Master Thesis

Vault 7 and the Paradox of Democratic Society

Jan Vording
S1500201

Leiden University

Master Crisis and Security Management

Supervisors:

Prof. Dr. Bibi van den Berg

Mr. Sergei Boeke

February 2018

(Intentionally left blank)

Details of the Author

Jan Vording

S1500201

j.vording@gmail.com

Title of Research Paper

Vault 7 and the Paradox of Democratic Society

Key words

Surveillance, cyber-surveillance, information ethics, intelligence agencies, WikiLeaks

Subject / Course

Master Thesis to Master Crisis and Security Management, Leiden University

(Intentionally left blank)

Acknowledgements

Before elaborating on the content of this thesis, I would like to express an acknowledgement to everyone who has supported me in writing this final assignment. That is in the first place Prof. Dr. Bibi van den Berg, my thesis supervisor. I would also like to thank my second reader, Mr. Sergei Boeke, who introduced me into the ‘world’ of cyber space and cyber security during his lectures. Their time, advice and dedication certainly contributed to the quality of this thesis.

I also want to thank my close friends, who have been supporting me in different ways. Sometimes they just functioned as great listeners, and in other occasions they encouraged me on how to proceed.

Last but not least, I would like to thank my family, and others I have in mind, who have supported me and who had to endure some absence from my side over the last months. I really appreciate your confidence and understanding.

Table of Contents

(Intentionally left blank)

1. Introduction

Government surveillance programs have come under scrutiny after the Snowden revelations begun in 2013. The revelations of this former NSA contractor have taught us that American Intelligence Services collect (meta)data of millions of American and foreign residents, such as call history, browsing history, and sometimes even passwords. The revelations led to a stricter legal regime for NSA - in form of the ‘‘USA Freedom Act’’[1] – which marked the first time that Congress and Senate agreed on real restrictions and a real oversight mechanism for the NSA. For more targeted espionage, the U.S. Government has a different organization which is called the CIA (Central Intelligence Agency). The CIA has a different scope than NSA. It is specifically aimed at gathering foreign intelligence, and is more like a classic ‘spy’ organization, since its task is to target individuals rather than gather bulk information.

On March 7, 2017 WikiLeaks released thousands of confidential documents from the American intelligence organization CIA. The documents include and describe sophisticated methods used by the CIA to hack computers, smart phones and even (internet-connected) televisions. WikiLeaks calls the leak ‘‘Vault 7’’ and claims that it is the largest amount of confidential documents ever released by the organization. The first publication part of Vault 7 is called ‘‘Year Zero’’. It is downloadable for anyone interested, online. The first publication contains an amount of 8.761 documents. As a result of this publication, the CIA has lost control of a number of its secret hacking tools, including malware, viruses and zero day exploits.

The leaks caused a big uproar in the media and journalists from reputable newspapers started questioning whether this would be new evidence of mass surveillance by American Intelligence Agencies. This thesis will devote attention to the question: are things really as serious as the media suggested in the first instance? To answer that question, the leaked documents were analyzed to compare the content with the reports of the popular press. Another important question the revelations raise is: how did WikiLeaks obtain the documents?

1.1 Research problem and objective

The objective of this research is to investigate how surveillance techniques are being perceived and framed by the popular press and to test whether this framing is adequate, both in understanding the relevant technical details and in reflecting current views in the academic literature. The Vault 7 publications place the American Federal Government and the CIA in a

difficult situation. The espionage techniques seemingly used by the CIA pose several fundamental questions. The leaks mean that potentially sensitive Intelligence methods are now available publicly, literally for everyone by a downloadable Torrent. In a time that Intelligence Agencies have been under intense scrutiny, the world is wondering: is Vault 7 yet another example of excessive mass surveillance practices by Intelligence Agencies? This question inevitably brings us to concerns about ethics and privacy. On the one hand, Governments and experts try to make the internet safer; hackers are being criminalized and sentenced when caught. In contrast, Intelligence Agencies seem to use methods (as made publicly by WikiLeaks) that are at least very doubtful. The use of so-called zero days [1] in order to break into phones, TVs and other personal appliances has potentially very broad implications. Although Intelligence Agencies might try to keep these zero day exploits secret, they do not know whether malicious actors have also identified them. In that case, potentially millions of people are at risk of being hacked. Another risk is leaking of information by employees, something that could be the case with Vault 7. The purpose of the CIA is to aggressively spy on individuals [2], so it would not be in the interest of CIA to use these zero days to massively spy on anyone (as this is not in their mandate [3]. However, when zero days become known to the public, the privacy of potentially hundreds of millions of people can be infringed: it could be possible that other (State) actors, criminals or hackers make use of the same vulnerabilities, with potentially far-reaching consequences. An important question originating here is: is the CIA (and so the American Government by extension) morally responsible for misuse of these zero-days and information in the future? In relation to this: while states try to make the internet safer they seem to buy zero days online through grey markets. Is that a desirable situation for a western democratic state?

1.2 Research Methods

This research is an explorative case study. The methodologies used are literature research, document analysis and online ethnography. These research methods have been used in the following manner. A literature study was conducted to construct a theoretical framework and to analyze and combine necessary knowledge of surveillance and the potential implications hereof on society. Next to this, the literature study enables the reader to make the distinction between ‘targeted’ and ‘mass’ surveillance, an important theme in this study. Online

[1] Zero-days are vulnerabilities in software that are unknown to those who would be interested in mitigation of the vulnerabilities (including the software designer). Until the vulnerability is patched, hackers, and other (malicious) actors can exploit them to adversely affect computers, and (personal) data. Source: Wikipedia. URL: https://en.wikipedia.org/wiki/Zero-day_(computing)

ethnography includes analyzing and summarizing popular media reports about Vault 7, and an analysis of expert findings. This resulted in the findings as presented in chapter 4. For the document analysis part, the researcher has downloaded and analyzed the Vault 7 files for understanding and comparison with media reports. This resulted in the findings as presented in chapter 5. The time period of the research is limited to three months, since the leaks have been published on March 7 and the draft thesis had to be submitted in June. The scope and research objectives are translated in this following research question:

How are the surveillance techniques of Vault 7 perceived and framed by the popular press and is this framing adequate when compared with academic literature and the content of Vault 7?

1.3 Research Outline

The structure of this thesis will be in the following order. The second chapter will describe the conceptual background of this study. A conceptual framework will be used to describe the phenomenon of surveillance and to accentuate the academic relevance of the case study. Chapter 3 will elaborate on data studied and analyzed from the Vault 7 Torrent as released by WikiLeaks on March 7, 2017. Chapter 4 will provide the reader with an analysis and summary of media coverage, and the fallout for both CIA and politics. Chapter 5 provides an analysis of the documents of Vault 7. Finally, the outcome of the literature study, the media study and the document analysis will be discussed in chapter 6.

2. Conceptual Framework

This chapter will elaborate on the concepts used to answer the research question. Although this study has an exploratory character, the research question will be framed and tested with existing academic literature to strengthen and explain the importance of this research paper. The combination of different academic sources will (1) provide a clear picture of the concept of surveillance and (2) substantiate an analytical framework that will be used to answer the research question. Every state has a different legal framework for surveillance. This thesis will mostly leave aside these state specific regimes and, instead, focus on the generic aspects of the surveillance debate. With practical examples, surveillance activities will be categorized. This will be done in the empirical part of the thesis, chapters 4 and 5.

2.1 Surveillance

Surveillance is a phenomenon that increasingly influences our daily lives. The word itself literally means ‘to watch over’ and can as such be used in both positive and negative ways.

Surveillance has been defined and studied in different ways by various scholars. One of the authorities in surveillance studies, David Lyon (2010) argues that surveillance has to be understood as any focused attention to personal details for the purposes of influence, management or control. More specifically, Lyon argues surveillance to be the garnering of personal data for detailed analysis. (Lyon, 2003) Gary T. Marx (2002) defines modern surveillance as "the use of technical means to extract or create personal data. This may be taken from individuals or contexts". (p. 5)

Various scholars such as Lyon (2010), Morrison (2015), and Spencer (2015) argue that we nowadays live in ''surveillance societies''. Although there are a lot of other important aspects of modern society, think of globalization, international development, climate change, terrorism, to name a few, surveillance and moreover cyber surveillance are crucial characteristics.

Surveillance of specific groups is not an entirely new phenomenon in liberal societies. However, it is precisely the purpose and scale of these surveillance practices that differentiates democratic states from police states (Bigo et al., 2014). All environments, whether public space, mobile phones, cars, and computers are increasingly connected to the internet, creating information that can be searched, mined and used by others, such as states, businesses and criminals. The 9/11 attacks caused huge transformations in surveillance practices: they were a catalyst for what is called ''pre-emptive surveillance'' (Broeders & Hampshire, 2013; Mitsilegas, 2015; Lyon, 2015). Since Intelligence agencies had not been able to predict, or at least prevent terrorists from attacking New York and Washington with hijacked planes on that day, the perceived state of emergency brought the U.S. Government to a position in which it started focusing on personal - every day - data. Mitsilegas (2015) argues that the turn to pre-emptive surveillance is based on four key features. Firstly, the *purpose* of data collection is no longer solely tracing criminal activity, but targeting huge amounts of personal data to predict future criminal or divergent behavior. The second one is the *nature* of the data. Pre-emptive surveillance increasingly focuses on personal, every day generated data such as boarding passes, CCTV images, telephone calls, browsing history, and many others. The third feature is the *scope* of data collection. This collection process, which is going on every day, 24/7 resulted in mass surveillance, which is characterized by bulk collection and storage. The fourth and last feature concerns *actors* of surveillance. States increasingly work together with private parties in their surveillance programs. This can be

seen as a part of a responsabilization strategy in which states and private sector govern and fight crime together.

2.2 The Academic debate on surveillance

There are scholars who are very critical about modern surveillance. Neil Richards (2013) states that surveillance has a harmful effect on the dynamics of power between the watched and the watching party. The inequality poses a risk of people to be coerced, discriminated or put under pressure by other means. Richards introduces a framework with four key elements that create a workable approach to the concept of surveillance. His first point is that we should recognize that surveillance exceeds the public domain and is also highly concentrated in the private sector[2]. Richards states that any solution must take the complex relations between the public and private sector into account. Secondly, he argues that we must recognize that secret surveillance is illegitimate and we should prohibit the creation of any domestic surveillance programs whose existence is secret. The third point Richards makes is that we have to recognize that total surveillance is illegitimate and we should not accept the idea that it is acceptable for governments to gather and store records of all online activities without authorization. The last point Richards makes, is that surveillance is harmful. He argues that surveillance is harmful because it has the potential of reducing the exercise of civil liberties.

Another argument and one of the main arguments in the discourse of resistance to (mass) surveillance is privacy (Lyon, 1995). However, the concept of privacy is difficult to define, because it is very context dependent. One example: big internet companies such as Google, Facebook and Microsoft offer citizens around the world many free services, enabling them to communicate, to do their work or just for relaxation. However, one should not forget that companies are profit-driven: if a service is free, then the customer is their product. Germany has for that reason a very complicated relationship with Google: when the company started its Street View project in 2010, many Germans were outraged because it would infringe their privacy[4], while in other countries no questions were raised. Public actions led to the eventual withdrawal of Google's Street view project in Germany[5].

[2] Dunn Cavelty (2013) offers two explanations: the information structure we use nowadays was never built to be secure: it contains a lot of vulnerabilities. Dunn Cavelty argues that this situation continues to exist because of the network effect: the benefits of a company or product increase when the number of users also increases. She calls it a 'winner takes all' case. The second explanation is given by the argument of big data. The most powerful actors today know that there is a lot of money to be made from gathering and analyzing masses of data, giving them no incentive to encrypt this information exchange.

In the classic interpretation, privacy is the right to be left alone (Warren and Brandeis, 1890). Privacy means one has control about one's own information without being disturbed or watched by others (Boeke, 2016). It is important to know that the legal right to privacy, as defined in article 8 of the ECHR, is a qualified right and not an absolute one. This means that under certain circumstances, such as crime fighting or the interest of national security, the right to privacy has to yield to other rights or interests. The question is of course how these different rights and interests are to be balanced. Dunn Cavelty (2014) argues that an "information ethics" is required centering on human dignity, including free speech and privacy. Consequentially, it would make little sense to discuss what is technically allowed (or not); what matters is impact on, i.a., privacy. On the other hand, the status of privacy as a core value in the surveillance discussion has been criticized. Lyon (2010) states that most concepts of privacy are exposed to the risk of becoming outdated, since nowadays data is collected, retrieved, shared and analyzed between organizations in such a way that we cannot speak of privacy anymore. Privacy therefore does not seem to have the power to make an argument against contemporary surveillance. The best way to detach the singular focus on privacy, Lyon argues, is to view surveillance as a form of social sorting. This social sorting means that people are being classified into groups, which can lead to injustice and inequity. Modern information systems and complex algorithms lay at the basis of this social sorting instrument. Fears that are associated with social sorting are mainly accentuated by accountability issues: large organizations are nowadays making judgements that affect the lives of millions of citizens, based on complex processing of (big) data. Lyon also argues that state surveillance empowered by new technological developments might lead to something we know as totalitarianism. Murakami Wood (2015) draws further on that idea and predicts a complete normalization of surveillance, which would become either a part of the ''free market'' information economies, or it will end up in frameworks of rights and regulations that only ostensibly provide means of redress for surveillance excesses. He argues that the logic of security might lead towards oppressive security states, on a national scale (reconstruction of national borders) or on a global scale. He compares this to the Chinese model but adds that totalitarian practices are also seen in liberal democratic nation states.

Cyberspace and surveillance in cyberspace are new phenomena in terms of International Relations (Choucri and Goldsmith, 2012). Over the past decade, the critical infrastructure of countries has become increasingly connected to the internet, which causes concerns for cyber vulnerabilities. This vulnerability is linked to a 'cyber arms' race by states, in order to acquire

and increase their cyber power, and even more: to deter other countries by their capabilities. Czosseck (2013) states, the private industry, organized cyber criminals, hacktivists and other entities are in a competition of obtaining more cyber knowledge and cyber talents, techniques and power. That leaves states with the question to ‘‘*…either coexist or to deal with them’’*. (p. 24)

This question has, to date, not received much attention in the surveillance literature. For example, Lyon’s 2010 review of the surveillance literature basically ignores the possibility of “cyber warfare” in which states battle with other states, with hacktivists, with criminals, and with other non-state entities such as terrorists. The question is what “information ethics” (Dunn Cavelty 2014) and “greater accountability in organizations processing personal data” (Lyon 2010) may mean in such a context.

