Vulnerabilities, Cybersecurity, and the Role of Law and Regulation herein

Kwetsbaarheden, cyberveiligheid en de rol van wet- en regelgeving hierin

Proefschrift ter verkrijging van de graad van doctor aan de
Erasmus Universiteit Rotterdam op gezag van
de rector magnificus
Prof.dr. A.L. Bredenoord
en volgens besluit van het College voor Promoties

De openbare verdediging zal plaatsvinden op
donderdag 11 november 2021 om 10:30 uur

Jian Jiang
Shanghai, China

Erasmus University Rotterdam

Promotiecommissie

Promotoren:	Prof. dr. N.J. Philipsen
	Prof. dr. E. Salzberger
Overige leden:	Prof. dr. M.G. Faure LL.M.
	Prof. dr. E. Carbonara
	Prof. dr. R. Sarel

This thesis was written as part of the European Doctorate in Law and Economics programme

An international collaboration between the Universities of Bologna, Haifa, Hamburg and Rotterdam.
As part of this programme, the thesis has been submitted to the Universities of Bologna, Haifa, Hamburg and Rotterdam to obtain a doctoral degree.

In memory of Prof. Dr. Manfred Neumann (1933–2016)

Preface and Acknowledgments

This thesis originates from my observations about the important role played by software vulnerabilities in the increasing number of cyberattacks globally. Nowadays, it is not difficult to conjure up images of hacked power plants, remote-hijacked public transportation systems, etc. Shortly before the completion of this thesis, one of the United States' largest oil pipelines, Colonial Pipeline, was hacked and forced to pay the hackers a ransom of nearly $5 million, according to the Wall Street Journal. By exploiting hidden vulnerabilities, hackers are plundering business secrets, stealing digital consumer records, and trying to reshape the world quietly.

Most of society lacks awareness of software vulnerabilities. Software vendors seem unlikely to discuss flaws in their products publicly, and the related markets of vulnerabilities are often opaque. My thesis tries to introduce to the readers a structured discussion and analysis of software vulnerabilities vis-à-vis the challenges of cyberattacks. I hope that my research will stimulate more contributions to this topic.

It has been a huge challenge to complete this thesis. The ongoing crises of COVID-19 has increased difficulties of my research work. It is with the support and assistance from many people that it has been possible to complete my thesis.

First and foremost, I would like to thank my supervisors, Prof. Dr. Niels Philipsen and Prof. Dr. Eli Salzberger, without whom my research would not have been possible. It is their creative insights, motivating guidance, inspiring advice, and patient help that led me to complete my research project. They guided me to organically incorporate economic analysis with legal theory and made a vital contribution to my thesis.

I am deeply indebted and wholeheartedly grateful to Prof. Dr. Michael Faure for his never-ending support, immense encouragement, and enlightening comments on the earlier drafts of my thesis. I wish to acknowledge Prof. Dr. Michael Faure's understanding and suggestions, which helped me to keep going.

I would also like to take this opportunity to express my gratitude to Prof. Dr. Alan Miller.

I am thankful for his support when I was developing my research ideas and economic models, as well as his trust in me on my academic journey. Alan contributed significantly to my thesis.

Special thanks must go to Prof. Dr. Jonathan Klick and Prof. Dr. Jarek Kantorowicz. The discussions with Prof. Dr. Jonathan Klick sharpened the econometric part of my research. The valuable ideas and insights in their lectures greatly improved my empirical work. Special thanks also go to Prof. Dr. Francesco Parisi, who gave my research project significant recognition and encouragement.

Parts of my thesis were presented at various conferences, among which were the EDLE conferences in Rotterdam, Bologna, and Hamburg, as well as the colloquium at the Cyber Centre at the University of Haifa. I would like to express my special gratitude to Prof. Dr. Kees van Noortwijk, Prof. Dr. Franziska Weber, Prof. Dr. Louis T. Visscher, Prof. Dr. Sharon Oded, Prof. Dr. Niva Elkin-Koren, Prof. Dr. Todd Kaplan, and Prof. Dr. Luigi Franzoni.

I would like to present my great appreciation to my colleagues in Rotterdam and Haifa, especially Marianne Breijer, Prof. Dr. Elena Kantorowicz-Reznichenko, Yulia Lischinsky, and Dr. Michal Ben-Gal. Their patience and supportive work have always been there for me. Sincere thanks go to all the members in the reading committee of my thesis, for their valuable time and remarks. They are Prof. Dr. Michael Faure, Prof. Dr. Emanuela Carbonara, and Prof. Dr. Roee Sarel.

I am expressing my heartfelt gratitude to Prof. Dr. Justus Haucap, Prof. Dr. Christian Koenig, Dr. Karni Chagal and Dr. Shu Li, for their constant support for me. Prof. Dr. Hans-Theo Normann also deserve special recognition for his encouraging comments on my empirical work in the thesis.

Finally, I wish to thank all my family members and friends, for accompanying me on this long journey and endorsing me with unconditional love.

Contents

List of Tables

List of Figures

Chapter 1: Introduction

The advent of the internet has created opportunities and developments that have far superseded our expectations. As our world becomes increasingly connected and indispensably dependent on various online or mobile software applications, it is more and more important to focus on the hidden threats behind the ever-changing virtual ecosystem. This interconnected world presents us with a range of challenges created by information technology and the trend in making the Internet of Things (IoT). Cyber threats and damage can occur when technology and power are in the "wrong hands". Indeed, the last decade has seen a rapidly increasing number of cyber-attacks, threatening individuals, companies, and governmental organizations alike.

1.1 The facts

Christmas 2019 was not an easy time for researchers and students at Maastricht University, because for several weeks they lost access to their working files, library services and emails kept on the university servers. On Christmas Eve, the systems of the university were under a severe cyberattack, called a "ransomware" attack, in which hackers deploy malicious software to block access to or encrypt the files in a computer system until the owner of that system pays a ransom. The attack affected almost all of the Microsoft Windows systems in the university and prevented the university from accessing its data and disabled its email services. According to public reports, the Maastricht University paid nearly $220,000 worth of bitcoin to restore critical systems that were hit by the ransomware attack[1]. But paying the ransom is not the happy end: once a website is hacked, all the usernames and passwords of the registered users are very likely to be leaked. Many users do not change their passwords for different websites, which means their private information on other websites is also endangered. Even if a cautious user uses different usernames and passwords for different websites, as long as there is some logical association between them, it is easy to crack these passwords with the current level of artificial intelligence algorithms.

This cyberattack was the latest of several severe attacks targeting large organizations

[1] https://portswigger.net/daily-swig/ransomware-attack-maastricht-university-pays-out-220-000-to-cybercrooks (retrieved on 30 November 2020)

or institutions in 2019. More than 20 municipalities in the U.S. were hit by cyberattacks that year[2]. In June 2019, Riviera Beach, a city in Florida was hacked and forced to pay a ransom of $600,000 in bitcoins[3] to hackers in the hope of getting back the city's compromised data[4].

In cases where the targets refuse to pay the ransom, the costs of such cyberattacks can be very high. In May 2019, in Baltimore, hackers digitally locked about 10,000 government computers and demanded about $100,000 in bitcoins to free them. As a result of refusal of payment by the Baltimore government, the city employees were locked out of their email accounts and the citizens were unable to access essential services for two weeks[5]. In 2018, the city of Atlanta refused a demand of $50,000 ransom by the hackers. According to media reports, the cost of fixing the damage of the attack amounted to $17,000,000[6].

Many people still remember today the notorious cyberattack named "WannaCry" on 12 May 2017. A group of hackers carried out a worldwide attack using stolen ransomware, WannaCry, to extort money from users of the Microsoft Windows system. It was reported to have infected more than 230,000 computers in over 150 countries, hitting not only the British National Health Service but also the Russian interior ministry, Chinese universities, the German state railway company, and many more countries and companies[7].

Earlier cyberattack cases went far beyond these and 2016 was a bonanza year. In February 2016 some hackers stole $81 million directly from the central bank of Bangladesh. In August the American National Security Agency found out that its own

[2] https://www.vox.com/recode/2019/5/21/18634505/baltimore-ransom-robbinhood-mayor-jack-young-hackers (retrieved on 30 November 2020)
[3] Bitcoin is an example of a decentralized virtual currency. Bitcoin is also known as cryptocurrency, meaning that it relies on cryptographic software protocols to generate the currency and validate transactions. See "Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury" (November 18, 2013), https://www.fincen.gov/sites/default/files/2016-08/20131118.pdf (retrieved on 30 November 2020)
[4] https://www.businessinsider.com/florida-city-paid-600k-hackers-shows-us-unprepared-for-threat-2019-6?r=DE&IR=T (retrieved on 30 November 2020)
[5] https://www.vox.com/recode/2019/5/21/18634505/baltimore-ransom-robbinhood-mayor-jack-young-hackers (retrieved on 30 November 2020)
[6] *Id.*
[7] The Economist (2017c)

self-developed cyber tools had been leaked online due to a previous cyberattack by a hacker group calling themselves the Shadow Brokers. And it was reported that the hacking of the Democratic National Committee's email servers and the subsequent leaking of embarrassing communications seemed to have been part of an attempt to influence the outcome of the US elections[8].

All these facts above demonstrate that institutions or individuals in the interconnected ecosystem are not well prepared for the coming wave of cyberattacks. Even if some common targets such as hospitals and universities have beefed up the security level of their online systems, there are still plenty of targets which are vulnerable to cyberattacks. In theory, as long as there are software vulnerabilities[9] in the online system, there is a possibility of remote attacks. According to the 2019 Trustwave Global Security Report, 100% of all the web applications tested by Trustwave, a leading information security company, possessed at least one vulnerability and the median number of vulnerabilities was 15[10]. No wonder many cybersecurity experts think that everything is hackable in today's cyber ecosystem[11]. Software vulnerabilities are especially important for cybersecurity. As the defenders of cyberattacks, enterprises, institutions, and individuals should timely patch the vulnerabilities in their systems to improve their defence capabilities greatly. In order to commit a cyberattack, hackers need to constantly find systems with unpatched vulnerabilities in order to raise the probability of success of cyberattacks. With the expansion of the internet and the acceleration of technology, the challenges of understanding software vulnerabilities and their link to cybersecurity nowadays are already upon us.

1.2 Some statistics

Statistics from multiple sources show us a more specific picture of current cybersecurity issues. The recent estimate of the worldwide cybercrime losses may amount to almost $600 billion annually, or 0.8% of the global GDP[12]. Furthermore, a new global survey

[8] The Economist (2017d)
[9] A vulnerability refers to a weakness in a system that can be utilized by an attacker to damage the system, obtain unauthorized access, execute arbitrary code, or otherwise exploit the system. See Knapp & Langill (2015). In the first section of chapter 4 of this thesis, we will discuss the vulnerability in detail.
[10] https://securenation.net/wp-content/uploads/2018/12/Trustwave_GSR_2019_Final-.pdf (retrieved on 30 November 2020)
[11] The Economist (2017d)
[12] The Center for Strategic and International Studies (February 2018), Economic Impact of Cybercrime—No

on CEOs reveals that U.S. CEOs place cybersecurity as their first business worry, ahead of new competitors and a recession[13]. In the rising tide of the Internet of Things, 64% of large and mid-tier businesses have already used IoT technology to some extent[14]. However, 57% of large and medium sized businesses consider cybersecurity concerns as the main barrier to greater IoT adoption[15].

When we turn to software vulnerabilities, which is the most important factor affecting the damage caused by the malware used in a cyberattack, the data does not lead to optimism. In the Trustwave Global Security Report 2019[16], a steep year by year increase of 1,250% is observed in ransom malware, which was almost non-existent in 2017. Every web application has at least one vulnerability, with the median number of vulnerabilities rising to 15, up from 11 in 2018. According to the Skybox Research Report 2020, the new count of vulnerabilities was 17,220 in 2019, representing a modest 3.8% increase compared with 16,391, the figure reported in 2018[17].

Although vulnerabilities are flaws in software and play a vital role in cybersecurity, software vendors seem to have different considerations. "How to balance the speed and the security" has always been a question to those decision makers. From the statistics of 2018[18], 58% of them feel pressure to roll out IT projects before they have undergone the necessary security checks and repairs. This number has improved compared to 65% in 2017[19] and 77% in 2016[20] due to the wide recognition that catching vulnerabilities early is far less costly than dealing with them later. But the bulk of software vendors still opt for speed over security.

Slowing Down, https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf (retrieved on 30 November 2020)

13 https://www.conference-board.org/pdf_free/press/Press%20Release%20--%20C-Suite%20Challenge%202019.pdf (retrieved on 30 November 2020)

14 Internet of Things Cybersecurity Readiness Report, https://www.singtel.com/content/dam/singtel/business/globalservices/Featured%20Articles/internet-of-things-cybersecurity-readiness.pdf (retrieved on 30 November 2020)

15 *Id.*

16 https://securenation.net/wp-content/uploads/2018/12/Trustwave_GSR_2019_Final-.pdf (retrieved on 30 November 2020) https://securenation.net/wp-content/uploads/2018/12/Trustwave_GSR_2019_Final-.pdf (retrieved on 30 November 2020)

17 Skybox (2020), https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/2020-VT-Trends_Executive-Summary.pdf (retrieved on 30 November 2020)

18 https://www2.trustwave.com/rs/815-RFM-693/images/TW_2018_Pressures_Security_Report_Final.pdf (retrieved on 30 November 2020)

19 https://www.windriverfinancial.com/wp-content/uploads/2019/02/Security-Pressures-Report-2017.pdf (retrieved on 30 November 2020)

20 *Id.*

In addition, after a severe cyberattack, generally the stock price of the target company is likely to fall, if it is a listed company. Oxford Economics, which studied 65 severe breaches in FTSE 100[21] companies, found that they tend to lead to share prices falling by an average of 1.8% following a cyberattack[22]. Although the stock price of the attacked company will fall, it is not clear whether the stock price of the maker of the compromised software is also about to fall after a massive cyberattack. This is an aspect which I will test as part of this thesis. A feasible hypothesis is that it is most likely to happen because the end-users of the affected software often lack professional skills and thus when facing a cyberattack, they lack not only the fast response to self-protect but also a rational response to the flawed products they use. It has been reported in earlier years that 81% of the victims fail to detect a breach themselves[23]. Even for security professionals, the shortage of security expertise is the third biggest operational pressure they are facing[24].

Last but not least, exploiting vulnerabilities can bring high returns. In a report on underground markets six years ago, it was already calculated that those attackers earned a 1425% return on investment in exploit kit and ransomware schemes[25].

1.3 Research questions and methodology

Based on the observations and statistics listed above, this thesis focuses on three aspects: (1) the vulnerabilities, which are inevitable as by-products of software, having a significant impact on cybersecurity; (2) cybersecurity, which is becoming one of the most important social concerns against the background of the booming trend of the Internet of Things; and (3) the law and regulation thereof, which is designed to address problems of vulnerabilities and cybersecurity in the long run.

---

[21] The Financial Times Stock Exchange 100 Index, also called the FTSE 100 Index

[22] https://www.telegraph.co.uk/technology/2017/04/12/cyber-attacks-knock-millions-ftse-share-prices/ (retrieved on 30 November 2020)

[23] https://trustwave.azureedge.net/media/13167/2015-trustwave-global-security-report.pdf?rnd=131657083010000000 (retrieved on 30 November 2020)

[24] https://www.optus.com.au/content/dam/optus/documents/enterprise/case-studies/2016_Security_Pressures_Report_from_Trustwave.pdf (retrieved on 30 November 2020)

[25] https://trustwave.azureedge.net/media/13167/2015-trustwave-global-security-report.pdf?rnd=131657083010000000 (retrieved on 30 November 2020)

My thesis aims to study the research question: How to understand vulnerabilities and their relevance to cybersecurity, as well as the role of law and regulation thereof?

There are several research sub-questions which will be addressed in the following chapters of this thesis:

1, How to understand cybersecurity, cyber threats, and their relevance to vulnerabilities?

2, What are the lifecycle and the intrinsic value of a vulnerability from an economic perspective?

3, What are the markets for vulnerabilities? Which of these markets is legal, and which is illegal? Who are the actors on the supply side, and who are the actors on the demand side?

4, What determines the price of a vulnerability in the black market?

5, How to understand the role of the government, its dilemma on vulnerabilities, and how to evaluate its related policy?

6, Is there any market failure or does the software vendor face sufficient market pressure after a cyberattack?

7, Is it feasible to make the software vendor liable for his "flawed" product? Will contract law or liability rules in torts apply? Is there a role for regulation?

The methodology I apply in my research is Law and Economics. Economic methods will be incorporated into legal study. Readers will find two economic models in the thesis. In addition, event study, an empirical method, will be used to analyse data.

1.4 The structure of this thesis

The structure of this thesis revolves around my general research question, and the arrangement of each chapter corresponds to its related research sub-question.

Chapter 1 - this chapter – introduces the topic and the thesis. Through facts and statistics, readers are presented with a panoramic view of the status and challenges of cybersecurity. Meanwhile, the research questions of this thesis and the arrangement of each chapter are also put forward here.

Chapter 2 provides a literature review, in which the relevant literature on vulnerabilities

and cybersecurity from the perspectives of economics (with a particular focus on market failure theory) and law are surveyed.

Chapter 3 delves into two case studies of cyber-attacks and unveils the mysteries of cyber-attacks. Both cases were landmarks in the history of cyber-attacks. The Stuxnet case was the watershed, indicating that virtual codes can cause physical damage to the real world, while the WannaCry case was a pioneering global ransomware attack. These case studies help us to understand cyber threats more clearly, and in particular the importance of the vulnerabilities, and the role of government agencies with respect to them. Chapter 1 to Chapter 3 correspond to research sub-question 1.

Chapter 4 focuses on the vulnerability from an economic perspective. In this chapter the lifecycle and the intrinsic value of a vulnerability are introduced. This chapter corresponds to our research sub-question 2.

Chapter 5 focuses on the bug hunters and different markets they are facing. Here, white, grey and black markets are introduced and compared. Chapter 5 corresponds to research sub-question 3.

In Chapter 6 an auction model is applied to analyse the price of a vulnerability in the black market. This is a theoretical and technical chapter, corresponding to research sub-question 4.

Chapter 7 is an extension of the model in Chapter 6, which analyses the impact of government agencies' involvement in the black market. Chapter 8 discusses intensively the dilemma of governments. Chapter 9 studies the role of the government in the light of new challenges for cybersecurity. In these three chapters, research methods from economics (modelling) as well as law (legal reasoning) are applied to analyse the government and its policy for dealing with vulnerabilities. These three chapters correspond to research sub-question 5.

Chapter 10 studies the problem of vulnerabilities from the perspective of market failure. We check whether there is sufficient pressure from the market on the software vendor

in the case of severe cyber-attacks. An empirical event study is carried out and its results could act as a proof of a market failure. If market failure exists, regulation may be needed to address it. This chapter corresponds to our research sub-question 6.

Chapter 11 turns our focus on the software vendor. It examines the feasibility of holding software vendors accountable for vulnerabilities exploited in cyberattacks from the perspectives of contract law and tort law. A combination of tort negligence and regulation is recommended as the effective legal tool to reduce social risks. In Chapter 12, I establish an economic model to study how to set the amount of the administrative fine, recommended in the previous chapter, to be imposed on the software vendor. Research sub-question 7 is linked to these chapters.

Chapter 13 concludes with some policy recommendations, based on the discussion in previous chapters.

Chapter 2: Literature Review

Cybersecurity is a complex topic, which heralds a host of problems emerging with the rapid development of information technology and the globalization of markets. It is a problem for which the market may fail to produce a solution. In a social environment of positive transaction costs, every party tends to select a security level not necessarily in line with the socially optimal one. The software companies may lack adequate incentives to invest in security sufficiently if they do not fully bear the cost of security problems. Individual users may act inefficiently because they are short of accurate information. Thus, cybersecurity is a problem that requires interdisciplinary and transdisciplinary solutions, which can only be achieved through collaboration between stakeholders from different backgrounds. In this chapter, we will review several aspects surrounding the issue of cybersecurity and related existing literature.

2.1 Cybersecurity and cybercrime

Although cybersecurity is not a new topic in academic research, there are only a few articles addressing it from the perspective of law and economics. Kobayashi (2005) is one of those. He argues that security goods have the characteristics of public goods. His article examines the optimal level of cybersecurity as compared with traditional security and finds that it is not easy for the government to deter ex ante cybercrime by implementing a sufficient level of punishment. Since the probability of detecting cybercrime is very low, the penalty imposed must be of huge magnitude[26]. Kobayashi also finds that if measures are taken individually by companies which only protect themselves, instead of collectively acting to stop cyberattacks in the first place, this route will lead to an overproduction of private security. An underproduction problem will also occur if companies have incentives to free-ride on the public security produced by others. Thus, Kobayashi suggests that the government should encourage companies to collectively produce information by facilitating the development of security cooperatives, a collective security action supported by contractual restrictions on

[26] For the basic economic analysis of crime, see Becker (1968). According to Becker's deterrence theory, the probability that an offence is discovered and the offender apprehended, the size of the punishment, and the form of the punishment are three variables that influence the behaviour of criminals. The deterrent effect of criminal law is mainly determined by the product of the probability and the size of the punishment. In the case of cybercrime, if the probability of detecting the attacker is low, the penalty must be of large magnitude to create a deterrent effect.

members. Furthermore, he suggests policies that facilitate the sharing of information and an antitrust policy that takes into account such information sharing among companies.

In contrast with traditional crimes, cybercrimes have many more direct victims, impacting the lives of nearly all citizens and companies. It imposes a large economic burden on our society and the defence work differs greatly from the traditional methods of prevention and deterrence. The problem of cybersecurity is growing on a daily basis, so it is imperative to identify the nature of the problem and the most effective solutions for it. Software vulnerability, which is the necessary condition for cyberattacks, is an important topic and therefore requires special attention. However, literature clarifying the relationship between software vulnerabilities and significant cyberattacks is limited.

2.2 Software vulnerability

Although the trade of software vulnerabilities and their derivatives (exploits, i.e., programmed tools exploiting the vulnerability) is global and lucrative, there are not many academic contributions on this topic.

