the resource is needed. Confidentiality refers to that only the ones who are allowed to access the resource should be able to do so. An attacker could compromise this confidentiality and get access to it, e.g. an attacker hacks into a system to get information he was not able to read otherwise.

Publicly known vulnerabilities are given an identification name and stored in databases. The NIST vulnerability database is such a database [33].

Exploit

Mattord and Whitman [34] gives the definition of an exploit:

"A technique to compromise a system" [34, p. 569]

Exploits are using the inherent weakness vulnerabilities in the systems we have and enables the attacker to compromise availability, integrity or confidentiality. The attacker can use exploits to

compromise software or hardware that has vulnerabilities. Exploits are usually in the form of program code, that the attacker runs in order to control the system in a way the attacker wants. There are various ways to get a hold of exploits, which will be discussed later in Section 4.2.2.

3.2.2 Software and Hardware Vulnerabilities

Many resources are spent on securing the software and hardware we use today. Yet, many vulnerabilities are discovered every day. In this section are some examples presented in order to give a basic understanding for that a lot of software and hardware can be compromised. Christian Florian[1] created statistics for 2013 on vulnerable operating systems, software and hardware, based on the NIST CVE database [33]. It resulted in graphical charts that show how the current vulnerabilities are distributed. Figure 1 depicts the vulnerability distributions from 2012 and 2013. The majority of vulnerabilities seem to be in application software and operating system software, while hardware vulnerabilities are quite low compared to software vulnerabilities.

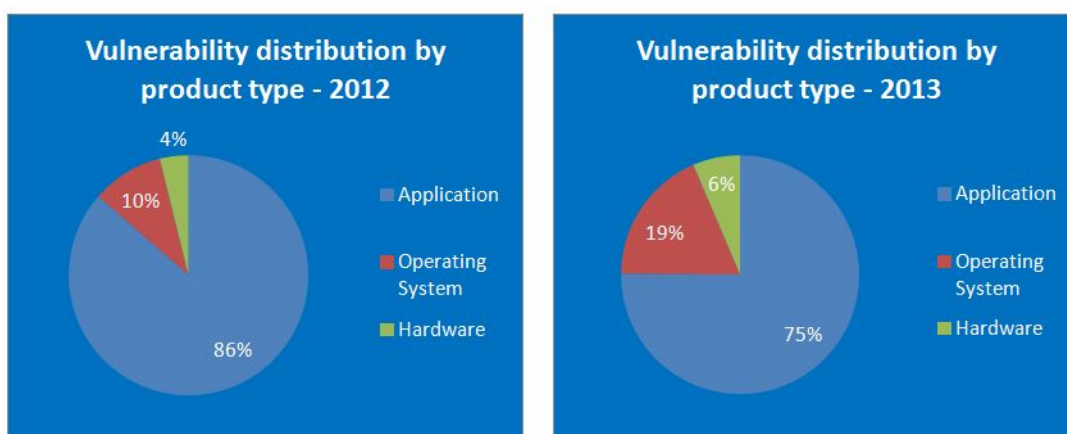


Figure 1: The amount of vulnerabilities in software and hardware compared between 2012 and 2013. Most of the vulnerabilities found are related to application software. (For 2013: Application 75%, Operating System 19%, Hardware 6%). [1]

Insecure Software

Most of the software we use today can be vulnerable to exploitation from attackers. Some of the places we find software running are in e.g. computers, smart phones and network equipment. Operating systems and applications running on such devices can have vulnerabilities residing in them.

Operating systems are one type of software that is being targeted by attackers. Figure 2 gives an overview of the most reported operating systems vulnerabilities in 2013. The operating systems could still have vulnerabilities that are not reported. The table shows that both Windows-

Table 2: A comparison of the amount of vulnerabilities in operating systems reported in 2012 and 2013. This table is adapted from the original figure by Florian [1]

Application	# of vulnerabilities	
	2013	2012
Microsoft Windows Server 2008	104	48
Microsoft Windows 7	100	42
Microsoft Windows Vista	96	41
Microsoft Windows XP	88	42
Microsoft Windows Server 2003	86	45
Microsoft Windows 8	58	5
Linux Kernel	158	45
Microsoft Windows Server 2012	51	5
Microsoft Windows RT	42	2
Apple iOS	89	86
Cisco IOS	34	36
Ubuntu Linux	72	6
Cisco IOS XE	23	9
Red Hat Enterprise Linux	54	2
openSUSE	49	0
Apple Mac OS X	63	21

and Linux/Unix-based systems are vulnerable. Google Android is an operating system that is widely used in smart phones, but it seems to not be a part of the table as it only had seven vulnerabilities registered for 2013 [35].

Applications are another type of software that is usually in the form of mobile and desktop applications. Their widespread use and popularity makes them a target for attackers. Figure 3 shows that widely used web browsers, plugins and stand-alone programs have vulnerabilities that could be exploited by attackers.

In most cases we trust applications to maintain our security and be protected from attacks. A single vulnerability in the program code is usually enough to be exploited and have drastic consequences. The following example will show how even widely used software for secure communications could be vulnerable.

Software exploit: a recent example

An example of a more recent application software exploit that has been *The Heartbleed Bug* which is described in the information website dedicated to this bug [36]. OpenSSL, the most popular open source implementation used for encrypting traffic on the internet suddenly was found to contain an error that could expose data to attackers. A programming error in OpenSSL's heartbeat library extension enables an attacker for every heartbeat (message to keep the connection alive) to read up to 64k of arbitrary memory contents. Both the server and client are affected.

Table 3: A comparison of the amount of vulnerabilities in applications reported in 2012 and 2013. This table is adapted from the original figure by Florian [1]

Application	# of vulnerabilities	
	2013	2012
Microsoft Internet Explorer	128	41
Oracle Java	193	58
Google Chrome	168	125
Mozilla Firefox	149	159
Mozilla Thunderbird	113	144
Mozilla Firefox ESR	100	115
Mozilla SeaMonkey	104	143
Mozilla Thunderbird ESR	87	109
Adobe Reader	65	25
Adobe Acrobat	63	24
Adobe Flash Player	56	66
Adobe Air	48	54

As the error has been introduced in 2011, it has gone unnoticed until April 2014 [36]. Bruce Schneier also commented on the case, describing it that we would need to assume that everything is compromised, while also explaining the magnitude of the problem as "*On the scale of 1 to 10, this is an 11*"[37].

Insecure Hardware

Hardware can be vulnerable to exploitation from attackers in similar ways as software is. The vulnerability can be either an intentional or an unintentional flaw in the software running inside the hardware, i.e. firmware, or it can be in the hardware itself. While the vulnerabilities in firmware usually are possible to fix with updates, hardware vulnerabilities are much more difficult to fix. In some cases a hardware vulnerability could result in that the hardware has to be replaced with a new fixed version [38, p. 15]. Following are some examples on firmware and hardware that could be exploited, even though the security protection measures were in place.

Firmware exploit: example 1

Our first example is about Wojtczuk and Tereshkin [39] that showed an attack on BIOS in 2010. They explained how BIOS updates usually are protected by integrity mechanisms that makes sure that the BIOS is signed before it is flashed at next boot. However, the BMP image is available to the OEM factories so that they can use their company logo. That logo does not need to be signed and therefore leaves a way to overwrite memory in bios and bypass the write protection that the BIOS initializes. The exploit is a buffer overflow that could allocate a bigger buffer because of this custom logo feature. While hardware was needed to create the exploit, the resulting knowledge was enough to that physical access to the machine was no longer needed in order to exploit and deliver the payload. An attack on BIOS enables the attacker to keep its persistence for their

malware while remaining hidden from the operating system. Drawbacks on such firmware exploit is that it is very firmware specific, offset-dependent and requires very complex debugging. It is this an example of how BIOS, even though has protection mechanisms, still has ways to be compromised.

Firmware exploit: example 2

The second example is about the *Intel Active Management Technology (AMT)*. The attack is described by Wojtczuk and Tereshkin [40], where an attacker can through remapping of memory then modify the programs that the Intel AMT chipset runs. This can result in resilient malware, or even surveillance software, which this context will not be removed even if a clean install of the operating system is performed.

The examples above showed how firmware could be exploited. In some cases, the underlying hardware itself is compromised or vulnerable. The next example shows how even military grade chips could contain vulnerabilities or backdoors.

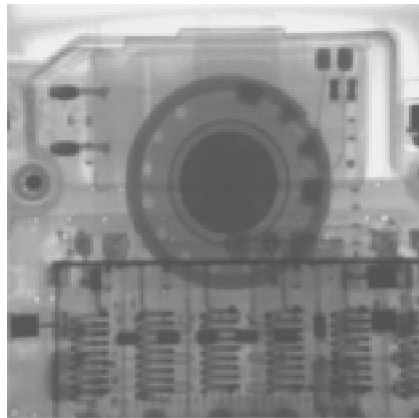
Hardware backdoors

Even military grade chips have been proved to not be completely secure, as described by Skorobogatov and Woods[38]. The researchers used a special technique to analyze a military grade chip. They found something that they concluded to be a backdoor that exists in the hardware chip itself, and not the firmware. The backdoor enabled the researchers to extract secret keys, among them the AES encryption keys and Passkey in addition to the key to activate the backdoor. This hardware backdoor is important to consider, as it is not possible to fix unless a completely new chip is made, in addition it was used in military installations, an area that should never have such backdoors.

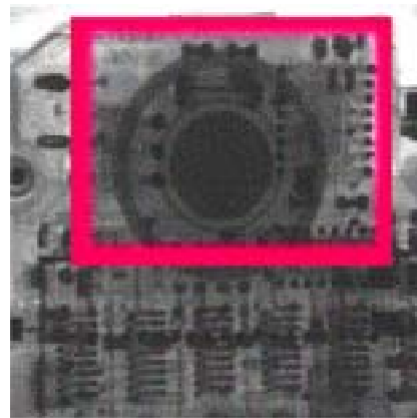
Hardware in hardware

In some cases of surveillance and other actions, the hardware can also contain hardware in itself. Hardware in hardware is already known and is described by GSM-mobilfunk[2]. An example of a hardware manipulated cell phone discovered by x-ray is shown in Figure 2.

The software and hardware we have discussed in this section provides the foundation in that software and hardware can contain vulnerabilities, even if there are protection measures in place. This can be exploited by attackers. Another important thing to notice is that underlying hardware that is compromised can subvert security modules that are built in software residing on "top" of such hardware. Security features like *Trusted Platform Module (TPM)* and hard drive encryption can be subverted when underlying hardware is exploited [41]. Attackers could exploit these flaws in order to e.g. steal information. A government would in most cases adhere to certain laws and regulations, but they can also use the same vulnerabilities as the criminals with malicious intent, in order to gain intelligence information. Some of the examples shown in this section are proof-of-concept and are not necessarily added to the NIST CVE database. Software and hardware can



Referenzröntgenbild eines Mobiltelefons (Teilansicht)



Röntgenbild eines hardware-manipulierten Mobiltelefons (Teilansicht)

Figure 2: Hardware can contain additional hardware. The picture shows two x-ray photos of cell phones where the right one contains additional hardware. [2]

still have vulnerabilities, but they are not always disclosed to the public. Exploits that attack such vulnerabilities are called zero-day exploits, and their role in surveillance will be discussed in Section 4.2.2.

3.3 Supply Chain Security

In order to secure the product all the way from the initial development and all the way to the user the Supply Chain Security (SCS) is important. By securing every step in the chain of development of software and hardware products, there will be a lower chance that it is modified in a way that it would contain malware or any other unwanted functionality. Surveillance software from a nation-state is an example of software that could be added into one or more of the steps in the supply chain.

Axelrod [42] explains how SCS works and what its crucial areas are. In addition, Axelrod gives a description about the shortcomings of security in current supply chains. One of the trends seems to be that customers are left with Commercial Off-The-Shelf (CoTS) that has little or no evidence from the manufacturers of not containing any flaws or malicious code.

It is important to acknowledge that Supply Chain Security is an important part of securing the company against malicious software and hardware. Microsoft [43] provides useful information regarding this issue where they state that a framework for Supply Chain Security should have the following properties:

"A framework for managing supply chain risk should rest on these principles:

- **Risk-based approach.** Governments should avoid using simplistic factors such as a product's country of origin to assess risk. The global character of many products means that attempts to prohibit products based upon country of origin could result in a broad ban of products.

This would lead to weakening open trade and relinquishing the benefits of global innovation. Instead, governments should rely on tested risk-management principles.

- **Transparency.** *Governments have a right to expect IT companies to provide an appropriate degree of visibility into their business processes and the controls that ensure the security of their product development and operations.*

One example of such transparency is Microsoft's Government Security Program, which gives eligible participating governments access to the source code for selected Microsoft products. While expecting transparency, however, governments also need to appreciate that businesses must protect their trade secrets and other intellectual property.

- **Flexibility.** *When governments move to adopt standards governing supply chain security, control and mitigation standards need to remain flexible.*
- **Reciprocity.** *The development of reciprocal international standards for supply chain security is essential for continuing to realize the benefits of the Internet that rely on the security and integrity of information technology systems." [43][p. 2]*

To our understanding, they provide the understanding that the whole process is vulnerable to modification of products, and is therefore necessary to protect. Microsoft seems to have an approach with business in mind, where they e.g. try to promote an open market and partial transparency.

An example that shows how difficult it is to verify and make sure every part of the Supply Chain is secure is described by Clarke and Knake[44] and is reflected in the following quote from their book:

"In The World Is Flat, Thomas Friedman traces the production of his Dell Inspiron 600m notebook from the phone order he places with a customer-service representative in India to its delivery at his front door in suburban Maryland . His computer was assembled at a factory in Penang, Malaysia. It was "co-designed" by a team of Dell engineers in Austin and notebook designers in Taiwan. Most of the hard work, e.g. the design of the motherboard, was done by the Taiwanese team. For the rest of the thirty key components, Dell used a string of different suppliers. Its Intel processor might have been made in the Philippines, Costa Rica, Malaysia, or China. Its memory might have been made in Korea by Samsung, or by lesser known companies in Germany or Japan. Its graphic card came from one of two factories in China. The motherboard, while designed in Taiwan, could have been made at a factory there, but probably came from one of two plants in Mainland China. The keyboard came from one of three factories in China, two of them owned by Taiwanese companies. The wireless card was made either by an American -owned company in China or by a Chinese-owned company in Malaysia or in Taiwan. The hard drive was probably made by the American company Seagate at a factory in Singapore, or by Hitachi or Fujitsu in Thailand, or by Toshiba in the Philippines." [44, p. 86]

This example shows the difficulty of ensuring that all parts of the supply chain can be secure. SCS can be much more complicated when the computer is consisting of that many different parts from different origins, and the idea that only less than 3 minutes would be needed to flash the firmware of a device if the attacker were to have access to it [41, p. 38].

3.4 Surveillance Software

In order to find out how a nation-state might distribute their surveillance software it is possible to look at current approaches for malware distribution seen in non-nation-state attacks.

3.4.1 Targeted Malware Distribution and Updates

There seems to be little information published about how national entities would distribute and update their surveillance software. The second best option would to turn to scientific publications about malware distribution and updates.

Technical Approach

There are various approaches that are able to target and attack single or multiple users. Following are papers relevant to technical approaches for distribution and updating of malware described.

Distribution

A possible way of distribution can be adapted from general malware distribution. By infecting executable binary files through compromised routers as described by Jack[45]. By modifying firmware and injecting the payload into all executable files passing through the router, it would be possible to affect a large amount of users in the targeted network. How computers can be infected is explained by Rossow, Dietrich and Bos [46], where 23 malware downloaders were analyzed and documented, and then further analyzed over more than a year. Another way is shown by Grobert, Sadeghi and Winandy [47], where they describe ways to infect computers through software distribution. Ways to infect executable files and how they can be run without being noticed are explained. This paper also mentions that law enforcements and governments can force other parties, e.g. ISP, to help them in order to distribute malicious software of their choice.