In his book ‘‘Surveillance after Snowden’’ (2015), Lyon gives critical but pragmatic input to the discussion on mass surveillance programs. He argues that societies should first of all start thinking more critically about technologies we use every day. A critical factor is the use of social media, which Lyon argues (p. 138) is not a ‘neutral’ or innocent fun activity. If ordinary citizens adopt more careful online behavior, this will contribute to a climate of change from a local level. The second point (p. 138) Lyon makes is that new practices should be shared. Those with expertise should help others understand what the use of new techniques means in terms of privacy, and democracy. Lyon argues that especially people working in the technical field should argue for strong (encryption) techniques, which can reduce unnecessary surveillance. Privacy should be an important factor in the design of products. Lyon’s third proposal (p. 138) is to focus on ‘first things’ – accountability and transparency and accountability have to be promoted in the structure of surveillance. This requires intervention in every layer of organizations that are devoted to the task of surveillance. The fourth recommendation by Lyon (p. 139) is that we have to speak ‘truth to power’. The mass surveillance revelations of Snowden show that Intelligence Agencies can potentially touch the private life of anyone. Politicians need to understand the implications hereof and need to know how to address these challenges. Therefore, Lyon argues (p. 139) that we should use different tactics. In his opinion activist and lobby groups that demand more accountability and transparency in surveillance practices play a very important role. A fifth important point Lyon makes (p. 139) is that awareness of vulnerabilities should be raised. The leaks of Snowden show that everyone can be subject to surveillance, and surveillance could harm individual groups because of mistakes and inadequacy. Especially – but not only – Muslim minorities,

which have been negatively framed by media over the years, are often prone of unwarranted surveillance. The sixth point Lyon (p. 140) makes, is that countries should make serious efforts to align law and policy, especially in the field of cyber and surveillance. While the Snowden revelations teach us that there is need for more transparency and democratic oversight of surveillance organizations, the law in most western countries is outdated and needs to be updated, both technically and ethically. The seventh point Lyon emphasizes (p. 140) is that we should press for change, but with patience. The time is now to press for change, but many of the changes that are needed take time in the sense of political process. Changes that have to be implemented at the highest level, do take a lot of time. The last point Lyon (p. 140) makes is that we should remember why the surveillance discussion is important. He argues that technical solutions such as encryption protocols and privacy trust marks are very important, but they don't appeal that much to one's imagination. Lyon points out that the broader implications, such as texting without fear to be disturbed or intercepted, and moving around without being nervous of who is tracking you and why, are important parts of human security, and we should foster that because this concept is linked with the flourishing of our human society.

Mass Surveillance versus Targeted surveillance

The Snowden revelations [6] have given an impulse to the discourse about state surveillance programs and the implications hereof for society (Bauman et al., 2014; Boeke, 2016). Companies and organizations have been responding to these surveillance programs by deploying encryption measures to safeguard their customers' data. At the moment of writing, there is no clear policy solution to transnational surveillance programs. (Van Hoboken, 2014) Such a solution requires an international agreement on the legal framework for (lawful) access to data of both individuals and organizations, ideally globally. It is therefore necessary to gain clarity about terminology, and especially the distinction between targeted surveillance and mass surveillance. Terms as 'mass surveillance' are often used by privacy advocates with respect to, for example, the Snowden revelations. (Bos-Ollerman, 2017). In the academic literature there is absence of a clear definition of 'mass surveillance', however the best way to define it is as 'bulk collection without discriminants' (Boeke, 2017; Bos-Ollerman, 2017). U.S. President Barack Obama came up with the following definition: ''*If a significant portion of the data collected is not associated with current targets, it is bulk collection; otherwise, it is targeted'.* [7] Targeted surveillance can be described as surveillance directed at particular individuals. Targeted surveillance can involve the use of specific powers by Intelligence

Agencies or other authorized public agencies, and it can be carried out overtly or covertly. It can also include the use of human agents. [8] The U.K. Regulation of Investigatory Powers Act (2000) explains that surveillance can be understood as 'targeted' if it is carried out for a specific purpose (investigation) or operation. [9]

In order to define whether the CIA Vault 7 documents resemble mass surveillance or targeted surveillance, I will use the framework that Boeke (2016) has introduced. The framework is developed to define the scope of technical communications collections programs, and consists of four variables.

Scope	National, at home	Foreigners, abroad
Level interception	Downstream	Upstream
Focus	Targeted, individual	Bulk collection
Data acquisition	Metadata	Content

Table 1: technical communications collection - the four variables (Boeke, 2016)

The first distinction Boeke (2016) makes is between domestic and abroad collection of data. He mentions the hypocrisy of national laws for intelligence agencies. Activities that are illegal when conducted on domestic ground, are allowed when carried out abroad. Boeke gives two reasons why his first point is important in the intelligence debate. The first is because most of the data intelligence agencies gather abroad is directly associated with their espionage mission, which includes gathering political, economic and military secrets. This type of espionage is generally an accepted international practice between states, and therefore hard to reduce in scope. An important second explanation Boeke gives, is that the impact of a domestic surveillance program can be more significant than collection abroad: when a state 'knows' everything about its citizens, it can easily use and abuse this knowledge to (physically) restrict freedom for certain persons, or deemed dissidents. The second variable Boeke (2016) introduces, is up- versus downstream data collection. Upstream collection means tapping cables, or intercepting satellite communications, downstream collection means that internet providers (ISPs), social media platforms or telecommunications companies are providing data because they are requested to do so by a government. In western democracies there are well-established procedures regarding privacy that ensure such an infringement of privacy is justified. It is important to note that ISPs will generally not cooperate with foreign intelligence agencies, and therefore foreign intelligence often takes place upstream, by intercepting cable or ether connections. Boeke argues that the upstream- downstream variable

is important because the ISPs are (unwilling) accomplices of the government conducting the surveillance activities. They are often forced by legal regimes to comply to the government's request, and in most cases they are prohibited by law to disclose their number of contacts (and information about the shared content) with intelligence agencies. The third variable Boeke (2016) introduces to characterize surveillance activities is the distinction between targeted and bulk collection of data. Bulk implies that data is collected without discriminants. Boeke argues that in general, upstream collection or signals collection abroad can be considered as bulk collection. The fourth variable (Boeke, 2016) is about the sort of data that is acquired: actual communications content (intercepting the actual content of a telephone call or e-mail), or metadata. The latter means data about data, such as time, and ip-adress. Metadata can betray the identity of a person. Boeke states that the use of metadata by governments and companies causes significant privacy risks, because metadata can contribute to government profiling.

3. Research Methodology

This chapter will elaborate on the methodology used to answer the research question. The first point which will be addressed is the research design. The case and the research question will

be discussed and introduced here. Secondly, the methods for data collection and analysis will be addressed. Lastly but importantly, the research validity will be discussed.

3.1 Research Design

The following research question has been derived from a study on theory, news and documentation about the Vault 7 leaks. The research question will be central to this research.

> How are the surveillance techniques of Vault 7 perceived and framed by popular press and is this framing adequate when compared with academic literature and the content of Vault 7?

Intelligence Agencies fulfil an important role in our Western Societies. Essentially, they are created to keep us safe from foreign states and non-state entities. What exactly happens inside these organizations is to a significant degree masked by secrecy, because of the nature of Intelligence work. Of course there is a legal framework applicable to ensure checks and balances. However, losing control of documents has embarrassed Intelligence agencies multiple times in history [10], such as the Watergate scandal [11], the Iraq war logs [12], and the Snowden NSA revelations [13]. Now that a huge amount of documents have been published, what exactly is their impact on society? Are Intelligence Agencies exceeding their tasks or do the revelations of WikiLeaks show us what 'normal' intelligence work looks like? The documents released by WikiLeaks could give a broader view on the position of Intelligence Agencies in our Democracies and as such could be the start of a public debate. Efforts will be made to grasp the complications that arise in intelligence work, mostly in terms of ethics.

3.1.1 Introduction of the case

This study is a single case study. There are very few comparable leaks, and Vault 7 constitutes a first big leak for the CIA. However, the phenomena discussed have been explained on the basis of the existing body of knowledge on surveillance. This strategy seems the most feasible because this is a unique case which has no similar precedent. The case was chosen because of the publication of Vault 7 by WikiLeaks during the thesis proposal writing process of the researcher, together with his general interest in intelligence agencies.

3.2 Collection of Data

In order to answer the research question, relevant data has been gathered from multiple sources. The background of the study is as follows: the theoretical part is covered by existing literature about surveillance in chapter 2. For the analysis part of the study, the CIA

documents[3] leaked by WikiLeaks will be analyzed, studied and discussed in a single chapter. Next to that, the news coverage on the Vault 7 leaks will be followed during the period March – June. The news items will be analyzed and summarized and will be discussed in a different chapter. These three 'streams' will eventually come together in a discussion about the ethical solutions for online surveillance programs.

For the collection of data, a triangulation of methods will be used in order to cast diverse viewpoints upon the topic. Mixing of data types, which is known as data triangulation, is thought to help in validating claims that could arise from a qualitative study (Denzin, 1970). The following methods will be used in the writing process of this thesis: desk research, literature study and online ethnography (studying online news sources).

3.2.1 Desk Research

To gain familiarity with the subject and relevant concepts, desk research will be deployed. The following sources will be used: Google Scholar, Leiden University Online Library, and other relevant open sources.

3.2.2. Literature study

In order to strengthen the discourse and to elucidate on important concepts, a literature study will be conducted. This will be literature on the most important theoretical concepts, as elaborated on in the conceptual framework. The literature will be derived from both Desk Research and the supervisor of this thesis.

3.2.3 Document Analysis

Since the WikiLeaks Vault 7 document collection is available through BitTorrent, the documents will be downloaded and studied for academic purposes. It will be investigated if these documents reveal anything about the scope of the CIA project or whether they show implications of mass surveillance techniques.

3.2.4 Online ethnography (media study) – How was the media study conducted?

Online ethnography is a research method which adapts ethnographic methods to study communities and cultures and combines it with the advantage of the internet [14]. It has a potential for broad application because a researcher can make use of all kinds of online communities and material. Since there is a lot of analysis, discussion and news about the

[3] The authenticity of the Vault 7 documents is unconfirmed by the CIA, nor denied. In their press release, the CIA states 'We have no comment on the authenticity of the material'.

WikiLeaks revelations to be found online, this method will enable the researcher to gather more relevant material and will help in achieving a more profound analysis.

Since the core of this research is based on a media study, it is important to explain how this study has been conducted. To prevent bias as much as possible, various International Media have been studied. Two of the most read and respected American newspapers have been chosen as a starting point: The New York Times and The Washington Post.

It is important to keep in mind that media in different countries report differently on certain issues, for example because of different regime types and media bias [15]. D'Alessio and Allen (2000) distinguish three types of bias. Firstly, coverage bias, which means actors are more or less visible in the news. Secondly a gatekeeping bias, which means that particular stories are selected or deselected, potentially on ideological grounds. Thirdly, they distinguish statement bias, which means that media coverage is 'biased' or slanted in favor of or against a certain actor. The potential media bias was a driving reason to verify and compare two of the biggest American Newspapers with a large research staff. For the same reason some European newspapers were selected, the Guardian and NRC. However, it quickly became clear that these new papers added no new insights in addition to The New York Times and The Washington Post. Therefore, the content of these newspapers will not be discussed.

After picking the media sources, it had to be decided what the search terms should be. Since the publication is called 'Vault 7', that was the first term to be chosen. The words 'CIA' and 'WikiLeaks' have been used to find relevant articles. For the latter two searches, the time frame was adjusted to 'everything after March 7, 2017' since that date marked the first publication of Vault 7. For the searches the 'Google News' search engine was used, in combination with the search engines of the media websites that were consulted.

The method of analysis is as follows. All the relevant news articles were read thoroughly. Subsequently, they have been coded. For The New York Times this has been done in the following manner: 1NYT1 (article 1), 1NYT2 (article 2), and so on. The same has been applied to the articles of the Washington Post. After the coding process, the articles have been summarized and sorted by date. The most important points that have been made in the papers, are summed up at the end of the chapter.

4. Media Coverage on Vault 7

This chapter elucidates the media coverage on the WikiLeaks Vault 7 publications, and will present an analysis thereof. The chapter is built up as follows. It will firstly describe the events that have occurred before Vault 7 was published by WikiLeaks. Secondly, it will present a timeline which enables the reader to get an overview different WikiLeaks publications between the 7th of March and the beginning of June. This timeframe has been chosen because the research scope is limited to three months. Subsequent chapters will substantiate an analysis of the publications by different International Media.

In the post 9/11 U.S. the argument of national security has been used many times to suppress media from reporting on sensitive surveillance issues. In some cases, a government pressurizes a newspaper to postpone or suspend publication of surveillance leaks. Just before the presidential elections in 2004, James Risen, an American journalist for the New York Times, came up with a report on a warrantless domestic wiretapping program [16]. Before publishing, the newspaper notified the White House about its intent to publish the story. Under strong pressure by White house officials, the publication was delayed for more than a year. A case of more indirect pressure was seen in 2010, when WikiLeaks published over 250.000 diplomatic cables. Under pressure of the Government, big financial organizations such as PayPal and Bank of America, refused transactions linked to WikiLeaks because they characterized the organization's activities as 'illegal'[17], an action that has had huge consequences for an organization that is strongly dependent on donations. Furthermore, WikiLeaks has shown over the years that it is certainly not a 'neutral' platform. WikiLeaks has been accused of being used and influenced by Russia to discredit the U.S., an example is the leaks of thousands of Clinton e-mails during the Democratic campaign for the presidency in 2016. The CIA, FBI and NSA delivered a report [18] about this alleged meddling of Russia at the early beginning of 2017, in which the director of National Intelligence unreservedly states:

''We have high confidence in these judgements...''