Algarni & Malaiya (2014) examine some of the most prolific discoverers of vulnerability located in Europe and the Far East, and suggest that a large percentage of vulnerability discoverers are not affiliated with software companies, and thus are free to disseminate their findings in any way they like. Multiple vulnerability markets have emerged as a result and many of them are not regulated. The paper identifies the actual vulnerability markets, as well as the motivation and methods of vulnerability discoverers. The authors explain that many of the discoverers appear to retire after a highly successful vulnerability-finding career because the reputation gained can bring them a more stable cash inflow. They also emphasize that the emergence of worldwide government agencies as vulnerability buyers has significant implications on vulnerability trades[27].

Researchers at RAND Corporation have made contributions to understand the

[27] In Chapter 7-9 of this thesis, we will discuss the role of government agencies in detail.

vulnerability markets as they exist in reality. Libicki, Ablon & Webb (2015) identify and compare white, grey and black markets for vulnerabilities[28]. Ablon, Libicki & Golay (2014) point out that the black market does not differ much from other typical criminal markets. It can be more profitable than the illegal drug trade because the distribution is accomplished electronically and worldwide. The link between market players is more direct because they can communicate, place orders, and get products through various channels. The black market is often linked with highly organized crime groups and state-backed hackers. The paper explains that the market for "zero-days", the most dangerous vulnerabilities, is a niche place of the black market and these vulnerabilities are also in demand in the legitimate grey market. The paper concludes that the underground market will continue to grow, innovate, and become more mature and relevant.

Herr (2017) discusses how to counter the proliferation of malware by targeting the lifecycle of the vulnerability in the US. Some states turn to export controls trying to block the international transfer of malicious software and limit its harmful effects. In fact, these export controls fail to check the transfer of malware because the motivations of those who develop and use this software are not taken into account. Furthermore, these controls undermine the efforts of legitimate security researchers to protect the public from cyber threats, because of the limitation on their research tools and capabilities. Herr proposes to raise the costs for cyber attackers by building and acquiring malicious software that depends on vulnerabilities. By reducing the time that a vulnerability is available for an attacker to use in the malware, the supply of vulnerabilities available to attackers is supposed to be reduced. This paper outlines four key activities to shorten the life cycle of vulnerabilities: expanding the accessibility of bug bounty programs by which individuals can receive recognition and rewards offered by websites, organizations and software developers for reporting bugs; reforming some pieces of federal law of the US; improving transparency about how long it takes software developers to issue security patches; and improving the transparency of patches for end-users.

[28] For detailed and complete information, please refer to Chapter 5 (section 5.4) of this thesis.

Some articles from the perspective of politics or ethics are based on interviews, discussions, and a summary of existing literature. Fidler (2015) analyses the U.S. domestic and international options for controlling the trade in zero-day vulnerabilities[29] and contributes to the growing debate about whether government agencies should disclose the vulnerabilities in their arsenals, and about the need to regulate the vulnerability trade. Some government agencies are claiming an entitlement to keep vulnerabilities (hence not disclosing them to the public) for some special purposes such as law enforcement or military needs. This phenomenon has been criticized by the public in the last decade. The author demonstrates that the regulation of the global vulnerability trade is difficult due to the pervasive politics in cyberspace. She concludes that domestically an increased executive branch oversight is the best national strategy to address the zero-day trade, and internationally voluntary collective action is the most feasible option. Since cyberspace is global, finding a solution to security problems in cyberspace requires global cooperation.

In terms of ethics, Egelman & Herley (2013) have made contributions. Their paper discusses ethical issues and implications related to markets for zero-day vulnerabilities and exploits.

Allodi, Shim & Massacci (2013) analyse the volume of attacks coming from vulnerabilities in the black markets, based on data they collected from Symantec's Data Sharing Programme WINE. They argue that the existence of black markets can be used as a proxy to estimate the final risk for a regular user. Furthermore, they propose to take vulnerability mitigation strategies based on the monitoring of black markets in order to improve cybersecurity.

In fact, the software vulnerability, as a kind of a secret, has its inherent intrinsic value. It is this intrinsic value that determines the inevitable existence of the relevant markets.

[29] A zero-day vulnerability is a flaw in a piece of software that is unknown to the programmer(s) or vendor(s) responsible for the application(s). In other words, the vulnerability has been discovered by someone who isn't directly involved with the project of the application(s). Because the vulnerability isn't known by the programmer(s) or vendor(s), there is no patch available. The term "zero" refers to the days between the time the vulnerability was discovered (by the programmer(s) or vendor(s)) and the first attack against it. After a zero-day vulnerability has been made public, it is then referred to as an n-day vulnerability, https://www.techrepublic.com/article/what-is-a-zero-day-vulnerability/ (retrieved on 1 December 2020)

There are always people who want to be aware of, and make use of, the secret, and are willing to pay for it. Although there is literature on the software vulnerability and its markets, no model has been established that discusses the value of the vulnerability. If there was an economic model explaining which variables have an influence on the market price of a vulnerability, policy or law makers would be better informed to make more reliable policies and laws focusing on those variables. This will be one of the contributions of this thesis.

2.3 Disclose or retain by the government

For law enforcement or intelligence purposes, government agencies may try to purchase vulnerabilities and keep them for their own purposes, especially those which are extremely dangerous - zero-days. The governments' participation in the trades for vulnerabilities raises concerns because many people think it will not only undermine public cybersecurity but also finance the underground market.

Swire (2004) develops a model for examining the choice between the open-source paradigm, which favours disclosure, and the military paradigm, which advocates secrecy, attempting to address the question of when disclosure may actually improve security. The paper specifies the factors that influence the decision about which security paradigm should be followed. It concludes that the following factors are relevant: "the extent to which attackers learn from previous attacks", "how easily attackers can exchange their knowledge", and "the total amount of cyberattacks". Swire argues that the traditional principle, according to which secrecy is always more likely to be effective, does not necessarily work in the realm of cybersecurity. This is because cyberattacks can be launched repetitively at little cost. By attacking the same target repeatedly, attackers are able to learn more and more secrets hidden by the defenders. Disclosure can often be an effective method to improve security by diverting cyberattacks, if the security level is perceived as high.

Bellovin, Blaze, Clark & Landau (2014) discuss the legality of hacking, i.e., is it legal for law enforcement authorities to use vulnerabilities for wiretapping in the internet? Law enforcement agencies complain about their loss of access to suspects' communications due to the progress of technology, and they require some complex

software specifically intended to create a security hole. The paper points out that this kind of eavesdropping capability makes wiretapping easier not only for law enforcement, but for everyone. However, legalized hacking of target devices through existing vulnerabilities in end--user software and platforms is mentioned as an alternative method. The exploitation of vulnerabilities will not stop. As long as eavesdropping remains an authorized inventory tool, even in the face of complex communication technologies, law enforcement agencies will seek ways to implement electronic surveillance, making use of vulnerabilities.

Herzog & Schmid (2016) examine the contradictory approaches of governments to manage zero-day vulnerabilities and related exploits. They argue that governments' participation in the market will finance the growth of the exploit market, thus leading to higher risks in the long run. Their discussions are based on a review and summary of the existing literature.

Mayer (2018) focuses on the similar issue of government hacking and examines how US federal law regulates government malware. The author argues that a faithful application of the Fourth Amendment principles implies that government hacking is inherently a search. Furthermore, reinvigorating super-warrant procedures and applying them to law enforcement hacking are also advocated. He concludes that government hacking is a legitimate and effective investigative technique, but appropriate procedural protections are required. According to the logic behind this article, if there is nothing inherently wrong with the government compromising computer systems, it should be no problem at all for government agencies to possess the related tools, i.e., the vulnerabilities.

Regarding the question of whether the government should retain vulnerabilities or disclose them, two articles - Herr, Schneier & Morris (2017) and Ablon & Bogart (2017) - study the issue from a new perspective: the rediscovery rate, which means how often vulnerabilities are discovered by multiple independent parties. If the likelihood of vulnerabilities being rediscovered is on average high, the government agency which holds vulnerabilities may not be the only one which knows of these secrets. So, the likelihood of these vulnerabilities' being used maliciously by other parties is also high.

In this case, it is socially risky for the government agency to keep vulnerabilities private - whereas a smaller overlap might justify retention.

Researchers from Harvard Kennedy School, Herr, Schneier & Morris (2017) address the issue of the rediscovery rate[30] by examining data sources of open-source software, including Chromium and the Android operating system. Their study finds that "the aggregate rediscovery rate for (their) dataset is 12.7%, ranging from 10.8% for Chrome between 2009 and 2017, to 21.9% for Android between 2016 and 2017. For Android and Chrome, more than 60% of all rediscoveries takes place in the first month after the original vulnerability's disclosure"[31].

In order to address a topic similar to vulnerability rediscovery - bug collisions, Ablon & Bogart (2017) from RAND team obtained rare access to a dataset of information about zero-day software vulnerabilities and constructed a sample matching what might be collected in the arsenal of intelligence or military community. They highlight two findings among several final results: "exploits and their underlying vulnerabilities have a rather long average life expectancy (6.9 years); for a given stockpile of zero-day vulnerabilities, after a year, approximately 5.7% have been discovered by an outside entity"[32].

The discrepancy between Herr, Schneier & Morris (2017) and Ablon & Bogart (2017) stems from differences in data sources. The former examines vulnerabilities from open-source software, which is a particular subset of the population of software. These vulnerabilities are not likely to represent the ones stockpiled by intelligence or law enforcement agencies. The dataset is more like a sample from the public domain. The latter use a dataset from a private organization, in which some of the vulnerabilities may already have been in use or for sale. This dataset represents more closely what an intelligence or law enforcement agency might have in their arsenal. It is not clear to what extent the vulnerabilities in these two articles are overlapping. In some ways, they

[30] The term of "rediscovery rate" refers to how soon another party finds the same bug independently after it was reported to the software vendor or obtained by the government. It shows how quickly a disclosed but unpatched vulnerability could be rediscovered by a malicious party and used to assault the related software. See Herr, Schneier & Morris (2017), p.7-8

[31] Herr, Schneier & Morris (2017), p.1

[32] Ablon & Bogart (2017), p.69

are complementary. The result of Ablon & Bogart (2017) may be more informative to analyse whether government agencies would, or should, disclose or retain vulnerabilities[33].

2.4 Liability related to vulnerabilities and cybersecurity

"Ship now, patch later" is one of the most universal philosophies in the commercial software industry[34]. Many people have come to believe that software is released and distributed so soon that there is not adequate time left for security checks. In addition, market dominance by a small number of companies is likely to compromise cybersecurity by creating a monoculture, a scenario in which more systems are vulnerable to the same software vulnerability. Picker (2004) addresses these issues. In this article, Picker suggests that concerns of cybersecurity can be remedied through the use of liability rules. However, imposing liability rules through ordinary tort law would not be sufficient, because it would be difficult to sort out problems of fault and causality relating to the software company, the attacker, and the victim who may also be negligent. In Picker's view, partial insurance is the most efficient solution which cares for the consumers using the early-stage product who may face greater risks. But this article does not tell us how to design such a partial insurance plan.

Goertzel (2016) focuses on lawsuits as a recourse for purchasers of defective COTS (commercial off-the-shelf) software, as opposed to software tailored according to a contract between the software developer and the user. The author discusses issues like whether such software is a product or a service and concludes that it is not easy for software users to sue the developer of flawed software relying on strict product liability or negligence rules in tort law. This article does not relate to liability in the case of cyberattacks.

Lichtman & Posner (2006) argue that although many security measures have been taken to address cybersecurity both publicly and privately, the existing measures are neither effective nor sufficient to address the harm caused by cybercrime, due to the difficulties

[33] In my opinion, such a decision involves a balancing of arguments. Law- or policy- makers should think about how to reduce the number of vulnerabilities for lawful purposes while keeping public cybersecurity robust. In Chapter 8 and Chapter 9 in this thesis, I will discuss this issue in detail.
[34] Goertzel (2016)

in identifying the perpetrators. Accordingly, the article proposes to publicly impose liability on Internet service providers (ISPs) for harm caused by their subscribers, which would hold third parties liable if they can take steps to voluntarily control the perpetrators. ISPs can be held jointly and severally liable for the spread of viruses. Class action lawsuits are applicable here if the individuals who suffered harm caused by a cyberattack are unable to bring an individual suit. The authors also emphasize their concern regarding the ineffectiveness of ISP liability in a globalized Internet environment. With the global reach of the Internet, and without the same stringent security laws, cyberattacks will be easily routed through countries with loose laws. Accordingly, global cooperation regarding cyberspace is particularly important.

2.5 Chapter summary

To summarize the above, there is very limited literature which analyses the issue of cybersecurity from the perspective of one of its components - software vulnerabilities.

Although scholars agree that vulnerabilities are valuable and there are also public or hidden markets for them, no economic model exists to analyse what are the factors influencing their market price. From the standpoint of a law maker, these factors provide precisely the information needed.

The role of the government in dealing with vulnerabilities needs to be viewed cautiously and comprehensively. Vulnerabilities are important not only in the context of public security, but also as a strategic source. In the existing literature, we find limited comprehensive and systematic analyses of the existing policies regarding the question of whether the government should disclose or retain vulnerabilities.

The existence of vulnerabilities reflects the fact that any software can contain flaws. The occurrence of cyberattacks proves that some of these flaws can be very dangerous. Should the problem of fatal flaws be addressed by solutions which are market based? Or do they need extra measures if some external conditions like a dominant market position hinder the functioning of the market? The existing literature does not seem to provide any concrete answers to these questions. It would be meaningful to understand this problem directly on the basis of theoretical and empirical analyses of the market.

The existing literature neither discusses the liability of defective software vendors in the case of cyberattacks, nor provides an economic model to help understand the related issues. However, such discussions or models would be very meaningful, because more and more cyberattacks are to be expected in the near future, especially with the trend of the IoT (Internet of Things). The influence of vulnerabilities in defective software will expand accordingly. A solution to hold the software vendor liable for its defective product in case of cyberattacks is as complex as to hold ISPs liable for the wrong actions of their subscribers. But the logic behind it is the same: There is merit in arguing that both of them in their positions can control and reduce the harm in cyberattacks.

Based on the existing contributions of scholars mentioned in this chapter, all the above are challenges faced by this thesis.

Chapter 3: Understanding Cyber Threats

In this chapter we are going to introduce two cases which can demonstrate the growing threats of cyberspace and the key role of vulnerabilities: the Stuxnet case and the WannaCry case. Unlike WannaCry, which was a global wide extortion cybercrime, Stuxnet was a cyberattack not for monetary interests but with the aim of physical destruction motivated by political interests. The Stuxnet event acted as a watershed in the history of how countries face threats in cyberspace, as it provoked sweeping changes in related policies and strategies.[35] It was the first indication that virtual coding could potentially destroy our physical world. Before Stuxnet, the virtual world and the physical world were thought to be completely separate.

3.1 Stuxnet case

Table 1: Summary of Stuxnet[36]

Timeframe:	2009-2010
Target:	Centrifuges[37] used in a nuclear plant in Natanz in Iran
Tool:	Stuxnet: a cyber weapon using four zero-day vulnerabilities[38] and infecting computer networks through USB drives.
Effects:	Successfully destroyed several centrifuges and set back Iran's progress in nuclear plan at least temporarily.[39]

Source: Baezner & Robin (2017), p.4

3.1.1 Background and chronology

Stuxnet was an advanced cyber-attack against an industrial control system, consisting

[35] Baezner & Robin (2017), p.5

[36] To know more about Stuxnet as a computer worm, refer to https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html (retrieved on 27 May 2021).

[37] A machine which purifies uranium in a nuclear facility.
See: https://fas.org/issues/nonproliferation-counterproliferation/nuclear-fuel-cycle/uranium-enrichment-gas-centrifuge-technology/centrifuge-works (retrieved on 1 December 2020)

[38] A zero-day vulnerability is a flaw in a piece of software that is unknown to the programmer(s) or vendor(s) responsible for the application(s). Because the vulnerability isn't known, there is no patch available. The term zero day refers to the days between the time the vulnerability was discovered (by the programmer(s) or vendor(s)) and the first attack against it. After a zero-day vulnerability has been made public, it is then referred to as an n-day vulnerability. See: https://www.techrepublic.com/article/what-is-a-zero-day-vulnerability/ (retrieved on 1 December 2020)

[39] Albright, Brannan & Walrond (2010)

of multiple zero-day exploits[40] used for the delivery of malware[41] that targeted and infected specific industrial control parts for the purposes of sabotaging an automated process.[42] Specifically, Stuxnet was able to continuously damage the centrifuges used in the uranium enrichment process in the Natanz nuclear plant in Iran during 2009 to 2010.[43] According to conservative estimates, about 1000 centrifuges in the Fuel Enrichment Plant (FEP) at Natanz were put out of control due to Stuxnet attacks, which set back Iran's nuclear progress successfully.[44] Stuxnet is widely regarded as the first cyber-attack to specifically target an industrial control system.[45] The Stuxnet event changed the world's attitudes, perceptions, and response patterns to software vulnerabilities, cyber-attacks, and cybersecurity.

Stuxnet happened against the background of Iran's nuclear scheme and its tense relationship with the USA.[46] The discovery of this cyber weapon raised awareness of cybersecurity issues all around the world, involving the participation of experts from several countries.[47] The chronology of related processes leading to the discovery of Stuxnet is as follows.

Table 2: Chronology of Stuxnet

Time	Events
06. 2010	A computer security firm in Belarus announced that it had discovered a computer worm[48] infecting Microsoft's Windows operating system, "using a vulnerability that had never been detected before".[49] Such a

[40] An exploit is a type of malware that takes advantage of vulnerabilities, which cybercriminals use to gain illicit access to a system (retrieved from https://www.malwarebytes.com/exploits/ on 1 December 2020); A zero-day exploit is the exploit that takes advantage of a vulnerability on the same day that the vulnerability becomes generally known. There are zero days between the time the vulnerability is discovered and the first attack. See Maurushat (2013)
[41] Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems (retrieved from https://www.malwarebytes.com/malware/ on 1 December 2020). Viruses, Trojans, spyware, and ransomware are among the different kinds of malware. (Retrieved from https://www.avg.com/en/signal/what-is-malware on 1 December 2020)
[42] Knapp & Langill (2015)
[43] Trautman & Ormerod (2018)
[44] Albright, Brannan & Walrond (2010)
[45] Knapp & Langill (2015)
[46] Baezner & Robin (2017), p.6
[47] *Id.*
[48] A computer worm is a standalone self-replicating program infecting and spreading to other computers through networks. See Collins & McCombie (2012).
[49] Gross (2011)

	discovery of a zero-day vulnerability is a substantial event. Among the more than twelve million pieces of malware discovered by antivirus experts every year, only fewer than a dozen pieces utilize a zero-day vulnerability.[50] Windows' zero-day vulnerability can be traded at a price of $100,000 on the black market because of its ability to be utilized for many nefarious purposes.[51]
07. 2010	Sergey Ulasen, the head of the Belarus security firm, alerted a number of authorities and then posted a report online informing the computer security industry about the worm, which was named "Stuxnet" by Microsoft later. Soon, one piece of troublesome information came to light: Stuxnet first appeared in June 2009, one year earlier, and its creator had modified the virus several times, secretly releasing at least three different versions before its discovery in June 2010.[52] In addition, researchers discovered that Stuxnet used four zero-day vulnerabilities instead of one, which was "unprecedented – one of the great technical blockbusters in malware history".[53]
08. 2010	The worldwide antivirus giant Symantec published a blog post and explained that the true purpose of Stuxnet was sabotage rather than espionage not seeking for any financial gain,[54] which was based on the observation that "of the 38000 initial Stuxnet infections, approximately 22000 were in Iran".[55] Meanwhile in Germany, Ralph Langner, an expert on Siemens PLCs (programmable logic controllers) came to a startling conclusion: "a well-funded organization, most likely a government with precise knowledge of its target, had written Stuxnet".[56]
11. 2010	The enrichment process of uranium in the nuclear plant of Natanz was completely stopped without any obvious reason.[57] Soon after Iranian experts admitted that Iranian nuclear installations were infected by a

[50] Zetter (2011)
[51] Gross (2011), Trautman & Ormerod (2018)
[52] Zetter (2011)
[53] *Id.*
[54] *Id.*
[55] Trautman & Ormerod (2018)
[56] *Id.*
[57] Farwell & Rohozinski (2011)

	computer virus.[58]
12. 2010	A US-based non-profit institution, the Institute for Science and International Security (ISIS), confirmed that "the Stuxnet worm is programmed to target elements configured in the same manner as the Natanz centrifuges".[59] A preliminary assessment paper for this Institute asserted that "Iran's centrifuges, ……, could have suffered from a systemic problem in manufacturing components or assembling centrifuges, leading to large-scale breakage in late 2009 or early 2010.[60]
01. 2011	The New York Times published a long story suggesting "that Stuxnet was a covert United States intelligence project to undermine Iran's efforts to make a nuclear bomb of its own".[61]

Source: Excerpted from Baezner & Robin (2017)

3.1.2 Stuxnet Features

This piece of malware, Stuxnet, surprised security experts worldwide due to its sophistication which required considerable resources in manpower, time and finance. First, it was believed that the development of Stuxnet must have required a team of five to ten programmers working full-time for at least six months[62]. Second, several different programming languages with encrypted components were used in coding[63]. Third, Stuxnet exploited four zero-day vulnerabilities instead of a single one[64]. Normally a Microsoft Windows zero-day can fetch about $100,000 on the black market because of its ability to be employed for a number of criminal purposes[65].

Stuxnet had two destructive effects. On the one hand, Stuxnet could secretly wear down and ultimately crack the centrifuge rotors used in the uranium purification facility, because the malware was able to manipulate the speed of rotors running at an abnormal rate; on the other hand, the uranium produced in the process were impure and unsuitable

[58] Albright, Brannan & Walrond (2010)
[59] Baezner & Robin (2017)
[60] Albright, Brannan & Walrond (2010)
[61] Broad, Markoff & Sanger (2011)
[62] Chen & Abu-Nimeh (2011), p. 92
[63] Chen (2010), p. 3
[64] Naraine (2010)
[65] Gross (2011)

for use because the centrifuges were not running at a fixed rate, but rather a variable one[66].