Updates

A whitepaper by Bellissimo, Burgess and Fu [48] shows the most common companies like Microsoft, Adobe, Mozilla and Apple and their methods for how they update their software, and the security used to do so. To our understanding, it is relevant, as a nation-state most likely could use a larger company to distribute and update its surveillance software. More advanced approaches are to distribute them over multiple information channels. In order to show the extent of malware distribution over various transmission channels can be, additional attacks are described by Shankarapani, Sulaiman and Mukkamala [49] where fragments of malware is spread via multiple RFID tags. When the fragments are combined, it will become a complete and working piece of malware. Similar attacks might be possible with software.

Social Approach

Social engineering in general is well known. This topic is described by Whitman and Mattord [34]. By using social skills, the attackers can convince or trick humans into doing what the attacker wants them to do, thus circumventing technical security measures. Hong[50] explains about how phishing, a type of social engineering can be used to e.g. trick users into installing malware on their computers. He further describes how the users fall for such attacks and then gives some advices on how to protect against it.

3.4.2 Government Use of Malware for Surveillance

Governments have been known to use malware in order to perform information intelligence or warfare operations. Gregory and Glance [23, p. 6] provide information on how backdoor trojans used by governments came fore in 2001 as the Magic Lantern software by NSA or FBI. This software captured encryption keys so that the FBI would be able to decrypt captured communication. The paper also explains the dilemma of whether an anti-virus company should detect government malware or not. Further is it described that Germany, Switzerland and the Austrian Police have been using surveillance trojans.

4 Nation-state Cyber Surveillance

A nation-state can perform cyber-surveillance in order to gather intelligence on domestic and foreign citizens. Based on our grounded theory study, we collected a lot of data on how nation-states in general can perform their surveillance. This section describes the types of data that we found them to collect, and how they can collect it.

4.1 Information that is Collected

Based on our assumption, anything that can be of interest for intelligence purposes would most likely be collected. The collected data can be many different types of information. This section gives examples of different types of information that could be collected. Note that it is not a comprehensive list of collected data and it is highly likely that additional information can be and is collected.

The first example of information that is being collected is shown in the information leaked by Edward Snowden regarding the PRISM program [51]. Multiple companies are allegedly a part of the PRISM program which seems to be a collaboration for intelligence information on demand [51]. The list of potential data that can be collected is long, including: e-mail, video chat, text chat, videos, photos, stored data, voice communication, file transfers, video conferencing, information on target activity and details from social networks. To our understanding, it also seems that it is possible through the PRISM program to have special requests, which could give away additional information. The PRISM program will be further discussed in Section 6.2.1

A second example is data collected in the Russian surveillance program, "System for Operative Investigate Activities" (SORM), as described by Lewis[52]:

"Three programs, SORM-1, SORM-2, and SORM-3, provide the foundation of Russian mass communications surveillance. Russian law gives Russia's security service, the FSB, the authority to use SORM ("System for Operative Investigative Activities") to collect, analyze and store all data that transmitted or received on Russian networks, including calls, email, website visits and credit card transactions. SORM has been in use since 1990 and its main function is that it collects both meta-data and content. SORM-1 collects mobile and landline telephone calls. SORM-2 collects internet traffic. SORM-3 collects from all media (including Wi-Fi and social networks) and stores data for three years." [52]

According to the quote, there is a lot of information being collected. Through the three SORM programs they cover telephone networks, Internet traffic and additional media, thus making it a comprehensive collection structure. It seems that information on all digital communication in Russia can be collected. Many different types of data are collected, including both metadata and

content data. Metadata and content data, as well as their differences will be described in the following two sections.

4.1.1 Metadata

Metadata is a set of data that gives information about other data[53]. Metadata are very effective and could be used for data aggregation, where for example governments could learn a lot more about domestic and foreign users. Surveillance related metadata could be information on who is connecting with whom, identity of the communication equipment and so on. In U.S., The Guardian published key extracts from a classified NSA presentation named *Content Extraction Enhancements For Target Analytics: SMS Text Message: A Goldmine to Exploit*[54]. It covered statistics for SMS and why it is an important source for intelligence. Metadata that allegedly are being collected for their intelligence purposes are:

- International Mobile Subscriber Identity (IMSI)
- Mobile Subscriber Integrated Services Digital Network Number (MSISDN)
- International Mobile Equipment Identity (IMEI)
- Short Message Entity (SME)

The presentation shows that not only pure metadata could be extracted, but also a mix of content- and metadata where text messages, names, images, tracking of users, missed calls, changed SIM-cards, roaming, travel-information, credit card transactions, money transfers, tracking of financial information and passwords could be found. Such information resulted in what they would call "analytic gems", which would enhance current analytics [54].

General metadata collection is not only limited to SMS as described in the *Directive 2006/24/EC of the European Parliament and of the Council* [55] which is the EU data retention directive. Examples are in section 5 of their EU report [55, p. 4-5] and covers detailed data on what the EU member states should retain. Types of data that the retention is collecting are phone numbers, names, addresses, user IDs, timestamps for calls, login and logout, IP addresses, type of Internet service used, phone IMSI and IMEI, as well as geographic data to cell phone towers. Only metadata are allowed to collect in the data retention directive, and it is stated that it is not allowed to retain data that could reveal the content of the communication [55, p. 5].

We did not find any other detailed information about other collection of SMS from other nation-states, but it is possible that similar actions are being taken in other nation-state's surveillance programs, e.g. in the Russian SORM-1[52].

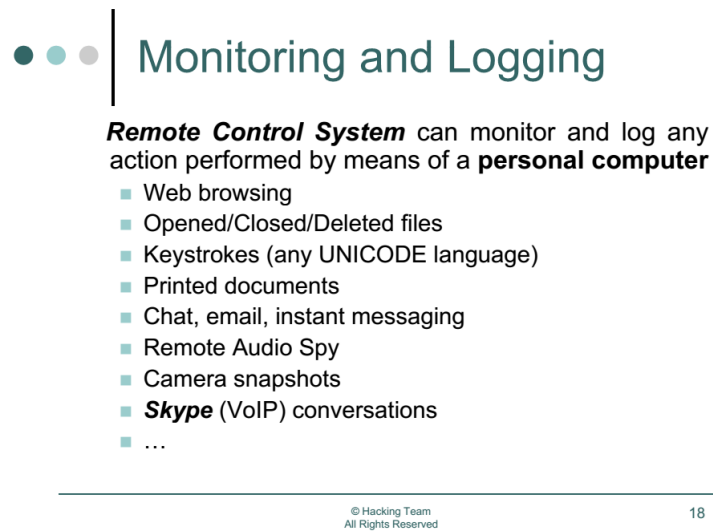
4.1.2 Content Data

While metadata gives information about the data, it is also useful for intelligence organizations to collect the content of the data that is being sent, thus given the term content data is being used. While there seems to be regulations on intelligence gathering in most nation-states, the foreign surveillance is very little limited when applied to foreign nation-states.

During the G20 summits of 2009, the British GCHQ intercepted information from foreign political representatives [56]. In addition, according to documents by Edward Snowden, the Belgian telecom, Belgacom, was hacked by GCHQ in order to better understand the company's infrastructure [57].

Software used for intelligence purposes shows even more in detail to what extent information can be collected. A surveillance software created by Hacking Team, provides surveillance software to governments [3]. Their software can collect a massive amount of information from both personal computers as shown in Figure 3, and smart phones as shown in Figure 4. The presentation slides in the figures show that almost every little detail of what the user is doing, could be collected. Another example of collected data is GhostNet surveillance software. Its origin is allegedly from China, but it is not confirmed. The GhostNet is capable of stealing files, log keystrokes and extract live camera and microphone streams [58].

Most information seems to be collected when possible. Other examples from the NSA is that administrators have been targeted in attempts to collect their administrator account details, a process which acts as a step-stone in order to provide access to suspected users [59].



● ● ● | **Monitoring and Logging**

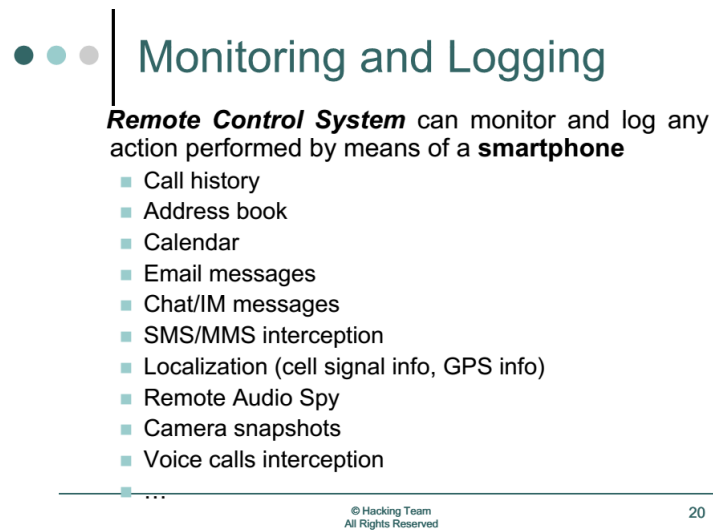
Remote Control System can monitor and log any action performed by means of a **personal computer**

- Web browsing
- Opened/Closed/Deleted files
- Keystrokes (any UNICODE language)
- Printed documents
- Chat, email, instant messaging
- Remote Audio Spy
- Camera snapshots
- **Skype** (VoIP) conversations
- ...

© Hacking Team
All Rights Reserved

18

Figure 3: The surveillance software provided by Hacking Team can gather information from personal computers. [3]



● ● ● | **Monitoring and Logging**

Remote Control System can monitor and log any action performed by means of a **smartphone**

- Call history
- Address book
- Calendar
- Email messages
- Chat/IM messages
- SMS/MMS interception
- Localization (cell signal info, GPS info)
- Remote Audio Spy
- Camera snapshots
- Voice calls interception
- ...

© Hacking Team
All Rights Reserved

20

Figure 4: The surveillance software provided by Hacking Team can also gather information from smart phones. [3]

4.2 Surveillance Categories

We found that there are different approaches on how to perform surveillance of the information in networks. This section contains material on how information can be captured. The two approaches are when data is moving in the network, i.e. data in transition, and data that is not moving in the network, i.e. data at rest. Nation-states have different approaches that are used in order to be able to perform surveillance and control the devices that are participating in the network. The two following examples show how the U.S. and China have tried to control individual devices:

- **Clipper Chip**

The Clipper Chip [60] is an example where a hardware implant was supposed to be shipped with all communication equipment sold in the US. It would encrypt the communication, and provide lawful interception when needed.

- **Green Dam Youth Escort**

Examples on attempts on control functionality has been seen in the Green Dam Youth Escort project in China as described by Hagestad II [61, p. 231-233]. Computers were to be shipped with pre-installed software that had filtering of web content with bad images or content, e.g. blocking online pornography.

Both of them are currently discontinued. We believe that it might not be feasible to control every device that is participating in networks, so instead the intelligence operations are relocated to central points in the networks. Two examples are not enough to conclude that this assumption is true, but it makes sense due to that the nation-states are approaching a centralized source of information instead of chasing after every single target.

Centralized solutions for information collection and filtering seems to be working very well. The U.S. UPSTREAM-program and the China's Golden Shield are both using the fact that participants in the network have to connect to central points to communicate to the outside world [51][21][p. 220-231]. This enables better control of the information flow and it is possible to better cover everyone that uses the Internet, compared to trying to control the user's devices through pre-installed software and hardware. The centralization can also be seen in India as described by Xynou[24] where many of them do not have Internet and computers in their home, but rather go to Internet cafes to access such services. The government knows this and obliges the internet cafe owner's to collect and store information on who is using the service, as well as when. The cafe owners are in addition required to take backups so that the data logs are not lost.

The two most feasible ways to collect information is either to collect it after it has left the device, or actively interact with the target when it is residing on the device. Two main approaches a nation-state could use are data in transition and data at rest.

4.2.1 Data in Transition

When data is moving and the nation-state wants to know about the data that are being sent, they can monitor a central point of communication, e.g. a telecom provider or Internet backbone. It is also possible for them to add probes to collect information from different infrastructures. If they are not already in control of such, they can take control of it. The main approach based on our observations is that they can collect all data passing through as long as they have legal means and processing powers to support this. It can however, be other ways that this is performed. An example of this is the SMS collection as described in Section 4.1.1, where all messages and their metadata could be collected.

The idea of intelligence organizations having access to telecom- and internet providers is not that new. Back in 2006, the American Civil Liberties Union published a somewhat biased whitepaper by the name *Eavesdropping 101: What Can The NSA Do?*[4] where they investigated how likely the NSA are performing surveillance and how it could be done. Figure 5 shows various probes that covers Internet Service Providers (ISPs), telecom companies, central switches, satellite communication, Internet exchanges and undersea cables. The probes makes use of that information need to pass through them in order to leave the nation-state, thus making it easier for intelligence agencies to collect data.

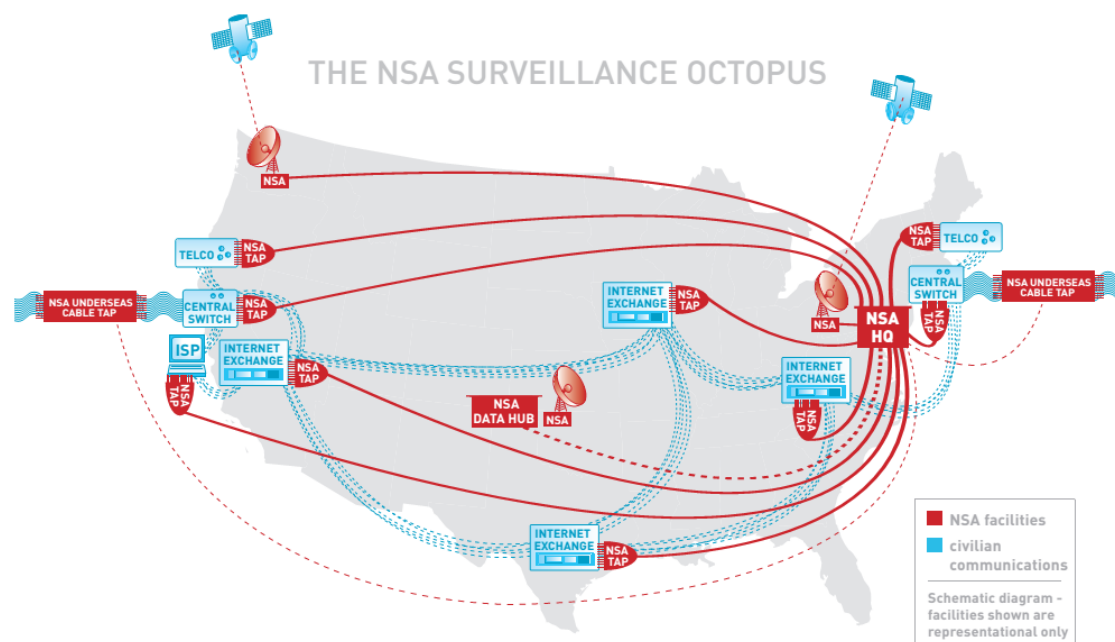


Figure 5: Infographic map from 2006 on how the ACLU believed the NSA could collect information from different probes.[4]

While it has been difficult to confirm occurrences of intelligence gathering through probes it was in 2013 gained more supporting data on the topic. In a news article by the name *NSA infected 50,000 computer networks with malicious software*[62] from *NRC Handelsblad* it was presented a slide from the leaked documents of Edward Snowden which further support the ACLU's beliefs on probes. The news article shows a world map with different types of probes in strategic positions around the world that allegedly are used for accessing wiretapping information from networks. The details were further supported by that Snowden in an interview explained that NSA has the option to collect data in other countries as well [63].