''...We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him''

According to this report, the influence of Moscow was embedded in a strategy that combines cyber operations with more overt efforts by the Russian government, third parties and online ‘‘trolls’’ – social media users who were paid to influence online discussions in the U.S. Although WikiLeaks pledges for more transparency, the organization has also built a name in misinformation campaigns. According to Zeynep Zufceki, a New York Times Reporter, WikiLeaks seems to have a playbook to gain maximum attention [19]. The first step is that they dump thousands of documents at once, leaving journalists with an almost unrealizable job of studying the significance in a short time. The second step is that WikiLeaks sensationalizes the publication with all kinds of sensational tweets. The news subsequently writes about the WikiLeaks story and unwittingly promotes their agenda. Zufceki states that WikiLeaks has exactly performed such a campaign in Turkey in 2016, when it shortly after the coup promised to publish thousands of e-mails of the ruling AK Party, leading to a media rush. Eventually the mailing lists did not include any interesting or harmful content [20]. The question is whether journalists have learned from these experiences.

4.1 First media reports before publication of Vault 7

On February 4, 2017. Edward Snowden [21] posted the message ‘‘What is Vault 7?’’ (see Annex 1: picture 4.1) on Twitter [22], together with the image of the Svalbard Global Seeds Vault [23]. On the same day, another WikiLeaks message was posted on Twitter [24], raising the question: ‘‘Where is Vault 7?’’ (see Annex 1: picture 4.2) showing a picture of the Merkers Saltmine [25] which had been a Nazi Gold storage in WWII. On the 6th of February, WikiLeaks posted another Tweet [26] with the question: ‘‘When is Vault 7?’’ (see Annex 1: picture 4.3), together with a photo of a turbine engine test. Just one day later, on February 7th, WikiLeaks put a new message [27] on Twitter: ‘‘Who is Vault 7?’’ (see Annex 1: picture 4.4), showing three photographs of respectively Bradley Manning, Julian Assange and Edward Snowden. On February 8 the next inscription was posted online [28], which came together with a dark image of a welding person, containing the question: ‘‘Why is Vault 7?’’ (see Annex 1: picture 4.5). And on February 9, WikiLeaks posted a photo [29] from an unrecognizable woman posting a mail, together with the message: ‘‘How did Vault 7 make its way to WikiLeaks?’’(see Annex 1: picture 4.6).

Shortly afterwards, people and media worldwide started ‘guessing’ what Vault 7 would be. Russia’s Sputnik News raised the question whether this would mean a new publication of

'Clinton emails'[4]. Apart from this, the mainstream media did not give particular attention to the tweets of WikiLeaks. Speculations and discussions mostly took place on online communities such as Reddit[5].

Some of the speculations were [30]:

1. A new publication on Clinton e-mails. By the first half of February, the FBI had released six parts of e-mails from Hillary Clinton's e-mail investigation [31]. The theory proposed that there were some deleted e-mails that the FBI could not release. Vault 7 would comprise these e-mails.
2. 9/11 Conspiracy theories. The third [32] tweet of WikiLeaks showed a jet engine, to be more specific a 'F119'[33] model. Theorists found that 119 backwards is '9/11'. Soon, conspiracy theories about possible gold under the former World Trade Center started to spread [34]. However, since WikiLeaks had not given any indications of an upcoming 9/11 leak, the theory seemed unlikely.
3. A leak on government spending or military projects, since the 5th tweet shows a photo from a military air force base.
4. Some discussions [35] were about a potential mass extinction event. This theory was connected to the first tweet of WikiLeaks, showing a photo of the Global Seeds Vault in Svalbard[36]. The theory proposed that Vault 7 had something to do with Climate Change.
5. Last but not least, one of the theories was the 'shadow government'[37] theory. CNBC News reported [38] in October 2016 that a new FBI publication would reveal information on a 'shadow government' which would exist of high-ranking state officials – some individuals referred to the '7th Floor Group [33].

A concluding remark here could be that no one really knew what was coming. The mainstream media did not have enough information to publish any valuable news on the coming publications, but the tweets did ignite some conspiracy theorists to discuss about what Vault 7 could be.

[4] Referring to the publication of thousands of private e-mails of Secretary Hillary Clinton by WikiLeaks during her Presidential campaign of 2016. See also https://en.wikipedia.org/wiki/Hillary_Clinton_email_controversy
[5] Reddit (www.reddit.com) is an American Social News Website. It is a platform for (not only nor limited to) political discussions, technological discussions, humor, entertainment and education.

4.2 Timeline of the leaks

WikiLeaks published Vault 7 on the March 7, 2017. It became immediately clear that the publications where leaks of confidential CIA documents. Soon afterwards, WikiLeaks started publishing more material. Since the scope of the research is limited by a timeframe of three months, the material between March 7 and the beginning of June has been analyzed, as can be seen in Annex 1 figure 4.7. Any material released after the beginning of June will not be discussed because of practical (timeframe of the research) considerations. Please note that the leaks all belong to the initial 'Vault 7' Year Zero leak. The leaks following the first one discuss separate 'chapters' which are not yet revealed in the first publication. They are all codenamed: the codenames often refer to specific hacking tools included. As the timeframe (Annex 1 picture 4.7) shows, 11 publications will be discussed in this thesis.

4.3 Statement of WikiLeaks at the publication of Vault 7

To get a good understanding of the media coverage and the discussion around the WikiLeaks publications, the choice has been made to summarize the WikiLeaks statements and compare them with the publications of the media. The first statement[40] of WikiLeaks was issued on March 7, 2017. It declared that WikiLeaks had begun a new series of leaks on the CIA, codenamed 'Vault 7'. The first part, 'Year Zero' would comprise thousands of documents and files from a highly-secured CIA network. According to WikiLeaks, the documents have been circulating among hackers for a certain amount of time. WikiLeaks furthermore states that the CIA herewith loses control of millions of lines of code, and zero-days. WikiLeaks states that the CIA has made software to infiltrate in Apple, Windows and Android including Samsung Smart TV's, '*which are turned into covert microphones'*[41]. WikiLeaks highlights that the CIA has become an organization with a 'substantial' fleet of hackers over the last years, an amount of 'over 5000 registered users'[1] and claims that the CIA had produced more than a thousand hacking systems, and 'weaponized' malware, and states that the scale of the operations has led to more produced code by the CIA than that Facebook uses. The Whistleblowers organization also claims that the CIA has made its own 'NSA' with less accountability. WikiLeaks states that 'its source' has stated that there is an urgent need to discuss these publications and policy issues in public, including the question whether the Intelligence Agency exceeds its mandated powers. The importance of secrecy of these 'cyber weapons' is highlighted by WikiLeaks: once a single weapon is loose, other actors such as rival states, cyber mafia and alike might use them. WikiLeaks points out that it edited the documents quite heavily: names of authors were erased, and it tried to avoid distribution of

‘armed’ cyber weapons until ‘consensus emerges on the technical and political nature of the CIA’s program and how such weapons should be analyzed, disarmed and published[2]’. Finally, the organization makes clear that it has also edited ‘tens of thousands’ of CIA targets and hacking machines throughout Europe, Latin America and even the U.S.

4.3.1.2 A misleading twitter Message of WikiLeaks on March 7, 2017

Along with the press release, WikiLeaks posted a Tweet[42] online which caused some confusion and controversy during the first hours after the publication of Year Zero. WikiLeaks stated that CIA ‘‘can effectively bypass Signal + Telegram + WhatsApp’’ (Annex 1: figure 4.8) and seemingly implied that encryption could be bypassed. This led to a lot of rumor online, but newspapers and experts soon found out that this claim was unfair. According to Nicholas Weaver, who is a Computer Security Researcher at the International Computer Science Institute in California the discussion is not about defeating encryption, despite the hype.[43] Weaver underlines that if you compromise a target’s phone, you do not have to care about encryption anymore. In fact, the encryption had not been broken but the CIA effectively managed to break into specific targeted smart phones, enabling the organization to read what the ‘suspect’ is typing.

4.4. Media coverage on Vault 7

International media reported extensively on and around the day of the release of Vault 7 ‘Year Zero’, the first publication of alleged CIA Documents by WikiLeaks. The individual articles that were used are included in Annex 2. In text, they are referenced to as follows. For the New York Times the reference is (1NYT’X’) with ‘X’ being filled in with the number of the article (1,2,3 and so on). For the Washington Post, the same applies with (1WP’X’).

4.4.1 The New York Times

On March 7, 2017 the New York Times (1NYT1) headline was: ‘‘*WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents’’.* The newspaper opened its item with the following statement:

‘‘In what appears to be the largest leak of C.I.A documents in history, WikiLeaks released on Tuesday thousands of pages describing sophisticated software tools and techniques used by the agency to break into smartphones, computers and even Internet-connected televisions.’’

The writers of the article furthermore state that if the documents are authentic, the release of them would be a huge blow to the CIA. A short introduction to what the documents entail is given. The newspaper reports that they contain highly sophisticated tools, used for spying on common computer tools such as documents in PDF format, Skype, and even Wi-Fi networks and commercial antivirus software. The New York Times reported that Vault 7 appears to fall in the same category [in terms of scale] as earlier big leaks of classified government information such as the diplomatic cables taken by Chelsea Manning or the Snowden leaks, which included hundreds of thousands of classified NSA documents about U.S. surveillance programs.

A short insight in the names and potential of the software tools, which seem to be often called after TV-series and alike, is given. The documents include a program called Wrecking Crew, which point out how to crash a targeted computer, while another document teaches the reader how to steal passwords using the autocomplete function in Internet Explorer. The New York Times points out that the initial release includes 7.818 web pages, together with 943 attachments: many of them have been (partly) redacted by WikiLeaks editors in order to prevent disclosing actual code for cyber weapons. Most of the documents date between 2013 and 2016. One revelation, the New York Times writes, can be especially troubling if confirmed: WikiLeaks said the CIA and its allied Intelligence Services have become able to compromise both Apple iPhone and Android smartphones, which allows Intelligence Officers to effectively bypass encryption which is used for popular messaging apps such as WhatsApp, Telegram and Signal.

Although the documents look authentic, there was no public confirmation of the authenticity of the leaked documents[6], which seem to have been produced by CIA's Center for Cyber Intelligence. The New York Times states that one government official has told them that the documents are real, and that a former Intelligence Officer had declared that he recognized some of the code names for CIA programs and hacking tools, making the leaks most likely genuine.

The New York Times interviewed Robert M. Chesney, who is a specialist in national security law at Texas University in Austin. Chesney compared the Vault 7 leak with a trove of

[6] The New York Times writes: ''*The agency appeared to be taken by surprise by the document dump on Tuesday morning. A C.I.A. spokesman, Dean Boyd, said, "We do not comment on the authenticity or content of purported intelligence documents."*

documents which was stolen from the National Security Agency in 2016 [44] by a group called Shadow Brokers, which published it online. Beau Woods, deputy director of the Cyber Starcraft Initiative at the Atlantic Council in Washington, said to the New York Times that he was not surprised by the recent publication. He argues that the CIA documents confirm in some regard the details on surveillance and intelligence abilities that technicians have been suspecting for a long time. Chesney furthermore states that the people who know a lot about security and hacking were expecting the CIA to investigate the hacking capabilities that have now leaked, and if it was not the CIA, they would expect countries such as China, Iran, Russia or private actors to do so. However, Woods states that the disclosures may raise concerns in both the U.S. and abroad: since the Cyber domain has an increasing impact on human society, the disclosures and potential misuse of software vulnerabilities can have serious consequences for our safety and security.

Zero-day Exploits

The newspapers furthermore elaborate about Zero-Day exploits. The New York Times asked Ben Wizner, director of the American Civil Liberties Union's Speech, Privacy, and Technology project for his reaction on the revelations. He states that the trove of documents suggest that the US Government has deliberately allowed vulnerabilities in customer electronic devices to persist, making spying easier. Wizner explains that the vulnerabilities will not only be exploited by American Security Agencies, but also by hackers and (hostile) governments around the globe. Wizner finally points out that patching security holes (zero-days) immediately, is the best way to make everyone's online life more secure.

The source of the leaks

The New York Times (1NYT1) writes that WikiLeaks does not identify the source of the Vault 7 leak, but instead states that the documents have been circulating among former US Government hackers and contractors for a while, and one of them has provided WikiLeaks with parts of the archive. The newspaper highlights the statement [45] of WikiLeaks in which the anti-secrecy organization writes that their source whishes public debate about security, and especially about the creation, use, proliferation and the democratic control of cyber arms.

The New York Times (1NYT1) asked James Lewis, an expert on cyber security at the Center for Strategic and International Studies in Washington about the attribution of the leaks. He argues that it is possible that a foreign state, in his opinion most likely Russia, stole the

documents by hacking or other means and delivered them to WikiLeaks, which may (contrary to their statements in the media) not know how they were obtained. Lewis underlines that according to the American Intelligence Agencies, Russia hacked servers and other targets of the Democratic Party during the Presidential election campaign in 2016, and shared the documents (mostly e-mails of Presidential candidate Hillary Clinton [46] and her campaign chairman John Podesta [47]) with WikiLeaks. Lewis thinks that a foreign power is much more likely to be the source of the leaks than a CIA whistleblower. The New York Times finally concludes that big government leaks are nowadays easier because of the ease of downloading, storing and transferring data in just seconds, compared to the use of photocopying for earlier leaks, such as the Pentagon Papers in 1971.

Security of individual users

Although we live in a time of increasing concern about privacy and security of phone calls and text messages, the New York Times states [48] that the revelations did not suggest that the CIA has been able to actually break encryption. Furthermore, WikiLeaks had redacted names and other information which could lead to identification of CIA workforce and other individuals.

However, the New York Times (1NYT1) mentions one program, named ‘‘Weeping Angel’’ which uses Samsung Smart TVs as covert listening devices. The article explains that, according to WikiLeaks, even when it appears to be that a TV is turned off, the television is able to record conversations around it and send them to a CIA server. A note which the newspaper makes here is that already in early 2015, Samsung started to include notions in its user agreements which explained the customer *‘‘Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition’’.* This means that also commercial companies have and use capabilities to ‘surveil’ and use gathered data for their own purposes.

New types of espionage tools?