Furthermore, Stuxnet used a two-phase attack including a delivery phase and an attack phase, which was very well-designed. The central control and supervisory system of the Iranian nuclear enrichment program was the so-called SCADA (supervisory control and data acquisition) system, manufactured by the German company Siemens. The purpose of Stuxnet was to enter the SCADA system first, then to cause the malfunction in the centrifuges. Like many sensitive and secret systems, the SCADA system was not directly connected to the internet for the purpose of security. By creating a measure called "air gap", operators ensured that the system was isolated from the external internet. To bridge this gap, in the delivery phase Stuxnet exploited Microsoft Windows vulnerabilities and prepared the Windows operating system as a platform for the next phase. In the attack phase, as long as there was some interaction between the infected Windows system and the protected SCADA system, perhaps using a USB stick, the malware was able to jump from the Windows platform to infect the SCADA system. After successfully completing these two phases, Stuxnet managed to manipulate the speed of centrifuges and bury a pre-recorded series of false data reports in the SCADA system, which led the operators to think that all the centrifuges were running at a fixed speed[67].

3.1.3 Implications of Stuxnet

The Stuxnet event was a sign of a changed world, which showed us that virtual codes could be designed to destroy the real physical world: from sabotaging a very precise piece of industrial equipment, to even threatening human lives. In this case, even "air-gapped" networks were at risk.

The Stuxnet case also reveals the fact that the success of cyber-attacks lies in the exploitation of vulnerabilities. The malware exploited four zero-day vulnerabilities, the most valuable vulnerabilities, to achieve its purpose: one concerning connecting USB sticks; one concerning the connection with the shared service of printers; the other two

[66] Rosenzweig (2013), p. 5
[67] Rosenzweig (2013), p. 3-5

concerning privilege escalation, which allowed the malware to execute software even in computers which had restricted access[68]. According to Baezner & Robin (2017), no modified versions of Stuxnet have been found since 2010. One important reason is that no new zero-day vulnerability has been found for modifying the old version of Stuxnet[69]. But if there is an active black market of vulnerabilities, then the situation is much less optimistic.

Attribution in cyberspace is much more difficult than in the real world. Even today the identity of the real attacker in the Stuxnet case cannot be confirmed. Several experts claimed that both the evidence and the motive pointed to the USA and Israel as the hidden attackers[70]. They have asserted that only a state could have developed such a complex and resource-consuming malware and it was specifically designed to target the nuclear facilities in Natanz in Iran[71]. However, it is very difficult to prove these allegations because all the cyberattacks are operated covertly.

3.2 WannaCry case

Table 3: Summary of WannaCry

Timeframe:	12. 05. 2017
Target:	Worldwide computers running outdated versions of Microsoft Windows operating system[72]
Tool:	Ransomware WannaCry; and EternalBlue, a well-designed tool to exploit an unknown vulnerability in the Microsoft Windows operating system to gain access to it[73]
Effects:	This cyber-attack infected more than 230,000 computers worldwide and cost computer users thousands of dollars in ransom money and billions in lost productivity[74]. It hit not only Britain's National Health Service (NHS) but also Russia's interior ministry, many Chinese universities, Germany's state railways and many more

[68] Naraine (2010)
[69] Baezner & Robin (2017)
[70] Lindsay (2013), p. 366; Nakashima & Warrick (2012); Zetter (2011), Baezner & Robin (2017), p. 8
[71] De Falco (2012)
[72] The Economist (2017e)
[73] *Id.*
[74] The Economist (2017c)

	various companies[75].

3.2.1 Background and chronology

The WannaCry cyber-attack happened on May 12, 2017. By exploiting a vulnerability in old versions of Microsoft Windows, the ransomware WannaCry encrypted data in the infected computers blocking customers from their data unless they could pay a ransom using Bitcoin[76]. WannaCry started first in the United Kingdom and Spain, then spread globally quickly, and affected hundreds of thousands of victims in at least 150 countries[77].

The successful invasion of WannaCry was attributed to the incorporation and use of EternalBlue, a tool exploiting the vulnerability in the Microsoft Windows system.

It was NSA who discovered the vulnerability and developed EternalBlue. Later, EternalBlue was stolen by a hacker group called Shadow Brokers from the U.S. National Security Agency and released online thereafter. After the theft was publicly reported, on March 14, 2017, Microsoft released a security update (MS17-010 advisory) to patch this vulnerability[78]. However, Microsoft did not specify this flaw until April 14, 2017, when the Shadow Brokers released a set of exploits including EternalBlue online[79].

Although Microsoft had released patches previously to fix the vulnerability, many organizations had either not applied these patches soon enough or were using old Windows systems which were past their life-expectancy date on the day WannaCry was launched in May 2017. As a result, many computers remained unpatched globally, including in hospitals, businesses, government offices, and many home use computers[80].

---

[75] The Economist (2017c)
[76] Please refer to footnote 3.
[77] Ransomware cyber-attack threat escalating – Europol (14 May 2017), BBC News (retrieved from https://www.bbc.com/news/technology-39913630 on 1 December 2020)
[78] Brad Smith (President of Microsoft), The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack (May 14, 2017) (retrieved from https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/ on 1 December 2020).
[79] Sean Michael Kerner, WannaCry Ransomware Attack Hits Victims with Microsoft SMB Exploit (May 12, 2017) (retrieved from https://www.eweek.com/security/wannacry-ransomware-attack-hits-victims-with-microsoft-smb-exploit on 1 December 2020).
[80] *supra* note 78

The chronology of the whole event is as follows:

Table 4: Chronology of WannaCry

Time	Events
Before 03. 2017	For years, a flaw, nicknamed "EternalBlue", in the Windows operating system had been used by the U.S. National Security Agency for the purpose of espionage. But the NSA didn't inform Microsoft about the flaw in its software until March 2017, after EternalBlue had been stolen by an outsider[81].
03. 2017	EternalBlue was stolen from the National Security Agency (NSA), America's electronic-spying outfit, by a hacking group "Shadow Brokers". Only after the theft did the NSA inform Microsoft of the flaw, leading the firm to rush out a fix[82].On March 14, 2017, Microsoft issued security bulletin MS17-010, which detailed the flaw and announced that patches had been released for all Windows versions that were currently supported at that time[83].
04. 2017	The hacking group calling itself "Shadow Brokers" released the cyber weapons stolen from NSA online, including EternalBlue[84].
05. 2017	It was on May 12th, 2017, that a piece of malicious software known as WannaCry spread across the internet. It demanded a payment in bitcoin to make it disappear, exploiting a vulnerability in the outdated Microsoft Windows system discovered by the NSA and then leaked online by Shadow Brokers. Within just one day the malware was reported to have infected more than 300,000[85] victims in at least 150 countries[86]. It caused disruption to Britain's National Health Service, Russia's interior ministry, Chinese universities, Germany's state railways and many

[81] Kshetri (2017)
[82] The Economist (2017c)
[83] Goodin (2017)
[84] *Id.*
[85] Kshetri (2017)
[86] Ransomware cyber-attack threat escalating – Europol (14 May 2017, BBC News) (retrieved from https://www.bbc.com/news/technology-39913630 on 1 December 2020).

	others[87].
08. 2018	A new variant of WannaCry attacked Taiwan Semiconductor Manufacturing Company (TSMC), causing several of its chip-fabrication factories to shut down temporarily. The malware attacked about 10,000 machines in TSMC's most advanced facilities[88].

3.2.2 WannaCry Features

In the WannaCry case, a software vulnerability had again become a key factor in determining the success of a cyber-attack. EternalBlue exploited a vulnerability discovered in the so-called Server Message Block, a piece of Microsoft Windows, which helps networking between computers. This vulnerability first appeared in Windows XP in 2001 and then remained hidden in all the following Windows versions. It helped WannaCry spread rapidly from computer to computer, as long as they were connected to the internet and had one specific port[89] (port 445) open[90].

WannaCry combines two kinds of malware. One is known as a worm, which is a type of malicious software whose primary function is to infect other computers while remaining active on the infected systems[91]. In short, a worm is designed to spread from computer to computer. The other is the encrypting ransomware, which is delivered by the worm. This ransomware encrypts the data on the hijacked computers, charging victims a ransom to restore access to their data. These two kinds of software are very different in terms of coding level. According to Check Point, a computer-security company in Israel, WannaCry's encryption software is very badly assembled, and it is practically impossible to decrypt a victim's data after the ransom has been paid. However, in contrast to the encryption software, WannaCry's worm, which spread itself very fast, is a very sophisticated piece of coding. It is because the piece of coding reuses the software EternalBlue stolen from America's National Security Agency (NSA). The EternalBlue part made WannaCry so threatening because a single click is able to infect

[87] The Economist (2017c)
[88] Kumar (2018)
[89] Through a series of ports, normally 1024 of them, computers manage their connections to one another. Each port is assigned a specific sort of task and can be opened and closed as needed.
[90] The Economist (2017e)
[91] Retrieved from https://searchsecurity.techtarget.com/definition/worm on 1 December 2020.

an entire network[92].

3.2.3 Implications of WannaCry

The role of the government is worth thinking about. In the WannaCry case, it is the NSA which discovered the vulnerability in Windows and designed the tool to exploit it. It is unclear how long the NSA had known about the vulnerability and kept it secret[93]. Only after the theft did the NSA inform Microsoft of the vulnerability, leading the software company to rush out a fix. Microsoft accused the NSA of losing control of the cyber weapon EternalBlue, the digital equivalent of a cruise missile[94]. This case is an example of the double-edged nature of government. On the one hand, for the intelligence services to spy on organized criminals and terrorists, intelligence agencies like the NSA and FBI prefer to leave the vulnerability open and keep it secret; on the other hand, given the rising costs of public security and cyber security, the government has the responsibility to share vulnerabilities with the software company so that it can be remedied as soon as possible. "When computers are ubiquitous, security is too important not to fix"[95].

The responsibility of software companies is another aspect worth considering. The targets of the WannaCry attack were the computers using an outdated version of the Microsoft operating system. In order to gain possibly more market share, software companies are constantly introducing new versions of software. At the same time, the old versions of the software are no longer serviced. Generally, all versions of software have a too short end-of-life. Let's take Windows 10 for example.

Table 5: Windows 10's end of service dates (reduced version)

Windows 10 version history	Date of availability	End of service for Home, Pro, Pro Education, and Pro for Workstations editions	End of service for Enterprise and Education editions

[92] The Economist (2017e)
[93] *Id.*
[94] Brad Smith (President of Microsoft), The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack (May 14, 2017) (retrieved from https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/ on 1 December 2020).
[95] The Economist (2017c)

Windows 10, version 1909	November 12, 2019	May 11, 2021	May 10, 2022
Windows 10, version 1903	May 21, 2019	December 8, 2020	December 8, 2020
…	…	…	…
Windows 10, version 1507	July 29, 2015	May 9, 2017	May 9, 2017

Source: Microsoft official website[96],

From the table above, we can see that for each version of the Windows 10 operating system, the expected service lifetime, from the date of availability to the date of end of service, is no more than three years. In our case, although Microsoft had released patches previously to remedy the vulnerability, by the day WannaCry was launched in May 2017 many organizations either had not applied these patches in such a short time or were using old Windows systems which were past their end-of-service date.

The WannaCry case can be considered as an alarm to everyone. Companies, users, and governments all need to wake up to the dangers of the cyber world, to be vigilant, especially to install patches in time, and to enhance cyber security awareness. Cyber-attacks are not new, but after WannaCry they should be taken more seriously.

For a user, the priority of cyber security is vulnerability management. In August 2018, more than one year after the worldwide cyber-attack WannaCry, a new variant of WannaCry forced Taiwan Semiconductor Manufacturing Company (TSMC), Apple's sole wafer supplier, to temporarily shut down several of its chip-fabrication factories. More than one year after the patch for the vulnerability exploited in WannaCry was released, one Windows 7 computer, which was installed on the internal network of TSMC, had still not had the patch installed, and became infected by the malware. As a result, the new variant of WannaCry spread to 10,000 machines in TSMC's most advanced facilities. The disruption had a dramatic effect on the company's financial performance, with a two-percent drop in its third-quarter revenue, nearly $170 million.

[96] Retrieved from https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet on 1 December 2019.

It is a good lesson in vulnerability management[97]. As long as vulnerabilities are not patched, the system is under potential attack by the existing malware and their variants.

3.3 Summary of Stuxnet and WannaCry

Based on the analysis of the two cases above, the following points can be summarized: The first is the impact of software vulnerabilities on the effectiveness of cyber-attacks. In both cases, zero-day vulnerabilities are involved. In the Stuxnet case, four zero-day vulnerabilities were exploited, so the malware was hidden deeply for a long time and the destruction wide-spread. In the WannaCry case, although the information related to the zero-day vulnerability had been revealed to the software company shortly before the attack, there were still many victims who had not fixed the flaw in time because of the very short interval between the announcement of the patch by the software company and the real attack.

Another alarming truth is that the current technological environment is exacerbating the consequences of cyber-attacks. Nowadays, we are in a new era of the internet of things (IoT). A modern auto is like a computer with four wheels and a plane is like a computer with two wings. More things are becoming vulnerable when computers are widely implanted into everything from cars and planes to pipelines and electricity grids. Today ransomware can encrypt your personal data in the computer, and tomorrow it will be possible to lock your body in the computerized car. In this context a computerized world and Internet of Things, cyber-attacks, which may previously have seemed to be of low-probability and high-impact, are becoming more and more high-probability and high-impact events[98]. The targets of cyber-attacks will include most likely smart grids or pipeline systems, which rely heavily on modern computers. Cyber-attacks on infrastructure will have an irreversible impact on the whole society.

The third point is the role of government intelligence services, like NSA or CIA. We have found that in both cases above, the key factor of a successful cyber-attack ultimately can be credited to the part of codes developed or funded by government

[97] TSMC WannaCry Hits OT Plants with a Hefty Price Tag
(Retrieved from https://www.skyboxsecurity.com/blog/tsmc-wannacry/ on 1 December 2020).
[98] The Economist (2017c)

agencies. The software written by the hacker himself to exploit vulnerabilities is not comparable with the one developed by a government-funded team. The government has the responsibility to protect public security, whereas it also has the duty to fight organized criminals and terrorists. In any case, what is most important is that the government should manage its cyber tools and cyber weapons more effectively, rather than allow those to be stolen by hackers.

Furthermore, it is very instructive to think about the social responsibility and product liability for the software developer, as well as the timely security measures taken by the users to repair vulnerabilities. With the existence of the black market for cyber weapons, vulnerability information and related malware will be circulated globally because of the extremely low cost to duplicate and spread, which makes cybersecurity a long-term topic to deal with seriously.

Last but not least, we see the world is changing drastically. Malware is no more merely a mischief limited within the cyber space. The virtual world is penetrating into the physical world. A cyber weapon coded by 0s and 1s can have a physically destructive impact on the real world. Like a missile, it can smash from household appliances to large infrastructure networks.

3.4 Chapter summary

The Stuxnet case and the WannaCry case are two landmarks in the history of cybersecurity. Stuxnet marks a point on the time dimension since the virtual world started to change the physical world directly; and WannaCry constituted the beginning of the booming ransomware cyberattacks worldwide.

From these two cases, we learn the significance of software vulnerabilities, especially the zero-days, to our cybersecurity. They highlight the roles of the governments, consumers, and software companies, as well as their social responsibilities. All these issues will be discussed in turn in the following chapters.

Chapter 4: The Vulnerabilities

As shown in chapter 1, continuously growing and increasingly devastating cyberattacks are prefiguring a host of new problems in today's social environment dominated by information technology, network interconnection, and the expanding globalization of the IoT (Internet of Things). Software vulnerabilities, as by-products of software programming, act as critical ingredients by, in the course of cyberattacks, posing threats to our cybersecurity. By exploiting vulnerabilities, hackers are able to facilitate better crafted cyberweapons, get around system defences, and initiate more effective attacks. Managing these vulnerabilities well has become a key component in the protection of cybersecurity. In this chapter I will study the vulnerability itself. I will start from the definition of vulnerability and its exploit, and then discuss its lifecycle and intrinsic value.

4.1 Vulnerabilities and exploits

4.1.1 The vulnerability

A vulnerability refers to a weakness in a system that can be utilized by an attacker to damage the system, obtain unauthorized access, execute arbitrary code, or otherwise exploit the system[99]. In other words, vulnerability is a piece of information which leads a system to be susceptible to a threat[100]. In the public media, the term "bug" is frequently used interchangeably with "vulnerability"[101]. As to disclosure or knowledge about vulnerabilities, there are several vulnerability repositories that provide interested parties with easy access to information regarding them[102]. The most prominent ones are CVE[103], NVD[104] and OVAL[105].

[99] Knapp & Langill (2015), p. 424
[100] Maurushat (2013), p. 77
[101] According to Grimes (2017), on average 5000-6000 new vulnerabilities are publicly announced every year. See Grimes (2017), p. 39
[102] Retrieved from the official website of The European Union Agency for Cybersecurity (https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits) on 2 December 2020.
[103] Common Vulnerabilities and Exposures, which is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). CVE offers a list of entries for publicly known cybersecurity vulnerabilities. Each entry of the vulnerability contains an identification number, a description, and at least one public reference (retrieved from https://cve.mitre.org/ on 1 December 2019).
[104] National Vulnerability Database, which is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics (retrieved from https://nvd.nist.gov/general on 1 December 2019).
[105] OVAL, Open Vulnerability and Assessment Language, is an open vulnerability repository sponsored by a non-profit entity CIS (Center for Internet Security) (retrieved from https://oval.cisecurity.org/repository on 1 December

Not all the vulnerabilities are known and the unreported ones, which are unknown to either software vendors or users, are the most critical to cybersecurity. These vulnerabilities are called "zero-day vulnerabilities" or simply "zero-days". Zero-day vulnerabilities are vulnerabilities that have not been publicly disclosed and are kept private[106]. A zero-day vulnerability has the potential to be exploited by cybercriminals because it exposes the program to external manipulation. Zero-day vulnerabilities exist not only in commonly used software, including Microsoft or Apple products, but also in some special software running critical infrastructure[107], such as smart grids. By exploiting a zero-day vulnerability, the probability of success of a cyber-attack will increase drastically, like using a secret weapon, because both the software maker and the software user are unaware of the coming threat. Therefore, this kind of vulnerability is of great value on the black market. For example, by the time the cyber-attack Stuxnet occurred, a Windows' zero-day could already fetch as much as $100,000 on the black market[108].

4.1.2 The exploit

To create an exploit is the next step after finding a vulnerability. An exploit is the offensive software code that takes advantage of the known vulnerability. It is written either by security researchers as a proof of an existing security threat or by attackers for use in their malicious operations[109] like illegal access, monitoring, stealing data, damaging the target system, etc.

It is often seen that exploits are incorporated into malware, being used as part of multi-component attacks, allowing an intruder to remotely access and gain elevated privileges into vulnerable computers. With the privileges of secret access, exploits can implant different malicious codes, for instance, some backdoor codes or spyware which can steal information from the infected systems.

2019).

[106] Retrieved from the official website of The European Union Agency for Cybersecurity (https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits) on 2 December 2020.

[107] Fidler (2015)

[108] Gross (2011)

[109] Retrieved from https://www.trendmicro.com/vinfo/us/security/definition/exploit on 2 December 2020.

When an exploit is used to leverage a zero-day vulnerability, it is referred to as a zero-day exploit.

4.1.3 Relationship between a vulnerability and its exploit

A vulnerability is merely a piece of information, whereas an exploit is the tool to leverage this information. Exploits are weaponized vulnerabilities written by skilled programmers, including lines of codes as well as sequences of commands. For simplicity, an exploit can be regarded as a combination of knowledge about a vulnerability and offensive codes based on it. For the same vulnerability, a programmer can write different codes for different purposes. Thus, for one vulnerability, there are several possible exploits. From the perspective of law, it is possible to treat the exploit as a wrongdoing whereas it is impossible to do the same for the vulnerability.

It is important to mention here that the term "exploit" is often misused by the public or mass media to refer to both the knowledge of the flaw which is the vulnerability, and the set of codes exploiting the knowledge which is the exploit. However, the distinction between "vulnerability" and "exploit" is crystal clear. Furthermore, the motivation for searching a system flaw and the motivation for making use of it are completely different in many cases.

4.2 Inevitability, lifecycle, and intrinsic value

4.2.1 Vulnerabilities are inevitable

Because vulnerabilities are by-products of programming, it is almost impossible to completely avoid vulnerabilities during the process of coding for two main reasons.

First, it is human beings who write the source code. Every programmer can make mistakes. Sometimes the mistake is a small logical negligence and sometimes it may be just an input error. According to Steve McConnell, a programming guru, on average people make between 15 to 50 errors in every thousand lines[110]. Careful checking in big software companies can push the number down to nearly 0.5 in every thousand

[110] Retrieved from https://labs.sogeti.com/how-many-defects-are-too-many/ on 2 December 2020. Industry Average: about 15 – 50 errors per 1000 lines of delivered code. This is known as the defects per KLOC (1000 lines of code).

lines[111]. In practice, the possible reduction in the number of vulnerabilities is limited[112]. However, it is possible but not economical to completely avoid vulnerabilities. For example, there are no known defects in the Space Shuttle Software of NASA, which is at the cost of thousands of dollars for every line of code (which does not rule out completely the existence of a vulnerability even then). No commercial software vendors can afford the same level of testing as NASA[113].

Second, the source code of most common programs is incredibly long. The following table gives a rough idea about how many lines compose the programs listed there. The longer the lines of code, the more complicated the problem of the potential vulnerabilities. Not only do the kinds of defects increase with program size, but also the number of defects. According to the software construction handbook, when a software product grows twice as large, it is likely to have more than twice as many vulnerabilities[114].