The NSA Upstream program is one of the current examples on collecting data from fiber cables and infrastructures that data is passing through [51]. It is not necessarily only NSA together with the rest of the Five Eyes¹ that are doing such, and it could be possible that this approach is being done by other nation-states. In some cases like the Russian SORM-2 [25] the ISPs are required to install expensive equipment that support surveillance of Internet traffic. While the SORM has some general overview information available, as discussed in Section 4.1, we have not found any further data on how this might look like. In China, a network monitoring solution from CISCO is used by The Ministry of Public Security (MPS) of China to track users' work histories and political tendencies[61][p. 223]. Sweden's FRA (the National Defence Radio Establishment) has some interesting similar properties to what has been seen in the other nation-state's surveillance, as described by Christopher Kullenberg[64]:

"The FRA has bought one of the fastest supercomputers in the world, and it is plugged directly into the central fiber-cables of the Swedish Internet Service Providers. They will consequently receive a copy of all traffic-data, and then process it in several steps in order to find patterns".[64]

It is not always possible to take control of an existing infrastructure for collection. There is another way that has been used and is related to that if they are not in control of a point where information flows through, they will instead attempt to become a the central collection point. According to an article published by *The Guardian* the British GCHQ created fake internet cafes in order to gather information on their allies during the G20 summits in 2009 [56]. It is well know that many people value free Wi-Fi and that behavior enables efficient capturing of data from the users of the "free" access point.

Information in Cleartext

Information collection infrastructures can gather all information that passes through. Some types of information are easier to get a hold of than others are. Unencrypted data traffic sent over the Internet can directly be read and interpreted, while encrypted data can be stored for deciphering at a later time when deciphering algorithms or keys become available. An example of unencrypted information that could be collected is the case of Yahoo [65], where the British intelligence agency, GCHQ, was collecting web camera sessions from Yahoo web-camera chats. Every

¹An intelligence alliance consisting of Australia, Canada, New Zealand, the United Kingdom and the United States.

5 minutes they were grabbing a snapshot, and then saving it in their database. If they wanted, they would be able to capture pure video as well. The capture contained whatever that was in front of the web-camera at that time, even including pictures of naked people. The reason that enabled GCHQ to capture such web camera imagery was that the video stream was being sent over the Internet unencrypted, something that enabled them to collect data from infrastructures they were in control of.

Yahoo web-camera chat is not the only service that has been prone to collection. A few months after the Yahoo headlines was Viber, a popular voice and text chat application, found to send data unencrypted. Images, Doodles, Videos, Location images were not encrypted, which means anyone in control of a network point between the sender and receiver can see what is being sent [66]. The un-encrypted information could potentially be collected through the intelligence organization's probes if they wanted to.

Encrypted Information

Incidents as with Yahoo and Viber would probably not have happened if they used proper encryption for their data communication. Encryption makes it difficult for intelligence organizations to gather information in transition, even when it is passing through their point of control. Intelligence organizations are aware that encryption can be hard to break and result in important information that could remain secret. In cases where the intelligence agency decide that the encrypted information is something they find to be of very high importance, they can then attempt to decipher the data, or store it until a later time when more processing power or new algorithms can decipher it.

Most intelligence organizations are aware of the problem regarding encrypted data, and because of this, some of them are working towards breaking encryption, as described in the news article *Spy agencies in the U.S. and U.K. bypass widely used encryption protocols* [67]. The article describes how intelligence agencies in the U.S. and the U.K. are focusing on defeating encryption and the various means that are being used. There are different approaches on how they aim to defeat encryption, as it can be defeated through various ways, either by technological or legal means. A lot of effort and money is allegedly put into this and if they succeed in breaking encryption protocols, then they will be able to achieve a high degree on information disclosure.

There is also another approach that can be used to get a hold on information that is encrypted while in transition. Instead of waiting for a time when it is feasible to decrypt information, the intelligence agency can instead attack the devices that are participating in the network. By having control of the device that is encrypting and sending information, it is then possible to collect the information before it is being encrypted. There is also the possibility to steal encryption keys so that further surveillance can be performed in a passive way at the probes in control of the intelligence organization. When attacking the devices that are participating in the network, we define it as being at rest within the device, thus it brings us to the second category of data collection; data at rest.

4.2.2 Data at Rest

In this thesis, the definition of data at rest is when data is residing in the device where the information is stored, and all the way, until it leaves the location or device. In order to access data at rest, it will require some sort of targeted access to the suspect's device. This can be achieved by legal or less legal means, by either physical seizing the equipment or perform a technical infiltration. It would be fair to assume that governmental agencies choose to adhere to laws and stay as much as possible within the policies and regulations that they have. Alternatives for targeted cyber surveillance are described in Section 4.2.2.

Targeted Cyber Surveillance

In order to perform targeted cyber surveillance it would in most cases be necessary to somehow examine information on their target's device. There are different ways that the governmental agencies could access this information. Possible ways to do this is to seize the device, or exploit it either locally or remotely. This section explains options we observed that could be used for performing targeted cyber surveillance by nation-states.

Seizing of devices

Seizing of devices is an approach that enables the nation-state to get a hold of the device. This can be done in a legal way where a warrant is required to seize the device [68]. The less legal way is also optional, in which the device is simply being stolen from their target. Seizing devices is not a part of a cyber-operation, but it is an effective way to get a hold of devices that store important information.

Device exploitation

The alternative to physically seizing the device is to use a semi-legal approach to infiltrate the device locally or remotely, e.g. phishing, and then rely on some sort of surveillance software or hardware installations for data collection. For most exploitation, there is a need to get a hold of exploits that can be used on vulnerable targets. In order to make sure that the exploit has a high rate of success it could be necessary to use zero-day exploits, i.e. exploits that are not yet disclosed to the world, and therefore not yet been patched [69, p. 1]. Such zero-day exploits can exploit vulnerabilities in software and hardware. Options for acquisition of exploits are shown in Table 4.

Hardware implants

Instead of exploiting the software and firmware through code, hardware with surveillance capabilities can be attached to the target's system. There are different types such of equipment ranging from simple key-loggers that Nikolay Grebennikov describes as "[...] *small devices that can be fixed to the keyboard, or placed within a cable or the computer itself*." [74], to advanced USB-hardware implants as explained in the leaked documents from Edward Snowden where, e.g. NSA is using *COTTONMOUTH I/II/III* to provide long range wireless access and options for

adding exploit software onto the target devices [75].

Software suites

After using an exploit, the nation-state would need to install specialized tools that can locate and extract intelligence information. Some commercial companies are aware of the demand and therefore specialize in lawful-interception software. In a CNET news article *Meet the 'Corporate Enemies of the Internet' for 2013*[76] commercial companies that provide surveillance technology to different nation-states are described. Such software suites can contain everything the nation-state needs to exploit and perform surveillance of their target's device. They aim to, and are most likely supporting a broad range of personal computer and mobile operating systems for their surveillance software [3, p. 19, 21]. Gamma Inc.[77] and HackingTeam[78] are two examples of such companies. Their software are in many ways similar to illegal surveillance software that any other criminal would use. In order to limit abuse, only authorized governments are allowed to buy such software[78, 77]. Citizen Lab has analyzed Hacking Team's surveillance

Table 4: Sources for exploits used in exploitation of devices.

Exploit source	Description
Publicly available	Publicly known exploits, i.e. not zero-day exploits, can be publicly accessed from e.g. web pages, or in exploit frameworks like metasploit[70]. The metasploit framework is usually used by penetration testers to perform penetration tests of networks. Less technically skilled people, and possibly nation-states, can also with low effort download and use this or similar frameworks to attack and exploit systems that are not properly updated. As the exploits already are known to the public, most up-to-date systems can be patched in order to protect against the exploits.
Black market	If a nation-state wants zero-day exploits for infiltration, they can enter the illegal black market, e.g. online market place where criminals buy and sell exploits. Governments' participation and motivation for entering the black market are described by Ablon, Libicki and Golay[71, p. 43].
Commercial companies	There is a more ethical way of buying exploits from the "gray market", by doing so from commercial companies that specializes in vulnerability research for government agencies and intelligence communities, e.g. VUPEN or ReVuln [72].
In-house research	Another way is to develop exploits is by using in-house resources in the government agency to find new exploits. According to a news article by Bloomberg are NSA and other "spy agencies", i.e. intelligence agencies, developing exploits [73]. While the challenges for developing them are not described, one could assume that the process can require a lot of work, something which further supports purchase of exploits in gray and black markets.

software and a shortened excerpt is provided in Appendix A.

Crimeware as a Service (CaaS)

Sometimes the nation-state either has too little capabilities or does not want to have the attack traced back to themselves. An available solution to this is to instead let another criminal organization perform the targeted surveillance. Sood and Enbody[79] describe how it is possible to outsource the cyber-attack to another entity, which in most cases is a criminal one. This option is available for anyone that has money to pay for the service. The only thing the person has to do is to register their credit card and give initial information about their target. This method requires little or no experience with hacking and enables exploitation and information gathering without having to confront their target in any way, thus leaving the risks of detection to the provider of the service.

Options for distribution

Based on our observations, we identified approaches for installing the surveillance software on the target. The list is not comprehensive, but it gives an idea of which distribution options that can be used for surveillance software distribution. The approaches are as following:

- Phishing
- Waterhole attack
- Remote exploitation of vulnerable services
- Physical installation via thumb drive or hardware implant

Options for Transferring Data to the Attacker

After performing exploitation of the device, the nation-state would like to transfer the data back to the attacker. They have many technical options available as we have described in [80]:

A: Transferring Collected Data over the Internet

- Using cleartext or encrypted network traffic
- During updates
- Embedded into unused fields in protocols
- Hiding origin by using proxies
 - TOR
 - Hidden Collection Infrastructure (described in Appendix A)

B: Transferring Collected Data Without Internet Connectivity

- Manual use of USB-stick

- Physically collect data through e.g. hardware maintenance
- Locally connected PC without internet, can use other infected computers as "proxy server" as seen with the SNAKE malware [81][p.19].
- Radio access through hardware implants [75].

5 Evaluation of Collected Intelligence Data

The different approaches described in Chapter 4 are to our understanding resulting in that nation-states collect massive amounts of data. In order to be able to comprehend with all this data, it is necessary to see how it is possible to store and interpret these data. In most cases, it is related to the Big Data issue. This chapter is included for completeness purposes.

5.1 Big Data

As everything starts to centralize around networks, the massive amount of data is making its way. Kaisler, Armour, Espinosa and Money[82] explains about Big Data and its issues. They also describe how the U.S. planned to invest \$200 million in development of new techniques and tools for handling Big Data. While it was not directly an intelligence related project, the Department of Defense was one of the participating parts in the initiative. One of their goals were to get a hold of and process massive amounts of information. We assume that many nation-states are working hard to cope with the issues brought by Big Data, and therefore we are investigating how massive amounts of information can be collected, stored and processed. Based on the information from Kaisler et al.[82], we observed that that an ideal solution for surveillance could have similar properties to the existing abilities in big-data:

- Extract everything
- Store everything
- Ensure its correctness
- Aggregate data
- Ensure confidentiality

If possible it would be best to store everything. However, if it is being used in surveillance, one would really want to make sure that the data are correct, i.e. that the data are not modified [22, p. 5, 6]. It is also very important that the target should not be able to discover or manipulate the surveillance [83]. If the data are as correct as possible, it will be easier to aggregate correct data about the target. Through aggregation, the nation-state can use the small bits and pieces of the target, which then can be combined to find information that is more detailed. Based on the leaked information from Edward Snowden, we observed that *XKEYSCORE*, a search tool used by the *Five Eyes* covers big data collection, processing, storing and aggregation [5]. The process of how a nation-state could perform their big data operations are depicted in Figure 6.

Large amounts of stored information could have drastic consequences if they were to be stolen or used in a way it was not supposed to be. Schneier[84] wrote an essay on this topic on whether



Figure 6: An example of how a nation-state handle "Big Data". The information is collected, and then processed, before it is stored. Whenever it is needed, the nation-state can aggregate the data [5].

a government or the private companies should store such data, and the conclusion seems to be reflected in the excerpt:

"Where does this leave us? If the corporations are storing the data already – for some business purpose — then the answer is easy: Only they should store it. If the corporations are not already storing the data, then – on balance – it's safer for the NSA to store the data. And in many cases, the right answer is for no one to store the data. It should be deleted because keeping it makes us all less secure." [84]

It is not currently possible to say anything on how they handle and aggregate information in other nation-states, but some of them, e.g. EU-member states are through the EU data retention directive are obliged to not retain data for more than two years from the date of communication [22, p. 5]. The two previous chapters have explained how cyber surveillance can be performed and how the massive amounts of data affect and enhance surveillance capabilities. In the next chapter, we present another side to this surveillance, where nation-states can be supported by suppliers in order to have an even greater capability for performing surveillance.

6 Nation-state Surveillance with Supplier Support

The conventional threat we have seen for the users of the cyber domain is that nation-states are performing surveillance. In order to perform their surveillance, the nation-states would use resources that are available to them. One of these resources can commercial companies, i.e. suppliers of products¹ or services, which can support the nation-states in their cyber surveillance. Support from suppliers could create additional risk as the threat model we had before is no longer applicable. This is because supplier support exploits the trust the users lay in the suppliers, thus it adds additional ways to collect information about the users of the cyber domain. This chapter describes the motivations for a supplier to support surveillance performed by the nation-states, ways suppliers can support them, and how the support affects the security and privacy of the users.

6.1 Motivation for a Supplier to Support Nation-state Cyber Surveillance

It is not always easy to understand why a supplier of products and would decide to help a nation-state to perform cyber surveillance, but in fact, they have multiple reasons to do so. They think about their own business, their economy and that all "shareholders" should be happy. In terms of privacy and security there seems to be a balance in the company between respecting their customers and respecting their government. Both the customers and government should be happy, and if they fail to do so, it could have rather large consequences. We investigated what types of motivations that a supplier can have to support nation-state surveillance. We distinguish between collaboration and support, due to that the supplier assisting with surveillance is not necessarily getting anything in return for helping the nation-state, contrary to a public-private partnership. We collected motivations of suppliers' support based on reasons for participating in collaboration, cooperation or support of a nation-state's cyber surveillance. The results are presented in this section.

6.1.1 Legal Pressure

Companies that decide to reside in a nation-state are bound by the nation-state's national laws and therefore have to comply with that. For example in India, as described in the presentation by Xynou[24, p. 12], various sections of their *Information Technology Act* states that that information can be intercepted by e.g. law enforcements, and if users are not giving away their encryption keys and failing to do so can result in a jail sentence of up to 7 years.

If a company neglect their government or work with something that is not in the best interest of the government, it could have consequences for the supplier. In the case of Lavabit, a

¹In our case; software or hardware.

company that delivered encrypted e-mail services, allegedly got cease and desist letters which resulted in that they shut down their service without saying anything of why they chose to do so [85]. The Wired got a hold on documents that further proved the U.S. government obtained search warrant for Lavabit in order to get detailed information about communication, in addition to crypto-keys and certificates [86]. The article further describes how Lavabit's owner was then faced with a tough choice to become complicit in crimes or shut down his service, where the latter one were chosen.