The New York Times states (1NYT1) that the WikiLeaks Vault 7 publication includes lists of software the CIA uses to create specific exploits and malware to perform hacking operations. However, they argue, many of the tools which the CIA developers use are tools used by other developers around the world as well. They call tools such as Python for coding languages,

Sublime text, which is a program to write code, and Git: a tool that improves collaboration between developers. But, according to New York Times, it also appears that the CIA relies on software which is specifically designed for spies, naming one specific tool: Ghidra. In one of the documents this tool is described as a reverse engineering environment, originally created by the NSA.

In a publication by the New York Times (1NYT2) on the same day, a New York Times reporter raises the question: '*Has encryption software changed the way the CIA behaves?*'. According to the WikiLeaks revelation – the New York Times states, CIA has been developing all kinds of tools that can 'bypass' encryption, capturing information before the encryption protocol makes it useless for the CIA operators.

On March 8, 2017, the New York Times headline was ''*CIA Scrambles to contain damage from WikiLeaks Documents''.* (1NYT3) According to the newspaper, investigators state that Russia was likely not behind the leak of Vault 7, but more probably a disaffected insider. While the FBI started research to anyone who had access to Vault 7 information - a group of hundreds of people - the CIA remained silent about the authenticity of the documents. However, the spokesman of the CIA, Ryan Trapani, did state the following:

''The disclosures equip our adversaries with tools and information to do us harm''.

Sean Spicer, the White House spokesman stated the following:

''*The release of these documents should be something that everybody is outraged about in this country''.*

Encryption and targeted surveillance

According to the New York Times (1NYT3) some important cyber security experts and hackers had expressed their doubts about how sophisticated CIA's Vault 7 tools really are. The New York Times notes that one of the documents described ways to quickly copy floppy disks, a storage device which is very out of date – in such a way that people under 30 probably have never used one. Another indication that the tools are not part of the most sensitive cyber espionage 'arms' the CIA has, is that none of the documents is classified above the level of 'secret/noforn' ('noforn' means not meant for foreigners), which is a relatively low classification according to the news editor.

With regard to encryption, experts point out that the CIA might have abilities to break into individual smartphones, but there is no evidence yet that the agency can break encryption protocols used by many popular messaging apps. The New York Times writes that instead of this, the CIA has to target individual phones, break into them and only then has the possibility to intercept calls and messages. The New York Times points out that instead of mass surveillance, the CIA programs are most likely aimed at targeted surveillance by casting a fish line at a specific target, instead of gathering data from an entire group or population. An expert interviewed by the New York Times, Dan Guido, director at a cybersecurity investment firm, agrees with this statement and tells the newspaper that there is a huge difference between wholesale surveillance and targeted surveillance. He emphasizes that the CIA is not sifting through a sea of information but is forced to look at devices one by one because of strong encryption technology.

The grey market of Zero-days

On March 8, 2017 (1NYT4) The New York Times published another article with the title ‘‘*WikiLeaks Documents point to scourge of Cyber weapons’’.* In this article, the New York Times digs into the background of the espionage program. Arguments for CIA to build and gather the Vault 7 hacking tools would be that they are needed to deal with the increasing technological sophistication of its targets. However, the New York Times writes, it is not yet clear how the CIA obtained the hacking tools. Some may have been discovered or designed by government researchers, while others may have been bought on the growing (shadow) online market for zero-days.

The online zero-day market is growing. There are multiple platforms on the Dark Web where hackers sell zero-day exploits [49]. This is emphasized by Ms. Perlroth, quoted by the New York Times (1NYT4). Perlroth states that Zerodium – which is a zero-day exploit broker that sells to governments – said it paid hackers one million dollars for an Apple exploit in October 2016. Secondly, the brokerage firm pays hackers $50.000 for an attack that could take over an individual machine, making use of the Safari or Internet Explorer browser. The firm even pays $80.000 for a similar attack via the Google Chrome browser.

On March 9th, 2017, the New York Times posted an op-ed (1NYT5) written by Zeynep Tufekci. She places some critical notes regarding the Vault 7 publications of WikiLeaks and the media reporting going along with it. Firstly, she focuses on the tweet (misleading in her

opinion) of WikiLeaks in which the organization states that the CIA has bypassed the encryption. According to Zeynep, all leading news organizations took the WikiLeaks tweets at face value. She mentions that the first news items mentioned all kinds of popular encrypted apps by name, such as WhatsApp, and Signal, and stated that they were bypassed or compromised by the CIA. However, after a closer examination, it turned out that not even one of these apps appears by name in the CIA files. Zeynep raises the question: What had gone wrong? Her analysis is clear. First, technology companies have (in the aftermath of the NSA Mass Surveillance revelations of Edward Snowden [6]) been introducing end-to-end encryption in their messaging apps, to reassure their customers that their privacy is not being compromised. Even WhatsApp, Signal and other companies behind popular apps, are not able to read what's inside an encrypted message. This posed a problem to Intelligence Agencies. And that is why they started to develop techniques to break into individual phones. Zeynep argues that via that way, the Intelligence Agencies could see the encrypted communications just like the individual user of the app would.

The second part of the discussion concerns the tendency of WikiLeaks to spread misinformation. Tufekci states that, if WikiLeaks had posted a tweet that would say something like ''*If the CIA targets your specific phone and hacks it, the agency can look into your content''* it would be much closer to reality. However: that would not generate as much media coverage. Nevertheless, it is needed to have extensive discussions about surveillance, and online espionage, Tufekci states. But, according to Tufekci, that is not what this WikiLeaks campaign has given us.

The last coverage on Vault 7 by the New York Times was on March 23, 2017 (1NYT9). The title of the article is ''*CIA Developed Tools to Spy on Mac Computers, WikiLeaks Disclosure Shows''*. This publication coincides with the second publication of WikiLeaks, called ''Dark Matter''[3]. The New York Times sums up that - according to this new WikiLeaks publication – the CIA had found ways to specifically hack iPhones, Android Smartphones, Microsoft Windows computers, Cisco routers and Samsung Smart TVs. Furthermore, the article explains how this spying software works: it infiltrates the firmware of chips inside computers. The New York Times interviewed Eric Ahlm from Gartner, a cyber-security research firm. He states that the approach of manipulating firmware, the most basic software on a computer or a phone – which is not being changed if the system gets updated or reinstalled – raises new concerns for the industry. The New York Times concludes with the fact that by means of an

agreement struck during the Obama administration, the intelligence community is supposed to share knowledge about critical security vulnerabilities with tech companies in order to fix them. This agreement is called 'Vulnerabilities Equities Process' [50]. This process was established to determine whether to withhold or disclose secret information about vulnerabilities in computer software. Disclosure helps software developers to fix important software issues, while withholding gives the Government and Intelligence Agencies the chance to use vulnerabilities for offensive purposes. Vault 7 suggests that a lot of key vulnerabilities were stockpiled and kept secret for use by the CIA.

4.4.2 The Washington Post

The Headline of the Washington Post on March 7, 2017 (1WP1) was: ''*WikiLeaks says it has obtained trove of CIA Hacking Tools''*.

The Washington Post reported that a big quantity of the CIA's hacking arsenal appears to have been leaked by WikiLeaks. It includes thousands of files revealing cyber tools that are used by the CIA to convert all kinds of consumer electronic devices into implements of espionage.

Generally speaking, the Washington Post covers the same themes as the New York Times did on the same day. The paper also concludes that the documents are probably legitimate, on the basis of experts and intelligence officials (anonymously) who suggested that they are legitimate, although there was no independent verification. The publication raises new worries about the ability of the CIA to safeguard its secrets in what is framed as an ''era of cascading leaks of classified data''. The Washington Post interviewed Nicholas Weaver, computer security researcher at Berkeley, CA, who states that at first sight the data is probably legitimate or contains legitimate documentation. This means that somebody has been able to extract data from classified CIA systems and additionally, is willing to let the world know about it. The newspaper furthermore elaborates on the information related to CIA hacking programs and malware included in the documents, like the New York Times did. Names like ''Assassin'', ''Medusa'' and ''Weeping Angel'' are mentioned, mostly programs that are used to steal data from iPhones, get control over Microsoft computers or even secretly transform Samsung Smart TVs into espionage systems, by covertly distracting voice data from microphones.

Domestic politics

In the publication of March 7, 2017 (1WP1), A former Intelligence Official points out in this Washington Post publication that any exposure of CIA tools is going to cause irreparable damage to the abilities of the US intelligence agencies to conduct their mission.

The newspaper raises the question whether this poses an early and potentially very awkward security issue for the new President Trump, who praised WikiLeaks during his campaign while he disparaged the CIA. The Washington Post points out that Donald Trump declared that he loves WikiLeaks during his campaign, more specifically at the moment he heard that a trove of documents related to Hillary Clinton, his Democratic opponent, had been posted on the website of the organization. In a statement in the Washington Post on May 16 (1WP7) President Trump's advisor on Homeland Security Tom Bossert argues that people should not point their finger at the Intelligence community, but at the hackers who are responsible for cyberattacks around the globe. According to the newspaper, recently the so-called 'WannaCry' malware infected 300.000 computers in more than 150 countries worldwide. [50] User's files have been held ransom, infected computers are completely blocked and show a message in which a ransom in bitcoins is asked. Cyber security experts have pointed out that the unknown hackers group have used a vulnerability in Microsoft software that was first discovered by the NSA. The hole was exposed when the NSA documents were leaked online. Homeland Security Advisor Tom Bossert defended the NSA, stating that this tool was not developed by the NSA to hold data ransom. Experts argue that the tools used by the hackers were stolen from the Equation group, a powerful group of hackers with ties to the NSA. The tools were sold earlier in an electronic auction by the group 'Shadow Brokers'. Salim Neino, CEO of the company Kryptos Logic in Los Angeles and interviewed by the Washington Post, says that the leaks have 'significantly' narrowed the gap between nations and individuals or cyber gangs. He argues that the ones who really want to hurt 'us' have begun to, because they are now cyber capable.

Russian influence?

Furthermore The Washington Post (1WP1) elaborates on a potential Russian influence. The editor writes that the counterintelligence investigation that now takes place at the CIA will also be likely to investigate whether Russia had a role in the theft of the agencies' documents. The paper writes that U.S. intelligence officials suspect WikiLeaks to have ties with the Russians, especially after the 2016 presidential campaign hacks on the Democratic Party

computer networks, where thousands of e-mails were stolen, files that U.S. intelligence agencies concluded were obtained by the Russians and subsequently handed over to WikiLeaks as part of the election meddling campaign by the Kremlin.

The Washington Post interviewed Cyber Security expert Jake Williams, who called the revelations *''explosive'',* since the material shows how anti-virus products are bypassed. Hackers that have been working at the NSA, stated that the CIA 'toolkit' looked comparable to NSA's. The Washington Post concludes with emphasizing that the CIA had always been seen as an agency that recruits spies, but nowadays it has seemingly taken a large role in electronic espionage. However, the focus is narrower than NSA's, which collects large amounts of data from all over the world.

Surveillance practices

On the same day, March 7, 2017, The Washington Post published another news item (1WP2), titled: ''*WikiLeaks: The CIA is using Popular TV's, smartphones and cars to spy their owners''.* The editor writes about powerful hacking capabilities and tools that potentially take surveillance into the homes and hip pockets of billions of users worldwide, showing how most of the tools people use every day can be turned to spy on their owners.

The Washington Post furthermore writes about the astonishment of many experts. Many of the technologies used by the CIA had already been discussed for years, but now many of these theoretical vulnerabilities had been used for real espionage tools. The Washington Post writes that WikiLeaks had edited the lists of its targets. In a statement WikiLeaks said it ''*included targets and machines in Latin America, Europe, and the U.S.''.* WikiLeaks also stated that the CIA undermines efforts to protect the cyber security of Americans, by developing intrusive technology and leaving tech companies uninformed about critical security flaws in their products.

The article moreover elaborates on encryption, and the strength of it. The Washington Post quotes a statement of the company Open Whisper Systems, which developed the messaging app Signal. They state that the CIA/WikiLeaks story today is about getting malware on phones and devices, not about breaking encryption, none of the exploits is in Signal, WhatsApp or other popular communication apps. One of the other points mentioned in the article is that spying is probably continuing to grow, and that also less advanced nations have been able to gain access to spying technology because of a robust and lightly regulated

industry of surveillance companies and contractors around the world. Jake Williams, a cyber expert interviewed by The Washington Post, calls the revelations explosive and argues that the zero-days which are now out in the open can be used against American interests.

The Washington Post published another article on the same day, with the title: ‘‘*New no-fault insurance claim: The CIA crashed my car’’* (1WP3). The writer repeats the most important revelations that have already passed by, such as espionage tools for Samsung TVs, and phones. After making that point, he cites a WikiLeaks claim [51] in which is stated that the CIA has notes about potential infections for vehicle control systems. The author ends the publication by stating that we should prepare for conspiracies about car crashes that have been engineered from the CIA headquarters. In another publication on the 7th of March (1WP4) Washington Post editor Ellen Nakashima elaborates on the cyber security debate in the article: ‘‘*Exposure of CIA hacking tools renews debate over Americans' cyber security vs. national security''.* Nakashima interviewed Ben Wizer, director of the American Civil Liberties Union who states that in a time of increasing hacking capabilities by governments and criminals, it is essential that US agencies do not undermine the security of our digital systems.

The Washington Post additionally explains about the ‘‘Vulnerabilities Equity Process’’, established during the Obama era, which basically calls the Intelligence community for sharing vulnerabilities for review with one another. However, according to Robert Knake, a former White House Official, it is ‘‘*not designed to disclose all vulnerabilities''*. The Electronic Privacy Information Center underwrites this in an analysis of the process, stating [52] that the process is not transparent, it is not clear what exactly triggers the process and how many vulnerabilities are handled with this process.

Michael Daniel, former cyber security advisor to President Obama, defends the practices of the CIA. He states that while the default assumption is to disclose vulnerabilities, in a ‘minority’ of cases the government will keep the flaw secret so it can be used in hacking operations. This decision has to be periodically reviewed, he states.

The editor concludes that there is no law that requires review, and it is argued that congress should pass a law that provides for such a review.