Table 6: The length of different Programs' Code

Program	Number of lines of code
Google (all products)	2billion
Linux (open source, as of 2015)	20.3million
Windows	50million
Android	12million

Data Source: The Economist April 8th, 2017: Why everything is hackable

From the two reasons above, it is nearly impossible to eradicate the risk of rising vulnerabilities in millions of lines of code before the users begin to use the code. In the recent era of the internet, we rely more on web applications than isolated computer applications. In 2019, Trustwave, a security research firm, reported the facts[115]:

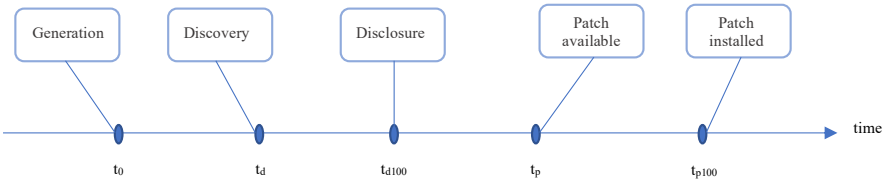
[111] McConnell (2004), p. 521; "Microsoft Applications: about 10 – 20 defects per 1000 lines of code during in-house testing, and 0.5 defect per KLOC in production" (retrieved from https://labs.sogeti.com/how-many-defects-are-too-many/ on 2 December 2020).
[112] The Economist (2017d)
[113] Retrieved from https://labs.sogeti.com/how-many-defects-are-too-many/ on 2 December 2020.
[114] McConnell (2004), p. 652
[115] 2019 Trustwave Global Security Report, Retrieved on 31 December 2019, from https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/

1) 100 percent of the web applications tested contain at least one vulnerability.
2) The median number of vulnerabilities detected per application in 2018 was 15, which was 11 in 2017. The largest number of vulnerabilities found in a single application was 38.
3) 9 percent of the vulnerabilities Trustwave detected were classified as high risk or critical. Of more than 45,000 vulnerabilities uncovered in 2018, high-risk vulnerabilities accounted for 7 percent and 2 percent were identified as critical.

4.2.2 A vulnerability's lifecycle

To better understand the vulnerabilities, Figure 1 presents a vulnerability's lifecycle[116], which starts from the generation of a vulnerability to the installation of the patch for it.

Figure 1: A vulnerability's lifecycle



The vulnerability's lifecycle can be divided into different phases by distinct events. As shown in the figure above, there are five significant events on the timeline: generation, discovery, disclosure, patch available, and patch installed, with corresponding timepoints marked as: t_0, t_d, t_{d100}, t_p, t_{p100}. It should be noted that the distances between different timepoints on the timeline do not correspond to the actual time interval between different events.

At timepoint t_0, a vulnerability is generated and shipped together with its corresponding software to end-users. Nobody knows the existence of the vulnerability. The subscript "0" of "t_0" refers to the beginning of the vulnerability lifecycle.

At timepoint t_d, the vulnerability is discovered either internally, by the software vendor

[116] This figure is adapted from the illustration by Frei (2013). In my opinion the exploit part in the original illustration is more like a derivative of a vulnerability than a part of the vulnerability lifecycle per se, so the exploit part is not included here.

itself, or externally, by anyone who is outside the software vendor, who is often called "a bug hunter". The subscript "d" of "t_d" refers to the event of discovery.

At timepoint t_{d100}, the vulnerability is disclosed publicly. This disclosure is done either by the outside discoverer, or by the software vendor, after having discovered the vulnerability or having received a vulnerability report from the outside discoverer. As from that point, the vulnerability information is not a secret anymore. It is known by all the interested parties, including the software vendor, software end-users, as well as all the potential cyber-attackers. The subscript "d100" of "t_{d100}" refers to the combination of the event of disclosure and the meaning of "100% known to the public".

At timepoint t_p, the patch for the vulnerability, which is developed and released by the software vendor, is available to all the software users and the public. The subscript "p" of "t_p" means that the patch for the vulnerability is available thereafter.

At timepoint t_{p100}, all the systems with this vulnerability are patched. This is the end of the vulnerability lifecycle. Before this timepoint, although the patch is already available, not all the users have the vulnerability patched. The risk of the vulnerability is still there to the systems without patch. The subscript "p100" of "t_{p100}" means that not only is the related patch available, but also all the users have the vulnerability patched.

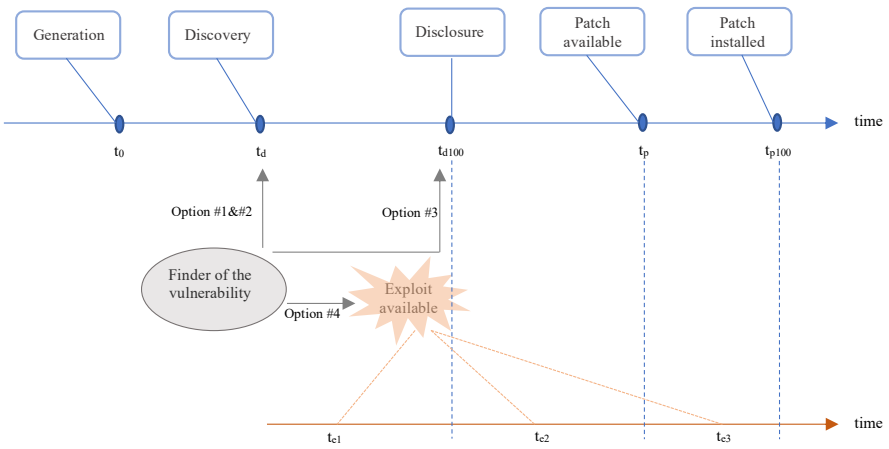
Based on the figure of a vulnerability's lifecycle, the available options of the vulnerability finder, can be clearly illustrated, as shown in Figure 2.

The way the vulnerability information is treated or managed is dependent on who is the vulnerability finder. The vulnerability can be reported to the software vendor, traded on the market, or disclosed online, etc. It seems unlikely that the bug hunter will merely keep the secret of the vulnerability to himself and do nothing at all. Doing nothing makes no sense because there is no guarantee that the same vulnerability will not be discovered by other parties. As time goes by, the likelihood of independent discovery of this vulnerability increases[117]. In general, there are four options available for the bug

[117] Frei (2013)

hunter once he has found a vulnerability: coordinated disclosure, taking the product vendor's bug bounty, full disclosure, and selling the vulnerability information or its derivative exploits[118]. The four options are illustrated in Figure 2.

Figure 2: Options of the vulnerability finder



Within option 1 and option 2, the vulnerability information flows into the knowledge of the product vendor. Option 1 is called "coordinated disclosure", in which the newly discovered vulnerability information is privately disclosed to the vendor of the affected software. Alternatively, the bug finder can also disclose the information to a national CERT program, the Community Emergency Response Team (CERT) program[119], or to another vulnerability program coordinator, so that the affected product vendor will be informed in time. Given the opportunity to analyse the vulnerability, the vendor can update the software before the detailed information of the vulnerability is publicly disclosed. When releasing the update, the software vendor recognizes the bug finder publicly for reporting the critical information.

Option 2 is the choice of the bug finder – to demand financial compensation in exchange for disclosure, when the affected software vendor provides a bounty program, a kind of incentive to bug finders. In contrast with coordinated disclosure, in which scenario the finder privately reports his finding to the software company to push the company to

[118] *Id.*
[119] Retrieved from https://www.ready.gov/cert on 1 December 2019.

initiate the related security patch as soon as possible, the bounty program is supposed to satisfy those bug hunters who expect financial compensation[120].

Option 3 is called "full disclosure". In this case, the vulnerability information flows instantly to the public. The finder discloses the vulnerability to all interested parties, publicly reminding everyone to be vigilant. When the software vendor is not responsible for its product or the software is not technically supported by its developer anymore, full disclosure motivates some defensive measures for potential cyberattacks. The disadvantage is that the potential attackers know the vulnerability information as well.

Option 4, selling, is another option for a bug hunter when he finds a vulnerability. He can sell either the information itself or its derivative, the exploit, to potential buyers, either directly or through a broker. The related markets will be introduced in chapter 5. Typical buyers are, for example, government agencies, cybersecurity companies for testing purpose, specialized companies as middlemen for the lucrative business of vulnerabilities or exploits, cyber criminals, etc.

If the finder is able to make an exploit from the newly found vulnerability, it is possible that he will sell the exploit. This is because an exploit has a longer period of value than its corresponding vulnerability. As a secret, the vulnerability information becomes worthless once it is publicly disclosed. An exploit has its value throughout its lifecycle. We analyse this issue with three possible scenarios in which an exploit is available, with corresponding timepoints of t_{e1}, t_{e2}, t_{e3}, as shown in Figure 2. The subscript "e" here stands for "exploit" and the numbers "1, 2, 3" refer to scenario 1, scenario 2, and scenario 3, respectively.

In scenario 1, the possible timepoint of exploit available t_{e1} is before the timepoint of disclosure t_{d100}, which means the vulnerability information is still unknown to most of the users. The exploit taking advantage of the vulnerability is most dangerous because

[120] It has often been reported in recent years that the bounty amount offered by software vendors is too low to provide incentives to bug finders, as indicated by the example of Apple (retrieved from https://www.vice.com/en_us/article/gybppx/iphone-bugs-are-too-valuable-to-report-to-apple on 2 December 2020).

of the unconsciousness and unawareness of most of the attack targets. The probability of success for a cyberattack is the highest, so the exploit is most valuable at timepoint t_{e1}.

If an exploit is not completed before, but after the disclosure time of its vulnerability, the timepoint when the exploit is available is t_{e2} in Figure 2, corresponding to our scenario 2. In scenario 2, because t_{e2} is before the patch available timepoint t_p, the probability of success of an attack using this exploit is still high, although some protection measures have been taken by some users after disclosure.

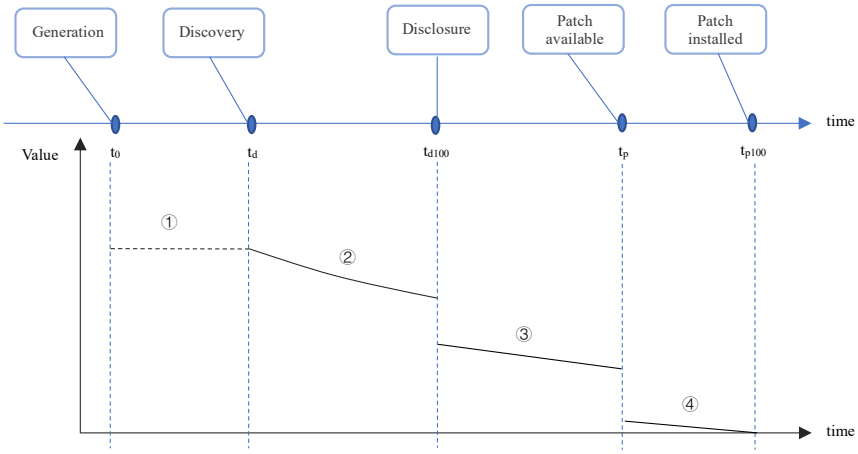
t_{e3} refers to the timepoint when an exploit is available after the affected vendor has released the patch. The exploit is still worth something because not all the users get the related vulnerability patched. The probability of success of a cyberattack is lower than in scenario 1 and scenario 2, but it is still positive. Only after all the users have the vulnerability patched in their systems, the corresponding exploit loses its value for direct attack.

4.2.3 Intrinsic value

As any kind of secret, the vulnerability information is born with its intrinsic value. Its intrinsic value depreciates as time goes by because the probability that the same vulnerability will be discovered by another party increases. A vulnerability loses its intrinsic value drastically when it is fully disclosed. A cyberattack exploiting the vulnerability can be understood as a passive disclosure if the vulnerability has never been disclosed before. Figure 3 illustrates the intrinsic value of a vulnerability. The critical timepoint t_{d100} refers to the disclosure event, which is the same as in Figure 1 and Figure 2. Before the first discovery timepoint t_d, the line is a dash line ①. This is because although the intrinsic value of the vulnerability exists, nobody discovers it. The explicit form of the line of intrinsic value starts from the timepoint t_d, i.e., the line ②. At the timepoint t_{d100}, when the information of the vulnerability is publicly disclosed, its value as a secret disappears. However, the vulnerability still can be utilized because the patch for it is not ready, so the intrinsic value plummets. See the line ③. At time point t_p, the line of value plummets again because the patch is available. The usage of the vulnerability is very limited. However, it will not drop to zero because there are

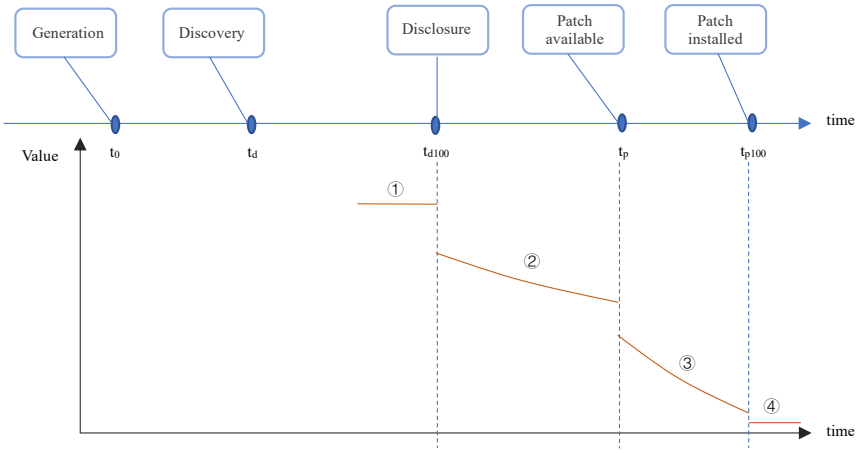
always some users who have not installed the patch in time. The line ④ in Figure 3 presents this. The intrinsic value of the vulnerability becomes zero since t_{p100}, when all the users have got patched.

Figure 3: Intrinsic value of a vulnerability with timeline



As a digital weapon which exploits the related vulnerability, an exploit also has its value of utilizing the vulnerability, as shown in Figure 4.

Figure 4: Intrinsic value of an exploit with timeline



An exploit is of the highest value if the existence of the affected vulnerability is unknown, i.e., the line ① in Figure 4. It is horizontal because its attack effect will not decrease as time goes by. The value of an exploit drops drastically after the disclosure timepoint. Its attack effect drops drastically because the information of the vulnerability

is known, and protection actions are taken by the software users. In Figure 4 it is the line ②. It is a decreasing line because the attack effect of the exploit is decreasing when more and more target systems are taking actions for self-protection. Line ③ stands for the value after the patch is available. Because the patch is the most effective solution for the related vulnerability, there is a big gap between line ② and line ③, which means the attack effect of the exploit drops a lot. For the same reason, line ③ is steeper than line ②. It is also a downward line because the attack effect of the exploit is decreasing because more systems with the vulnerability are getting patched. Even after all the flawed computers are patched, at timepoint t_{p100}, the value of an exploit will not drop to zero, which is line ④ in Figure 4. In this situation, the exploit cannot be used for attack purposes anymore, but it can be used as a good example for other cyber tools. Professionals can easily change some lines to create a new tool. Compared to other scenarios, the value of the exploit is the lowest, but never zero, because it is still worth something.

4.3 Chapter summary

In this chapter we focused on the vulnerability itself and its exploits. Initially we defined a vulnerability and its links and differences with an exploit. These two concepts are frequently misused by the popular media. Then we introduced the zero-day vulnerability, which is the most dangerous and socially destructive type of vulnerability.

In the next step, we discussed the inevitability of a vulnerability, its lifecycle, and its intrinsic value with timeline. It is not difficult to understand that the vulnerability loses its intrinsic value as a secret after information about it is publicly disclosed. Although the intrinsic value of an exploit depends directly and largely on its affected vulnerability, it is not completely synchronized with the value change of the vulnerability; rather it depends on the effects of its attack. Because the exploit is the work of new coding based on the affected vulnerability, the value-added part of the coding still has its value of a tool or as an example of programming even when the vulnerability has completely disappeared.

Chapter 5: Bug Hunters and Vulnerability Markets

From the discussion of the life cycle of vulnerability in Chapter 4, we know that a vulnerability is socially risky as long as: 1) it is found by someone; and 2) it is left unpatched. Finders of vulnerabilities play an important role here. They have the ability to find vulnerabilities, but this does not necessarily mean they will exploit them. The person who discovers a vulnerability is not necessarily the person who exploits it. Generally speaking, discovering a vulnerability requires not only sophisticated expertise but also a deep understanding of software programming. In contrast, exploiting a vulnerability does not require such technical skills and keen insight, especially when many kinds of ready-made toolkits are easier to find. In some cases, a prepared hacking toolkit is sufficient to complete a successful cyberattack. All an attacker needs are repeated mechanical attempts and enough patience. In this chapter we focus on these researchers looking for vulnerabilities. This thesis distinguishes between "bug hunter" and "vulnerability finder". The terms "bug hunters" or "hunters" or "vulnerability hunters" are used to stand for those who plunge into the activities to look for vulnerabilities. Similarly, "vulnerability finders" or "finders" or "bug finders" are terms used to stand for those who have found and identified vulnerabilities. A hunter is a potential finder. In terms of the chapter structure, first we study the bug hunters as a specific group itself, and then we analyse the vulnerability markets they are facing.

5.1 Who are the hunters?

When the masses or the media think of these finders, one word may come up - hacker. But are they really hackers? According to the practice of the cybersecurity industry, hackers are usually classified into three categories: black hat, white hat, and grey hat. Two criteria are applied to determine the classifications: their goal and the legitimacy of their actions[121].

Black hat hackers are usually associated with cybercrime. Financial gain and/or malicious destruction are usually their two main goals. They are often involved in illegally accessing systems, stealing critical data, especially personal and financial

[121] https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html (retrieved on 01 Feb. 2020)

information, modifying or destroying digital assets or even physical assets, cyber ransom, cyber espionage, etc. The composition of this group of hackers is relatively mixed. Some of them have extensive knowledge about breaking through firewalls and bypassing security protocols. They are also responsible for programming to exploit vulnerabilities. Others are amateurs who can merely fiddle with some off-the-shelf hacking tools.

White hat hackers are known as ethical hackers, who use their professional skills to find unknown vulnerabilities in order to improve the overall security level of the target system. White hat hackers perform penetration tests of the target system. By applying the same hacking method as the black hat hackers, they perform vulnerability assessments for the owner. They are security specialists working for companies as employees or contractors, who hack legally.

Grey hat hackers are those who are between white hat hackers and black hat hackers. Their motivations are relatively complex. They may not have the malicious and offensive nature of black hat hackers, but they also do not have the sense of mission of white hat hackers on security issues. Their behaviour is illegal because their intrusion and tests are not allowed by the system owner when they are hunting for unknown vulnerabilities in the target system. But they will not exploit the vulnerabilities found to steal or destroy data. They are like unlocking experts, unlocking the safe but not taking things. Like all white hat hackers, they are very skilled security experts and can rely on their expertise to find unknown vulnerabilities in the system. Unlike all white hackers, their testing is still considered illegal because of the lack of permission from the owner prior to their attempts to penetrate the system. Their behaviour is more secret and unknown to others, whereas the behaviour of white hat hackers is known. Many of them are freelancers. Once vulnerabilities are found, they may choose either to report the information to the owner, to post it online for others to see, or to sell it secretly.

Vulnerability finders are those professional researchers or organizations searching for and identifying vulnerabilities[122] rather than exploiting them by themselves. This

[122] CEPS Task Force (2018)

group includes not only individual finders but also institutional finders. When we look at the relationship between vulnerability finders and hackers, we see that all individual vulnerability finders fit the broad definition of hacker, but not the other way around. White hat and grey hat hackers focus more on discovery, or searching for unknown vulnerabilities, while black hat hackers focus more on attack, or exploiting the known vulnerabilities. White hat hackers are in essence potential vulnerability finders, because they legally use the methods of hacking to look for vulnerabilities. After they find unknown vulnerabilities, they are vulnerability finders. Mikko Hyppönen, a famous cybersecurity expert and columnist, stated that the money-making malware started between 2003 and 2004[123]. From the perspective of behaviour, bug hunters are hackers because they use hacking methods. From the perspective of motivation, they hunt bugs not only for the challenge, but for the tangible or intangible benefits afterwards. The group of bug hunters includes not only individuals, but also organizations. Like a hunter looking forward to the harvest after prey hunting, these technical researchers are looking forward to the harvest after bug hunting.

5.2 Where are they?

According to the 2019 Hacker Report[124] by HackerOne[125], the world's largest hacker community working as a platform for vulnerability coordination and bug bounties, there are more than 300,000 registered hackers, covering almost every corner of the globe. All of them are supposed to be white hat hackers or ethical hackers.

Among all these hackers, India accounts for 27%, with the largest number. The US accounts for 11%, ranking second. Russia in third place accounts for 5%. Next places are Pakistan and the United Kingdom. These five countries compose over 51% of all hackers in the HackerOne community.

---

[123] See the interview with Mikko Hyppönen, a computer security expert and columnist, Chief Research Officer at F-Secure, in the documentary "Zero Days-Security Leaks for Sale (2014)", at 10'30".

[124] https://www.hackerone.com/sites/default/files/2019-02/the-2019-hacker-report_3.pdf (retrieved on 01 Feb. 2020)

[125] HackerOne is one famous bug bounty platform, organizing vulnerability finders to report their discoveries to software vendors or related organizations. See Hacker Powered Security Report 2019.pdf, https://www.hackerone.com/resources/reporting/the-hacker-powered-security-report-2019 (retrieved on 01 Feb. 2020).

From the perspective of bounty[126] income in 2018, finders in the US earned 19% of all bounties, together with India (10%), Russia (6%), Canada (5%), and Germany (4%) being the top five countries. The following five countries are Netherlands, Egypt, United Kingdom, China, and Argentina. Finders in these ten countries earned nearly 60% of all bounty amounts through the HackerOne community.

The white hat hackers included in the 2019 Hacker Report can be regarded as a sample, which gives us a rough idea of the global distribution of potential vulnerability finders. From the perspective of technical skills, there is no difference between white hat hackers or grey hat hackers. It is reasonable to suppose that we can rely on this data to estimate the geographical distribution of freelancer bug hunters.

5.3 Some observations

Although hunters claim that financial incentives are not the most important incentives, observation from real data often suggests otherwise. From the surveys of the HackerOne platform and other researchers, we conclude the following observations:

1) Geographically, white hat hackers are distributed not only in developed countries but also in developing countries. In countries like India, Pakistan, Egypt, Thailand, Algeria, Morocco, Latvia, Philippines, Romania, Hungary, Chile, Ethiopia, and Indonesia, we can find records of active activities of local researchers[127].

2) The number of white hat hackers in developing countries is growing rapidly, especially in the past two years. Consider India, for example. Whereas in 2018 hackers in India accounted for 23.3% of the total registered hackers on the HackerOne platform, in 2019 this number climbed to 27%[128]. At the same time, the total number of registered hackers on the platform increased by almost 80%[129].