While not in context with the Lavabit case, Bruce Schneier also stated at the RSA 2014 conference about the general problem of legal pressure on vendors [87]:

"[...]but the truth is you won't be able to find the vendor that isn't vulnerable to legal pressure from somebody,"[87]

His statement further support our observations in that legal pressure is a motivation for a vendor to support nation-state cyber surveillance, which as a result could affect privacy and security of the users in cyber space.

6.1.2 Patriotism

According to Bloomberg and its interviewed sources is patriotism something that could motivate companies to cooperate with the U.S. intelligence [88]. Patriotism is not only limited to the U.S. as any other company located in another nation could feel motivated to support their home country, or defend national security.

6.1.3 Staying in Control

Companies want control of their business to have as much as possible. The news article *How the U.S. forces Net firms to cooperate on surveillance* [89] published by CNET describes how U.S. companies prefer to help their government and why they might choose to do so. We observed some interesting information in the article and have therefore provided it in the following excerpt:

"Jennifer Granick, director of civil liberties at Stanford University's Center for Internet and Society, said, referring to the government's pressure tactics:

"They can install equipment on the system. And I think that's why companies are motivated to cooperate [and] use their own equipment to collect for the government. They would rather help than let any government equipment on their service, because then they lose oversight and control."
"[89]

Jennifer Granick states that the companies would rather help the government than to risk that they might lose oversight and control of their business. One plausible explanation could be that companies would like to have maximum control of their business, something that is quite similar to the problems seen in criminal cases involving computer systems. In these cases, the government would take control of, or even seize their equipment in order to secure evidence. The

result can be that it will take long time before the company can get their systems back up and running, something that could affect their business and revenue. The Lavabit case described in Section 6.1.1 is related to this problem about staying control as the owner of Lavabit shut down the service because he otherwise risked that his service for encrypted communication would be compromised, and therefore not provide a high degree privacy as the company advertised [86].

6.1.4 Economical

Some companies could receive "investments" or money as support for their business or legally sell information, but it could also stretch as far as being pure bribery. A supplier could of various reasons decide to support surveillance activities for a nation-state if it can lead to increased revenue and resources for the supplier. While in some countries in Africa and Asia there are a higher frequency of bribery in general, there are also similar activities happening in the other parts of the world. There are different approaches to this such as the case where NSA supported the RSA through a \$10 million contract as described in a news article by Reuters [90]. This was allegedly done with intention of getting the RSA to implement a Random Number Generator (RNG) which the RSA did not know was flawed, something that enabled the NSA to more easily break encrypted data [90]. According to statements by NSA Director Lt. Gen. Michael Hayden [91, p. 2] there are known occurrences of bribery:

"there are instances where we learn that foreign companies or their governments bribe, lie, cheat and steal their way to disenfranchise American companies. [..]"[91, p. 2]

6.1.5 Mutual Sharing of Information

Normal instances of information sharing occur internally between allied intelligence agencies, but also in a public-private relationship. One example of information sharing between intelligence agencies is the Five Eyes [92], an alliance consisting of USA, Britain, Canada, New Zealand and Australia. They share what they have gathered with other intelligence agencies that are part of this alliance, in order to keep each other updated. While it is not confirmed, we assume that other alliances also are sharing information.

The public-private relationship also seems to play an important role. There has allegedly been mutual sharing of information between companies and government [88]. Jones, Kovacich and Luzwick[20] quotes a statement by Harris Miller, the president of the Information Technology Association of America (ITTA) on what we observe is information sharing between suppliers and government:

"government leadership in a meaningful partnership with industrial leadership is essential and that all of the involved parties need to share information to reduce vulnerabilities and improve network security."[20][loc. 7355]

While the quote does not state anything about other nation-states; it gives an indication that the U.S. desire sharing of information between industries and governments. The importance of

public-private partnerships in cyber security is also mentioned by Busch and Givens[93, p. 3, 4], as the mutual information sharing and support enables them to better protect their systems against electronic threats.

6.2 How a Supplier Can Support Nation-State Surveillance

Any nation-state today will be able to perform some sort of surveillance, and the only differences are that some have more resources, technology and skills than the other ones. There is also another option that could influence the ability for a nation-state to perform surveillance, namely supplier supported surveillance. If a supplier through various reasons decide to help the nation-state to perform surveillance, the nation-state would have a greater chance of success because it is exploiting the user's trust that they have to the supplier. One could barely imagine the possibilities of one or more suppliers of well-known software and hardware helping the nation-state to compromise or get information about their targets. A supplier of products or services has many ways to either directly or indirectly support a nation-state with surveillance. Support options that we observed are presented in this section.

6.2.1 Disclosing of Requested Intelligence Information

A supplier can of various motivations decide to give away information to a nation-state. This can be through legal requests as stated in their Privacy Policy and Terms & Conditions, or it can be other formal and informal contracts that enables them to share information with a nation-state.

Terms of Service

In general, the end-users have very little or no ways to protect their privacy. A non-profit organization by the name Council of European Professional Informatics Societies (CEPIS) confirms this in a decision [94] that they are concerned about the risks implied by insufficient management and vulnerabilities in design of the specter of software and services. The decision document also states that the end users in most cases have no other choice than to accept the conditions if they want to use the products or services.

While it is not a direct option for supporting nation-state surveillance, some suppliers are reserving their rights to give information about themselves and their customers if the requesting authority has a valid reason and it complies with the supplier's policy. Suppliers can often through their terms and conditions or privacy policy give away information when needed, while still reserving themselves against legal actions by offended customers. However, this depends on the nation-state's laws and the supplier's geographic location. An example is taken from NETGEAR's terms and conditions for their web site and products on how they act upon requests from legal authorities:

"We will share information if we think we have to in order to comply with the law or to protect ourselves. For example, we will share information to respond to a court order or subpoena. We

may also share it if a government agency or investigatory body requests. We might also share information when we are investigating potential fraud. We may share information for other reasons we may describe to you.” [95]

The quote serves as an example only, as it is not observed whether NETGEAR is giving away information or not.

In order to comply with law and protect many suppliers are willing to share information. Any government agency request seems to be sufficient, as the policies do not state the thresholds of such requests. We observed that information sharing through terms of service is covered by Electronic Frontier Foundation (EFF)[96]. EFF has analyzed policies of *"Internet companies — including ISPs, email providers, cloud storage providers, location-based services, blogging platforms, and social networking sites — to assess whether they publicly commit to standing with users when the government seeks access to user data."*[96][p. 3].

Giving Access

If a nation-state would have to send a legal request every time they wanted to get a hold of information about the supplier or its customers, it would be a slow and not very efficient process. In 2013, the disclosed PRISM[51] program, a NSA surveillance program, showed that there could be an easier way to get the information needed with less bureaucracy involved. Most of the participants are well known large suppliers of software and IT services. EFF has in another publication described what we currently know about the PRISM, while referencing to a PRISM document:

"Information sharing between the FBI, NSA, and CIA has been routinized through 'software which would automatically gather a list of tasked PRISM selectors every two weeks to provide to the FBI and CIA.' [...]"[97]

Another example of information sharing is based on a joint article by The Guardian and Washington Post [98] where it is described that Microsoft has compelled to hand the NSA access to encrypted messages in Outlook and Skype. Microsoft replied to the Guardian with a statement that says that they only provide customer data in response to legal processes and that they reject such requests if they find it to not be valid [98]. We find it difficult to determine whether Microsoft are willingly giving away information, or that they have been forced to do so. Based on the NSA slides about the PRISM program, it does however give indications that e.g. Microsoft and other large suppliers have given away a lot of information. However, some of the PRISM participants have stated that they do not want to give away such information unless it is according to law. In fact, some of the participating suppliers have stated that they want a higher degree of transparency and want to be better able to talk about the information that they give away. An excerpt from Microsoft's statement is as following:

"[...]There are aspects of this debate that we wish we were able to discuss more freely. That's why we've argued for additional transparency that would help everyone understand and debate these important issues. [99]"

We observe that there is some uncertainty whether the information sharing is willingly or unwillingly being done. While the U.S. PRISM program is to our understanding, one of the very few examples of publicly known supplier collaboration programs for cyber surveillance. While it is not confirmed, we might find similar collaboration programs in other nation-states as well. A collaboration program does not necessarily need to exist in a formal context with contractual agreements, but informal requests from other nation-state's governments could have similar properties.

A general understanding of giving direct access is not only limited to the U.S. PRISM program, but the approach is quite special in the way that it enables the nation-state to get information they need about their targets more easily from the suppliers, as it does not need to exist court orders for every request. This method would also enable the nation-state to get information about their targets without having to interact with them. Figure 7 shows a model based on our observations. The general way of getting detailed information about the user would have been to surveil their target, something that would require some sort of interaction by attacking the target. If the supplier gives away the necessary information to the nation-state authority, there would no longer be a need to interact with the targets. By not having to interact with the target, the nation-state can use this as an advantage to get most of the information they need by

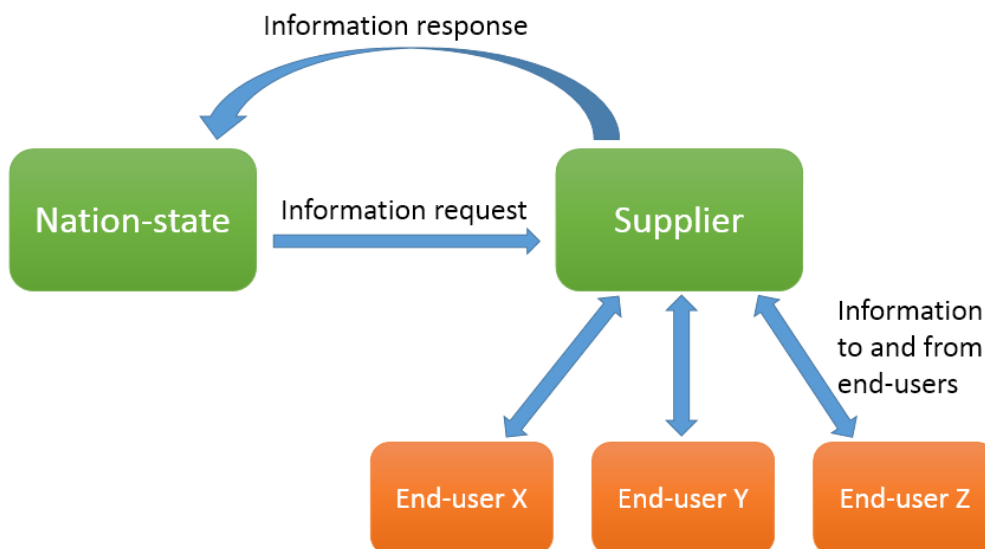


Figure 7: Through passive surveillance can the nation-states use the supplier's help to obtain information about their targets.

querying the company of the service their target individual is using. This is quite similar to the passive reconnaissance used in penetration testing. Another advantage of this approach is that it would not leave any traces or affect the target, unless the nation-state find it necessary to further investigate or prosecute the target with physical or digital means.

6.2.2 Manipulating Their Products and Services

Depending on the motivation of a supplier to support nation-state surveillance a supplier of hardware, software or services can enable nation-states to perform surveillance inside and outside cyber space that they would otherwise not be able to do. This subsection covers our observations of options on how a supplier can intentionally and unintentionally manipulate their products and services, which can be used in order to support targeted nation-state cyber surveillance.

Giving Access to Manufacturers and Intermediate Supplier's Premises

Access to premises and systems has already been seen in many occasions. Many ISPs and telecommunication providers in different nation-states are working with or are related to the government, which opens for nation-states to wiretap information passing through[89, 52][21][p. 43]. By letting the nation-state have their equipment installed the supplier is supporting the nation-state surveillance, which the nation-state would not as easily been able to do otherwise. For supply chains access to premises and systems not limited to the manufacturing part as it can be intercepted at any part of the supply chain. Therefore, all suppliers that handle products before they arrive at the nation-state's target are able to provide support for interception, which then can enable the nation-state to add their backdoors at will. The news article *Glenn Greenwald: how the NSA tampers with US-made internet routers*[100] explains how interception of products can take place:

"The NSA routinely receives – or intercepts – routers, servers and other computer network devices being exported from the US before they are delivered to the international customers.

The agency then implants backdoor surveillance tools, repackages the devices with a factory seal and sends them on. The NSA thus gains access to entire networks and all their users. The document gleefully observes that some "SIGINT tradecraft . . . is very hands-on (literally!)."[100]

By having access to premises and systems of suppliers of products and intermediate supply services the nation-state is able to intercept and compromise the products before they are delivered to the customers.

Based on our observations throughout our research, we suggest some types of suppliers that are prone to giving nation-states access to their premises:

- Manufacturers of software or hardware
- ISPs
- Shipping
- Customs
- Postal services
- Telecom providers

While communication providers are real-life examples of support through giving access to their premises and systems, it is also possible for other types of suppliers to give access to their products and services. For example, Microsoft has since 2003 provided access to their Windows source code to participating national and international bodies, e.g. Russia, China, NATO and the UK [44]. While the intention of providing insight to the source code of Windows, we note that it can be used to improve security, but also to identify vulnerabilities that can be used for targeted attacks.

Not Detecting Malicious Behavior

Anti-virus companies were in the beginning of 2000 not agreeing on whether to detect malicious programs from governments as described by Gregory and Glance[23][p. 6]. The anti-virus companies had different opinions. Some stated that they would detect such malicious programs, e.g. F-secure said they will detect such, and other companies were reluctant to detecting as it, e.g. Symantec stated they would not detect government malware[23][p. 6]. At the end of 2013, Bruce Schneier reopened this discussion on whether anti-virus companies actually are detecting them or not [101]. He did so by joining a group of experts and publicly asking anti-virus companies if they were detecting malicious programs from governments. He further added that the consensus of the companies that have replied so far (ESET, F-Secure, Norman, Shark, Kaspersky, Panda and Trend Micro) is that they would not comply with any requests from a government if asked to not detect malware.

Anti-virus companies are aware of this debate on whether to detect or not detect malicious software from governments and law enforcements. F-secure even has a separate part of their policy which covers that they explicitly state that they would detect all such government spying programs [102], which they confirm that they will detect all such programs. Dating back to 2009, Johnston and Harley[103] have written a white paper that discusses the problems with surveillance software by government and law enforcement. An important detail the white paper describes is about the supplier related issue in which security companies want to cooperate with law enforcement agencies, but are faced with the practical and ethical dilemma where they would have to defeat their own purpose of identifying malicious software.

While some of the vendors of anti-virus have decided to detect all such programs, it is still unknown what the rest of them would actually do. We believe that it would be wise to be aware of that some anti-virus companies might decide to take the government's side and not detect the surveillance software.

Neglecting to Patch Vulnerabilities

If a company finds vulnerabilities in their software, they can decide to not patch it and instead let the government use this for lawful interception. In a news article by Bloomberg it is explained how Microsoft allegedly keeps governments updated on bugs, e.g. vulnerabilities, before they are fixed, something which enables the government to use it for both defensive and offensive measures until the vulnerabilities are patched [88]. Vulnerabilities are usually patched as soon as possible in order to protect the products from attackers. Security issues would arise if a supplier supports a nation-state by not patching, or waits for a certain amount of time before patching them in order to support "lawful interception". Products that are vulnerable to attackers in the form of both malicious "hackers" and nation-state surveillance would qualify for the term "Swiss cheese" if a supplier choose to deliberately leave holes in their software.

Adding Backdoors

Another option a supplier of software and hardware can have to support nation-state surveillance is to deliberately add backdoors, e.g. an intended flaw, which can be used for lawful interception. As the supplier is in charge of their development and supply chain of their products, they would be able to add such backdoors at their will. If a supplier decides to do this, they would make it easier for the nation-state as it would no longer be necessary to spend resources on finding ways to exploit a supplier's software. By having a supplier adding backdoors to their products it will result in improved chances of successful exploitation of a nation-state's target as it the planted backdoor is already known and probably tested before it was deployed. The drawbacks of such backdoors would be that if it is disclosed to a third party, it could result in massive damage in terms of the supplier's reputation. The lawful interception backdoor could also be used by attackers with malicious intent to compromise and steal information from the device.