The following publication of the Washington Post (1WP5) was on the 23rd of March, 2017. Title: ‘‘*The CIA may have hacked iPhones and macs before they even got to customers, but*

probably not yours''. The author writes that WikiLeaks claims that these products might be infected by the CIA before they get delivered to the customer, but experts state that it's very unlikely that this happens on a large scale. The article points out that no matter how secure you try to have your devices, you have to understand that the firmware of the product could already been infected, even in a new device. And there is not much you can do about it.

On the 31th of March, 2017 The Washington Post (1WP6) published an article with the title: ''*WikiLeaks 'latest release of cyber tools could blow the cover on agency operations''.* It describes the WikiLeaks publication of ''Marble Framework'', the third in the series of Vault 7 publications. It describes how the CIA software evades detection of anti-virus systems. Cyber security experts expect some foreign policy issues in the near feature, because the leaks can lead to attribution of cyber operations to the CIA. The CIA responded on the third publication, stating that ''*Dictators and terrorists have no better friend in the world than Julian Assange, as theirs is the only privacy he protects''.* They did not comment on the authenticity of the material. Experts state that the costs of replacing the cyber arsenal of the CIA is going to be costly.

4.5 Summing up: the most important themes

1. The Vault 7 leak appears to be the largest leak (in terms of volume) of state secret (CIA) documents in history;
2. The documents are probably authentic, as news reporters and experts state they are most likely 'legitimate';
3. The CIA has probably been using zero-day exploits for its secret hacking programs, some of which have been potentially bought on the shadow market facilitating malware exploits;
4. End-to-end encryption is still considered safe, as the documents, and journalist and expert opinions, do not suggest that encryption has been broken. Instead, the CIA has to break into devices itself in order to spy on communications;
5. Some experts argue that the CIA hacking programs are not focused on mass surveillance, but on targeted surveillance. However, this seems somewhat underexposed in the first media reports.
6. It could be the case that WikiLeaks has ties with Russia and so these leaks could be part of the Russia – U.S. tensions, however there is no evidence that Russia has stolen the documents.

7. The CIA is able to hack many consumer products that are used on a daily basis: computers, phones, routers, anti-virus systems and even Samsung Smart TVs.
8. The leaks of CIA documents (Vault 7) renew the debate on cyber security, Intelligence Agencies and privacy.
9. Other state and non-state entities might profit from the knowledge they can gather from Vault 7 documents. This is potentially harmful to U.S. interests.
10. After the end of March, there were no more substantive articles in the media about new Vault 7 publications.
11. The cyber-attacks by hackers in May show that stockpiling zero-days by Intelligence Agencies can have a profound negative impact: if leaked, as was the case here, it empowers cyber criminals to build and exploit malicious software, affecting thousands of citizens and companies worldwide.

5. Analysis of the Vault 7 Torrent

5.1 The First trove of CIA Documents: Vault 7 'Year Zero'

After weeks of silence about Vault 7, shortly after midnight on March 7, 2017, WikiLeaks started tweeting[53] again. The tweet (Annex 1: picture 4.9) linked to a torrent file containing a file of approximately 500MB. WikiLeaks stated that the password would be made public by 9AM. It now became clear that the first publication would be called 'Year Zero'.

As stated in the next Tweet (Annex 1: picture 4.10), WikiLeaks released the password [54] which was kind of remarkable: *'SplinterItIntoAThousandPiecesAndScatterItIntoTheWinds'*

The password relates to a famous quote of 35th President of the United States, John F. Kennedy [55]. According to an official report of the New York Times[54] President Kennedy stated he wanted "to splinter the CIA in a thousand pieces and scatter it to the winds". The angriness of Kennedy towards the CIA arose from the (failed) Bay of Pigs invasion [56] in Cuba and the proposed false flag operation (known as 'Operation Northwoods [57]') which the CIA proposed to subvert the Fidel Castro regime. According to Samuel Halpern [58], who is the author of the book 'The assassination of John F. Kennedy', the President was having difficulties keeping the CIA director 'in line'. Kennedy believed that the agency was becoming a sort of 'state within a state'. His relationship with the CIA never normalized, since Kennedy was assassinated just a month after this statement.

5.1.1 Downloading and opening the Torrent

In order to download a Torrent, a BitTorrent client – such as uTorrent [59] is needed. Once installed, it is possible to download the WikiLeaks documents after clicking the link, which was given in the Tweet on March 7, 2017. As the Vault 7 torrent is downloaded on a personal computer using Microsoft Windows, it has to be opened with the so-called '7z' decrypting software[60]. The extracted folder is called 'Year Zero'. It can only be opened by entering the password as provided by WikiLeaks. When opened, it becomes clear that the 'Year0' folder contains multiple underlying folders, as to be seen in Annex pictures 5.1, 5.2, 5.3, 5.4 and 5.5. When opened, it appears that 'Year0' contains multiple folders (Annex 1 picture 5.2). The amounts of data WikiLeaks claims to have published in this 'Vault 7' leak, are inside the 'Vault 7' folder (Annex 1 picture 5.3) When the 'Vault 7' folder is opened, it becomes clear that it has two underlying folders: ''CMS'' and ''Files'' (Annex 1 picture 5.4). The ''CMS'' folder has 7.810 underlying 'links' – so-called ''user-pages'' which can be opened in a

browser. As the name clarifies, they include personal notes and meeting notes of alleged CIA employees, although they are anonymized. They also link to descriptions of malware- and hacking tools. The ‘’Files’’ folder contains a (partly incomplete) organizational flow chart of the CIA cyber operations department. Within the ‘‘CMS’’ folder there is another folder called ‘‘Files’’ (Annex 1 picture 5.5) which contains word documents, images, .ZIP-, PDF- and executable files. The files inside are dated from 2012 until 2016.

Annex 1 picture 5.6 shows a small part of the content of the ‘‘CMS\Files’’ folder. At first sight, it contains numerous documents with ‘strange’ names – related to movies, games, songs, and artists. For example, one tool is called ‘Weeping Angel’, which is a character in the Science Fiction series ‘Doctor Who’ [61]. Another tool is called ‘Maddening Whispers’ – which can be related to the online game World of Warcraft.

5.1.2 Vault 7: Year Zero – What’s inside?

Once the files were downloaded, they were first quickly scanned by the researcher. Since the ‘Vault 7’ publication, - as described earlier - contains 8.761 documents of all sorts, not all could be processed in the available time span. Apart from that, many documents are edited by WikiLeaks or are left empty – waiting for later publication by WikiLeaks. An additional but important note to be made is that the researcher is not an IT-professional, making this chapter not an in-depth analysis of the documentation, but more an overview of the most important documents. In order to get that overview, a three step approach was used, which is as follows:

1. The summary of WikiLeaks has been studied and the most important tools described by the organization have been summarized;
2. The researcher himself has studied the most important documents and gives a general explanation on what we know and what we do not know after having studied them.
3. To include field expert analysis, the blog of Bruce Schneier, a cyber security professional has been studied. An overview of his findings is presented under 5.13.

5.1.3 What’s in the Vault 7: Year Zero documents according to WikiLeaks?

At first, WikiLeaks claims [62] – on the basis of the documents - that the malware and hacking tools of the CIA are built by the Engineering Development Group (EDG), which is a software development group within the CCI (the Center for Cyber Intelligence). This Center for Cyber Intelligence belongs to the Directorate for Digital Innovation, one of the five

directorates[63] of the CIA. The EDG develops, tests and (operationally) supports Trojans[7], backdoors[8], and malware exploits[9] for covert operations worldwide. In the first publication, WikiLeaks reports about the following CIA tools, malware and methods:

a. A tool called ‘‘Weeping Angel’’

   Weeping Angel is a tool which is according to WikiLeaks developed by the CIA’s Embedded Development Branch (EBD). It infects Samsung smart TVs, and can transform them into covert microphones.

b. Infection of vehicle control systems used by modern cars

   In one of the ‘user-page’ notes, ‘‘*Vehicle systems’’*[51] is called. However, no more explanation is given in the documentation.

c. Attacks to remotely hack and control smart phones

   According to WikiLeaks, the CIA can infect popular phones (iPhones and Android), making it possible to covertly activate cameras and microphones in order to listen in.

d. WikiLeaks claims the CIA has made use of 24 ‘Zero-days’

   WikiLeaks states that ‘Year Zero’ documents show that the CIA makes use of ‘undisclosed vulnerabilities’ (zero-days) and hides these security flaws from the big software and hardware manufacturers.

e. A tool called ‘‘Hammer drill’’

   ‘‘Hammer drill’’[64] is a tool that creates fingerprints of CD/DVD usage: it collects information about how files on a CD/DVD are used an is able to collect this data on demand and send it to the CIA.

f. A tool called ‘‘Brutal Kangaroo’’

   This tool enables the CIA to hide data in images or on ‘covert’ parts of disks [65].

[7] Trojan horse, or Trojan, could be described as any malicious computer software which is used to hack into a computer system by misleading users of its true intent. See: https://en.wikipedia.org/wiki/Trojan_horse_(computing)

[8] A backdoor is an (often) secret method to bypass normal authentication a computer system, or any other connected device such as home routers. Backdoors are often used to get remote access to computers, or to obtain access to plain text in cryptographic encrypted systems. See: https://en.wikipedia.org/wiki/Backdoor_(computing)

[9] An exploit is a piece of software that makes use of vulnerabilities in order to cause unintended behavior in a computer system, such as gaining remote control or DDOS attacks. See: https://en.wikipedia.org/wiki/Exploit_(computer_security)

g. Malware called ‘‘Medusa’’ and ‘‘Assassin’’

According to WikiLeaks, these malware tools were developed by the CIA’s Automated Implant Branch (AIB) and are effectively attack systems for automated ‘‘infestation and control’’ of systems [66].

h. Multi-platform malware called ‘Hive’[67]

The malware tool ‘HIVE’ provides customizable ‘implants’ for the most common operation systems such as Windows, Linux, Mac OS X, Solaris and even software used for internet routers. The malware communicates with a Listening Post and command and control infrastructure, and connects through an HTTPS connection with the web-server of a ‘cover-domain’ – a so called ‘honeycomb’[68] server. Because the malware can emulate a valid SSL authentication, the infected computer will seem to operate normally. However, the connection with the honeycomb server gives the CIA possibilities to execute jobs on the computer of to receive secretly gathered information.

i. ‘‘Umbrage’’

The Umbrage project includes techniques to erase or alter ‘fingerprints’ left behind by CIA operations. The Remote Devices Branch (RDB) of the CIA has collected a library of attack techniques that are used by other states or (foreign) actors, including Russia. Umbrage gives the CIA the possibility to misdirect attribution by leaving different ‘fingerprints’ behind. According to the WikiLeaks analysis, Umbrage covers, among others: key loggers, password collection, anti-virus avoidance and webcam capture.

j. ‘‘Fine Dining’’

Fine dining [69] is a standardized questionnaire that CIA employees have to fill out when requesting a ‘special operation’. The Operational Support Branch (OSB) of the CIA uses these requests to decide which technical requirements are needed in order to extract information from targeted systems. The questionnaire asks the officer information such as which state or actor has to be targeted, which operation system it is about, is the system connected with the internet. It includes a list of file types which can be ‘ordered’ to hack, like audio files, text, video and so on.

5.2 The second publication: Project Dark Matter

On March 23rd WikiLeaks released the second trove of documents, under the name 'Project Dark Matter'. It contains 12 documents, mostly .pdf documents describing procedures for installing malware implants onto targeted PCs. They also include information about compatible operating systems, potential installation problems and traceability.

This CIA Project contains documentation which specifically reveals methods to infect Apple Mac firmware. Infecting firmware means that 'underlying' software is infected, so even if an operation system is re-installed the infection will persist. The documents reveal that the list of devices includes Macs and iPhones. In this second publication, WikiLeaks discusses the following tools:

a. ''Sonic screwdriver''

   The tool Sonic Screwdriver [70] is a tool which is able to execute code on peripheral devices (such as CD/DVD/USB) while an Apple notebook or desktop is booting. The infection is stored on the firmware of the Ethernet adaptor of the Apple product, which means that re-installing of the system does not undo the infection of Sonic Screwdriver.

b. ''DarkSeaSkies, DarkMatter, SeaPea and NightSkies''

   The project 'DarkSeaSkies' consists of various programs, called 'Dark Matter', 'Sea Pea', and 'NightSkies'. These tools are used to respectively infect and persist in disk drives, kernel-space[10] and user-space[11] of Apple MacBook computers. A newer version of NightSkies, version 1.2 is especially designed for Apple iPhones and is 'expressly designed to be physically installed onto factory fresh phones' according to WikiLeaks statement. [71]

c. ''Triton, Dark Mallet'' and ''DerStarke''

   Triton, Dark Mallet and DerStarke are malware tools used to infiltrate on Mac OS X[12] software.

[10] Kernel-space is the computer program that is the core of the computer system, with control over the complete system, such as MS Windows or Apple OS. See: https://en.wikipedia.org/wiki/Kernel_(operating_system)
[11] User-space is the area in software where personal applications are runt. See: https://en.wikipedia.org/wiki/User_space

5.3 The third publication: Marble Framework

On March 31st, 2017, WikiLeaks released the third part [72] of the Vault 7 revelations. now became clear that the 'modus operandi' of WikiLeaks seemed to be: a publication of documents every Friday, so just before the weekend. This third trove of documents contains a .zip file. When extracted, 6 folders will unfold: 'Farble', 'Marble', 'Marbleextension', 'Marbleextensionbuilds', Marbletester' and 'Stringobfuscation'. In total they include 676 source code files. Most of the files have '.PY', '.MK' or '.MD', '.SLN', '.CPP', or '.H' extensions, mostly programming extensions. Without this software and necessary program skills, it is not possible to gain more knowledge about the content. According to WikiLeaks, the Marble Framework is used by the CIA in order to hinder anti-virus companies and IT security investigators from attributing hacks and the affiliated tools to the CIA. The Marble Framework works in such a way that it makes text fragments disappear, making it an important part of the CIA's anti-forensic approach tools. The documents also include a 'deobfuscator'[4] which makes it possible to reverse the disappearance of information. The documents reveal that the CIA – in order to frustrate attribution - even uses multiple other languages such as Korean, Russian, Arabic and Chinese, which makes it even harder for experts to attribute the hacks to the right party.