3) On worldwide average in 2018, the bounty cash inflow to a top vulnerability finder

[126] A bug bounty or bug bounty program is a reward given for finding and reporting a vulnerability (bug) in a particular software product. Many IT companies offer bug bounties to drive product improvement and get more interaction from end users or clients. See https://www.techopedia.com/definition/28637/bug-bounty (retrieved on 01 Feb. 2020).

[127] See 2019 Hacker Report and 2018 Hacker Report by HackerOne.

[128] *Id.*

[129] From around 166,000 (2018) increased to 300,000 (2019).

is 2.7 times the median annual wage of a software engineer in the same home country. In some countries the difference is even wider, especially in less developed countries, which we can observe in Table 7. In the table 20 countries (regions) are listed and the multiplier is found by dividing the upper range of bounty earners for the region by the median annual salary of a software engineer for the related region. For technical experts in developing countries, their average salary level is relatively low. Bug hunting activities can improve their financial situation greatly, which is illustrated by the higher multipliers in the table.

Table 7: Bug Bounties VS. Median Annual Salary

Developing Countries	Multiplier	Developed Countries	Multiplier
India	16 x	Hong Kong (China)	7.6 x
Argentina	15.6 x	Belgium	2.7 x
Egypt	8.1 x	Australia	2.7 x
Philippines	5.4 x	Canada	2.5 x
Latvia	5.2 x	US	2.4 x
Pakistan	4.3 x	Sweden	2.2 x
Morocco	3.7 x	Germany	1.8 x
China	3.7 x	Italy	1.7 x
Poland	2.6 x	Netherlands	1.7 x
Bangladesh	1.8 x	Israel	1.6 x

Source: The 2018 Hacker Report by HackerOne

4) Although many software companies have divisions dedicated to vulnerability testing and the security of their products, there are external freelancers working on their own as bug hunters. What they need is only an internet connection. White hat hackers don't need to cross the border physically and they don't have to apply for a working permission. If they can get good rewards by selling the bugs they find, the population of people doing this will definitely grow. Algarni & Malaiya (2014) pointed out that "a large fraction of the vulnerabilities, perhaps a majority of them, are discovered by outside discoverers. [...] Many external discoverers are freelancers either working on their own or on a contract basis". They studied two popular internet browsers, Safari

and Chromium, and found that 80% of the vulnerabilities of Safari and 64% of the vulnerabilities of Chromium were discovered by outsiders, people who were not engaged in discovering vulnerabilities internally in software companies. These external finders have their own motivations. For those in the developing areas, the financial motivation is probably critical.

5) There is one particularly noteworthy statistic in the 2018 Hacker Report: nearly 25% of hackers have not reported a vulnerability that they found because of lacking a channel to disclose it. In the case where companies do not have a vulnerability disclosure policy (VDP)[130], by which we mean - a published process and channel that publicly states how a vulnerability can be safely reported and provides a "safe harbour" for the hacker, the safest legal way for a bug hunter with the vulnerability information is not to disclose the information. They may be forced to try other channels such as social media, in which case their reports are frequently ignored or misunderstood. They may also turn to some other place to sell the information, because if they don't sell it as soon as possible, the vulnerability is likely to be found by others. If they sell it in the illegal market, this is socially risky.

6) Algarni & Malaiya (2014) pointed to an intriguing phenomenon they observed after they studied some top vulnerability finders. Most of the top vulnerability finders were active and credited with discovering vulnerabilities during the first three years of operation. Then these successful finders disappeared from the scene for the following years. The authors explained that this was because after they had gained a reputation as successful vulnerability finders, they started their service for software companies or security service providers on a contract basis, or they initiated their own business as a security expert. From the perspective of economics, reputation itself is also a financial incentive. It is an intangible asset that can bring stable cash flows in the future.

Based on the six observations above, we can draw our conclusions: outsiders play a key role in the process of vulnerability discovering, and the numbers of people looking for

[130] Vulnerability Disclosure Policy (VDP): an organization's formalized method for receiving vulnerability submissions from the outside world. This often takes the form of a "security@" email address. The practice is defined in ISO standard 29147. Unlike a bug bounty program, a VDP does not offer hackers financial incentives for their findings.

vulnerabilities is increasing, especially those from developing countries. Furthermore, financial incentives are the most fundamental incentives and reputation is essentially another kind of financial incentive that can bring stable cash flows in the future. Therefore, the assumption of profit-maximization in economics can be applied to bug hunters and finders.

5.4 The vulnerability markets and market players

Researchers looking for vulnerabilities can be simply divided into insiders and outsiders. Insiders include technical people who work for software companies, and they are not the object of this thesis. If an insider sells externally a vulnerability found internally, he has committed theft of company secrets. We focus on outside vulnerability finders, because we know that many of the vulnerabilities were found by those individuals and organizations.[131]. If these finders sell their discoveries to someone else rather than reporting to it to the related software developers, such behaviour will lead to potential social risks. Next, we will discuss the markets they face when making their decisions.

When it comes to a market situation, both the supply side and the demand side must be defined. A vulnerability finder is on the supply side. Because the vulnerability has its intrinsic value, which has been discussed in Chapter 4, the vulnerability finder has the incentive to cash in on his discovery. Meanwhile, he is facing the risk that others are going to find the same vulnerability soon, so he has the incentive to cash in on his discovery as soon as possible. Sometimes it happens that those two or more vulnerability hunters independently find the same vulnerability, which is called "vulnerability rediscovery". Some scholars have studied this issue and presented different views of this phenomenon. Herr, Schneier & Morris (2017) state that "15% to 20% of vulnerabilities are discovered independently at least twice within a year. For just Android, 13.9% of vulnerabilities were rediscovered within 60 days, rising to 20% within 90 days, and above 21% within 120 days. For the Chrome browser we found 12.57% rediscovery within 60 days……". They believe that the rediscovery rates presented in their paper underestimate the true rate of rediscovery. This is because their

[131] Algarni & Malaiya (2014)

study is restricted to the high- and critical-severity bugs, but low- and medium-severity vulnerabilities are rediscovered more frequently[132]. Ablon & Bogart (2017) focused on zero-day vulnerabilities, the most critical-severity vulnerabilities. They show that for a given stock of zero-day vulnerabilities, the rate of rediscovery within a year is approximately 5.7%[133]. A rational finder is very likely to choose a strategic combination to maximize his benefits. Not all the vulnerabilities are the same. Some of them are extremely dangerous like zero-day vulnerabilities, whereas others are not. If it is possible, the finder will choose to disclose a normal vulnerability in the legal market to gain reputation, while selling the zero-day vulnerability secretly in the illegal market for a high price, as long as it is difficult for this behaviour to be identified.

In principle, the finder can choose either to shout it out as a whistle blower, or to inform the vendor so that the vulnerability can be fixed, or to offer his discovery to the highest bidder.

To become a whistle-blower, the most practical approach is to inform an authority like CERT, the Community Emergency Response Team (CERT) program in the United States. The finder voluntarily submits his finding to CERT, the official coordinator, or to other similar organizations, then the software vendor gets the chance to patch the vulnerability. As a result, the finder gets some recognition as a capable researcher. However, this does not seem very attractive because the finder gets only some degree of recognition but no financial reward. This is especially so for those "who have already established themselves or who need money more than publicity"[134]. Because normally there is no cash inflow for this kind of disclosure, we do not include it in our market analysis.

On the demand side are the buyers who the finder is facing when he wants to sell his newly found vulnerability. According to the difference in legitimacy and the type of buyers, there are three markets: the white market, the grey market, and the black market. Everyone in these markets has his own purpose, trading off his costs and benefits. All

[132] Herr, Schneier & Morris (2017), p. 1
[133] Ablon & Bogart (2017), p. xii
[134] Algarni & Malaiya (2014)

these three markets apply to zero-days[135].

5.4.1 The white market and market players

The white market encompasses sales of vulnerabilities between the finders and the buyers – software vendors or those who will turn their purchases over to software vendors so that they can be fixed[136]. Unlike traditional system-based cyberattacks, which are the attacks intended to compromise a computer or a computer network[137], nowadays web-based cyberattacks, which are the attacks occurring on a website or web applications[138], have taken up a large share of total cyberattacks. According to Trustwave's 2018 Global Security Report, "100% of web applications tested displayed at least one vulnerability, with 11 as the median number detected per application"[139]. As software vendors want to patch their products, website owners also want to discover vulnerabilities in their web applications to improve their security. They provide compensations to researchers for reporting vulnerabilities, for instance, the US Department of Defense as well as Starbucks.

Market players on the demand side are software vendors, web applications owners, third-party platform companies, and brokers.

The white market includes not only bug bounty programs run by software vendors themselves, such as Apple, Google, Microsoft, and Facebook, but also independent bug bounty platforms, such as HackerOne and Bugcrowd. Brokers' programs, such as TippingPoint's Zero Day Initiative (ZDI), Verisign's iDefense, and some hacking contests, such as Pwn2Own, play important roles in the market as well. "The white market tries to pull in security researchers by making their case on ethical grounds, citing responsibility to disclose, and offering recognition in lieu of high pay-outs"[140].

In the white market, the recommended way of disclosure is called "responsible disclosure" or "coordinated vulnerability disclosure" (CVD), which is "a process aimed

[135] It refers to both zero-day vulnerabilities and zero-day exploits which take advantage of zero-day vulnerabilities.
[136] Fidler (2015) and Libicki, Ablon & Webb (2015)
[137] https://www.javatpoint.com/types-of-cyber-attacks (retrieved on 01 Feb. 2020)
[138] *Id.*
[139] https://www.trustwave.com/en-us/resources/security-resources/security-statistics/ (retrieved on 01 Feb. 2020)
[140] Libicki, Ablon & Webb (2015), p. 45

at mitigating or eradicating the potential negative impacts of vulnerabilities"[141]. In contrast with full disclosure, which is a "public release of all details of the vulnerability, often without any mitigation measures to protect users…… CVD is a process aimed at mitigating or eradicating the potential negative impacts of vulnerabilities" [142]. Householder, Wassermann, Manion & King (2017) define it as "the process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of vulnerabilities and their mitigation to various stakeholders, including the public"[143]. During the course of CVD, an important actor is the coordinator, who is a "person or organization that facilitates the coordinated disclosure process"[144]. The coordinator can be either a third-party platform, or the vendor itself. Many software vendors have created their own ad-hoc bug bounty programs to compensate those security researchers for the efforts in searching for flaws in their products. Table 8 is a glance list of bug bounty programs by some reputable companies in 2020.

Table 8: Company Bounty Programs 2020

Name	Pay-out ($)	Notes
Intel	500 – 30,000	Intel's bounty program mainly targets its hardware, firmware, and software.
Yahoo	up to 15,000	Yahoo has its dedicated team that accepts vulnerability reports from security researchers and ethical hackers.
Snapchat	2000 – 15,000	Snapchat security team reviews all vulnerability reports and acts upon them by responsible disclosure. The company will acknowledge the submission within 30 days.
Apple	up to 1,00,000	Apple's bug bounty program now covers iOS, macOS, watchOS, tvOS, iPadOS, and

[141] CEPS Task Force (2018), p.5
[142] *Id*.
[143] Householder, Wassermann, Manion & King (2017), p. 3
[144] CEPS Task Force (2018), p. 6

		iCloud, as well as all devices that run on these operating systems. The maximum pay-out amount for finding a bug has been increased to $1 million, which is a big leap from the previous $200,000 maximum[145].
Facebook	500 – no limit	Under Facebook's bug bounty program users can report a security issue on Facebook, Instagram, Atlas, WhatsApp, etc.
Google	up to 50,000	Depending on the impact of the bug found, researchers could net as much as $50,000 for a single report[146].
Mozilla	500 – 5000	The bounty is offered only for bugs in Mozilla services, such as Firefox, Thunderbird and other related applications and services.
Microsoft	mostly up to 15,000 or 20,000 or 30,000	Different bounty ranges apply to vulnerabilities in different products[147].
Twitter	140 – 15,000	The bounty rewards possible security vulnerabilities in their services.
Paypal	50 – 30,000	The minimum bounty amount for a validated bug submission is $50 USD and the maximum bounty for a validated bug submission is $30,000 USD[148].
Uber	up to 10,000	The vulnerability rewards program of Uber primarily focused on protecting the data of users and its employees.

Source: https://www.guru99.com/bug-bounty-programs.html[149]

[145] https://lifehacker.com/earn-up-to-1-million-from-apples-expanded-bug-bounty-p-1837106598 (retrieved on 01 Feb. 2020)
[146] https://threatpost.com/google-record-high-bug-bounty-payouts/152354/ (retrieved on 01 Feb. 2020)
[147] https://www.microsoft.com/en-us/msrc/bounty (retrieved on 01 Feb. 2020)
[148] https://www.paypal.com/us/webapps/mpp/security-tools/reporting-security-issues (retrieved on 01 Feb. 2020)
[149] Mainly referenced: https://www.guru99.com/bug-bounty-programs.html (retrieved on 15 Feb. 2020), and the rest referenced respective official websites.

Third-party bug bounty platforms like HackerOne[150] and Bugcrowd[151] coordinate reports by global security researchers for their discoveries. Normally they have a worldwide client base. Once the bug in the report is detected correctly, the specific company will pay the bounty amount to the vulnerability finder. One example is Dropbox, a file hosting service provider, offering services like cloud storage, file synchronization, personal cloud, and client software. Dropbox allows security researchers to report vulnerabilities on HackerOne. The minimum pay-out was $12,167 and the maximum amount was $32,768. Many known companies like Yahoo, Shopify, PHP, Google, Snapchat, and Wink are using the service of these platforms to reward vulnerability finders[152]. Another case is the bug bounty program HACK THE PENTAGON, which is a bug bounty program of the US Department of Defense on a third-party platform[153]. In January 2019 the European Commission launched its EU-FOSSA 2 bug bounty program, which rewards hackers if they find critical bugs in open-source software used by the EU institutions[154], using three bug bounty platforms: HackerOne, Intigriti, and Deloitte[155].

5.4.2 The grey market and market players

Fidler (2015) defines the grey market as a marketplace which "refers to the trade between vulnerability sellers and government agencies or other non-criminal clients". Potential buyers include governments, security service firms who use vulnerabilities for penetration testing or cyber defence research, dealers, and brokers. The security firm base is considered to be much smaller than the government base[156]. "Governmental buyers are the most typical final customers for zero-days in the grey market, but zero-days often first pass through brokers"[157].

The US government is one of the reported buyers in the grey market. The NSA, the National Security Agency, was a publicly identified government purchaser that devoted

[150] https://hackerone.com/bug-bounty-programs (retrieved on 15 Feb. 2020)
[151] https://www.bugcrowd.com/bug-bounty-list (retrieved on 15 Feb. 2020)
[152] https://www.guru99.com/bug-bounty-programs.html (retrieved on 15 Feb. 2020)
[153] https://www.hackerone.com/hack-the-pentagon (retrieved on 15 Feb. 2020)
[154] https://ec.europa.eu/info/news/eu-fossa-bug-bounties-full-force-2019-apr-05_en (retrieved on 15 Feb. 2020)
[155] https://juliareda.eu/2018/12/eu-fossa-bug-bounties/ (retrieved on 15 Feb. 2020)
[156] Telephone Interview with Richard Bejtlich, Chief Security Strategist, *FireEye*, (7 May 2014).
[157] Fidler (2015), p.416

$25.1 million in fiscal year 2013 for "additional covert purchases of software vulnerabilities from private malware vendors", according to the top-secret documents released by NSA leaker Edward Snowden[158], although the NSA relies mostly on its in-house staff hunting for vulnerabilities[159]. Reuters reported that the U.S. government "has become the biggest buyer in a burgeoning grey market where hackers and security firms sell tools for breaking into computers" and "the Department of Defense (DoD) and U.S. intelligence agencies, especially the NSA, are spending so heavily for information on holes in commercial computer systems, and on exploits taking advantage of them"[160]. The US government is not alone. In 2015 the Italian grey marketeer Hacking Team, a Milanese seller of intrusion and surveillance tools to governments and law enforcement agencies, was hacked. The released sensitive corporate data and customer history provided us with an excellent insight into global governments[161] active in this market. Countries in every continent are covered, and the total value of the invoices amounted to €4,324,350, among which, most notably, a contract with Sudan valued at €480,000[162]. Hacking Team sold exploits to Bahrain, Egypt, Morocco, Russia, Saudi Arabia, Sudan, and UAE, none of which has a sparkling record of democracy and freedom[163], and some were accused of violating human rights and the use of violent oppression[164].

The involvement of governments in the grey market has been controversial. Governments have been criticized by the public media for their collecting and stockpiling of software flaws, rather than reporting them to the software companies. On

---

158 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 (retrieved on 15 Feb. 2020)

159 Fidler (2015), p.416

160 Joseph Menn, Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback, *REUTERS* (10 May 2013), http://www.reuters.com/article/2013/05/10/us-usa- cyberweapons-specialreport-idUSBRE9490EL20130510 (retrieved on 15 Feb. 2020).

161 Africa: Egypt, Ethiopia, Morocco, Nigeria, Sudan
America: Brazil, Chile, Colombia, Ecuador, Honduras, Mexico, Panama, United States
Asia-Pacific: Azerbaijan, Kazakhstan, Malaysia, Mongolia, Russia, Singapore, South Korea, Thailand, Uzbekistan, Vietnam, Australia
European: Cyprus, Czech Republic, Germany, Hungary, Italy, Luxemburg, Poland, Spain, Switzerland
Middle East: Bahrain, Lebanon, Oman, Saudi Arabia, UAE
https://www.csoonline.com/article/2944333/hacking-team-responds-to-data-breach-issues-public-threats-and-denials.html (retrieved on 15 Feb. 2020)

162 *Id.*

163 The Economist (2017b)

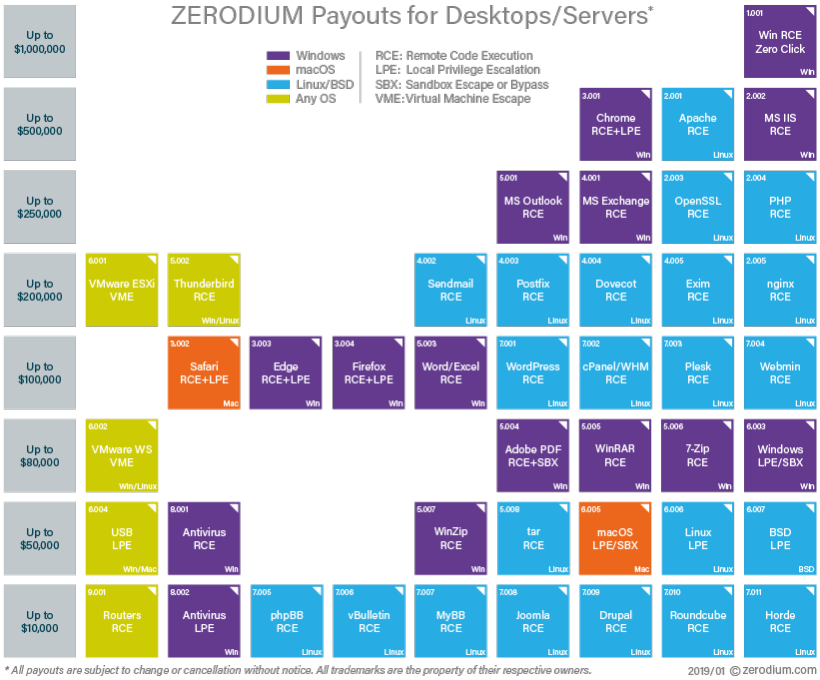
164 https://www.zdnet.com/article/hacking-team-ceo-were-the-good-guys/ (retrieved on 15 Feb. 2020), https://www.csoonline.com/article/2944333/hacking-team-responds-to-data-breach-issues-public-threats-and-denials.html (retrieved on 15 Feb. 2020)

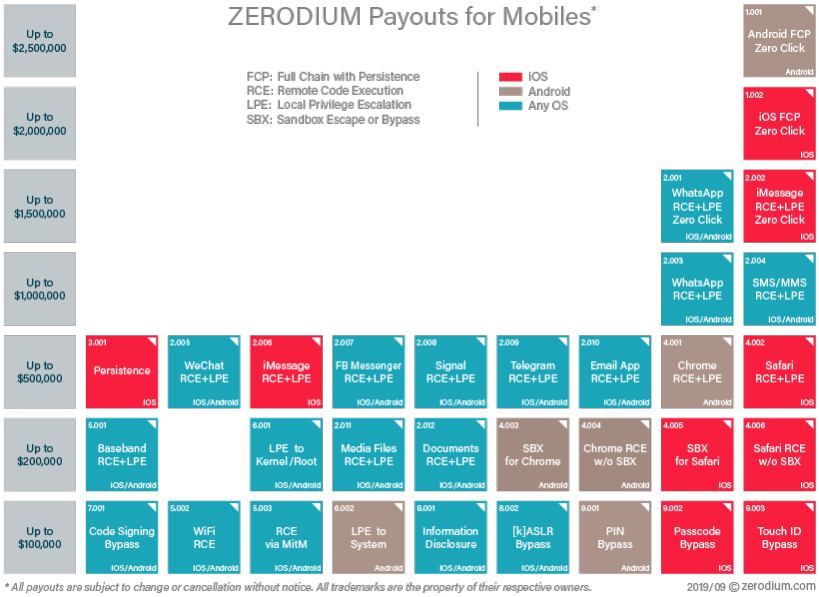
this issue, governments suffer from contradictory incentives: on the one hand, they are willing to have all the vulnerabilities patched for the overall cybersecurity; on the other hand, it is easier to conduct espionage and surveillance, if some vulnerabilities are left unpatched[165]. The government's participation in the market is criticized as helping catalyse the expansion of the grey market, which is believed to have potentially harmful ramifications[166]. The role of government will be discussed in detail from chapter 7 to chapter 9.