It should be noted that deliberate creation of a security flaw or backdoor is of course against best practices and could have severe consequences in terms of the suppliers' reputation and security of its products. Section 3.2 described the problem of insecure software and hardware. With that in mind, it is important to understand that many resources are spent on securing the suppliers products so that they can defend against malicious attackers. By deliberately adding security flaws in software and hardware, it will work against the resources spent by the suppliers to secure the products they supply. Both software and hardware can have vulnerabilities added. Each of the categories are presented in the following paragraphs.

Software

Accidental faults in software, e.g. operating systems, applications and browser plugins are common and exist in software that is made today, so it could be questioned whether it is realistic that a supplier would ever need to add backdoors to their software. However, a controlled backdoor could contain additional functionality and could be tested before it is deployed. This enables the nation-state to perform lawful interception when needed.

Hardware

A supplier could add backdoors into hardware itself or in the firmware. The first option is that the hardware itself contains “hard coded” gates, and therefore will make the backdoor permanent, thus it is not possible to fix with an update and requires the hardware to be completely replaced. While leaving a permanent backdoor available for law enforcement, it will also be available for attackers with other malicious intentions.

A second option is to add backdoors in firmware. Firmware attacks are shown to be possible as described by Brossard[41], which also covers how a nation-state would perform the backdooring[41][p. 7, 47]. Through exploitation of a vulnerability in hardware it was possible to flash the attacker’s firmware, which contained additional surveillance functionality that would avoid protection mechanisms and anti-virus due to it was located at the hardware level. Firmware attacks also had functionality for removing traces of surveillance as it could be remotely flashed with stock firmware. What a supplier could do in this case is to add firmware backdoors all the way through the supply chain they control and even at a later time supply surveillance software through their firmware updates from their web site. While there are certain ways to try to make sure that the hardware is benign, does it require that a skilled code reviewer analyzes the source code before compilation, or physically extract the firmware with a dedicated tool [41].

A third option that uses hardware implants is also possible. However, it would require the supplier to add the implants into the products they are producing, or have the nation-state adding the implant at a later time. This case is similar to the cell phones with additional hardware inside as shown in Section 4.2.2.

Certificate and Code Signing

When people are using their devices to securely access information, surf the web or installing software it is important that they can confirm that the data is supplied by the official company, and not by a malicious third party. Public-key cryptography in the form of digital signatures and certificates are in place to ensure security, but unfortunately the security is based on the trust of the supplier. If a nation-state were to force a supplier dealing with digital certificates into signing software or creating certificates, it would enable the nation-state to impersonate the official supplier of web-services or software.

SSL-certificates

One such hypothetical attack is described by Soghoian and Stamm[104] where an attack by the name *compelled certificate creation attack* enables them to exploit the trust in the protocols used for securing access to resources on the Internet, e.g. Secure Socket Layer (SSL) and Transport Layer Security (TLS). The protocols are found in the Public Key Infrastructure (PKI) and can with the hypothetical attack be exploited so that the government can perform Man-In-The-Middle attacks (MITM). The government can then sit between the communicating devices and listen in or modify the "secured" data traffic that passes through. The attack will avoid that the user gets warnings about incorrect certificates. The whitepaper explains how the web browser we use today is trusting hundreds of different Certificate Authorities (CAs), i.e. suppliers that are responsible to grant and approve SSL-certificates. As the CAs are located in various countries in the world, a government could get a CA to support them through issuing them a certificate for a website of their choice. They would then be able to perform Man-in-the-middle attacks, thus eavesdropping on the data that the user has trusted the company they think they are interacting with. While some certificates could enable impersonation of a specific website, could intermediate certificates e.g. be used in surveillance appliances that would be able to decrypt information[104][p 3].

Code signing

While SSL-certificates are used to secure communication over the Internet, software are signed in a similar way. Few people would question a digital signature coming from e.g. Microsoft or Adobe as long as they see that the official supplier signed the software. Code signing serves a purpose and is explained by Microsoft that the private keys for code signing are representing the organization's identity, and could be traced back to the organization, thus blaming them for the code that was distributed [105]. From a supplier's perspective, a nation-state could either steal or ask for the keys, or get the supplier to sign the piece of software for them. In that case, the software containing surveillance functionality would not be considered as a potential threat, as it ensures that the software came from the supplier, and that it has not been altered after it was published by them. An example of a digital certificate is shown in Figure 8. Stuxnet, an advanced piece of malware targeting specific industrial control systems, used signed certificates to appear legitimate [106]. It is not publicly known how widespread the use of code signing for surveillance software is, but statements from Chris Wysopal, the CTO at Veracode, said that NSA has access to vendor code signing keys, which was used to creating advanced malware like Stuxnet, Duqu and Flame[67]. His statements could indicate that some nation-states have capabilities to perform vendor code signing.

Digital signatures for web and software usage are protection mechanisms against third parties that intend perform malicious actions, but they provide no more protection that the supplier of these signatures provide. If the trusted supplier breaks this trust by supporting nation-state surveillance, it would only provide protection against third party hackers, but not the nation-states.

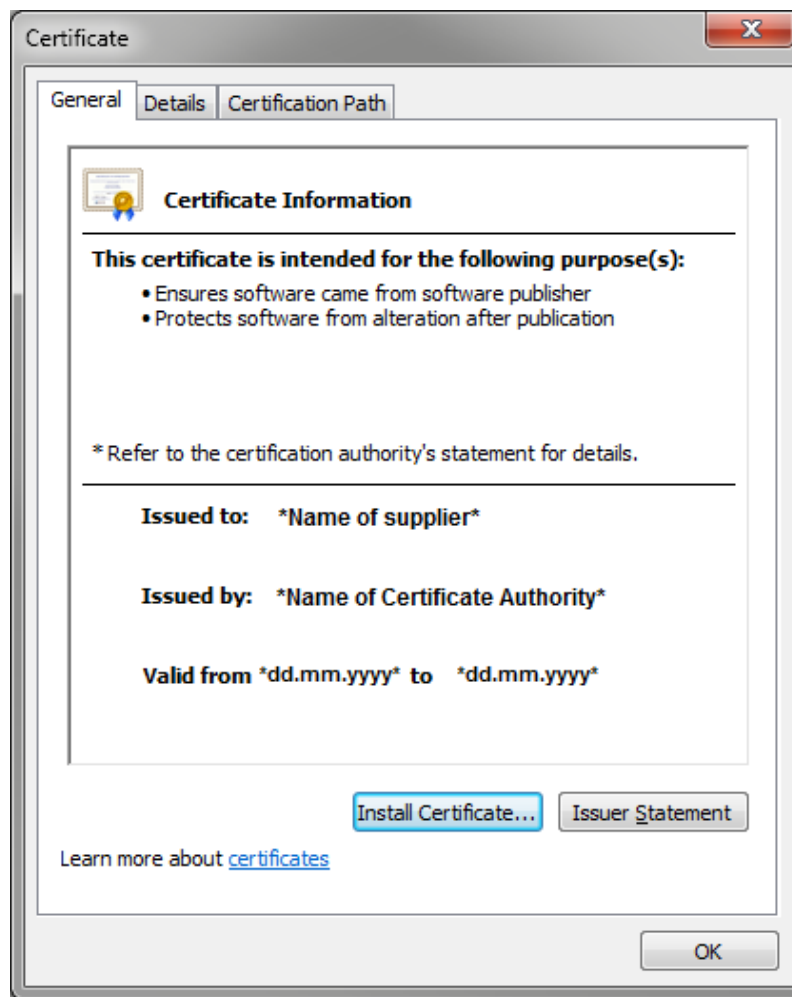


Figure 8: An example of a digital software certificate. It contains the name of the supplier and certificate authority, in addition to the time it is valid.

Distribution

A supplier of software or hardware could distribute surveillance software in the products they supply and thereby provide a more efficient way to install surveillance software onto the targets, compared to manual distribution of surveillance software to each target. The general way a supplier of software and hardware could support a nation-state for distribution of surveillance software is to add it to the product in a part of the supply chain before the customer gets a hold of it, or to provide it later through update functionality. In commercial surveillance software intended for lawful interception for governments, e.g. *Remote Control System* or *FinFisher*, has the infection vector relied on social engineering through spearphishing and fake software updates for popular software, respectively[7, 107]. The supplier of *FinFisher* even suggests in the mar-

keting brochure that an example of usage of the *FinFisher* system is to deploy it at a ISP in order to deploy surveillance software on target systems [107, p. 1]. In order to trick the target into installing the software, the target is then presented with fake updates for popular software like iTunes, Firefox, etc., through a Man-in-the-Middle (MITM) attack [108, 109]. However, in order to exploit the target, it would require the target to click on the fake update and would therefore not have a perfect success rate.

Our observations indicate that with supplier supported distribution of surveillance software it would no longer be necessary to compel ISPs into adding surveillance systems into their network equipment. In addition, it would not be any doubt in that the supplier of the product is the legitimate one because the supplier can digitally sign the software and therefore be able to bypass doubting targets, as it would present fewer security warnings than unsigned software. In addition, the suppliers have prerequisite capacity and knowledge of how to distribute their products, and would therefore be more than able to support distribution of surveillance software, e.g. in the form of software and hardware.

Combined Attacks

Multiple suppliers could work together in order to distribute surveillance software. By having multiple pieces of code that individually does not make any meaning, but together they result in malicious code. As we have described in [80], pieces of code in a combined attack can be distributed in two or more suppliers in the following ways:

- Operating system software
- Be a part of popular applications or an additional application
- Added in the development process
- Added into hardware or added as extra hardware
- Sent through updates from trusted vendors

A combined attack would obfuscate the malware, and make it difficult to detect. Ideally, it would be stealthy, untraceable, and immune to malware detection.

7 Discussion of Differences in Mitigation

In order to protect devices and individuals that are participating in cyber space it is important to have ways to mitigate the cyber surveillance performed by nation-states. In this section, we discuss differences between mitigation of conventional and supplier supported nation-state cyber surveillance. Some of the mitigations we presented in [80], can help as guidelines for protecting ourselves when we access cyber space. The mitigations are not comprehensive as it would require additional research to identify, test, and verify that all of them would be effective.

Due to the debate around the Snowden documents, some of the mitigations have already been discussed by experts in the information security field, e.g. Bruce Schneier, which has done a great job by informing the individuals on how to protect themselves against nation-state cyber surveillance [110, 101].

7.1 Without Supplier Support

Cyber surveillance performed by nation-states without help from suppliers is in most cases sufficient for performing surveillance of data in transition and at rest. However, they are limited in which that they have to deliberately infiltrate a device or get control of a centralized point of communication, in order to perform their cyber surveillance. Mitigations covering nation-state surveillance performed without supplier support are presented here:

- Regularly patch your operating system and applications.
- Keep anti-virus definitions up-to-date.
- Learn how to protect yourself against social engineering.
- Read the terms and conditions before you decide whether to accept or deny a service from a supplier. EFF's analyses of privacy policies can help you to make a decision [96].
- Use strong encryption standards that are open-source [110].
 - Use of HTTPS, TLS and VPN-standards can provide more protection against centralized nation-state surveillance in cyber space.
 - While the OpenSSL bug (Heartbleed[36]) showed how open source encryption can contain a critical vulnerabilities, it does at least have the potential to be audited due to that its source code is publicly available, contrary to proprietary closed source code.
- Use proxy chains, e.g. Tor¹, to hide in the network[110].

¹<https://www.torproject.org/>

7.2 With Supplier Support

If we take into consideration that a supplier can help a nation-state to perform cyber surveillance, it changes the threat landscape. We are not just facing surveillance on a level of what we consider an adversary, but we now also have to defend ourselves against suppliers that we believed would protect our privacy and security. When taking supplier supported nation-state surveillance into consideration, there are additional mitigations that need to be done in order to be protected as best as possible. The mitigations we present here are supplementing the mitigations in Section 7.1, and covers nation-state cyber surveillance with support from suppliers that produce a product or provide a service:

- Be careful when choosing anti-virus provider. It could be an idea to choose providers that explicitly state that they will detect nation-state malware. More information can be found in Section 6.2.2.
- Nation-states continue their work and we can assume that there is no trusted supplier. However, we suggest that each individual should exclusively use products, i.e. software or hardware, and services from vendors that they trust.
 - The supplier will need to show that they control all steps of their supply chain, including steps before and after it leaves the hands of the supplier. However, securing the whole supply chain can be difficult as described by Thomas Friedman at Page 16.
- Be aware that certificate authorities' valid digital signatures for software and web sites can be issued to or stolen by nation-states, making the users believe that accessed the resource is benign [104].
- Use trusted, sophisticated and professional security services, including monitoring, intrusion detection and prevention, statistical analysis and sandboxing.
- The most important thing users of cyber space can do to protect themselves are:
 - Be more careful about which information that is stored and communicated on devices that are connected to Internet and telecom providers.
 - Implement separation of duty where important information is divided into smaller pieces of information, that alone does not make any sense, but together provides the full meaning.

In this section we presented suggestions for mitigation of nation-state cyber surveillance with and without supplier support. When a supplier supports the nation-state in performing cyber surveillance, we find it more difficult to protect ourselves against it, due to that the suppliers' actions decide our level of security and privacy. It might seem to be a lot of work by taking all these mitigations into consideration, but we recommend that it is done in order to be better able to mitigate the nation-states' cyber surveillance that we are facing today. For the readers who

are worried about their privacy and security: we recommend that you should be aware of the problem about nation-states performing surveillance with and without support from suppliers. However, do not let it completely change your behavior towards use of communication and resources in cyber space [80].

8 Discussion of Research Questions and Implications

In this thesis, we have investigated the options nation-states have to perform cyber surveillance, in particular looking at the role of suppliers. The massive amounts of information generated in the year after Edward Snowden leaked the documents about how the U.S. and its allies perform surveillance in cyber space has been helpful to understand how the current situation might be today. However, the amount of available material has been highly focused on describing the U.S. surveillance and how they can perform surveillance on their own citizens.

In our case, it is not really our interest to see only what the U.S. and their allies can do, but rather find out to what extent they and other nation-states in the world today, can perform surveillance of domestic and foreign targets. An unfortunate result of the debate in the recent year is that the U.S. have been focused by researchers and security personnel, which in our case has resulted in that larger parts of the thesis is biased towards how they are performing their surveillance.

Based on what we have covered in this thesis, we find the nation-states' options for cyber surveillance technically feasible. However, there exists another bias due to the uncertainty in that a lot of material are related to news articles which are based unconfirmed leaked documents, and that in some cases, statements by persons with insider-knowledge have decided to stay anonymous. It would have been much easier to say more specific how things are being done if there were some nation-state confirmed sources that could further support the results in this thesis. There is however certain patterns, that while not always into detail, indicate the options that are available for a nation-state to perform cyber surveillance. Let us have a look at the research questions.

8.1 RQ1: Which options for distribution of surveillance software are available for a nation-state?

While trying to adhere to centralized solutions for surveillance it is in some cases, e.g. when encryption is used, it is needed to perform targeted surveillance. The nation-state have options for distribution including use combinations of Man-In-The-Middle attacks, spearphishing or even physical intervention in order to install surveillance software onto their target's devices. The nation-states are constantly looking for a way to most efficiently being able to perform surveillance of as many individuals as possible because the more information they have, the better they are able to make educated decisions.