5.4 The fourth publication: Grasshopper Framework

'Grasshopper', the fourth release of WikiLeaks within the Vault 7 series, was published on April 7th, 2017. It contains 27 documents [73]. The files are all documents in .pdf format. Most of the files are 'User guides', explaining how to install and configure tools. Some documents, such as 'Grasshopper-v2_0_2-UserGuide' contain 134 pages with information about configuration and settings. According to WikiLeaks, Grasshopper is a platform which is used to build specific – custom made - malware packages for Windows machines. Grasshopper is a highly sophisticated set of tools that is deployable in different ways. The program is used to infiltrate in Windows software and is able to send a 'pre-installation survey' of the targeted computer system to the CIA, so the CIA operator knows which additional tool is needed to gain access to that specific machine. From this publication becomes clear that the CIA also uses a persistence mechanism called 'Stolen Goods' which is partly based on already existing Russian malware. Grasshopper seems particularly good in avoiding attention from well-known anti-virus software such as Symantec, and Kaspersky, which do not detect Grasshopper.

5.5 The fifth publication: HIVE

The HIVE project [74] documentation was published by WikiLeaks on April 14th, 2017. The publication contains six .pdf documents: a 'User Guide', a 'Developers Guide', a 'Developers guide (figures)', a document called 'Hive Beacon Infrastructure', one called 'Hive Infrastructure Installation and Configuration Guide', and a document called 'Infrastructure Switchblade'. The User Guide contains information about deployment of the tool, about post-deployment (it includes a chapter about a 'Self-delete' function of the program) and it includes a troubleshooting chapter. The tool makes use of a legitimate looking HTTPS-connection[13] and makes connection with the internet through a cover domain making it able to hide its presence to the user of the affected machine. Hive makes use of command and control (C&C) servers[14], which give every target a specific IP address. According to WikiLeaks, the domains have been covered by privacy services making it impossible to identify who is behind it. The connection that is set up between the command and control server and the infected computer, is protected by a cryptographic protocol[15].

5.6 The sixth publication: Weeping Angel

On the 21th of April, 2017, WikiLeaks released a document [75] regarding CIA's Weeping Angel project. As already shortly named in the first Vault 7 publication, Weeping Angel implant (software) designed for Samsung smart televisions. The publication contains one .pdf document called 'EXTENDING_user_Guide.pdf'. The document contains 31 pages, describing key features, installation, compatibility, and furthermore how to set up a Wi-Fi hotspot, a webserver and how to exfiltrate audio. It also gives information about installing, testing, limitations and the history of the tool. The publication gives insight on how the tool works and how it has to be installed on a targeted TV. In the introduction is stated: 'The EXTENDING tool is an implant designed for Samsung F Series Smart Televisions. The implant is designed to record audio from the built-in microphone and egress or store the data'. The 'Key features' chapter elaborates on themes such as 'Live listening', 'Remote audio file retrieval' – which means that the audio can be transmitted via the Wi-Fi router to CIA. The

[13] HTTPS is a communications protocol that its considered secure and is widely used over the world wide web. See: https://en.wikipedia.org/wiki/HTTPS

[14] Command and Control servers are central computer systems issuing commands to connected computers. This is mostly called a 'botnet', in which the connected computers 'fulfil' the 'orders' given by the C&C server. See: http://whatis.techtarget.com/definition/command-and-control-server-CC-server

[15] A cryptographic protocol performs a security related function, mostly in a way that it protects information. It uses cryptographic methods to establish this. See: https://en.wikipedia.org/wiki/Cryptographic_protocol

tool furthermore has a ‘Fake off’ function, which means that when the user turns the TV off, the processor (and so the microphone) will still be running in order to record voice data.

5.7 The seventh publication: Scribbles

Documentation on the project ‘Scribbles’[76] was released by WikiLeaks on April 28th, 2017. The publication contains 4 .pdf files: a user guide (‘Scribbles v1.0 RC1 –User Guide’), the source code (‘Scribbles Source Code’), a checklist (‘Scribbles v1.0 RC1 – IVVRR Checklist’) and a review worklist (‘Scribbles v1.0RC – Readiness Review Worksheet’). Scribbles is a tool that is able to ‘watermark’ documents. The User Guide explains how to set up the tool, how to configure the watermark parameters, how to deal with errors and it includes compatibility information. The tool is able to operate on popular text writing platforms, such as Microsoft Office 2013. Every time a document (watermarked by Scribbles) is opened by anyone, it will covertly load a secret file which gathers data like user name, time and date, and IP address, and sends it to a CIA server. However, this is only possible when the affected user has an internet connection. Tools like Scribbles enable the CIA to track (potential) whistleblowers.

5.8 The eighth publication: Archimedes

On May 5th, 2017, WikiLeaks released the tool ‘Archimedes’[77]. This publication contains 9 documents, in .pdf format. There is a User Guide (‘Archimedes 1.0 User Guide’), there are 3 addendums (‘Archimedes Addendum 1.1., 1.2, and 1.3’) a manual called ‘Fulcrum Manual’, a file called Fulcrum SRS v.06, and a file called ‘Fulcrum PSP testing Results’. The User Guide explains how the CIA attacks computers within LAN[16] networks and re-directs them through an infected computer with the Archimedes malware, bringing the infected computer effectively under control of the CIA. In IT-language, this is called a man-in-the-middle attack: computer A sends a package of data to computer B, but in between is an infected computer that makes a copy of all the data. It is even possible to alter the information which A sent to B, making it possible to deploy other malware on computer ‘B’ without the user knowing it. Fulcrum is, according to the Archimedes User Guide, an older version of Archimedes. It does not include more relevant information then Archimedes provides.

[16] LAN: Local Area Network, is a (inter)connection of computers within a seperated area, such as a school, a hospital or a home

5.9 The ninth publication: After Midnight and Assassin

On May 12th, 2017 WikiLeaks published 13 documents [78] belonging to the ‘‘After Midnight’’ and ‘‘Assassin’’ project. The files are all in .pdf format, most of them are User Guides, although there is a document called ‘Training’, and a few called ‘Quicker Start’. The After Midnight User Guide contains 68 pages of information about its features. The Assassins User Guide even contains 204 pages of information. Both documents describe how the implants have to be installed and how they have to be operated. Midnight and Assassin are malware frameworks and are most likely built by the CIA. They are designed for Microsoft Windows. The tools enable CIA operators to install and execute malware on the infected computer. The malware establishes a secure HTTPS connection with a so-called ‘‘Listening Post’’ system called ‘‘Octopus’’. The infected computer subsequently communicates with the listening post at a configured time schedule, and will see whether there are updates or tasks that have to be performed.

5.10 The tenth publication: Athena

The tenth publication [79] in the Vault 7 series was called ‘Athena’ and has been published on May 19th, 2017. It contains 5 documents – a user guide, a demo pdf-file, design files and a technology overview file. The User Guide contains 49 pages of information, outlining the capabilities of Athena: the Athena system consists of a builder, a tasker, a parser, a listening post, an installer, and offline capabilities. According to the User Guide, the Athena project focusses on Microsoft Windows computers, and is compatible with almost all recent versions of the Windows platform. Chapter 3 of the User Guide explains that Athena gives the CIA operator remote control to the infected computer, enabling the operator to retrieve and deliver files to that system.

5.11 The eleventh publication: Pandemic

Published on June 1st, 2017, ‘Pandemic’ [80] is the last publication that is included in this thesis. The publication includes 5 .pdf documents: ‘Pandemic 1.1’, ‘Pandemic 1.1RC1’, ‘Pandemic 1.1RC1-IVVRR Checklist’, ‘Pandemic 1.0’, and ‘Pandemic 1.0-IVVR Checklist’. Pandemic, again, is a persistent malware implant for Microsoft Windows. It is able to communicate with remote users in the same network as the infected computer. It works in the following way: computer user A (infected with ‘Pandemic’ malware) shares a file with computer user B. Computer ‘B’ receives the files that were expected, but during transfer time they were modified and infected by the malware. The infected machine B is now capable to

spread the malware further to other computers, which is why the program was called ‘pandemic’. According to the document ‘Pandemic 1.1’, the tool does not make any physical changes to the targeted file on the disk.

5.12 Researchers’ analysis of Vault 7 file: Weeping Angel

Shortly after deciding to research the WikiLeaks Vault 7 documents, the researcher has downloaded the torrent file for scientific purposes. As shown in the introducing part of this chapter, the folder was extracted, opened and explored. One of the most important findings, that has been underexposed in the media, certainly in the first days, is about the trove of documents called ‘‘Weeping Angel’’. While the media reported that the CIA is listening in through Samsung Smart TVs, the truth is somewhat more nuanced. The user guide [81] of the tool Weeping Angel, published by WikiLeaks on the 21th of April, 2017, explains that Weeping Angel can *only* be used when someone configures the implant specifically, and then deploys it onto a TV by making use of an USB stick. The conclusion that can be drawn from this is while the Weeping Angel tool seems very sophisticated in a way that it can record sound while the TV appears to be turned ‘off’ it still has to be installed by physical means, and thus absolutely cannot be seen as a form of mass surveillance.

5.13 Experts findings on Vault 7

During this research project, the blog of internet security expert Bruce Schneier, *Schneier on security* [82] has been critically followed. Schneier is Chief Technology Officer at IBM Resilient and has been regularly blogging on security issues since 2004. Schneiers’ first blog about the Vault 7 leaks is on March 7 [83]. Schneier writes that WikiLeaks had released thousands of CIA documents. He clarifies that one of the first WikiLeaks statements, being the one in which the organization states that the CIA can effectively bypass the encryption of popular conversation apps, has to be interpreted in the following way: the CIA is able to hack individual devices, and can by that way bypass encryption. The organization is not able to break the encryption itself. Schneier furthermore states that the UMBRAGE documents are interesting, because they reveal the CIA can possibly misdirect attribution by making use of the digital ‘fingerprints’ of f.e. Russia. However, he is not convinced that the CIA actually uses this opportunity. In a second blog on March 21, Schneier writes [84] that, despite official sources telling that the U.S. Government prioritizes defense over offense and that ‘‘zero day stockpiling is the exception, not the rule’’[85], the CIA seems to be hoarding zero-day vulnerabilities. That is not only the case for the CIA, also the NSA engages in these practices

[86]. According to the Washington Post, the NSA designs most of their malware implants itself, but is also covertly purchasing zero-days from private malware vendors, mostly located in Europe. In 2013, their budget for these additional purchases was 25.1 million U.S. Dollars [87]. Schneier also writes that WikiLeaks sent e-mails to big tech companies such as Google, Apple, Microsoft and the others mentioned in the documents. However, instead of sharing vulnerabilities the organization made demands, which remain unclear until now. Schneier has confidence that Russia, China or other cyber powers are able to hack WikiLeaks, and so he proposes the idea that the CIA should inform the tech companies involved about the vulnerabilities, before criminals will be able to misuse them for their own purposes. On April 10, Schneier blogs about the fourth WikiLeaks CIA tools dump [88]. In this blog, Schneier writes that he still has absolutely no idea who leaked the documents to WikiLeaks. He argues that until now, there wasn't found anything illegal in the dump of documents. The CIA documents all seem to be hacking tools. Schneier writes that there is nothing inside the documents that reveals anything about programs or targets. Schneier makes a comparison to the Snowden leak, which included sensitive information about espionage on Americans, programs that swept up most of the communications worldwide. These were programs that showed the public the powerful capabilities of the NSA. According to Schneier, the CIA leaks do not include anything like that. They include just hacking tools, and what they demonstrate is that the CIA stockpiles and uses zero-days, contrary to the stated position of the Government [89].

5.14 Summing up: the most important take-aways from the Vault 7 documents and expert findings

1. Vault 7 constitutes of thousands of documents, and with publications almost every week the end of leaking state secrets information is not nearby.
2. The WikiLeaks revelations give an insight in the hacking arsenal of the CIA. However, names, targets and even a lot of source code have been edited.
3. Because of the Snowden NSA revelations, providers of popular messaging apps have started applying end-to-end encryption. The encryption itself has proven to be secure, therefore the CIA has been developing techniques to break into individual phones in order to read messages before they become encrypted.
4. The CIA has tools to hack and infiltrate most contemporary, daily used ICT's.
5. By using weaknesses and methods revealed by Vault 7, foreign state- and non-state entities can make use of them and use them against the interests of ordinary citizens.

6. The potential impact of the tool ‘Weeping Angel’, which turns the microphone of a Samsung Smart TV into a ‘listening post’ for the CIA, has been somewhat overexposed in the media. In the first days after the publication of Vault 7, various media reported that the CIA would be able to listen to anyone owning a Samsung Smart TV. But as the document study shows, the malware used for this covert listening practices still has to be uploaded on the TV by physical means (a USB stick) which makes this practice similar to classic spying methods.

6 Discussion and recommendations

At the beginning of this research project, the following research question was formulated:

> How are the surveillance techniques of Vault 7 perceived and framed by popular press, and is this framing adequate when compared with academic literature and the content of Vault 7?

As previously discussed in chapter 2 and 3, the existing literature and the conceptual framework of Boeke (2016) will be used to answer the research question.