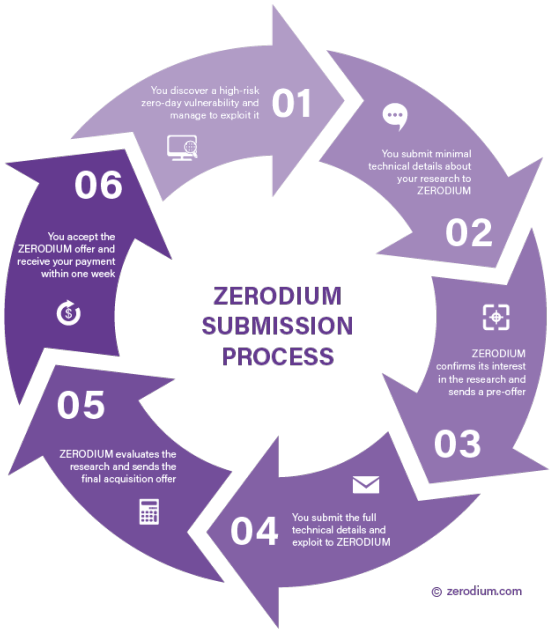
Dealers in the grey market carry on their business on a buyer/reseller mode. They resell vulnerabilities, usually to governments and security service companies. Some of them "have their own vulnerability discovery teams selling directly to governments"[167]. In many cases, these companies rely on annual contracts to maintain business with their clients. Endgame, a former vulnerability and exploit trade company which was acquired by another security company Elastic in 2019[168], guaranteed a minimal delivery of 25 zero-day vulnerabilities per year for an annual contract value of $2,500,000[169]. In addition, Huang, Siegel & Stuart (2018) from MIT stated that zero-day exploits cost roughly $150,000 every month for a subscription service[170]. ZERODIUM is one of the dealers focusing on high-risk vulnerabilities with fully functional exploits, who pay very high rewards (up to $2,500,000 per submission)[171]. According to The Economist, there are more than 200 exploit companies like ZERODIUM in the world[172]. Figure 5 shows ZERODIUM's pay-outs for Desktops/Servers, Mobiles, submission process for zero-days, as of March 2020.

[165] The Economist (2017d)
[166] Fidler (2015), p. 411
[167] Fidler (2015), p. 417
[168] https://www.businesswire.com/news/home/20191008005937/en/Elastic-Completes-Acquisition-Endgame-Leader-Endpoint-Protection (retrieved on 15 Feb. 2020)
[169] https://wikileaks.org/hbgary-emails//fileid/12242/4279 (retrieved on 15 Feb. 2020)
[170] Huang, Siegel & Stuart (2018), p. 16
[171] https://zerodium.com/program.html (retrieved on 15 Feb. 2020)
[172] The Economist (2017b)

Figure 5: ZERODIUM's pay-outs and submission process







Source: https://zerodium.com/program.html

Brokers are those who source vulnerabilities from finders and offer them to potential customers for a 10% to 15% cut of the final sale[173]. Vulnerability brokers serve as a firewall to keep the identity of the buyer and seller confidential. Thus, the seller does not know how his discovery will be used. It is pointed out that "Governmental buyers are the most typical final customers for zero-days in the grey market, but zero-days often first pass through brokers"[174] .

As to the supply side, because the transaction of vulnerabilities in both the white market and grey market are legal, vulnerability hunters may play on both sides of the fence. They can submit some bugs in the white market for peace of mind income, while selling others in the grey market reaping higher profits. If they are participants in hacking contests like Pwn2Own, they are likely to "use only known techniques, so as to keep new techniques a secret from white-market vendors"[175].

[173] Fidler (2015), p. 418
[174] *Id.* p. 416
[175] Libicki, Ablon & Webb (2015), p. 45

Although transactions in the grey market are not illegal per se, they can nevertheless be socially risky because they make cyberspace defence much more complicated, especially in the case the government's stockpile of vulnerabilities or exploits is stolen by hackers. In the field of cybersecurity, a very asymmetric nature exists - attacking is rather easy, whereas defending is rather difficult.

The grey market is thought to be much more lucrative than the white market, because buyers pay not only for the vulnerability per se, but also to obtain a guarantee that the vulnerability can be exploited. Classes of vulnerabilities include proofs of concept (POCs)[176], pseudo-exploits and some evidence that a vulnerability is exploitable for which purpose. It is estimated that prices in the grey market are ten times those of the white market[177].

5.4.3 The black market and market players

The black market is in fact a market for cybercrime[178], which is a long-standing profitable option for a vulnerability finder. On the supply side, sellers include freelance bug hunters and organizations. On the demand side, buyers include individual criminals and criminal organizations[179]. Some governments may turn to the black market if legitimate sellers refuse to service them, for example, those governments known for suspected terrorism, violent oppression, or human rights violations[180]. In addition, it also should be noted that black-market sellers are aware of the legal markets and operate simultaneously in both illegal and legal markets[181].

Trades are largely conducted online, including widely accessible sites and restricted-access marketplaces. In this highly developed marketplace, digital tools and weapons are traded, like exploit kits, botnets, DDoS, and attack services (as well as the fruits of crime, such as stolen credit card numbers and bots)[182]. Only a very small portion of this

[176] A POC demonstrates that a fully functional exploit is possible on a target system, but it does not include final steps to make it weaponized. See Libicki, Ablon & Webb (2015), p.44
[177] Libicki, Ablon & Webb (2015), p. 44
[178] Ablon, Libicki & Golay (2014), p.1
[179] *Id*. pp. 5-6
[180] Fidler (2015), p. 415
[181] *Id.* p. 416
[182] Libicki, Ablon & Webb (2015), p. 44

underworld bazaar deals with zero-day vulnerabilities and exploits which are like luxury goods. Instead, half-days (or "1-days" or "2-days"), vulnerabilities for which the patch is already available but not yet widely implemented, are more popular. They are more likely to meet the mass demand for malware to commit ordinary cybercrime within a limited budget[183].

A sale in the black market is confidential and, hence, is not clearly documented or publicly available. RAND's experts estimated that on average the price level in the black market is about ten times the price level in the white market[184]. The figures cited by Fidler (2015) confirmed this[185]. In the black market, a Flash zero-day exploit can fetch $30,000-$50,000[186].

5.5 Comparisons of White, Grey, and Black Markets for Vulnerabilities

5.5.1 Comparisons made by RAND experts

Libicki, Ablon, & Webb (2015) compare the three markets and come to the short summary provided in Table 9.

Table 9: Comparisons of White, Grey, and Black Markets for Vulnerabilities

	White Market	**Grey Market**	**Black Market**
Use of 0-days	Defensive only (used to make products or customers safer)	Offence or defence	Offence
Products	Vulnerability information only	Vulnerability information; PoC[187]; pseudo-exploits; fully functional/ weaponized exploits	Vulnerability information; PoC
Participants	Bug bounty offers, contests, brokers.	Buyers are more interested in targeted	

[183] *Id.* p. 46
[184] *Id.* p. 48
[185] Fidler (2015), pp. 415 – 416
[186] Ablon & Bogart (2017), p. 86
[187] *supra* note 176

		type of attack	
Price	1x	10x	10x
Motivation to participate	Responsible disclosure (doing the "right" thing); notoriety; financial gain	Financial gain	Financial gain
Business model	Work directly with affected vendor; work through bug bounty; participate in contest; work with reseller (e.g., iDefense, ZDI)	Subscription-based; vouchers; or customized solution	"Half-days" are more prevalent

Source: Libicki, Ablon, & Webb (2015), p. 48

5.5.2 Complementary comparison and analysis

As for the comparison of white, grey, and black markets, we can continue our analysis by addressing the following eight aspects:

1) Legal, legitimate, and illegal

One can distinguish between "legal" market - the white market transactions, and "illegal" market - the black-market transactions. The grey market might be considered legal, but its negative security ramifications mean that it is questionable not only because of its ethical influence, but also because of its potential impact on cybersecurity.

2) Agent mechanism

Roy Lindelauf, a researcher at the Netherlands Defence Academy, mentioned that "More than half of exploits sold are now bought from firms rather than from freelance hackers……" [188] . Similarly, an empirical analysis from NSS Labs found that "Specialized companies are offering zero-day vulnerabilities for subscription fees that are well within the budget of a determined attacker (for example, 25 zero-days per year for USD $2.5 million); …… half a dozen boutique exploit providers have the capacity

[188] The Economist (2013)

to offer more than 100 exploits per year"[189].

Firms, no matter whether they are platform companies, or dealers, or brokers, play a very important role of agent in the vulnerability markets. When the client is the software vendor, it is concluded as a white market trade; when the client is the government, it is then concluded as a grey market one.

However, the agent mechanism has its own disadvantages, among which the most significant two are: inconsistent goals and asymmetric information. Agents have incentives to deliberately drive the price up, inducing their clients to form a long-term expectation of high price level, in order to increase their own profits. This happens quite often when there exists asymmetric information. For example, a dealer is likely to increase the price drastically when he meets a government, which lacks market information while having a rather loose financial budget. In addition, when there is no good price or suitable buyer in the legal markets, a profit orientated seller may turn to opportunities in the illegal market.

3) Price level in different markets

Perhaps careful readers have noticed that in the above table of market comparison – the price level of the grey market is almost the same as that of the black market. Based on interviews with grey market and white market participants, RAND's experts pointed out that "the grey market is thought to be more lucrative than the black market, and both are distinctly more lucrative than the white market. Many estimates put prices in the grey and black markets at ten times those of the white market.[190]"

This may run counter to our intuition. We will think naturally that the price of the black market should be the highest, because sellers will demand extra payment to compensate for the risks from illegality. Why is reality inconsistent with our intuition?

First of all, we should note that the main products sold in the grey market are different from those in the black market. Although they are all vulnerabilities, they are

[189] Frei (2013), p.1
[190] Libicki, Ablon & Webb (2015), p.44

vulnerabilities of different risk levels. To meet the needs of intelligence or law enforcement departments of governments, vulnerabilities of high-risk or more secret nature are more favoured in the grey market, like zero-days. In comparison, weaponized exploit kits or other ready-made digital tools are more popular in the black market to meet the mass demand. Zero-days are too luxurious for ordinary criminals.

Second, the main buyers in the grey market are governments, while most of the buyers in the black market are criminals or criminal groups. Governments have a higher ability to pay than criminal gangs. They normally have annual budgets allocated for this special purpose, whereas criminals need to take the cost of buying criminal tools into account.

Based on the two points above, it is logical that the price in the grey market is approximately equal to the price in the black market, or a bit higher, even considering the difference in legality between the two markets. This phenomenon can also be logically explained by the implications of the price model in Chapter 6, which means if a buyer values a vulnerability more, he is going to offer a higher price. This reflects the competition between different valuations, rather than the competition between markets.

Furthermore, let's suppose an autocratic government, which is on the UN blacklist for violations of human rights, wants to compete with a democratic government for the same zero-day vulnerability. The autocratic government cannot buy it in the grey market, so it must rely on help in the black market. A democratic government can buy the vulnerability in the grey market. If the two governments hold the same valuation, the seller will definitely sell to the democratic government because the transaction is legal. To get the vulnerability, the autocratic government must have a higher valuation, which leads to a higher price of the black market. In this case, the price in the black market is higher than that in the grey market. Here the logic behind the transaction reflects the competition between markets.

4) The relationship between each two markets

The relationship between the white market and any of the other two markets is

competitive. This is because, for any vulnerability, the software vendor has the incentive to get it in order to improve security of his product. For a software vendor, it is not the problem of whether or not to buy the vulnerability. It is the problem of the price he can buy it, ideally getting it for free. For a seller, vulnerabilities can be sold either in the grey market (or maybe the black market) for more money, or in the white market for more reputation plus some money.

The division between the grey market and the black markets is blurred. As RAND experts mentioned: "sellers who are driven only by money will often bounce between markets chasing the pay-out"[191]. Fidler (2015) also demonstrated that sellers are either aware of or operate simultaneously in both the illegal and legal markets[192]. Buyers in the grey market may also choose the black market in some special cases, especially when they want to hide their identities completely. Vulnerabilities traded in the grey market and vulnerabilities traded in the black market to a certain extent cannot overlap. Governments do not need normal vulnerabilities or exploits made for mass criminals, and the zero-day vulnerabilities which they are keen on are too expensive for mass criminals in the black market. Many criminals need only easy-to-use cyber weapons, rather than sophisticated vulnerability secrets. The grey market and the black market are to some extent overlapping. For the same vulnerability, they may be competitive; for many vulnerabilities of different security levels, they may be complementary.

So, the white market competes with the grey market and the black market as a whole. Essentially, it is the legitimate market vs. the illegitimate market, rather than white market vs. grey market or white market vs. black market. When a seller makes a decision when facing these three markets, he will take the price of the white market as his reserve price. Subsequently, he will consider whether to sell his discovery in the grey market, in the black market, or to go back to the reserve price in the white market. The competitive nature of the white market vis-à-vis the grey, or black market, increases the seller's bargain power in the latter. Specifically, the seller will take the white market price as his reserve price when he faces the grey or black market.

[191] Libicki, Ablon & Webb (2015), p. 47
[192] Fidler (2015) p.416

5) Spill over effect

Government participation in the grey market seems to benefit the black market. First, governments rely much on their agents, dealers, or brokers, for the business in the grey market. It is possible that some agents participate in both grey and black transactions. Cashflow from governments will help them to expand into additional activities. Second, governments' funding will attract more freelancers and institutional bug hunters. With the revenues obtained from governments, they can upgrade their equipment to the best level and hire additional professionals, and thus will find more vulnerabilities accordingly. If the vulnerability discovered is not the one demanded by the government, it is likely to flow into the black market.

6) Contract and payment

Many grey market tractions are subscription-based. Contractors probably play a large role in the grey market, depending on the existing relationships with the government[193]. This is different from the business model in the white market or the black market (see Table 9).

In addition, the ways of pay-outs are noteworthy for these three markets. Both white market buyers and governments may pay upfront. However, the brokers adopt a gradual scheme in order to prevent "double dipping", which means the seller sells the same item to different buyers simultaneously. "Typically, they pay 50 per cent up front, 25 per cent in 30 days if the zero-day flaw is not discovered, and then the final 25 per cent after another 30 days"[194]. This gradual payment scheme is also adopted in the black market. Once a timeframe is set, the terminating of payments within the timeframe is possible if the vulnerability is patched during the period.

7) The black market and nature of cyberspace

As for the transactions of zero-days, the relationships between either the white market and the black market, or the grey market and the black market, are competitive. Based on this, we can speculate that an increase of prices in competitive markets (especially the bounty amount in the white market) will affect the transactions of zero-days in the

[193] Fidler (2015), p. 423
[194] https://www.theregister.co.uk/2018/04/15/mature_bug_bounty_market_bsidessf (retrieved on 20 Feb. 2020)

black market. A report in 2018 confirmed this[195]. The transactions of zero-days in the shadow world will never disappear, because there are always a few rogue governments resorting to the black market for their offensive purpose. They have no other access to zero-days but money. In addition, the black market will remain threatening to cybersecurity. One reason is that half-days or one-days are still valuable. Even if a patch is available, many users still do not patch the vulnerability in time. These vulnerabilities are favoured in the black market because they are cheaper than zero-days. The other reason is determined by the nature of cyberspace which is already outlined above: in this virtual space, attacking is relatively easy and cheap, whereas defending is relatively complicated and costly. Cyber weapons are always needed by the dark side.

8) The military

The military is a significant buyer in the vulnerabilities market. The cyber force has become an important part of the military in many countries. Hans Folmer, commander of Taskforce Cyber in the Dutch Army, described this as "We always operate as joint forces: army, navy, air force, and cyber is part of that"[196]. For example, the Royal Netherlands Army started in 2013 to train cyber soldiers to defend and attack in cyber space[197]. Some security experts personally ranked the US, Israel, and Russia as top three countries with advanced cyber capabilities[198].

From the defensive perspective, the military will have its bug bounties for outside researchers to purchase their discoveries during attacks. Between October 9 and November 15 of 2019, the US Army initiated its second bug bounty event "Hack the Army", during which its public military websites were hacked by a total of 52 individual hackers from around the world. The Army paid out more than $275,000 for 146 vulnerabilities detected over this span of five weeks[199].

---

[195] https://www.fifthdomain.com/industry/2018/09/25/why-the-market-for-zero-day-vulnerabilities-on-the-dark-web-is-vanishing/ (retrieved on 20 Feb. 2020)
[196] Documentary: Zero-days, security leaks for sale (2014), at 14'45"
[197] *Id.* at 13'58"
[198] https://blog.f-secure.com/top-5-countries-with-offensive-cyber-capabilities/ (retrieved on 20 Feb. 2020); https://www.fxempire.com/education/article/so-who-has-the-most-advanced-cyber-warfare-technology-444874 (retrieved on 20 Feb. 2020)
[199] https://www.stripes.com/news/hackers-earn-275-000-in-bug-bounties-after-finding-security-flaws-on-army-websites-1.615168 (retrieved on 20 Feb. 2020)

However, as for the offensive perspective, there is no public information. In some sense, a cyber weapon is about which vulnerability will be used, and the vulnerability is the first step for controlling and dominating defence and offence in cyberspace.

5.6 Chapter summary

In this chapter, first we learned that bug hunters are distributed all over the world, not only in developed countries but also in developing countries. From the statistics, we found that financial incentives constitute their main motivation for bug hunting.

In addition, we compared the three markets for vulnerabilities: the white market, the grey market, and the black market. We find that there is a clear competitive relationship between the white market and both the grey and the black markets. There is some complementarity between the grey market and the black market. This is because the respective buyers in these two non-white markets have different requirements for the risk level of vulnerabilities. The main buyers in the grey market are the governments, who need high-risk and secretive vulnerabilities such as zero-days. Normal buyers in the black market are criminal organizations, and they are likely to need a vulnerability toolkit that exploits a vulnerability maybe of a lower risk level, but affordable and easy to operate.

Based on the conclusions in this chapter, we will build an economic model in Chapter 6 to discuss the theoretical price of vulnerabilities in the black market.

Chapter 6: The Price Model

We have learned about the intrinsic value of a vulnerability in Chapter 4 and about the different vulnerability markets in Chapter 5. From various bounty programs of the software vendor, we can know the prices of vulnerabilities in the white market. The subscription contracts between the resellers and government agencies reflect the price level of vulnerabilities in the grey market, although most of them are classified. We will discuss the role of the governments thoroughly in Chapters 7 to 9. In this chapter, we apply an auction model to theoretically study the vulnerability price in the black market.

The price in the white market is relatively transparent. As we have noticed in chapter 5, there is competition between the white market and markets outside it. Based on this, we suppose a seller will set the white market price as his reserve price when making his decision. In other words, the black-market price is equal to the reserve price plus an incremental price. This incremental part can be understood as a risk premium[200]. Without this incremental part, the seller will not sell his discovery in the black market, and the buyers there will get nothing. Having the white market price as the reserve price reflects the fact that the white market price is the bargaining power of a seller in the black market. The higher the white market price, the higher the prices in other markets.

In the black market, transactions are often conducted in a confidential way. When there are several buyers at the same time, they don't know about each other, let alone exchange information. To minimize the risk that the seller will sell the same vulnerability information to others secretly, the buyer and seller normally agree on payments over a period of time, as introduced in Chapter 5. If there is proof that the seller did not sell on an exclusive basis or if the vulnerability is patched before the timeframe is over, the buyer can terminate payments early.

All these fit exactly the classic auction model named “sealed-bid first-price auction”, which originally models a situation where “all buyers place their bids in sealed

[200] The term of “risk premium” reflects the maximal risk that the seller is willing to take. If the real risk is lower than this maximal risk, there exists room for profit.

envelopes and the highest bidder wins and pays the highest bid"[201]. There are two important features of this model: 1) each buyer must form an expectation of what are the bids made by his rival buyers and different expectations will result in different bids; 2) each buyer's valuation of the subject is independent of the valuations of his rival buyers. There is no common value shared among the buyers. Each buyer is assumed to draw his valuation from a distribution and each draw is statistically independent of the draws made by others. These two features are in line with the reality in the vulnerability black market. We apply this sealed-bid first-price auction model here to analyse the incremental part of the price of a vulnerability[202].

We follow the prerequisites that 1) the buyers do not share any common value and 2) each buyer has his own valuation which is independent of the valuations of his rival buyers. We also assume that each buyer draws his valuation from a uniform distribution. In addition, each buyer must anticipate the bids made by his rivals before his own bid.

6.1 Setting the market parameters

(a) Players

We set one seller and n anonymous buyers. These n buyers bid for the vulnerability offered by the seller.

(b) Price structure

The price in the black market is set as a composition of two parts. One is the reserve price b_w, which is the price level from the white market, i.e., the bounty amount (the "b" in b_w means "bounty" and the "w" means "white"). We suppose b_w is given in our model, because the white market price is transparent, and it is logical that the seller will regard it as his reserve price in the black market. If he cannot get a good price outside the white market, at least he can turn back. The other part is the incremental price from the black market b_b (the big "b" in b_b means "bid" and the small "b" means "black"). All the buyers compete on this incremental part. The highest bidder for the incremental part wins the competition. The final price in the black market, which

[201] For a detailed knowledge of the auction model, see Shy (2008), Chapter 10.

[202] The original model models the total price, but I modify and apply it to model the incremental price of a vulnerability. The total price in my thesis includes one part of incremental price and the other part of reserve price.

the seller can receive for the transaction, p_b, is the sum of the reserve price b_w and the incremental price b_b, or $p_b = b_w + b_b$.

(c) Valuation and bid

Valuation is a mental activity, while placing a bid is an action. Each buyer forms his valuation of the incremental price first, then offers his bid for this part. We define the possible valuation range of the incremental price as $[0, V^H]$, where V^H is the possible highest valuation. The distribution of valuation V follows a uniform distribution.

(d) Actions

A buyer $i \in N$, where N is the set of buyers and the number of the elements in N is n, draws his valuation v_i from the interval $[0, V^H]$ with equal probability. The valuation v_i is buyer i's maximum willingness to pay for the incremental price in the black market, where $v_i \geq 0$. Each buyer only knows his own valuation without knowing the valuations of others, except that all other buyers' valuations are randomly distributed on the interval $[0, V^H]$ with equal probability. Then he bids a price $b_i(v_i)$ accordingly, where his bid b_i is a function of his valuation v_i, $0 \leq b_i \leq v_i$. As to the buyer whose valuation $v_i = 0$, he bids a price $b_i(0) = 0$. In our model, the vulnerability is sold to one buyer exclusively. We do not consider the problem of double dipping, in which the same vulnerability is sold to more than one buyer secretly and simultaneously. This is in line with reality, as explained in section 5.5.2 of this thesis. So the action of each buyer is simple: to bid according to his own valuation. All the buyers take their actions once and for all, simultaneously and independently.