The original approach of cyber surveillance seems to be that the nation-states in the beginning wanted to control every single device used for communication by having software and hardware installed on them. This approach is not feasible in the Internet society we live in today, as it would

require every device to contain some sort of backdoor. First, it would be very difficult to make sure every device was running the surveillance software. Secondly, due to insecurity in software, adversaries or nation-states could perform lawful interception by exploiting it. The nation-state's instead looked for centralized points of communication and then used them for surveillance purposes. These centralized points exist at e.g. ISPs and telecommunication companies. Using the fact that all the information has to pass through these points it is then possible to cover every device without ever having to install surveillance software on them. The communication is what the nation-states are targeting, so it makes sense that suppliers are requested to help them to collect information.

Most of the software and hardware today is not as secure as they should have been, and the nation-states and criminals are exploiting the vulnerabilities. The exploit market is using this as an opportunity to earn money. The nation-states can buy tools to perform lawful interception from gray and black markets that sell exploits, software and services. One quite interesting detail to note is that is actually not that much difference between the state of the art malware used by criminals and the software for lawful interception provided by commercial gray-market suppliers. The most significant difference is that the latter of them are controlling who that can buy their products, in order to limit misuse and ensure ethical use. In terms of distribution, surveillance software can be difficult to distribute due to that firewalls and updated operating systems and applications provide basic security from remote exploitation.

The major approach of distribution of surveillance software seems to be exploiting the human errors through social engineering; e.g. spearphishing. As the exploits are ready and functional, it only remains to trick the target into open the file that contains the exploit. Therefore, it might not always be necessary to have supplier-supported options available for distribution, but as we get better at protecting the individuals against social engineering, the supplier-supported options are then suddenly much more crucial. New ways will then be necessary to install surveillance software on the devices, and if the supplier-supported distribution is not already utilized, it will be soon to come.

8.2 RQ2: At which part of the supply chain could software or hardware manufacturers add surveillance to their products?

In terms of the second research question, it is possible for the manufacturers to add surveillance functionality at any part of the supply chain of their control. However, the supply chain seems to be a bit longer than what the suppliers expected. They might have good control of their own part of the supply chain, but the chain can be more easily "broken" in the time before and after it is produced by the supplier. Manufacturers e.g. build their software on software provided by other entities; this makes it difficult to ensure that nothing is tampered with. Heartbleed[36], a flaw in the OpenSSL software, resulted in that many types of software and firmware that built their functionality around OpenSSL had been completely open for exploitation.

When the products enter the premises of the supplier, they might secure the processes very well because they take security seriously. Unfortunately, it could be that the products are tampered with at one of the intermediate suppliers that handle the products, before they reach the hands of the targets. We observed that the products could be intercepted later in the supply chain, after it leaves the control physical or digital control of the supplier. By intercepting and installing backdoors into the digital software or physical products after it leaves the supplier, it is possible to make sure that the products contains surveillance software. It seems reasonable to add the exploit at a later point of the supply chain as it would yield a higher chance that a specific target would receive the surveillance software. In addition, it also enables the nation-state to minimize the impact of backdoored products, which otherwise could be exploited by adversaries. Based on our observations, we can say that the nation-states can exploit the fact that it is almost impossible to protect every part of the supply chain.

8.3 RQ3: What is the result if a supplier of software or hardware is working together with a nation-state in order to perform cyber surveillance?

A result of a supplier working together with a nation-state in order to perform surveillance is that it will enhance the surveillance as the nation-state gets more and easier access to information about their targets. Every individual that does not want to be under surveillance, will have fewer ways to protect themselves, as the safeguards that we use today are not applicable anymore if the nation-state cyber surveillance is done with support from the suppliers.

Some users will not react to this at all, while others will try their best to protect themselves. Different individuals have different things to hide. Some believe that they have nothing to hide, but they might change their opinion if their whole history of communication are stored, or even exposed for blackmailing at a later time. Other individuals could lose faith in their suppliers and governments, and therefore become more aware and selective on which providers they will use. Some users might start to use paid services that focuses on security and privacy, and will be alternatives to the suppliers of e.g. search engines, social media, and application software, etc. Most of the users however, will probably keep using free services, as they do not think that their user information is worth that much. The desired amount of privacy and security will depend on whether it is a company or an individual that is buying the products, as they have different requirements.

We already find it difficult to protect ourselves from threats from adversaries outside the supply chain, and now if suppliers were to help with cyber surveillance, it would undermine the last security we get by trusting the supplier in that their products are safe. The supply chain can be compromised, leaving security measures unusable in protection against nation-state cyber surveillance. Most security measures will in the best-case scenario only be effective against criminals.

One of the more interesting supplier-related supports could come from anti-virus suppliers. In the beginning, these suppliers were not agreeing when they were asked if they should or should not detect surveillance software from governments. Now, some of them already have made their public decision to detect all of them, but it still leaves a problem in which that they need to choose between protecting the users of their products, or support the government in their cyber surveillance. We note that the issue boils down to the issue of conflict in legislation that aims toward both increased surveillance and at the same time increasing the privacy of every individual[103].

It seems to be difficult for suppliers, as the choices they make will affect either their customers or the nation-states. If the suppliers support nation-state cyber surveillance, it could lead to a loss of customers; due to that information is disclosed about their participation in nation-state cyber surveillance. This could damage the supplier's reputation, and the loss of customers can negatively affect their revenue. What we have observed is that some of the companies that were affected by the leaked documents from Edward Snowden, have tried to rebuild their reputation by updating their policies or ask for reforms [111, 112, 113].

A supplier working together with a nation-state in order to perform cyber surveillance will result in that the nation-state will be better able to perform surveillance in cyber space. This could lead to that domestic and foreign customers, suppliers and nation-states change their behavior because they cannot anymore trust the systems they use.

The nation-states will probably perform their cyber surveillance as normal, while finding new and efficient ways to collect, process and store information in order to pursue their goals.

8.4 RQ4: How can we protect ourselves against cyber surveillance which is a result from a nation-state that has support from suppliers?

What we really wanted to find out is what we can do to defend ourselves against the threats that are imposed by a supplier that helps the nation-state to perform surveillance in cyber space through installation of surveillance software and monitoring of Internet and telecom communications. First of all, it will be very difficult and there is actually not that many options except being careful about what you share on the Internet. There are some areas we can be better at like using open encryption standards, carefully choose what information we share in cyber space, and which suppliers we share it with.

Some nation-states want to protect against surveillance from other nation-states, and has looked at ways to better protect their networks. After the documents from Edward Snowden became public, Germany was looking into how they could separate their Internet[114]. There have been examples of attempts in shortening the supply chain by producing certified secure routers in-house in Germany, in which the company produce hardware and software in-house[115]. If other nation-states follow this principle, we might see a move towards a nationalization of the Internet, where products and services become nation-state specific. We believe that nationalization of

products and services is not the way to solve the problem of nation-state cyber surveillance, due to that it will affect trade relations and trust among nation-states.

We provided suggestions for how to mitigate nation-state cyber surveillance with and without supplier support. While the mitigations were intended for innocent individuals that want to connect to cyber space without compromising their privacy, we do not know what the results will be if criminals or terrorists use the same mitigations for malicious purposes.

As we get better to protect ourselves against the threats imposed by attackers in the form of nation-states and criminals, e.g. by using secure and open encryption standards, it will result in that they need to find new ways to collect information about us. One thing is true; just because we get better to protect our communication and devices, there is no way that the attackers will just stop.

8.5 Final Thoughts

During the research we have seen some changes in how we perceive the cyber society we take a part in today. The extensive use of cyber space has made us dependent on the suppliers of software, hardware and services. This makes us vulnerable, as we have to trust that not only that the suppliers of communication and products protect us as best as they can from criminals, but that we need them to protect us against nation-states as well.

The conventional threat landscape for nation-state cyber surveillance changes when suppliers through different motivations decide to support the nation-state's in their work. In some nation-states, this trust has been broken or never existed in the first place. As we see it, we are left with the choice of trusting the suppliers in that they wish us all the best, and are not subverting our security and privacy. It is then up to the suppliers that we rely on, to decide if they will choose one of the sides, or decide to stay neutral.

Most nation-states already have the capabilities and motives to perform cyber surveillance, and the suppliers give them further options to achieve their goals in doing that.

9 Future Work

During the research have collected a lot of data and observed how cyber surveillance by nation-states are performed. There is however, not enough data to support the findings in order for it to be applicable for all nation-states. It would be necessary to acquire more information from other sources, and to focus more broadly on all nation-states, in order to get a better view on the real situation for supplier-supported surveillance in today's society. The following sections suggest further research that complement and support this thesis.

Additional Sources

While the U.S. whistleblowers have resulted in that a lot of information is available about the U.S. and their allies, it is still a need for more information to support the findings that show how surveillance could be performed by other nation-states. The need for additional sources is especially with scientific sources in mind as many of the findings are based on news articles and unofficial information. With more scientifically approved information to support the current findings, it would be possible to make better conclusions about the ways cyber surveillance is performed by nation-states.

Investigate Supplier Supported Operations

There is little information on which companies that are supporting nation-states in terms of surveillance. One of the reasons can be that the involved parties are keeping quiet about it, as it would be newspaper headlines if someone were to find out how they subvert the suppliers' trust in order to allow the nation-state to perform surveillance. Areas that would be interesting to know more about are for example:

- Analysis of update mechanisms to see if a vendor could use unique serial numbers for each client to distribute surveillance software to selected targets. Examples are Microsoft Windows Update, Adobe Flash Update, Apple updates, anti-virus updates, etc.
- Further investigate which suppliers that are most likely to assist nation-states in cyber surveillance.

Investigate Cyber Surveillance Options for Every Nation-state

It would be interesting to investigate what each nation-state in the world is able to do in terms of cyber surveillance. This would also most likely give indications on their cyber offense capabilities as well. In addition, it would be interesting to see what the collected information is used for in terms of anti-terrorism, economical gain, political reasons and so on. To systematically investi-

gate every nation-state's cyber surveillance will be time consuming, but it should be feasible to do by interested researchers.

Adapt Risk Frameworks for Cyber Surveillance

In the same way that risk frameworks support the identification, evaluation and mitigation of conventional risks, it would now be necessary to have descriptions and mitigations for risks that are introduced by the nation-states. Guidelines should also be developed in order to address trust relationships and risk, or suppliers that provide products and services to the customer.

10 Conclusion

Many nation-states have many options for performing surveillance in cyber space today. While they are able to perform cyber surveillance by themselves, help from suppliers of products and services can contribute by enabling the nation-states to more easily perform the cyber surveillance. Some nation-states have support from suppliers, and the reasons that the suppliers decide to do so can be many.

There are differences in the amount and quality of information about nation-states and how they are performing cyber surveillance. Therefore, our report does only indicate what is currently being done, but it is not enough to conclude whether all our results are true. It is however, possible to say that it is happening, as there are common methods used by multiple nation-states.

Nation-states have made earlier attempts to perform surveillance of every communication device by having hardware or software installed onto it. We observed that this method was not feasible, so instead of chasing after every person of interest the nation-state would instead take control of a central point of communication or logistics that is vital, e.g. ISPs, telecom, or postal services, etc., and use it for monitoring of communication. This enables the nation-state to more easily cover as many users and devices as possible. Unfortunately for nation-states, centralized cyber surveillance does not always work due to encryption, which makes the cyber surveillance more difficult. In order to bypass encryption, the nation-states would need either perform cryptanalysis, or turn to targeted cyber surveillance by distributing surveillance software to their targets. Surveillance software enables the nation-states to collect the data before it leaves the device. By using software and exploits from publicly available sources, commercial companies or illegal sources, the nation-state can get the tools they need to perform targeted surveillance. These tools are exploiting vulnerabilities that reside in the devices we use. Distribution aims to mimic and exploit popular software in order to have a higher chance to succeed. The more popular the product or service is, the more it will be targeted. The nation-state can also distribute surveillance software by using help from suppliers and exploits.

With a supplier supporting a nation-state in cyber-surveillance, it helps the nation-state to be better able to perform their cyber surveillance. The nation-state can then exploit that we trust our suppliers, while we become exposed to their cyber surveillance. Each of the involved parts: users, suppliers and nation-states have their own way to react when they learn about a nation-state's cyber surveillance. Users might change their behavior; e.g. stop using services, while others keep using them even though they know that they are monitored. Suppliers might lose customers and revenue, which the suppliers react to by attempting to regain their trust through increased transparency and promises that their products are secure. Nation-states will probably look for new ways to perform their cyber surveillance through use of suppliers. We can conclude that

if supplier supports nation-state cyber surveillance it changes the threat landscape, resulting in that we need to find new ways to assure that our communication and devices are secure.

A supplier can add surveillance software to their products at most parts of the supply chain that is under their control. However, a nation-state does not necessarily need the products to be compromised in the supply chain of the manufacturer, as backdoors can be inserted before and after the supply chain in control of the supplier. Tampering with products before they arrive at the target's destination can be performed in the physical world as well as in the digital one. The amount of motivation for a supplier to help a nation-state varies a lot, and it seems not to be a consensus as the different suppliers have different motives and relationships to their nation-state.

There are different approaches on how we can mitigate nation-state cyber surveillance. Encryption is currently the most effective way to better secure against cyber surveillance, but it is also advised to be careful about which information the users of cyber space are sharing, and whom they share it with. This is because some nation-states have ways to subvert the security measures we rely on. From a supplier's perspective, increased control of the supply chain is something that would help. While an extension of control in the supply-chain could be more work, it could be more secure. Users might change their behavior and share less information. As we improve our use of encryption and find ways to circumvent the cyber surveillance that is being performed today, the nation-states will look for new ways and might turn to the suppliers for help. If suppliers help nation-states to perform their surveillance in cyber space, it will be very few ways to protect ourselves against surveillance as e.g. digital signatures no longer can be trusted. Therefore, we cannot do anything else than to trust the suppliers in that they do not sell us out.

Bibliography

- [1] Florian, C. February 2014. Report: Most vulnerable operating systems and applications in 2013. online. <http://www.gfi.com/blog/report-most-vulnerable-operating-systems-and-applications-in-2013/> [Accessed 24-April-2014].
- [2] Bundesamt für Sicherheit in der Informationstechnik. 2003. Gsm-mobilfunk: Gefährdungen und sicherheitsmaßnahmen. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/cae/servlet/contentblob/475756/publicationFile/30778/gsm_pdf.pdf [Accessed 18-December-2013].
- [3] Hacking Team. November 2011. Remote control system v5.1. online. http://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf [Accessed 18-March-2014].
- [4] American Civil Liberties Union. January 2006. Eavesdropping 101: What can the nsa do? <https://www.aclu.org/national-security/eavesdropping-101-what-can-nsa-do> [Accessed 2-May-2014].
- [5] The Guardian. July 2013. Xkeyscore presentation from 2008 – read in full. <http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation> [Accessed 8-May-2014].
- [6] Hacking Team. February 2012. Remote control system. online. <http://www.hackingteam.it/images/stories/RCS2012.pdf>) [Accessed 18-March-2014].
- [7] Marczak, B., Guarnieri, C., Marquis-Boire, M., & Scott-Railton, J. February 2014. Hacking team and the targeting of ethiopian journalists. online. <https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/> [Accessed 18-March-2014].
- [8] Marczak, B., Guarnieri, C., Marquis-Boire, M., & Scott-Railton, J. February 2014. Mapping hacking teams’ “Untraceable” spyware. online. <https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/> [Accessed 18-March-2014].
- [9] Leedy, P. 2012. *Practical research : planning and design*. Pearson Education, Upper Saddle River, N.J. Harlow, ISBN:9780132899505.
- [10] Tremblay, M. 2010. Cyber-surveillance. Encyclopedic Dictionary of Public Administration. http://www.dictionnaire.enap.ca/Dictionnaire/63/Index_by_word.enap?by=word&id=21 [Accessed 22-April-2014].