Scope	National, at home	Foreigners, abroad
Level interception	Downstream	Upstream
Focus	Targeted, individual	Bulk collection
Data acquisition	Metadata	Content

Table 2: technical communications collection - the four variables (Boeke, 2016)

Now that the news reporting on this topic has been studied, summarized and analyzed in chapter 4, and the documents of Vault 7 have been analyzed in chapter 5, the framework of Boeke (2016) can be used in order to define whether the media frames this topic as ‘mass surveillance’ or as ‘targeted surveillance’. Starting with the first variable, ‘scope’. The newspapers have so far not given any indication that the CIA espionage tools are aimed at US citizens. That means that the news coverage on this item does not give us a factual suspicion that the CIA is not adhering to its mandate, which holds that it is not allowed to spy on residents. The second variable, ‘level interception’ becomes very clear when analyzing the media. Both the New York Times and the Washington Post write about hacking tools, the hacking of individual phones and devices, and listening-in on Samsung TVs. These examples typically represent upstream interception of data. The third variable, ‘focus’ remains somewhat unclear: especially in the first days after the WikiLeaks publications, reporters seem to follow WikiLeaks. For example, it takes a while before the Samsung Smart TV story is nuanced; in the first days after the Vault 7 publications, one could think that the CIA could basically infiltrate any smart TV. A study of the documents, and expert opinion, shows that this is not true. Furthermore, in the news of March 7, the New York Times cites WikiLeaks about alleged Vehicle Control hacking by the CIA. During this research, there was no evidence found for that in the documents that have yet been published. If the ‘Vault 7’ publications of WikiLeaks have proven something, it is that the media is still a perfect platform for Julian Assange to gain maximum attention. On the day WikiLeaks published

Vault 7, international media rushed to cover the story. The headlines indicated that this could be a new mass surveillance episode, or at least an Intelligence Agency that exceeded its power. However, the fact that the CIA, (according to The New York Times and security expert Bruce Schneier) seems to buy zero-days on grey markets to hack individual devices gives us an indication that this program is focused on individual targets, which is in line with the scope of the CIA. When you read popular newspapers on March 7th, you might think now that the Vault 7 revelations resemble a new mass surveillance program. The document study and expert opinion show that, although there should be a debate about the ethical aspects of this CIA program, Vault 7 most probably resembles targeted surveillance. The last variable, 'data acquisition' is certainly about gathering of content in this case. According to The New York Times and The Washington Post, the CIA has abilities to listen-in via TVs, and has methods to hack individual devices in order to bypass encryption. This means the CIA is able to gather the data itself.

The analysis of the data itself teaches us that the amount of data which has been published by WikiLeaks, is too big to analyze in a short time. Personal details, such as employee names and targets, which could potentially reveal something more about the scope and background of the hacking tools, have been mostly redacted. What becomes clear is that the CIA has a big toolbox of hacking tools, and is able to hack most everyday modern devices. If we apply the framework of Boeke (2016) it becomes clear that the Vault 7 revelations do not suggest 'mass surveillance' since the documents give no indication that the (hacking) tools of the CIA are used for bulk collection purposes.

While these tools can be seen as intrusive, the discussion is more complex than suggested by a singular focus on privacy. What we are currently facing is an increasing tension in the cyber domain. Nation states, private companies, and non-state entities such as hacktivists, cyber criminals are gaining more cyber capabilities and influence than ever before. As Dunn Cavelty (2013) argues, the internet is not designed as a secure place. Private companies and everyone else interested in (big) data have no particular interest in making internet a highly secure place, since big data means profits and an accessible and open network makes the internet platform easier to use, reaching more clients.

The insecurity of cyberspace leaves governments and their intelligence agencies with the question: how to regulate it? On the one hand, western democratic governments have to be accountable and transparent. But on the other hand, cyber space is developing rapidly and

poses all kinds of herefore mentioned threats, such as aggressive foreign nation states or hackers. This poses a dilemma, and means that governments, and their intelligence agencies, have to find means to counter aggression and insecurity from previously unexpected quarters.

The literature gives us quite a few insights in how governments can cope with this. Richards (2013) proposes a legal framework that accentuates the importance of cooperation between governments and the private sector. His point of view is that surveillance is harmful and that we should not allow governments to secretly spy on us, citizens, without authorization. This would make a point for targeted surveillance.

However, Lyon (2010) warns for the dangers of social sorting that come together with surveillance. Since targeted surveillance per definition is based on social sorting (along with specific written algorithms for profiling) this poses another problem to governments. They should really have a strong case for specific social sorting programs, since leaking discriminatory algorithms is potentially damaging to governments' reliability.

If we take the starting point of Czosseck (2013) there certainly is a case for stricter government regulation, and surveillance: the internet is an unsafe heaven, increasingly being misused by cybercriminals and malicious states. However, there is a big paradox in this case. The director of an intelligence agency might be honest and dedicated in his intentions to combating foreign (cyber) criminals and gaining strategic knowledge, but doing so he might be creating something that has similarities with a totalitarian state. Bruneau & Dombroski (2014) support this reasoning, arguing that without decisive political and societal action the intelligence community will remain 'a state within a state' (p.23) and prevent democratic consolidation. The latter means that they are fully accepted as 'part of the game' by both the mass and elite of a certain democratic system in a specific country (p.3). Transformation to a more transparent intelligence community wil require continual efforts (p.23) from both civilians and intelligence professionals: key is a balance of efficiency and transparency.

The use of zero-days by intelligence agencies in order to build a cyber-arsenal is certainly not making the internet safer. Egelman et al. (2013) give a few arguments for and a few arguments against zero-day markets. The first argument 'for' is that tech companies need all the help they can get (p.2/3). Secondly, they argue, having good relations with (responsible) hackers increases the chance of being up-to-date with the pace of developments (p.3). However, there are many arguments against (p.3). Injecting money into these (dubious) markets is morally suspect. States, they argue, should not be involved in cybercriminal

circles. A second point they make against these markets, is the so-called ‘cobra effect’: paying for zero-day exploits creates an incentive for criminals to design extra bugs inside for later harvest. A final point they make: it is probably more efficient to train developers to make fewer mistakes, then paying huge amounts for zero-days. The question we can raise here is: do we want to preserve the status quo, or do we want to make the internet safer and stop supporting the grey markets where these zero-days are being traded?

If we want so, then governments should start thinking of passing more laws to regulate the heavily present private sector on the internet. As Lyon (2015) proposes, privacy should become an important part in product design. It should become compulsory to improve the security of connected devices, such as phones, computers, and certainly Internet-of-Things devices, including periodic updates to ensure their security. Manufacturers should be held accountable by law to protect citizens’ interests (mostly their private data) that go along with the use of their products. In Europe a part of this ‘shift’ might yet have started by means of the General Data Protection Regulation (GDPR), which forces organizations to take privacy seriously and adapt measures to ensure compliancy through the entire process. If we do not make the internet more secure by designing security into all our products, vulnerabilities will remain on a large scale, making abuse very easy. This point of view is supported by Thierer (2015) who argues that IoT developments cause considerable privacy and security related risks. However, he argues (p.117), policy solutions should not derail experimentation and innovations. Governments should not implement strict policy measures ex ante (p.118) because of rapid developments in this field. Thierer (p.119) argues for a ‘layered approach’ in which can be protected without derailing beneficial forms of economic and social innovation that flows from IoT developments. Governments should guide technological developments (p.119), simple legal principles are therefore greatly preferable, which could be supplemented by self-regulation and ex post policy.

7 Conclusion

This Master thesis was centered around the question ‘‘How are the surveillance techniques of Vault 7 perceived and framed by popular press and is this framing adequate when compared with academic literature and the content of Vault 7?’. In order to answer that question, a literature study on surveillance has been conducted. Various international media as well as the Vault 7 files itself have been studied and analyzed.

The media analysis has shown that WikiLeaks still has a lot of influence over news reporters, especially caused by their modus operandi: they make a lot of noise and publish thousands of documents at once. The media, also in this case, first reported that this was something very big, and in a way it was: such big revelations about the working methods of intelligence agencies are unique. But experts looked into it, as well as I, the researcher, did, as time passed by. That led to a more nuanced, somewhat different conclusion. The documents do embody an impressive toolbox that is used to infiltrate in targeted ICTs, but they are not aimed at mass surveillance. Cyber security experts, interviewed by the various newspapers that are included and summarized in this research paper, agree on this.

In order to contribute to an important academic discussion, I have elaborated on concepts of surveillance developed by various international researchers. The Vault 7 publication should not be seen and studied in a way that it poses something entirely new in the relationship between states and citizens. From former revelations of top-secret material, the most controversial and recent one being the NSA revelations, we know that states spy on a large scale. As Lyon (2010) argues, we should not solely focus on privacy when working on legal frameworks for surveillance. Instead, and that is what I argue, we should be realistic in a way that foreign states, and non-state entities are gaining cyber powers rapidly, which is threatening the security of citizens.

Intelligence Agencies will always, as described in the conceptual chapter of this thesis, operate in a certain ‘darkness’. That darkness, being secrecy, is needed in order to counter foreign threats. Revelations like Vault 7 can contribute to the discussion about what intelligence agencies should do or should not do, and to developing more transparency as an important requirement of democratic societies. But as it now seems, these revelations have increased the possibilities for malicious actors to use the vulnerabilities that are lying on the ‘street’.

8 References

Books and literature

Bauman, Z., Bigo, D., Esteves P., Guild, E., Jabri, V., Lyon, D. and R. B. J. Walker (2014) After Snowden: Rethinking the Impact of Surveillance. Journal of International Political Sociology, Volume 8, Issue 2 June 2014, Pages 121–144

Boeke, S. (2016) Reframing ‘‘Mass surveillance’’ in: Terrorists’ Use of the Internet: Assessment and Response 136, 307

Bigo, Didier and Carrera, Sergio and Hernanz, Nicholas and Jeandesboz, Julien and Parkin, Joanna and Ragazzi, Francesco and Scherrer, Amandine, Mass Surveillance of Personal Data by EU Member States and Its Compatibility with EU Law (November 6, 2013). Liberty and Security in Europe Papers No. 61. Available at SSRN: https://ssrn.com/abstract=2360473

Bos-Ollermann, David Cole, Federico Fabbrini and Stephen Schulhofer (2017). Surveillance, Privacy and Trans-Atlantic Relations

Broeders, Dennis & James Hampshire (2013) Dreaming of Seamless Borders: ICTs and the Pre-Emptive Governance of Mobility in Europe, Journal of Ethnic and Migration Studies, 39:8, 1201-1218, DOI: 10.1080/1369183X.2013.787512

Bruneau, T. C., & Dombroski, K. R. (2014). Reforming intelligence: The challenge of control in new democracies.

Cavelty, M. D. (2013) Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. Science and Engineering Ethics.

Crowdy, T. (2008). The enemy within: a history of spies, spymasters and espionage. Oxford: Osprey Pub.

Czosseck, C. (2013). State actors and their proxies in cyberspace. In Peacetime Regime for State Activities in Cyberspace (pp. 1–24). Tallinn, Estonia: NATO CCDCOE Publication.

D. d’Alessio and M. Allen (2000). Media bias in presidential elections: a meta-analysis. Journal of Communication, Volume 50, Issue 4. Pages 133–156

Denzin, N. (2006). Sociological Methods: A Sourcebook. Aldine Transaction.

Egelman, S., Herley, C., & Van Oorschot, P. C. (2013, December). Markets for zero-day exploits: Ethics and implications. In Proceedings of the 2013 workshop on New security paradigms workshop (pp. 41-46). ACM.

Foucault, M. (1995). Discipline and Punish: The Birth of the Prison. New York: Vintage Books.

Farwell, J.P. & Rafal Rohozinski (2011) Stuxnet and the Future of Cyber

Hoboken, J.V.J. (2014) Privacy and Security in the Cloud: Some realism about technical solutions to transnational surveillance in the Post-Snowden era, 66 Me. L. Rev. 487 - 534.

War, Survival, 53:1, 23-40

Lyon, D. (1995) 'Whither shall I flee? Surveillance, Omniscience and Normativity in the Panopticon' Christian Scholars Review 41(4), 653- 678

Lyon, D. (2010) Surveillance, power and everyday life. In: P. Kalantzis-Cope and K. Gherab-Martin (eds.) Emerging Digital Spaces in Contemporary Society. Houndsmills, UK: Palgrave Macmillan.

Lyon, D. (2015). Surveillance after Snowden. Cambridge, UK: Polity Press, 2015

Marx, Gary T. (2002) What's New About the "New Surveillance"? Classifying for Change and Continuity. Surveillance & Society, [S.l.], v. 1, n. 1, p. 9-29, sep. 2002. ISSN 1477-7487

Mitsilegas, V. (2015) The Transformation of Privacy in an Era of Pre-emptive Surveillance. Tilburg Law Review 20: 35 –57.

Morrison, E. (2015) Surveillance society needs performance theory and arts practice, International Journal of Performance Arts and Digital Media, 11:2, 125-130, DOI: 10.1080/14794713.2015.1084812

Murakami Wood, D. (2013) Globalization and Surveillance: The Watched World. Rowman & Littlefield Publishers, Lanham, Maryland, U.S.A.

Richards, Neil M. (2013). The Dangers of Surveillance (March 25, 2013). Harvard Law Review. Available at SSRN: https://ssrn.com/abstract=2239412

Warner, M. and Johnson, L.K. (2007) Handbook of Intelligence Studies, Routledge: New York.

Spencer, Shaun B. (2013) The Surveillance Society and the Third-Party Privacy Problem. South Carolina Law Review, Vol. 65, No. 2, 2013. Available at SSRN: https://ssrn.com/abstract=2387732

Thierer, A. D. (2015). The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation.

Warren, D. and Brandeis, L.D. (1890) The Right to Privacy, Harvard Law Review 4, no. 5, 193–220, doi:10.2307/1321160.

Weblinks

[1] 114th Congress (2015-2016), *H.R.2048 - USA FREEDOM Act of 2015 - https://www.congress.gov/bill/114th-congress/house-bill/2048/text*. .

[2] CIA, "CIA - scope of work," *2017*. [Online]. Available: https://www.cia.gov/about-cia/todays-cia/what-we-do. [Accessed: 15-May-2017].

[3] "CIA - Central Intelligence Agency Activities," *2017*. [Online]. Available: https://www.cia.gov/about-cia/privacy-and-civil-liberties/CIA-AG-Guidelines-Signed.pdf. [Accessed: 15-May-2017].

[4] NYTimes, "Germany's complicated relation with Google Streetview," 2013. [Online]. Available: https://bits.blogs.nytimes.com/2013/04/23/germanys-complicated-relationship-with-google-street-view/?_r=0.

[5] "Searchengineland: Google stopped streetview in Germany." [Online]. Available: https://searchengineland.com/google-has-stopped-street-view-photography-germany-72368. [Accessed: 15-Mar-2017].

[6] Wikipedia, "Revelations of Edward Snowden." [Online]. Available: https://en.wikipedia.org/wiki/Edward_Snowden. [Accessed: 30-Mar-2017].

[7] "National Research Council, Bulk Collection of Signals Intelligence: Technical Options, 2015 Options."