(e) Utilities

The utility of buyer i is affected by all the buyers' bidding prices. Its realization is not known to buyer i before all other players take their actions simultaneously. If buyer i wins in the bidding, his utility function will be in an expected form. It will consist of two parts: one part is the difference between v_i and b_i: $v_i - b_i$. This is the utility of buyer i, when it is certain to be realized. The other part is a probability $\omega_i(b_i) \in [0, 1]$, at which buyer i will win if he bids the price of b_i. The expected utility from the black market is the product of these two parts: $(v_i - b_i) \times \omega_i(b_i)$, $v_i, b_i \in \mathcal{R}_+$, $\omega_i \in [0, 1]$. So the complete utility of buyer i from the black market is $u_i =$

$(v_i - b_i) \times \omega_i(b_i)$.

(f) Sequence

The sequence in our model is as follows: First, each buyer i learns his own valuation v_i for the incremental part in the price structure. Next, each buyer i bids his price b_i simultaneously only knowing his rival buyers' valuations are randomly drawn from the same uniform distribution. Finally, the single seller sells the vulnerability to the highest bidder. The final price is the price from the white market plus the highest bid price for the incremental part. This final price is the income to the seller.

To summarize the above (a) to (f):

The final price in the black market p_b includes two parts: the reserve price b_w and the incremental price b_b: $p_b = b_w + b_b$. The seller will take the bounty amount b_w as his reserve price when he sells in the black market. The incremental price b_b reflects the risk premium between the illegal market and the legal market.

I assume that there are n buyers and one bug hunter as the single seller. Each buyer draws his valuation v_i from the interval $[0, V^H]$, then bids a price b_i. The utility function of buyer i is: $u_i = (v_i - b_i) \times \omega_i(b_i)$.

The seller, the vulnerability discoverer, receives all the bids from the buyers and then chooses the highest bidder b_i as the price for the incremental price b_b. His income from the transaction in the black market equals the final price p_b he receives, which is the sum of b_w and b_b.

Furthermore, we must note that both the "valuation" and "bidding price" in this chapter are referring to the incremental price or the incremental part, which will not be mentioned specifically in the following text. Next, we apply the auction model to get the bidding prices for the incremental part first, then the expected incremental price. Based on this, we can get the expression of the whole price in the black market.

6.2 Assumptions

1) All the buyers bid independently and spontaneously. Each buyer only knows his own

valuation without knowing the valuations of other buyers, except that all other buyers' valuations are randomly distributed on the interval $[0, V^H]$ with equal probability. We also assume that these buyers are experienced and understand the market size and number of participants very well. So every buyer can estimate that there are n-1 other competitors except himself.

2) The seller also knows that each buyer's valuation is drawn randomly from the interval $[0, V^H]$ with equal probability.

3) The buyer's valuation and bidding price obey the uniform distribution;

4) The seller will not wait to sell[203], if his profit is positive.

6.3 Bidding prices for the incremental part

With no loss of generality, we focus on the actions available to buyer i, who sets his bid b_i. The probability that buyer i wins the aution is

$$\Pr\{b_i > max\{b_1, b_2, \dots b_{i-1}, b_{i+1}, \dots b_n\}\} = \left(\frac{b_i}{B^H}\right)^{n-1}$$

where B^H is the highest bidding price among the buyers. Similar to the distribution of valuation, we assume that any bidding price b_i also follows a uniform distribution, which is our assumption 3. To guarantee that buyer i wins the auction, the bidding price of any his rival must be located in the range $[0, b_i]$. Since the whole range is $[0, B^H]$ and we assume the distribution of the bidding price as a uniform distribution, the probability that the buyer i wins against one competitor is $\frac{b_i}{B^H}$. There are $n-1$ competitors in total, so that the probability that buyer i wins the auction is $\left(\frac{b_i}{B^H}\right)^{n-1}$.

In the case where buyer i wins the auction, his surplus is the difference between his valuation v_i and his bid b_i, $surplus = v_i - b_i$. The utility function of buyer i, i.e. his expected surplus, is the product of his surplus if he is the winner, and the probability

[203] This is in line with the actual situation. According to Herr, Schneier & Morris (2017): "For Android and Chrome, more than 60% of all rediscoveries takes place in the first month after the original vulnerability's disclosure". The same vulnerability is possible to be rediscovered by others very soon. So, the seller will choose to close the deal once he receives all the bidding prices.

that he wins:

$$U_i(b_i) = (v_i - b_i)\left(\frac{b_i}{B^H}\right)^{n-1}$$

Any buyer i chooses b_i to maximize his utility function.

$$maxU_i(b_i) = max(v_i - b_i)\left(\frac{b_i}{B^H}\right)^{n-1}$$

The first-order condition for maximum utility is $\frac{dU_i(b_i)}{db_i} = 0$.

$$\begin{aligned}
\frac{dU_i(b_i)}{db_i} &= \frac{d\left[(v_i - b_i)\left(\frac{b_i}{B^H}\right)^{n-1}\right]}{db_i} \\
&= (v_i - b_i)\frac{d\left[\left(\frac{b_i}{B^H}\right)^{n-1}\right]}{db_i} + \left(\frac{b_i}{B^H}\right)^{n-1}\frac{d(v_i - b_i)}{db_i} \\
&= (v_i - b_i)(n-1)\left(\frac{b_i}{B^H}\right)^{n-2}\frac{1}{B^H} + \left(\frac{b_i}{B^H}\right)^{n-1}(-1) \dots\dots\dots * \\
&= (v_i - b_i)(n-1)\left(\frac{b_i}{B^H}\right)^{n-1}\frac{1}{b^i} - \left(\frac{b_i}{B^H}\right)^{n-1} \\
&= (v_i - b_i)\left(\frac{b_i}{B^H}\right)^{n-1}\frac{(n-1)}{b^i} - \left(\frac{b_i}{B^H}\right)^{n-1} \\
&= \left(\frac{b_i}{B^H}\right)^{n-1}\left[(v_i - b_i)\frac{(n-1)}{b^i} - 1\right] \\
&= \left(\frac{b_i}{B^H}\right)^{n-1}\left[\frac{(v_i - b_i)(n-1) - b^i}{b^i}\right] \\
&= \left(\frac{b_i}{B^H}\right)^{n-1}\left[\frac{(v_i - b_i)n - (v_i - b_i) - b^i}{b^i}\right] \\
&= \left(\frac{b_i}{B^H}\right)^{n-1}\left[\frac{(v_i - b_i)n - v_i + b_i - b^i}{b^i}\right] \\
&= \left(\frac{b_i}{B^H}\right)^{n-1}\left[\frac{n(v_i - b_i) - v_i}{b_i}\right]
\end{aligned}$$

In other words, to maximize the utility, the condition $\frac{dU_i(b_i)}{db_i} = \left(\frac{b_i}{B^H}\right)^{n-1}\left[\frac{n(v_i-b_i)-v_i}{b_i}\right] = 0$ must be satisfied, which mathematically means that part of the numerator must be equal to zero: $n(v_i - b_i) - v_i = 0$. Solve $n(v_i - b_i) - v_i = 0$ for b_i yields: $b_i = \frac{(n-1)v_i}{n}$.

To guarantee the validity of first-order condition, we test the related second-order condition: $\frac{d^2U_i(b_i)}{db_i{}^2}$ to see what is the condition to make $\frac{d^2U_i(b_i)}{db_i{}^2} < 0$. For simplicity of calculation, we directly use an intermediate step of the previous calculation of first-order condition, which is marked with "*":

$$\frac{dU_i(b_i)}{db_i} = (v_i - b_i)(n-1)\left(\frac{b_i}{B^H}\right)^{n-2}\frac{1}{B^H} + \left(\frac{b_i}{B^H}\right)^{n-1}(-1)$$

Then the second-order derivative

$$\begin{aligned}
\frac{d^2U_i(b_i)}{db_i{}^2} &= \frac{d}{db_i}\left(\frac{dU_i(b_i)}{db_i}\right) \\
&= \frac{d}{db_i}\left((v_i - b_i)(n-1)\left(\frac{b_i}{B^H}\right)^{n-2}\frac{1}{B^H} + \left(\frac{b_i}{B^H}\right)^{n-1}(-1)\right) \\
&= \frac{d}{db_i}\left(\frac{v_i(n-1)}{(B^H)^{n-1}}(b_i)^{n-2} - \frac{(n-1)}{(B^H)^{n-1}}(b_i)^{n-1} - \frac{1}{(B^H)^{n-1}}(b_i)^{n-1}\right) \\
&= \frac{v_i(n-1)}{(B^H)^{n-1}}(n-2)(b_i)^{n-3} - \frac{(n-1)}{(B^H)^{n-1}}(n-1)(b_i)^{n-2} - \frac{(n-1)}{(B^H)^{n-1}}(b_i)^{n-2} \\
&= \frac{v_i(n-1)}{(B^H)^{n-1}}(n-2)(b_i)^{n-2}\frac{1}{b_i} - \frac{(n-1)}{(B^H)^{n-1}}(n-1)(b_i)^{n-2} - \frac{(n-1)}{(B^H)^{n-1}}(b_i)^{n-2} \\
&= \frac{(n-1)}{(B^H)^{n-1}}(b_i)^{n-2}\left[\frac{v_i(n-2)}{b_i} - (n-1) - 1\right]
\end{aligned}$$

To gurantee $\frac{d^2U_i(b_i)}{db_i{}^2} < 0$, $\frac{v_i(n-2)}{b_i} - (n-1) - 1 < 0$ must be satisfied. Accordingly we have the second-order condition: $b_i > \frac{(n-2)v_i}{n}$. Our solution for first-order condition is $b_i = \frac{(n-1)v_i}{n}$, it is obvious $\frac{(n-1)v_i}{n} > \frac{(n-2)v_i}{n}$, given $v_i > 0, n > 0$. The solution for

first-order condition $b_i = \frac{(n-1)v_i}{n}$ satisfies the requirement of second-order condition automatically. So far the test of second-order condition is completed and the solution $b_i = \frac{(n-1)v_i}{n}$ is valid.

Now we can write our result in a more general way. Each buyer i with valuation v_i bids $b_i = \frac{(n-1)v_i}{n}$, i.e.

$$\begin{pmatrix} b_1 = (n-1)v_1/n \\ b_2 = (n-1)v_2/n \\ . \\ . \\ . \\ . \\ . \\ . \\ b_n = (n-1)v_n/n \end{pmatrix}$$

These n equations constitute a Nash equilibrium, in which each bidder maximizes his own utility. None is willing to move becasuse none can benefit himself by unilaterally deviating from the equilibrium, given that all other competitors stick to their bid equations presented here.

To summarize the above, we have worked out the equilibrium bidding prices of each vulnerability buyer:

$$b_i = (n-1)v_i/n, i = 1, 2, \ldots,$$

6.4 The incremental price

From the equilibrium solution of the auction bids above, we see it is the valuation of the vulnerability of each buyer that decides his bid, i.e., the bidding price is the function of the valuation. The valuation is what each buyer has in mind independently, while his bidding price is a function of the valuation combined with market conditions.

In addition, we can observe that the bidding price b_i is a monotonically increasing function of the valuation v_i. Behind a higher bidding price b_i there must be hidden a higher valuation v_i. The key factor to become a winner in the auction is to have a higher valuation[204].

[204] One may wonder whether it is possible that buyer A with a higher valuation than buyer B bids lower than B, which would lead to the result that player B becomes the winner? The answer to that question is that this possibility

Furthermore, each buyer's valuation determines the probability that he will be the winner in the auction. This means no other valuation exceeds the valuation of the winner. Since the valuation is made by each buyer independently, given an exact valuation $\tilde{V}$, $\tilde{V} \in [0, V^H]$, the probability that the highest valuation among n buyers does not exceed $\tilde{V}$ is $\left(\frac{\tilde{V}}{V^H}\right)^n$. Note here the power is n, which means not only the other $n-1$ valuations but also the highest valuation $v_i = \tilde{V}$ itself are compared with $\tilde{V}$. It ensures no valuations escape outside the range $[0, \tilde{V}]$. The power of the expression $\left(\frac{\tilde{V}}{V^H}\right)^n$ is n, which means we compare $\tilde{V}$ with all the valuations of n buyers.

The incremental price from the black market is an expected value, which the seller faces before his decision-making. Two important components are found here. One is the bidding price which is the function of the valuation. The other is the probability to win in the auction which is also the function of the valuation. The expected value of the incremental price in the black market is the sum of the products of these two parts above given all possible valuations.

To calculate the expected value of the incremental price, we need the density function associated with the probability function because the distribution of the valuation is continuous. The density function is $\frac{d(\frac{v}{V^H})^n}{dv} = n(V^H)^{-n}v^{n-1}, for\ 0 \le v \le V^H$. The bidding price is a function of valuation, i.e. $b = \frac{(n-1)v}{n}$, which is the result in last section. So the expected value of the incremental price is the integral of the product of the density function and the bid function from 0 to V^H:

$$b_b = \int_0^{V^H} \left[\frac{n}{(V^H)^n}v^{n-1}\right]\left[\frac{(n-1)}{n}v\right]dv = \frac{n-1}{n+1}V^H$$

does not exist in equilibrium. The equilibrium state refers to the final state after sufficient experience has been accumulated. If this happens once by chance, it is not the final equilibrium state, because player A can change his position through his adjustment in the next turn. Although our auction is only one turn, it concludes the equilibrium solution, which is the stable state in the final turn after all the players have accumulated enough experience and are able to make the most rational decision. Nobody is willing to move from his position by changing his action, given all the others unchanged. The equilibrium solution obtained is a theoretically stable solution.

The specific calculation process of the bug hunter's expected revenue is as follows:

$$b_b = \int_0^{V^H} \left[\frac{n}{(V^H)^n} v^{n-1}\right]\left[\frac{(n-1)}{n} v\right] dv$$

$$= \int_0^{V^H} \left[\frac{n}{(V^H)^n} v^{n-1}\right]\left[\frac{(n-1)}{n} v\right] dv$$

$$= \int_0^{V^H} \left[\frac{n-1}{(V^H)^n}\right][v^n] dv$$

$$= \left[\frac{n-1}{(V^H)^n}\right] \int_0^{V^H} v^n dv$$

$$= \left[\frac{n-1}{(V^H)^n}\right]\left[\frac{1}{n+1}\right][(V^H)^{n+1} - (0)^{n+1}]$$

$$= \frac{n-1}{n+1} V^H$$

$$\therefore b_b = \frac{n-1}{n+1} V^H$$

6.5 The total price and the expected revenue to the seller

We suppose the bounty amount b_w from the white market is given. From the calculation above, we know the incremental price from the black market $b_b = \frac{n-1}{n+1} V^H$. The total price p_b in the black market calculated by the seller is his reserve price b_w plus the expected incremental part $b_b = \frac{n-1}{n+1} V^H$:

$$p_b = b_w + \frac{n-1}{n+1} V^H, i = 1, 2, \dots, n$$

This total price is also the expected revenue from the black market to the seller, when he makes his decision whether to sell the vulnerability in the black market.

6.6 Analysis of the model result

By applying the sealed-bid first-price auction model, we conclude two things:

- The bidding price for the incremental price $b_i = (n-1)v_i/n, i = 1, 2, \dots, n$, which is the Nash equilibrium solution. This price describes the demand side of the vulnerability trade.
- The price in the black market $p_b = b_w + \frac{n-1}{n+1} V^H (i = 1, 2, \dots, n)$, which is also the expected revenue of the black-market trade to the seller, or the vulnerability finder. This

price describes the supply side of the vulnerability trade.

We suppose all the participants in the auction are rational people, and one underlying assumption is that they have a good understanding of the market and have rich auction experience. These are reflected in the facts that the number of the players is known[205] and the valuation of any buyer is independent of others[206]. Because only the winner has positive utility, every buyer will do his best to ensure his success.

6.6.1 The equilibrium bidding price

From the form of the equilibrium solution $b_i = \frac{(n-1)v_i}{n}$, we observe the following properties[207]:

(a) b_i increses monotonically with v_i, i.e. $v_k \geq v_j \Leftrightarrow b_k \geq b_j$, for all buyers $j, k = 1, 2, \dots, n$. It means that a buyer with a higher valuation bids higher than a buyer with a lower valuation. As we have explained before, the situation in which the winner who bids higher but with a lower valuation will not happen, because this situation is not stable. Another buyer who has a higher valuation can take action to raise his bidding price to win. Our solution is the equilibrium solution, which is stable and no one has an incentive to move from it. In this equilibrium status, the buyer with the highest valuation is to bid highest.

The real implication of this property is that if the black market is sufficiently open, buyers who urgently need a high-risk vulnerability most, such as some bad governments or criminal groups, can get the vulnerability by raising their prices.

(b) b_i increases monotonically with n. That is, every buyer increases his bid when the number of the buyers increases. A bigger number of buyers means the probability of winning to every buyer is lower, thus the buyers increase their bids correspondingly. When n is a very big number, b_i will be close to v_i. Formally, $b_i \to v_i$ as $n \to \infty$.

[205] In reality, although the exact number is impossible to get, as an experienced buyer who knows the market quite well can estimate the rough number of his competitors.
[206] This means the buyer is quite experienced and has objective knowledge about how much is the vulnerability worth to him.
[207] Shy (2008), p. 349.

(c) b_i is smaller than v_i as long as $v_i > 0$. If v_i reaches the bottom of the range of the valuation 0, $v_i = 0$, there is no other non-negative value smaller than 0 for b_i, so that $b_i = v_i = 0$. This is easy to understand: The difference between v_i and b_i is the surplus for a buyer.

(d) b_i is not influenced by the possible highest valuation V^H. Every buyer bids only according to his own valuation v_i.

6.6.2 The total price

The total price in the black market is influenced by three factors: the price in the white market, the total number of players in the black market, and the expected highest valuation in the black market.

(a) The price in the white market is the reserve price of the seller. We have discussed this before. The reserve price acts as a kind of bargaining power of the seller. Buyers have to pay more than the reserve price level to get what they want in the black market.

(b) With an increasing number of players n, $\frac{n-1}{n+1}V^H = (1 - \frac{2}{n+1})V^H$ increases. This reflects the market situation. The more active the black market is, the higher the expected revenue to the vulnerability seller.

(c) A higher V^H, the upper boundary of the possible valuation, leads to a higher expected total price p_b in the black market. Unlike b_i, the expected price p_b is not influenced by any individual valuation v_i. Instead, it is influenced by the possible highest valuation level in the market place as a whole. In reality, the historical highest price for the similar risk level vulnerability may be used as V^H.

(d) Although the individual valuation v_i does not appear in the final expression of the total price p_b, we should notice that the formula of p_b only expresses a static result. It is like the result of a certain time section or time point, where only the highest possible valuation of the market V^H affects the seller's expected revenue. However, if we switch to a dynamic perspective, v_i has its impact. This is because today's v_i may become the highest historical valuation V^H for tomorrow, which will impact

tomorrow's expected revenue in the market.

6.7 Chapter summary

In this chapter, we have applied the auction model to derive the expected price of the black market faced by a vulnerability seller. From our model results, it follows that this expected price of the black market depends literally on three factors: the price level in the white market, the number of players in the black market, and the historically highest willingness to pay, i.e. the valuation V^H, for the difference between a white market and the black market. From a dynamic perspective, every buyer's valuation for today will collectively influence the estimate of possible highest valuation for tomorrow.

Based on the result of our model, we see that as long as a black market exists, buyers in need of crucial vulnerabilities can achieve their goals by raising their offers close to their inner valuations. With an expectation of increasing price differences between the black market and the white market, vulnerabilities finders, who are mostly profit oriented, are likely to enter the market places outside the white one.

Chapter 7: Preliminary Discussion about the Government

As explained in Chapter 5, similar price mechanisms and price levels can be observed in the grey and the black market[208]. Some government agencies, e.g., intelligence agencies, are active not only in the grey market but also in the black market[209]. In this chapter, I will extend the price model in Chapter 6 to analyse the impacts from the involvement of government agencies in the black market. Then, I continue to discuss the role of the government from the implications of this extended model.

7.1 A brief review of the non-white markets

In Chapter 6, we calculated the theoretical price of the vulnerability in the black market. As we know from Chapter 5, the price levels of vulnerabilities in non-white markets, i.e., the grey market and the black market, are comparable. Therefore, the price level obtained from the price model for the black market can be applied to the grey market. This price mechanism in these non-white markets is described by Hoffman Alex (2019) as selling to the highest bidder and those bid winners intend to use vulnerabilities offensively.

This argument can be made more precise. As the grey market is legal and the black market is illegal, the seller will face greater risks in the black market, which can be interpreted as his costs for conducting illegal activities. Because trading in the black market is illegal, the seller must deduct these costs from his revenues (i.e., the market price he receives) to calculate his profit. However, for a grey market trade, the seller's profit is the market price per se. Therefore, at the same price level, a rational seller will always choose the grey market. In reality, many transactions in the grey market are subscription-based to guarantee the seller's profit, as introduced in section 5.5.1 of this thesis.

It is argued that the distinctions between the grey and black markets seem to be ad hoc

[208] See section 5.5.1 in this thesis.

[209] Hoffman (2019): "These markets are driven by the consumers: the NSA ……, other government agencies, intelligence/defence "pure plays" (that is, companies whose primary revenue is government contracts), foreign governments, and occasional independent bad actors. This industry contributes to the cyber-mercenary backbone of the much larger military–industrial-complex spine and involves many of the same players."

and arbitrary, and the vulnerability industry contributes to the cyber-mercenary backbone of the much larger military–industrial-complex spine[210]. It is obvious that government agencies and a host of bad actors, from adversarial nation states to criminal gangs, compose the main array of actors[211].

In addition, a lot of money is involved in the non-white markets. According to data on the grey market in 2019, Zerodium, a leading platform for vulnerabilities, offered up to US$2 million[212] for high-risk zero-days[213], and the ultimate destination for and use of these would not be disclosed[214].

In the following, we will model the impacts of government agencies' involvement in the black market on the general cybersecurity.

7.2 The extended model

7.2.1 Settings of the model

In this section we design a model to study the probability that a vulnerability will flow to criminals in the black market, considering the involvement of government agencies.

Following the same settings and assumptions of our price model in chapter 6, we suppose there are n buyers in the black market. Further, we suppose that within these n buyers, the proportion of criminals is β, i.e., βn buyers are criminals. The rest are intelligence or military agencies. Here we notice $0 < \beta < 1$ and β equals the total number of criminals divided by total buyers n in the black market.