- [11] Hosein, G. & Palow, C. W. 2013. Modern safeguards for modern surveillance: An analysis of innovations in communications surveillance techniques. *OHIO STATE LAW JOURNAL*, 74, 6. <http://moritzlaw.osu.edu/students/groups/oslj/files/2013/12/13-Hosein-Palow.pdf> [Accessed 22-April-2014].
- [12] Lee, N. 2013. The afterlife of total information awareness. In *Counterterrorism and Cybersecurity*, 51–62. Springer New York. http://dx.doi.org/10.1007/978-1-4614-7205-6_4.
- [13] Hypponen, M. 2013. The cyber arms race. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, CCS '13*, 941–942. <http://doi.acm.org/10.1145/2508859.2516756>, ISBN: 978-1-4503-2477-9.
- [14] Department of Homeland Security. September 2007. Homeland security act of 2002. online. http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf [Accessed 14-December-2013].
- [15] Electronic Frontier Foundation. 2014. What is the nsa domestic spying program? online. <https://www.eff.org/nsa-spying/faq#1> [Accessed 15-April-2014].
- [16] Harding, L. February 2014. How edward snowden went from loyal nsa contractor to whistleblower. online. <http://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract> [Accessed 15-April-2014].
- [17] ACLU. March 2014. Edward snowden and aclu at sxsw. SXSW. <https://www.youtube.com/watch?v=UIhS9aB-qgU> [Accessed 11-March-2014].
- [18] The Guardian. December 2013. The long arm of us law: what next for edward snowden? online. <http://www.theguardian.com/world/2013/dec/02/edward-snowden-nsa-whistleblower-us-law> [Accessed 22-April-2014].
- [19] April 2014. List of government mass surveillance projects. online. https://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects [Accessed 16-April-2014].
- [20] Jones, A., Kovacich, G. L., & Luzwick, P. G. 6 2002. Global information warfare: How businesses, governments, and others achieve objectives and attain competitive advantages. <http://amazon.com/o/ASIN/B001PKT4ME/>.
- [21] II, W. H. Mars 2013. Red dragon rising. NSM security conference 2013. https://www.nsm.stat.no/Documents/Kurs%20&%20konferanser/Sikkerhetskonferansen2013/Hagestad_%20RedDragonRising2.zip Zip contains one PDF [Accessed 19-March-2013].
- [22] Electronic Frontier Foundation. 2014. European union. online. <https://www.eff.org/issues/mandatory-data-retention/eu> [Accessed 16-April-2014].

- [23] Gregory, M. A. & Glance, D. 2013. Cyber crime, cyber security and cyber warfare. In *Security and the Networked Society*, 51–95. Springer International Publishing. http://dx.doi.org/10.1007/978-3-319-02390-8_3.
- [24] Xynou, M. December 2013. India's surveillance state. online. http://events.ccc.de/congress/2013/Fahrplan/system/attachments/2291/original/30c3_powerpoint_presentation.odp [Accessed 27-March-2014].
- [25] Soldatov, A. & Borogan, I. 2013. Russia's surveillance state. *World Policy Journal*, 30(3), 23–30. <http://wpj.sagepub.com/content/30/3/23.short>.
- [26] The Guardian. 2014. The nsa files. online. <http://www.theguardian.com/world/the-nsa-files> [Accessed 22-April-2014].
- [27] Washington Post. 2014. Nsa secrets. online. <http://www.washingtonpost.com/nsa-secrets/> [Accessed 22-April-2014].
- [28] Schneier, B. February 2014. Nsa surveillance: What we know, and what to do about it. RSA Conference 2014. <http://www.rsaconference.com/events/us14/agenda/sessions/1143/nsa-surveillance-what-we-know-and-what-to-do-about> [Accessed 22-April-2014].
- [29] Schneier, B. February 2014. Nsa surveillance and what to do about it. MIT. <http://bigdata.csail.mit.edu/node/154> [Accessed 20-February-2014].
- [30] Schneier, B. April 2014. Schneier on security. online. <https://www.schneier.com/> [Accessed 22-April-2014].
- [31] Gesellschaft für Informatik. September 2013. FAQ-Liste zu sicherheit und unsicherheit im internet. Gesellschaft für Informatik (GI). <http://www.gi.de/fileadmin/redaktion/Download/GI-FAQ-Ausspaehung2013-V1.0.pdf> [Accessed online 14-December-2013].
- [32] Microsoft. 2014. Definition of a security vulnerability. online. <http://technet.microsoft.com/en-us/library/cc751383.aspx> [Accessed 16-April-2014].
- [33] National Institute of Standards and Technology. April 2014. Search cve and cce vulnerability database. online. <https://web.nvd.nist.gov/view/vuln/search> [Accessed 16-April-2014].
- [34] Whitman, M. E. & Mattord, H. J. 2007. *Principles of Information Security*. Course Technology Press, Boston, MA, United States, 3rd edition, ISBN: 1423901770.
- [35] CVE Details. 2013. Google android: List of security vulnerabilities. online. http://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/year-2013/Google-Android.html [Accessed 24-April-2014].
- [36] Codenomicon. April 2014. The heartbleed bug. online. <http://heartbleed.com/> [Accessed 24-April-2014].

- [37] Schneier, B. April 2014. Heartbleed. online. <https://www.schneier.com/blog/archives/2014/04/heartbleed.html> [Accessed 24-April-2014].
- [38] Skorobogatov, S. & Woods, C. 2012. Breakthrough silicon scanning discovers backdoor in military chip. In *Cryptographic Hardware and Embedded Systems – CHES 2012*, Prouff, E. & Schaumont, P., eds, volume 7428 of *Lecture Notes in Computer Science*, 23–40. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-642-33027-8_2.
- [39] Wojtczuk, R. & Tereshkin, A. 2010. Attacking intel® bios. *Invisible Things Lab*. <http://www.blackhat.com/presentations/bh-usa-09/WOJTCZUK/BHUSA09-Wojtczuk-AtkIntelBios-SLIDES.pdf> [Accessed 15-January-2014].
- [40] Tereshkin, A. & Wojtczuk, R. 2009. Introducing ring -3 rootkits. *Black Hat USA*. <http://www.blackhat.com/presentations/bh-usa-09/TERESHKIN/BHUSA09-Tereshkin-Ring3Rootkit-SLIDES.pdf>.
- [41] Brossard, J. 2012. Hardware backdooring is practical. *BlackHat, Las Vegas, USA*. https://media.blackhat.com/bh-us-12/Briefings/Brossard/BH_US_12_Brossard_Backdoor_Hacking_Slides.pdf [Accessed 30-March-2014].
- [42] Axelrod, C. 2011. Assuring software and hardware security and integrity throughout the supply chain. In *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*, 62–68. <http://dx.doi.org/10.1109/THS.2011.6107848>.
- [43] Microsoft. February 2013. Supply chain security. online. http://download.microsoft.com/download/B/8/2/B8282D75-433C-4B7E-B0A0-FFA413E20060/supply_chain_security.pdf [Accessed 27-Jan-2014].
- [44] Clarke, R. A. & Knake, R. April 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins e-books, reprint edition, <http://amazon.com/o/ASIN/B003F1WMAM/>.
- [45] Jack, B. 2006. Exploiting embedded systems. *Black Hat Europe*. <http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Jack.pdf> [Accessed 18-December-2013].
- [46] Rossow, C., Dietrich, C., & Bos, H. 2013. Large-scale analysis of malware downloaders. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, Flegel, U., Markatos, E., & Robertson, W., eds, volume 7591 of *Lecture Notes in Computer Science*. http://dx.doi.org/10.1007/978-3-642-37300-8_3.
- [47] Grobert, F., Sadeghi, A., & Winandy, M. 2009. Software distribution as a malware infection vector. In *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, 1–6. ISBN:978-1-4244-5647-5.
- [48] Bellissimo, A., Burgess, J., & Fu, K. 2006. Secure software updates: disappointments and new challenges. *Proceedings of USENIX Hot Topics in Security*

- (HotSec). http://www.usenix.org/event/hotsec06/tech/full_papers/bellissimo/bellissimo.pdf [Accessed 18-December-2013].
- [49] Shankarapani, M., Sulaiman, A., & Mukkamala, S. 2009. Fragmented malware through rfid and its defenses. *Journal in Computer Virology*, 5(3), 187–198. <http://dx.doi.org/10.1007/s11416-008-0106-0>.
- [50] Hong, J. January 2012. The state of phishing attacks. *Commun. ACM*, 55(1), 74–81. <http://doi.acm.org/10.1145/2063176.2063197>.
- [51] Washington Post. June 2013. Nsa slides explain the prism data-collection program. online. <http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/> [Accessed 7-April-2014].
- [52] Lewis, J. A. April 2014. Reference note on russian communications surveillance. Center For Strategic & International Studies. <http://csis.org/publication/reference-note-russian-communications-surveillance> [Accessed 30-April-2014].
- [53] Press, O. U. 2014. metadata. <http://www.oxforddictionaries.com/definition/english/metadata?q=metadata> [Accessed 28-May-2014].
- [54] The Guardian. January 2014. Nsa dishfire presentation on text message collection – key extracts. online. <http://www.theguardian.com/world/interactive/2014/jan/16/nsa-dishfire-text-messages-documents> [Accessed 17-January-2014].
- [55] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. March 2006. Directive 2006/24/ec of the european parliament and of the council. Official Journal of the European Union. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF> [Accessed 1-May-2014].
- [56] MacAskill, E., Davies, N., Hopkins, N., Borger, J., & Ball, J. June 2013. Gchq intercepted foreign politicians’ communications at g20 summits. online. <http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits> [Accessed 30-March-2014].
- [57] SPIEGEL, D. September 2013. Inside the NSA’s Secret Efforts to Hunt and Hack System Administrators. online. <http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html> [Accessed 18-March-2014].
- [58] Information Warfare Monitor. March 2009. Tracking ghostnet: Investigating a cyber espionage network. online. <http://www.f-secure.com/weblog/archives/ghostnet.pdf> [Accessed 29-April-2014].
- [59] Gallagher, R. & Maass, P. March 2014. Inside the NSA’s Secret Efforts to Hunt and Hack System Administrators. online. <https://firstlook.org/theintercept/article/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/> [Accessed 24-March-2014].

- [60] Electronic Privacy Information Center. February 2002. The clipper chip. <https://epic.org/crypto/clipper/> [Accessed 11-Mar-2014].
- [61] Hagestad II, W. T. 3 2012. *21st Century Chinese Cyberwarfare*. IT Governance, ISBN:9781849283342.
- [62] Boon, F., Derix, S., & Modderkolk, H. September 2013. Nsa infected 50,000 computer networks with malicious software. NRC Handelsblad. <http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/> [Accessed 2-May-2014].
- [63] Norddeutscher Rundfunk. January 2014. Snowden-interview: Transcript. online. http://www.ndr.de/ratgeber/netzwelt/snowden277_page-4.html [Accessed 20-February-2014].
- [64] Kullenberg, C. 2009. The social impact of it: Surveillance and resistance in present-day conflicts. *How can activists and engineers work together*, 37–40. http://fiff.de/publikationen/fiff-kommunikation/fk-2009/fiff-ko-1-2009/fiko_1_2009_kullenberg.pdf [Accessed 14-May-2014].
- [65] Ackerman, S. & Ball, J. February 2014. Uk spies on millions of yahoo! webcams, ogles sex vids - report. The Guardian. <http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo> [Accessed 19-March-2014].
- [66] Baggili, I. & Moore, J. April 2014. Viber security vulnerabilities: Do not use viber until these issues are resolved. online. <http://www.unhcfreg.com/#!/Viber-Security-Vulnerabilities-Do-not-use-Viber-until-these-issues-are-resolved/c5rt/BB4208CF-7F0A-4DE1-92A4-529425549683> [Accessed 29-April-2014].
- [67] Ragan, S. September 2013. Spy agencies in the u.s. and u.k. bypass widely used encryption protocols. CSO Online. <http://www.csoonline.com/article/739246/spy-agencies-in-the-u.s.-and-u.k.-bypass-widely-used-encryption-protocols?page=1> [Accessed 10-Feb-2014].
- [68] Bennett, D. 2012. The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations. *Information Security Journal: A Global Perspective*, 21(3), 159–168. <http://dx.doi.org/10.1080/19393555.2011.654317>.
- [69] Levy, E. July 2004. Approaching zero [attack trends]. *Security Privacy, IEEE*, 2(4), 65–66. ISSN:1540-7993.
- [70] Metasploit. May 2014. Penetration testing software. <http://www.metasploit.com/> [Accessed 6-May-2014].
- [71] Ablon, L., Libicki, M. C., & Golay, A. A. 2014. Markets for cybercrime tools and stolen data. *Research Reports*, (RR-610-JNI), 81.

- [72] Menn, J. May 2013. Special report: U.s. cyberwar strategy stokes fear of blowback. Reuters. <http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510> [Accessed 19-March-2014].
- [73] Robertson, J. & Riley, M. May 2014. U.s. contractors scale up search for heartbleed-like flaws. Bloomberg. <http://www.bloomberg.com/news/2014-05-02/us-contractors-scale-up-search-for-heartbleed-like-flaws.html> [Accessed 7-May-2014].
- [74] Grebennikov, N. March 2007. Keyloggers: How they work and how to detect them (part 1). Securelist. https://www.securelist.com/en/analysis/204791931/Keyloggers_How_they_work_and_how_to_detect_them_Part_1 [Accessed 7-May-2014].
- [75] December 2013. Nsa's ant division catalog of exploits for nearly every major software/hardware/firmware. Leaksources. <http://leaksource.info/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/> [Accessed 7-May-2014].
- [76] McCullagh, D. March 2013. Meet the 'corporate enemies of the internet' for 2013. CNET. <http://www.cnet.com/news/meet-the-corporate-enemies-of-the-internet-for-2013/> [Accessed 07-May-2014].
- [77] Group, G. 2013. Company profile. <https://www.gammagroup.com/Gammagroup.aspx> [Accessed 7-May-2014].
- [78] Hacking Team. March 2014. Customer policy - hackingteam. online. www.hackingteam.it/index.php/customer-policy [Accessed 18-March-2014].
- [79] Sood, A. K. & Enbody, R. J. 2013. Crimeware-as-a-service—a survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, 6(1), 28 – 38. <http://dx.doi.org/10.1016/j.ijcip.2013.01.002>.
- [80] Hämmerli, B. April 2014. Cyber-Überwachung: Technische Möglichkeiten und Grenzen. Swiss Academy of Engineering Sciences. Presentation created with support from Eirik Bae.
- [81] BAE Systems. March 2014. The snake campaign. online. http://info.baesystemsdetica.com/rs/baesystems/images/snake_whitepaper.pdf [Accessed 11-Mar-2014].
- [82] Kaisler, S., Armour, F., Espinosa, J., & Money, W. Jan 2013. Big data: Issues and challenges moving forward. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, 995–1004. <http://dx.doi.org/10.1109/HICSS.2013.645>.
- [83] Cross, T. 2010. Exploiting lawful intercept to wiretap the internet. *Black Hat*.