[8] Wikipedia, "Targeted Surveillance," 2018. [Online]. Available: https://en.wikipedia.org/wiki/Targeted_surveillance.

[9] "Regulation of Investigatory Powers Act 2000."

[10] "Biggest U.S. Intelligence leaks in History."

[11] "Watergate scandal," *Washington Post*.

[12] The Guardian, "The Iraq War logs."

[13] BBC News, "Snowden NSA Revelations."

[14] Wikipedia, "What is Cyber ethnography?" [Online]. Available: https://en.wikipedia.org/wiki/Cyber-ethnography. [Accessed: 15-Mar-2017].

[15] Wikipedia, “Media Bias.” [Online]. Available: https://en.wikipedia.org/wiki/Media_bias. [Accessed: 16-Mar-2017].

[16] T. N. Y. R. of Books, “The Reporter Resists His Government.”

[17] BBC News, “BBC: PayPal says it stopped Wikileaks payments on US letter,” 2010. [Online]. Available: http://www.bbc.com/news/business-11945875. [Accessed: 30-Mar-2017].

[18] F. CIA, “Background to ‘Assessing Russian Activities and Intentions in Recent US Elections’: The Analytic Process and Cyber Incident Attribution.”

[19] “Opinion about the WikiLeaks CIA cache - Zeynep Tufceki,” 2017. .

[20] Mirror.co.uk, “WikiLeaks releases thousands of pages on Turkish ruling,” 2017. .

[21] Wikipedia, “Edward Snowden,” 2017. [Online]. Available: https://en.wikipedia.org/wiki/Edward_Snowden. [Accessed: 16-Mar-2017].

[22] WikiLeaks, “Twitter message: What is Vault 7?,” 2017. [Online]. Available: https://twitter.com/wikileaks/status/827828627488268290/photo/1?ref_src=twsrc%5Etfw&ref_url=http%3A%2F%2Femptylighthouse.com%2Fvault7-everything-we-know-about-wikileaks-new-vault-7-project-719935292. [Accessed: 16-Mar-2017].

[23] WikiLeaks, “Twitter message: Global Seeds Vault,” 2017. [Online]. Available: https://www.croptrust.org/our-work/svalbard-global-seed-vault/. [Accessed: 16-Mar-2017].

[24] WikiLeaks, “Twitter message: Where is Vault 7?,” 2017. [Online]. Available: https://www.croptrust.org/our-work/svalbard-global-seed-vault/. [Accessed: 16-Mar-2017].

[25] WikiLeaks, “Twitter Message: Merkers saltmine,” 2017. [Online]. Available: https://en.wikipedia.org/wiki/Nazi_gold. [Accessed: 16-Mar-2017].

[26] WikiLeaks, “Twitter message: when is vault 7?,” 2017. [Online]. Available: https://twitter.com/wikileaks/status/828537075460890625/photo/1?ref_src=twsrc%5Etfw&ref_url=https%3A%2F%2Fwearechange.org%2Fvault-7-wikileaks-releases-series-cryptic-tweets%2F. [Accessed: 16-Mar-2017].

[27] WikiLeaks, “Twitter message:who is vault 7?,” 2017. [Online]. Available: https://twitter.com/wikileaks/status/828889235994324992/photo/1?ref_src=twsrc%5Etfw&ref_url=https%3A%2F%2Fwearechange.org%2Fvault-7-wikileaks-releases-series-cryptic-tweets%2F. [Accessed: 16-Mar-2017].

[28] WikiLeaks, “Twitter Message：why is vault 7?,” 2017. [Online]. Available: https://twitter.com/wikileaks/status/829324362943696896/photo/1?ref_src=twsrc%5Etfw&ref_url=https%3A%2F%2Fwearechange.org%2Fvault-7-wikileaks-releases-series-cryptic-tweets%2F. [Accessed: 16-Mar-2017].

[29] “Twitter Message：How did vault 7 made its way to WikiLeaks?” [Online]. Available: https://twitter.com/wikileaks/status/829693251133272064/photo/1?ref_src=twsrc%5Etfw&ref_url=https%3A%2F%2Fwearechange.org%2Fvault-7-wikileaks-releases-series-cryptic-tweets%2F.

[30] “Reddit Forum - speculations on Vault 7,” 2017. .

[31] FBI, “FBI - Clinton e-mail investigation.”

[32] “WikiLeaks tweet - When is vault 7 - Jet engine.” .

[33] “Wikipedia - Airplane engine F119.” .

[34] “Reddit - complete summary on Vault 7,” 2017. .

[35] “Reddit forum - Discussion on WikiLeaks,” 2017. .

[36] “Global Seeds Vault in Svalbard,” 2017. .

[37] “Reddit forum - Theory on shadow government.” .

[38] “CNBC News: New FBI release on Clinton email probe refers to ‘Shadow Government,’” 2017. .

[39] NYTimes, “The New York Times: Trove of Stolen Data Is Said to Include Top-Secret U.S. Hacking Tools.” [Online]. Available: https://www.nytimes.com/2016/10/20/us/harold-martin-nsa.html?_r=1. [Accessed: 20-Mar-2017].

[40] WikiLeaks, “WikiLeaks: Statement of March 7, 2017.” [Online]. Available:

https://wikileaks.org/ciav7p1/.

[41] “Samsung: privacy notions on Smart TV,” 2017. [Online]. Available: http://www.samsung.com/uk/info/privacy-SmartTV/. [Accessed: 20-Mar-2017].

[42] “WikiLeaks: encryption bypass.” [Online]. Available: https://wikileaks.org/ciav7p1/#FAQ. [Accessed: 15-Mar-2017].

[43] “Wired.com: DON’T LET WIKILEAKS SCARE YOU OFF OF SIGNAL AND OTHER ENCRYPTED CHAT APPS.” [Online]. Available: https://www.wired.com/2017/03/wikileaks-cia-hack-signal-encrypted-chat-apps/. [Accessed: 15-Mar-2017].

[44] “The Guardian: Hacking group auctions ‘cyber weapons’ stolen from NSA.” [Online]. Available: https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group. [Accessed: 25-Mar-2017].

[45] “WikiLeaks Vault 7 statement 7 march.” [Online]. Available: https://wikileaks.org/vault7/. [Accessed: 07-Mar-2017].

[46] “Wikipedia: Clinton e-mail affairs,” 2017. [Online]. Available: https://wikileaks.org/clinton-emails/. [Accessed: 20-Mar-2017].

[47] Wikipedia, “Wikipedia: John Podesta e-mail affairs,” 2017. [Online]. Available: https://wikileaks.org/podesta-emails/. [Accessed: 20-Mar-2017].

[48] T. N. Y. Times, “WikiLeaks releases trove of alleged C.I.A. Hacking Documents.”

[49] Wired.com, “New Dark Web-market is selling Zero-Day Exploits to Hackers,” 2015. [Online]. Available: https://www.wired.com/2015/04/therealdeal-zero-day-exploits/.

[50] “The Vulnerability Equities Process.” [Online]. Available: https://epic.org/privacy/cybersecurity/vep/.

[51] WikiLeaks, “WikiLeaks claim about hacking vehicle systems.” [Online]. Available: https://wikileaks.org/ciav7p1/cms/page_13763797.html. [Accessed: 22-Mar-2017].

[52] “VEP Process - Electronic Privacy Information Center.” [Online]. Available: https://epic.org/privacy/cybersecurity/vep/.

[53] “WikiLeaks tweet on passport release Vault 7,” 2017. [Online]. Available: https://twitter.com/wikileaks/status/838910359994056704?ref_src=twsrc%5Etfw&ref_url=http%3A%2F%2Fwww.zerohedge.com%2Fnews%2F2017-03-06%2Fwikileaks-releases-encrypted-vault-7-torrent-will-unveil-password-tuesday-9am. [Accessed: 08-Mar-2017].

[54] “New York Times report on J.F.K. statement about CIA,” 1960.

[55] “Wikipedia: President of the U.S. John F. Kennedy.” [Online]. Available: https://nl.wikipedia.org/wiki/John_F._Kennedy. [Accessed: 10-Mar-2017].

[56] “Wikipedia: Bay of pigs invasion.” [Online]. Available: https://en.wikipedia.org/wiki/Bay_of_Pigs_Invasion. [Accessed: 10-May-2017].

[57] “Wikipedia: operation Northwoods.” [Online]. Available: https://en.wikipedia.org/wiki/Operation_Northwoods. [Accessed: 10-May-2017].

[58] “News.com.au WikiLeaks Vault 7 password is an Anti-CIA JFK Quote,” 2017. [Online]. Available: http://www.news.com.au/finance/work/leaders/wikileaks-password-is-an-anticia-jfk-quote/news-story/d6c1cc5385c4f1330bb87f1be2ecefa3. [Accessed: 20-Mar-2017].

[59] “uTorrent - Torrent Client.” [Online]. Available: http://www.utorrent.com/intl/nl/. [Accessed: 20-Mar-2017].

[60] “7z decryption software.” [Online]. Available: http://www.7-zip.org/7z.html. [Accessed: 21-Mar-2017].

[61] “BBC: The weird names the CIA gives its hacking tools.” [Online]. Available: http://www.bbc.com/news/technology-39219637. [Accessed: 20-Mar-2017].

[62] “WikiLeaks claims about hacking tools.” [Online]. Available: https://wikileaks.org/ciav7p1/. [Accessed: 25-Mar-2017].

[63] WikiLeaks, “WikiLeaks: Organization chart of the CIA.” [Online]. Available: https://wikileaks.org/ciav7p1/files/org-chart.png. [Accessed: 21-Mar-2017].

[64] WikiLeaks, “WikiLeaks HammerDrill publication.” [Online]. Available: https://wikileaks.org/ciav7p1/cms/page_17072172.html. [Accessed: 23-Mar-2017].

[65] WikiLeaks, “WikiLeaks Brutal Kangaroo publication.” [Online]. Available: https://wikileaks.org/ciav7p1/cms/page_13763236.html. [Accessed: 23-Mar-2017].

[66] WikiLeaks, “WikiLeaks: Medusa and Assassin publications.” [Online]. Available: https://wikileaks.org/ciav7p1/.

[67] “WikiLeaks Malware Tool Hive.” [Online]. Available: https://wikileaks.org/ciav7p1/. [Accessed: 23-Mar-2017].

[68] “WikiLeaks Hive Honeycomb server user manual.” [Online]. Available: https://wikileaks.org/ciav7p1/cms/files/UsersGuide.pdf. [Accessed: 26-Mar-2017].

[69] WikiLeaks, “WikiLeaks Fine Dining publication.” [Online]. Available: https://wikileaks.org/ciav7p1/. [Accessed: 23-Mar-2017].

[70] WikiLeaks, “WikiLeaks Sonic Screwdryer publication.” [Online]. Available: https://wikileaks.org/vault7/document/SonicScrewdriver_1p0/. [Accessed: 23-Mar-2017].

[71] WikiLeaks, “WikiLeaks statement on Dark matter.” [Online]. Available: https://wikileaks.org/vault7/.

[72] WikiLeaks, “WikiLeaks Marble Framework Publications.” [Online]. Available: https://wikileaks.org/vault7/document/Marble/. [Accessed: 23-Mar-2017].

[73] WikiLeaks, “WikiLeaks Grasshopper Framework.” [Online]. Available: https://wikileaks.org/ciav7p1/cms/page_12353652.html. [Accessed: 23-Mar-2017].

[74] WikiLeaks, “WikiLeaks Hive Project Documents.” .

[75] WikiLeaks, “WikiLeaks Wheeping Angel Tool.” [Online]. Available: https://wikileaks.org/vault7/document/EXTENDING_User_Guide/page-4/#pagination. [Accessed: 24-Mar-2017].

[76] WikiLeaks, “WikiLeaks Scribbles Project.” [Online]. Available: https://wikileaks.org/vault7/#Scribbles. [Accessed: 24-Mar-2017].

[77] WikiLeaks, “WikiLeaks Archimedes Documents.” [Online]. Available: https://wikileaks.org/vault7/#archimedes. [Accessed: 25-Mar-2017].

[78] WikiLeaks, “WikiLeaks After Midnight Publication.” [Online]. Available: https://wikileaks.org/vault7/#AfterMidnight. [Accessed: 26-Mar-2017].

[79] WikiLeaks, “WikiLeaks Athena Publication.” [Online]. Available: https://wikileaks.org/vault7/#athena. [Accessed: 20-May-2017].

[80] WikiLeaks, “WikiLeaks Pandemic Publication.” [Online]. Available: https://wikileaks.org/vault7/#pandemic. [Accessed: 02-Jun-2017].

[81] WikiLeaks, “Wheeping Angel User Guide.” [Online]. Available: https://wikileaks.org/vault7/document/EXTENDING_User_Guide/page-4/#pagination. [Accessed: 02-Jun-2017].

[82] “Schneier on Security Blog.” [Online]. Available: https://www.schneier.com/. [Accessed: 15-Oct-2017].

[83] “Schneier on Security: 1st blog on Vault 7.” [Online]. Available: https://www.schneier.com/blog/archives/2017/03/wikileaks_relea.html. [Accessed: 16-Oct-2017].

[84] “Schneier on Security: 2nd blog on Vault 7.” [Online]. Available: https://www.schneier.com/blog/archives/2017/03/wikileaks_not_d.html. [Accessed: 16-Oct-2017].

[85] “Wired.com Government Agencies tell they don’t stockpile Zero-days,” *2017*. [Online]. Available: https://www.wired.com/2014/11/michael-daniel-no-zero-day-stockpile/. [Accessed: 20-Oct-2017].

[86] “Schneier on Security: NSA is hoarding Zero-days.” [Online]. Available: https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html. [Accessed: 20-Oct-2017].

[87] “Washington Post: U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show.” [Online]. Available: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html?utm_term=.a9cda0782c85. [Accessed: 21-Oct-2017].

[88] “Schneier on security: third blog on Vault 7.” [Online]. Available: https://www.schneier.com/blog/archives/2017/04/fourth_wikileak.html. [Accessed: 21-Oct-2017].

[89] “Schneier Statement on fourth document dump by WikiLeaks.” [Online]. Available: https://www.schneier.com/blog/archives/2017/04/fourth_wikileak.html. [Accessed: 21-Oct-2017].