- [84] Schneier, B. February 2014. Who should store nsa surveillance data. online. https://www.schneier.com/blog/archives/2014/02/who_should_stor.html [Accessed 8-May-2014].
- [85] Goodin, D. August 2013. How might the feds have snooped on lavabit? online. <http://arstechnica.com/tech-policy/2013/08/how-might-the-feds-have-snooped-on-lavabit/> [Accessed 7-April-2014].
- [86] Poulsen, K. October 2013. Edward snowden's e-mail provider defied fbi demands to turn over crypto keys, documents show. Wired. http://www.wired.com/2013/10/lavabit_unsealed/ [Accessed 9-May-2014].
- [87] Thomson, I. February 2014. Schneier: Nsa snooping tactics will be copied by criminals in 3 to 5 years. The Register. http://www.theregister.co.uk/2014/02/26/nsa_snooping_tactics_will_be_copied_by_criminals_in_35_years/ [Accessed 26-February-2014].
- [88] Riley, M. June 2013. U.s. agencies said to swap data with thousands of firms. online. <http://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html> [Accessed 30-March-2014].
- [89] McCullagh, D. July 2013. How the u.s. forces net firms to cooperate on surveillance. online. <http://www.cnet.com/news/how-the-u-s-forces-net-firms-to-cooperate-on-surveillance/> [Accessed 08-April-2014].
- [90] Menn, J. December 2013. Exclusive: Secret contract tied nsa and security industry pioneer. Reuters. <http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220> [Accessed 9-May-2014].
- [91] Madsen, W. 2000. {NSA} chief denies massive eavesdropping, industrial espionage. *Computer Fraud & Security*, 2000(7), 13 – 14. [http://dx.doi.org/10.1016/S1361-3723\(00\)07022-6](http://dx.doi.org/10.1016/S1361-3723(00)07022-6).
- [92] Landau, S. Jan 2014. Highlights from making sense of snowden, part ii: What's significant in the nsa revelations. *Security Privacy, IEEE*, 12(1), 62–64. <http://dx.doi.org/10.1109/MSP.2013.161>, ISSN=1540-7993,.
- [93] Busch, N. E. & Givens, A. D. 2012. Public-private partnerships in homeland security: Opportunities and challenges. *The Journal of the Naval Postgraduate School Center for Homeland Defense and Security*, 24. <https://www.hsaj.org/?fullarticle=8.1.18> [Accessed 10-May-2014].
- [94] Verbeek, J. September 2013. Assisting eu citizens with reliable ict security information. Council of European Professional Informatics Societies (CEPIS). 51st CEPIS Council Meeting: Election Candidates and Meeting Documentation.

- [95] Netgear. April 2014. Privacy policy. online. <http://www.netgear.com/about/privacy-policy/> [Accessed 6-April-2014].
- [96] Foundation, E. F. May 2014. Who has your back? 2014: Protecting your data from government requests. online. <https://www.eff.org/sites/default/files/who-has-your-back-2013-report-20130513.pdf> [Accessed 16-May-2014].
- [97] Electronic Frontier Foundation. May 2014. How the nsa is transforming law enforcement. online. <https://www.eff.org/deeplinks/2014/05/how-nsa-transforming-law-enforcement> [Accessed 29-May-2014].
- [98] Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S., & Rushe, D. July 2013. Microsoft handed the nsa access to encrypted messages. online. <http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data> [Accessed 07-April-2014].
- [99] Microsoft. July 2013. Statement from microsoft about response to government demands for customer data. online. <http://www.microsoft.com/en-us/news/press/2013/jul13/07-11statement.aspx> [Accessed 07-April-2014].
- [100] Greenwald, G. May 2014. Glenn greenwald: how the nsa tampers with us-made internet routers. The Guardian. <http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden> [Accessed 16-May-2014].
- [101] Schneier, B. December 2013. How antivirus companies handle state-sponsored malware. online. https://www.schneier.com/blog/archives/2013/12/how_antivirus_c.html [Accessed 6-April-2014].
- [102] F-Secure. 2014. Policy on detecting government spy programs. online. http://www.f-secure.com/en/web/labs_global/policies [Accessed 6-April-2014].
- [103] Johnston, C. & Harley, D. 2009. Please police me. *12th Association of Anti Viru Asia Researchers International Conference*, 7. http://go.eset.com/us/resources/white-papers/Please_Police_Me.pdf [Accessed 12-May-2014].
- [104] Soghoian, C. & Stamm, S. 2012. Certified lies: Detecting and defeating government interception attacks against ssl (short paper). In *Financial Cryptography and Data Security*, Danezis, G., ed, volume 7035 of *Lecture Notes in Computer Science*, 250–259. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-642-27576-0_20.
- [105] Microsoft. 2014. Managing the digital signature or code signing keys. online. <http://msdn.microsoft.com/en-us/library/windows/hardware/ff548699%28v=vs.85%29.aspx> [Accessed 7-April-2014].
- [106] Chen, T. & Abu-Nimeh, S. April 2011. Lessons from stuxnet. *Computer*, 44(4), 91–93.

- [107] November 2011. Finfisher finflyisp - the surveillance catalog. Wall Street Journal. <http://projects.wsj.com/surveillance-catalog/documents/267850-merged-finfly-isp/> [Accessed 15-May-2014].
- [108] Rosenbach, M. November 2011. Troublesome trojans: Firm sought to install spyware via faked itunes updates. SPIEGEL ONLINE. <http://www.spiegel.de/international/germany/troublesome-trojans-firm-sought-to-install-spyware-via-faked-itunes-updates-a-799259.html> [Accessed 15-May-2014].
- [109] May 2013. Mozilla accuses finfisher makers of 'hiding' under name. BBC News. <http://www.bbc.com/news/technology-22372027> [Accessed 15-May-2014].
- [110] Schneier, B. September 2013. Nsa surveillance: A guide to staying secure. online. <http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance> [Accessed 11-March-2014].
- [111] Computer Weekly. November 2013. Us tech firms call for nsa reforms. online. <http://www.computerweekly.com/news/2240208318/US-tech-firms-call-for-NSA-reforms> [Accessed 31-May-2014].
- [112] Timberg, C. May 2014. Apple, facebook, others defy authorities, notify users of secret data demands. The Washington Post. http://www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-af-2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html [Accessed 29-May-2014].
- [113] BBC. May 2014. Cisco calls for curb on nsa surveillance efforts. online. <http://www.bbc.com/news/technology-27468794> [Accessed 31-May-2014].
- [114] Reuters. February 2014. Merkel, hollande to discuss european communication network avoiding u.s. <http://www.reuters.com/article/2014/02/15/us-germany-france-idUSBREA1E0IG20140215> [Accessed 30-May-2014].
- [115] Traber, E. & Haimerl, S. March 2014. Merkel, hollande to discuss european communication network avoiding u.s. LANCOM. http://www.lancom-systems.de/pdf/presse/PM_2014-399_E.pdf [Accessed 11-March-2014].
- [116] Golovanov, S. April 2013. Spyware. hackingteam. online. https://www.securelist.com/en/analysis/204792290/Spyware_HackingTeam [Accessed 18-March-2014].
- [117] VUPEN Security. 2014. About vupen security - company profile and industry recognition. online. <http://www.vupen.com/english/company.php> [Accessed 18-March-2014].

A Hacking Team's Surveillance Software

Citizenlab have written two analyses of the spyware developed by HackingTeam. In [7] and [7, p. 13] they described a piece of surveillance software which goes by the name of *Remote Control System (RCS)*. RCS has also been discussed in [116] before. Following section is describing relevant information from their work.

This HackingTeam describes on their website that they develop and sell surveillance technologies exclusively to governments and intelligence agencies[78]. While they stated that they control their sales and makes decisions if their customer should be able to buy it or not. It is described that Hacking Team is focusing on targets that are using encryption, as it is difficult to collecting encrypted communication after it leaves the device[3].

The RCS surveillance software can be distributed through, e.g. spear-phishing. When installed, it is stealthy and tries to avoid detection. It can infect both computers and mobile phones, and has a wide range of supported devices as shown in Figure 9.

RCS has capabilities to steal information from the target. Information that the RCS can gather is as described in HackingTeam's presentation[3] as shown in Figure 10. The software can also perform surveillance on mobile phones as depicted in Figure 11.

Key features of the RCS [7, 8]:

- Least amount of user interaction to implant.
- Support mass surveillance



Figure 9: The RCS supports a wide range of platforms. [6]

Monitoring and Logging

Remote Control System can monitor and log any action performed by means of a **personal computer**

- Web browsing
- Opened/Closed/Deleted files
- Keystrokes (any UNICODE language)
- Printed documents
- Chat, email, instant messaging
- Remote Audio Spy
- Camera snapshots
- **Skype** (VoIP) conversations
- ...

Figure 10: The RCS can gather information from personal computers. [3]

Monitoring and Logging

Remote Control System can monitor and log any action performed by means of a **smartphone**

- Call history
- Address book
- Calendar
- Email messages
- Chat/IM messages
- SMS/MMS interception
- Localization (cell signal info, GPS info)
- Remote Audio Spy
- Camera snapshots
- Voice calls interception
- ...

Figure 11: The RCS can gather information from smart phones as well. [3]

Drawbacks of the RCS [7, 8]:

- Lacks digital forensics (integrity) for evidence.

Means of replication as described by [116] it can replicate itself by [7, 8]:

- USB-drives
- Infect virtual Vmware machines
- Infect BlackBerry and Windows CE devices

Other functionality is to update itself and install additional drivers. Encryption can be used when working with files and control servers.

Phishing and spear-phishing with e-mail and social engineering in Skype are used to distribute the surveillance software. Either of these methods get a user to [7, 8]:

- A: For the RCS-surveillance software, clever attempts in concealing the .exe file was done by using long extensions, and change the icon to an Adobe pdf-appearances shown in Figure 12.
- B: Exploiting vulnerabilities in Word Documents, which then downloads the payload. The exploits that we observed were; Adobe Flash in Word document, and RTF files with DOC extension.

CitizensLab suspects that VUPEN, a French [117] has sold exploits to RCS, as the RCS ones are very similar to VUPEN's exploits. VUPEN has also sold exploits to NSA[?]. Exploits known from the RCS, are based on what CitizenLab gathered between 2013 and beginning of 2014, which also strengthens their beliefs that HackingTeam is partner with a professional exploit vendor [7]. CitizensLab suspects that 21 governments are using this software. This suspecting is based on that they found endpoints there, as shown in Figure 13.

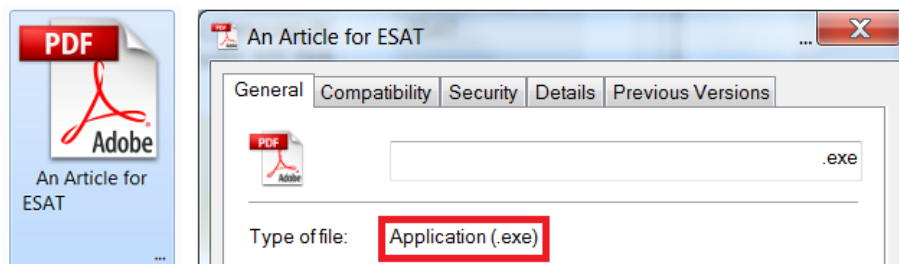


Figure 12: The RCS can be distributed through masquerading it as a benign pdf-document. [7]

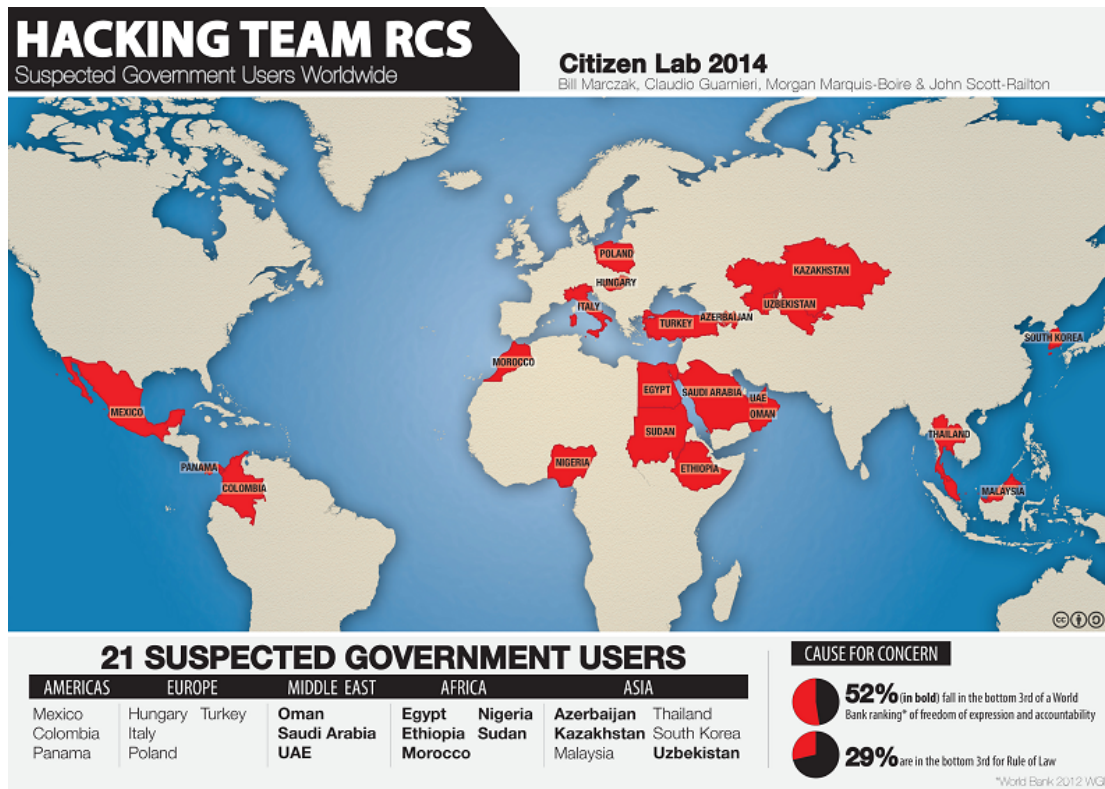


Figure 13: Citizenlab suspected that 21 governments use the RCS surveillance software. [8]

Citizenlab also found out that HackingTeam is using a “collection infrastructure” that is removing the direct link between a government and the surveillance software that gathers data. Such an infrastructure has its goal to that one should not be able to trace surveillance software back to the government that is in control of it. Proxy chains similar to Tor is used. The Hacking Team also seemed to control their own certification server, due to that they have their own valid SSL-certificate. This SSL-certificate would enable secure and “trusted” communication.

2014 Results Table

B Table from the EFF 2014 Report

	Requires a warrant for content	Tells users about government data requests	Publishes transparency reports	Publishes law enforcement guidelines	Fights for users' privacy rights in courts	Fights for users' privacy rights in Congress
Adobe	★	★	★	★	★	★
amazon.com	★	★	★	★	★	★
Apple	★	★	★	★	★	★
at&t	★	★	★	★	★	★
COMCAST	★	★	★	★	★	★
CREDO mobile	★	★	★	★	★	★
Dropbox	★	★	★	★	★	★
facebook	★	★	★	★	★	★
foursquare	★	★	★	★	★	★
Google	★	★	★	★	★	★
Internet Archive	★	★	★	★	★	★
LinkedIn	★	★	★	★	★	★
Lookout	★	★	★	★	★	★
Microsoft	★	★	★	★	★	★
myspace	★	★	★	★	★	★
Pinterest	★	★	★	★	★	★
Snapchat	★	★	★	★	★	★
Sonic.net	★	★	★	★	★	★
SPIEGEL	★	★	★	★	★	★
tumblr	★	★	★	★	★	★
Twitter	★	★	★	★	★	★
verizon	★	★	★	★	★	★
Wickr	★	★	★	★	★	★
WIKIMEDIA	★	★	★	★	★	★
WORDPRESS	★	★	★	★	★	★
YAHOO!	★	★	★	★	★	★