The seller will have a minimum requirement for the extra income to be gained in the illegal market, supposing that the white market is a legal market and hence risk-free. This minimum requirement for extra income equals the expected penalty for illegal transactions in the black market. A higher expected penalty leads to a higher minimum requirement for extra income. If this minimum requirement is not reached, the seller

[210] Hoffman (2019)
[211] Schwartz & Knake (2016)
[212] Zerodium, "Our exploit acquisition program." https://zerodium.com/program.html (retrieved on 20 Apr. 2020).
[213] Goodin (2019)
[214] Hoffman (2019)

still will not sell his discovery in the black market. For instance, let us suppose that the penalty can be quantified to 100, and the probability of being traced in an illegal transaction is 50%. The expected penalty is 50 in this case, which equals the seller's minimum requirement for extra income in the black market[215].

Following the above instance, let's continue to suppose two scenarios: in scenario A, the white market price is 100, and the black-market price is 160; in scenario B, the white market price is 100, and the black-market price is 140. In scenario A, the real extra income for a transaction in the illegal market is 60, which is the difference between 160 and 100. In scenario B, similarly, the real extra income for a transaction in the illegal market is 40. Here we suppose that sellers are risk neutral. In scenario A, a seller will choose the black market to trade, because 60, the real income, is higher than 50, the seller's minimal requirement of extra income. In other words, the seller's profit in the black market is 10, which is a positive number. In scenario B, a seller will not choose the black market to trade, because 40, the real income, is lower than 50, the seller's minimal requirement of extra income. In other words, the seller's profit in the black market is -10, which is a negative number.

Now we see if the income difference between the illegal market and the legal market cannot cover the seller's minimal requirement of extra income for an illegal transaction, which reflects the expected penalty level, he will stick to the legal market. We set the seller's minimal requirement of extra come as V_r.

7.2.2 Scenario "0" - without government agencies

In this scenario "0" that the government agencies are not active in the black market, there are only βn buyers in the black market, most of whom are criminals. Here the "0" means "no government involvement". The probability that the seller will turn back to the white market is $\left(\frac{V_r}{V^H}\right)^{\beta n}$, i.e., every individual valuation v_i from these βn

[215] The white market is the comparison base, rather than the grey market. This is because the buyers in the grey market are government agencies. These government agencies only need vulnerabilities with specific functions, for instance, those of intelligence value. There are a considerable number of vulnerabilities that are not demanded in the grey market. In comparison, the demands for vulnerabilities in the white market and the black-market are more general and extensive. In our discussion, it is more common to take the white market as the comparison base.

buyers is smaller than the valuation V_r set by the seller. We use $p_0(\beta)$ to stand for the probability that the vulnerability will flow to any of the criminals in this scenario "0". Accordingly, $p_0(\beta) = 1 - \left(\frac{V_{(r)}}{V^H}\right)^{\beta n} = 1 - \left[\left(\frac{V_{(r)}}{V^H}\right)^n\right]^{\beta}$.

7.2.3 Scenario "1" - with government agencies

In the scenario "1" that the government agencies are involved in the black market, there are n buyers, including βn criminals and $(1-\beta)n$ government agencies. The probability that the seller will turn back to the white market is $\left(\frac{V_r}{V^H}\right)^n$. So, the probability that the vulnerability will flow into the black market is $1 - \left(\frac{V_r}{V^H}\right)^n$. Based on our assumptions in section 6.2, the probability that the vulnerability will flow to any of the criminals is $\left[1 - \left(\frac{V_r}{V^H}\right)^n\right]\beta$. We use $p_1(\beta)$ to stand for this probability: $p_1(\beta) = \left[1 - \left(\frac{V_{(r)}}{V^H}\right)^n\right]\beta$.

7.2.4 Properties to discuss

(a) $p_0(\beta)$ is a concave curve and $p_1(\beta)$ is a line.

(b) Given conditions $0 < \left(\frac{V_{(r)}}{V^H}\right)^n < 1$ and $0 < \beta < 1$, the curve of the function $p_0(\beta)$ is graphically above the line of the function $p_1(\beta)$, except for two endpoints where $\beta = 0, \beta = 1$. This can be proved mathematically, and it is more intuitive on the graphics. See the following two illustrations given different $\left(\frac{V_{(r)}}{V^H}\right)^n$ values. Figure 6 illustrates the case when $\left(\frac{V_r}{V^H}\right)^n = 0.2$. Figure 7 illustrates the case when $\left(\frac{V_r}{V^H}\right)^n = 0.5$.

Figure 6: Illustration in case of "0.2"

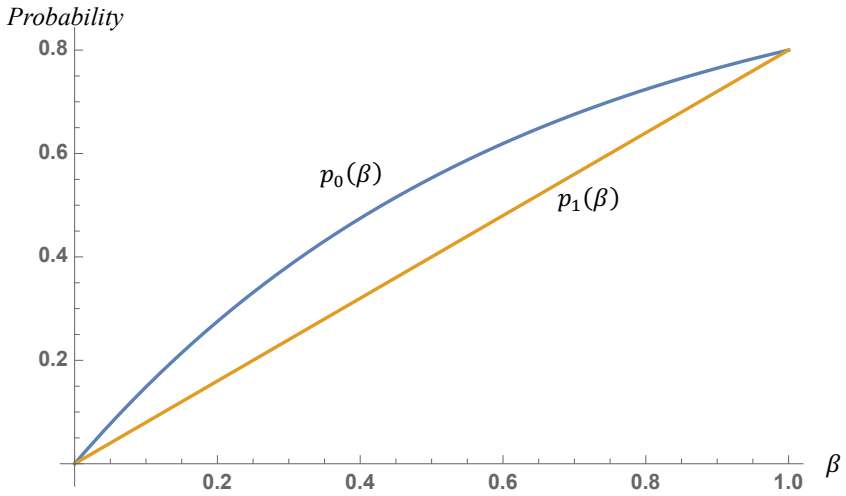
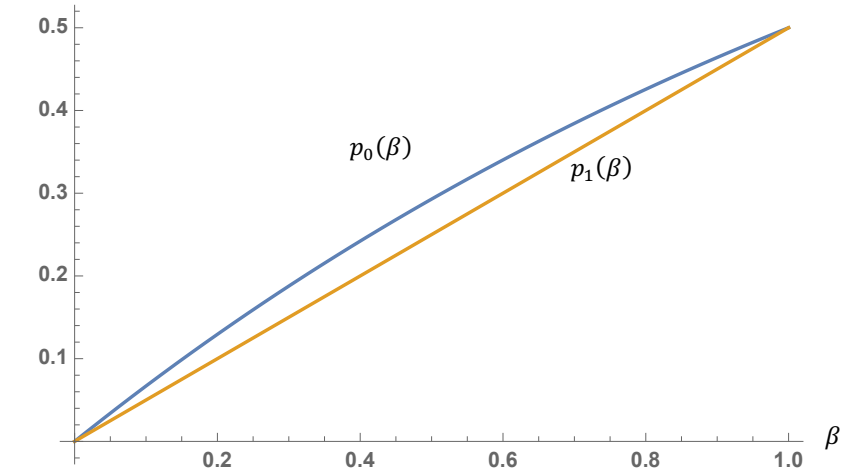


Figure 7: Illustration in case of "0.5"

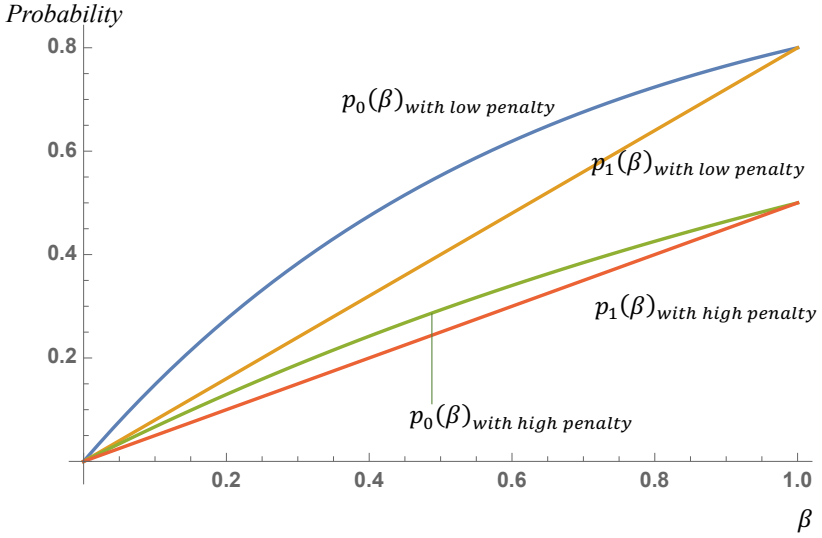


On the two illustrations above, the blue curves present $p_0(\beta)$ and the yellow curves present $p_1(\beta)$. Given that all other conditions are equal, the probability that criminals get the vulnerability is higher without government involvement. This is because in the scenario with government involvement, government agencies compete with criminals to get the vulnerability. It seems good if the government wins the competition, but it

can be worse in the case that the government's stockpile can be easily hacked. This hacked result could also be imagined or presented graphically: the line $p_1(\beta)$ will move in parallel upwards to a position above $p_0(\beta)$.

(c) According to the value of $\left(\frac{V_r}{V^H}\right)^n$, we have different sets of $p_0(\beta)$ and $p_1(\beta)$. The lower value of $\left(\frac{V_r}{V^H}\right)^n$ will lead to higher values of set of $p_0(\beta)$ and $p_1(\beta)$. The lower the value of $\left(\frac{V_r}{V^H}\right)^n$, the bigger the difference between $p_0(\beta)$ and $p_1(\beta)$. Graphically in Figure 8 below, the blue curve and the yellow line are with lower value of $\left(\frac{V_r}{V^H}\right)^n$, and the green curve and the red line are with higher value of $\left(\frac{V_r}{V^H}\right)^n$. In other words, when V^H and n are fixed, a higher penalty leads to a lower probability that the vulnerability flows to criminals. And the impact of the change of the penalty amount is very significant. This is what the policy makers should take into account when they want to have fewer vulnerabilities flowing into the hands of criminals.

Figure 8: Comparison of the two cases



In addition, we notice the relationship between the penalty amount and the difference

between the two scenarios. If the penalty level is low, the difference between the "0" and "1" scenarios is big. If the penalty level is high, the difference between the "0" and "1" scenarios is small. In other words, if the penalty is big and effective, the significance of government involvement decreases significantly.

7.3 Implications

1) From the static or short-term perspective, the governments' participation in the black market weakens, to some extent, the probability of the vulnerability flowing to criminals. This only holds under the assumption of exclusive transaction. We assume that the payment mechanism agreed by the buyer and seller can ensure that the seller sells to the buyer exclusively within a specified period. If this assumption is broken, arguments based on this short-term conclusion are untenable.

2) From the dynamic or long-term perspective, the governments' participation in the black market increases not only the number of players who are active in the market, but also the anticipation of the highest valuation in the market, which will lead to both an expectation of increasing revenue and an increasing number of vulnerability discoverers entering the black market[216].

3) Adding to the implications that directly follow from the model, we should realize that the government's stockpile can be hacked successfully, as explained above in Section 7.2.4 (b). If the government fails to keep its vulnerabilities and equivalent tools properly, criminals will not only have the vulnerabilities they paid for in the black market, but also those they stole from the government's stockpile. It will be very risky from a social point of view and harmful, both from the short and long run perspectives.

This point was proven four years ago when the hacking group Shadow Brokers[217] published information on stolen NSA files (including archived zero-days) on the Internet[218]. It was also observed that some "zero-day exploits later used […] had clear connections to the NSA or a related U.S. hacking arm"[219].

---

[216] For detailed information, please refer section 6.6.2 of this thesis.
[217] Schneier (2017)
[218] Hoffman (2019); Perlroth & Sanger (2017)
[219] Hoffman (2019)

4) For governance purposes, it is important to take steps to increase the expectation of transaction penalties in the black market. This expected punishment directly affects whether the seller chooses to trade illegally. Further, in the short run, the impact of a government's involvement in the black market will become less significant with the expectation of severe punishment. This implication is supported by Becker's theory of criminal law, which was formalized by Nobel Laureate Becker Gary in 1968.Becker's theory states that potential criminals are economically rational and respond significantly to the deterring incentives by the criminal justice system. They compare the gain from committing a crime with the expected cost, including the risk of punishment, the possibility of being apprehended, etc.[220]

7.4 Chapter summary

In this chapter, we extended our model from Chapter 6 to analyse the involvement of government agencies in the black market. Although it is socially risky in the long run, it does not seem so bad in the short run, as long as the sale is exclusive. In contrast, it is (even) more important that government agencies prevent their stockpiles from being stolen. Furthermore, it is crucial to increase the expectation of transaction penalties in the black market, as this directly affects the decision-making of the seller.

In the next two chapters, I will continue to discuss the dilemma encountered by the governments, the new ecosystem of cybersecurity they are facing, and related new challenges which they have to reconsider. All these are leading us to a clear and objective understanding of the role of the government and its related policies.

[220] Becker (1968)

Chapter 8: Government's dilemma and the VEP

In the previous chapter, I discussed what are the impacts of government agencies participating secretly in black market transactions. The more common situation is that government agencies acquire vulnerabilities in the grey market. Transactions in the grey market frequently take place through dealers and brokers. This situation inevitably leads to the principal-agent problem in which the interests and objectives of these dealers and brokers are not entirely consistent with the interests and objectives of governments. On the other hand, the grey market operates independently and at cross purposes with software industry initiatives. In order to ensure the interests of the dealers and restrict them from selling to third parties, grey market businesses are often subscription-based or exclusively contract-based. In fact, as long as vulnerabilities are obtained through outsiders, there is an agency problem involved, and its management should be taken into account by the government not only as a buyer in the grey market, but also as a regulator of all markets.

In this chapter, I focus on the responsibilities of governments after obtaining high-risk vulnerabilities, e.g., zero-days. I am going to discuss the role of the government from the perspective of social responsibility - Should government agencies hold their own stockpiles of zero-days rather than reporting them to the impacted vendor directly?

From the perspective of general cybersecurity, the ideal state is that all information about the vulnerability should be reported to the impacted vendor directly. After all, the vendor is in the best position to lead subsequent coordination efforts and finally deliver a patch for the vulnerability. Before a solution is available, the risk of a vulnerability being exploited can be reduced by keeping the number of entities which need to be aware of the flaw to a minimum[221].

However, from the perspective of the government, this issue is not that simple. Although the entire Cyberspace is open and borderless, the related administration and regulation are nation-based and separate. This causes an enormous problem which leads

[221] The importance of vulnerability disclosure policies (9 Aug 2019), https://cybertechaccord.org/the-importance-of-vulnerability-disclosure-policies/ (retrieved on 16 May 2020)

to hidden criminals and malicious state hackers worldwide. These bad actors pose a threat to the national security of various countries, especially democratic countries. Hoffman (2019) identifies this issue as a moral hazard, which "presents governments that purport to be democratic with a conundrum." Governments can either report the vulnerability to the software vendor contributing to the cybersecurity of their own citizens, or they can weaponize it and cloister it in an offensive stockpile for potential future use against adversaries[222].

As discussed in Chapter 7, if the governments' stockpiles were hacked, the probability of cyberweapons falling into the wrong hands would increase, thus social risks would also increase correspondingly.

Whether the government should disclose or keep vulnerabilities has aroused widespread concern in academia and the media. In January 2020, both The Wall Street Journal and The New York Times reported that the U.S. National Security Agency (NSA) alerted Microsoft to a zero-day vulnerability in Windows 10[223]. Neither the software maker, nor the U.S. agency found any evidence that the vulnerability had been exploited maliciously[224]. Public media unanimously commented that NSA "has taken a significant step toward protecting the world's computer systems"[225], which represents "a philosophical shift that the NSA has long sought to balance its dual mission of foreign intelligence and cybersecurity"[226]. Prior to this, NSA had been criticized as "following the agency's typical approach of keeping quiet and exploiting the flaw to develop cyberweapons"[227].

This event seems to herald that the U.S. government has started to attach greater importance to public cybersecurity at the expense of intelligence gathering. In the remainder of this chapter, I will examine systematically the role of the government with this dual mission.

---

[222] Hoffman (2019)
[223] Barnes & Sanger (2020); Volz (2020)
[224] Volz (2020)
[225] Barnes & Sanger (2020)
[226] Volz (2020)
[227] Barnes & Sanger (2020)

8.1 The dilemma: to disclose or to retain

In principle, government agencies are confronted with the following dilemma, when they deal with zero-day vulnerabilities newly discovered by themselves or purchased from outside markets: should they disclose such vulnerabilities, allowing them to be patched as soon as possible, or should they retain these flaws in their stockpiles for national security purposes?[228]

Except for the duty of ensuring general cybersecurity, the government is simultaneously in charge of intelligence gathering, law enforcement, national security, and secret military missions, all of which require the use of zero-day vulnerabilities. Decisions biased towards disclosure by the government are likely to undermine the ability of law enforcement to investigate crimes, intelligence agencies to carry out surveillance operations, and the military to fulfill offensive cyber tasks. On the other hand, decisions biased towards retaining are likely to undercut general cybersecurity, leaving many people open to the threats of cyber-attacks[229].

"To disclose or to retain" is a tough choice that many governments face. For instance, among the US government agencies, opinions on this issue are conflicting. The more defensive-minded agencies are the Departments of Treasury, Commerce, and Homeland Security, who want to disclose the vulnerability information to vendors for improving the nation's cybersecurity. Other agencies such as defence or the intelligence community take the position of national security, by wishing to keep the vulnerability for intelligence or military purposes[230]. The White House acknowledged that "the government sometimes relies on zero-day vulnerabilities for intelligence and other, related purposes, rather than disclosing such vulnerabilities and allowing them to be patched"[231] Furthermore, it was also "categorically rejected in the White House blog that the government should completely forego the vulnerability as a tool to conduct intelligence collection"[232].

[228] Schwartz & Knake (2016)
[229] *Id.*
[230] Healey (2020)
[231] Sanger (2014); Schwartz & Knake (2016)
[232] Schwartz & Knake (2016)

8.2 Government hacking

According to Schwarz and Knake (2016), there are circumstances where retention of zero-days by government agencies for the purposes of law enforcement or national security is legitimate, given conditions such as clear limits and adequate oversight[233].

Mayer (2018) provides a technical framework for analysing government malware and concludes that "government hacking is inherently a search"[234]. When it becomes more and more prevalent that encryption and anonymization tools are used in modern cyber technology, the government will predictably increase its resort to malware and government hacking will only become more common. Vulnerability or related malware have become "one of the few technical countermeasures available to the government" [235] . This is because the increasing pervasiveness of device and communications encryption is frustrating conventional electronic surveillance techniques of law enforcement agencies. To be able to hack is "a legitimate and effective investigative technique" needed by law enforcement agencies, so nothing is inherently wrong with the government agency compromising computer systems for investigation purpose[236].

Schwartz & Knake (2016) illustrate the point by an example: it is better for a law enforcement agency to keep the vulnerability, at least until the end of the investigation, if the law enforcement agency has an ongoing investigation on a suspect and the only information is coming through communications legally intercepted through a previously unknown vulnerability. Mayer (2018) additionally notes, that "appropriate procedural protections are vital" and that "present practices leave much room for improvement".

8.3 US policy: the VEP

Although it sounds reasonable for government agencies to retain vulnerabilities because they might be useful for their missions such as surveillance or law enforcement, government agencies have to face pressure from all sides. Their reputation was

[233] *Id.*
[234] Mayer (2018), p.1
[235] *Id*, p. 90
[236] *Id.*

damaged by accusations that they had known about these security flaws but still held on to them. They were also accused of being responsible for "hundreds of millions of dollars in preventable damage by allowing vulnerabilities to circulate"[237]. The VEP policy is the direct product of the dilemma of disclose or retain. The VEP, Vulnerability Equities Process, is an attempt by the US government to explain how the government determines whether to disclose or to retain a zero-day vulnerability.

8.3.1 What is the VEP

To be precise, in the first place, the VEP is a US policy which seeks to balance two security interests: the national security and the general (commercial and personal) cybersecurity interest[238].

Secondly, the VEP is an outcome of a structured process of the White House, rooted in sensitive criteria of when to disclose a vulnerability or to retain it[239]. When the government or its contractors discover or purchase vulnerabilities, decisions must be made according to VEP to determine whether these vulnerabilities should be revealed to the appropriate vendor for patching or restricted and utilized by federal agencies for the purposes of law enforcement and intelligence missions[240].

Thirdly, the VEP is a deliberate process biased toward responsible disclosure, but it is not governed by any " hard and fast rules", as explained by White House Cybersecurity Coordinator Michael Daniel[241].

8.3.2 History of the VEP

The history of the VEP will help us understand VEP further.

The initiation of the VEP was in 2008 when President George W. Bush ordered the US government to develop a "joint plan" for dealing with offensive cyber capabilities and

[237] Barnes & Sanger (2020)
[238] Schwartz & Knake (2016)
[239] Healey (2020)
[240] Schwartz & Knake (2016)
[241] Daniel (2014)

specifically called for a "Vulnerabilities Equities Process." Two years later the formal policy of VEP was promulgated by the Office of the Director of National Intelligence[242].

In 2013, the Obama administration commissioned the President's Review Group on Intelligence and Communications Technologies ("President's Review Group") to seek to resolve how the government should manage vulnerability equities. In December of the same year, a report containing recommendations was issued by the President's Review Group, but it did not mention the existing VEP[243].

Although this report did not specifically refer to VEP, its content was of great significance to the development of VEP. First, it was recommended that the government should "do nothing to subvert, undermine, weaken, or make vulnerable generally available commercial software". Secondly, it suggested that government security agencies should not be given carte blanche in the use of zero-day vulnerabilities. A senior-level, inter-agency approval process employing a risk-management approach was recommended "before approving use of the zero-day rather than patching a vulnerability". Thirdly, it emphasized that "the interests of citizens should not be dismissed out of hand when the government stockpiles malware"[244]. These three points above were reflected in the original text: "US policy should generally move to ensure that Zero-Days are quickly blocked, so that the underlying vulnerabilities are patched on government and other networks. In rare instances, US policy may briefly authorize using a Zero-Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments"[245].

In 2014 the administration of President Barack Obama revived the VEP. It was testified by Admiral Mike Rogers, head of both NSA and US Cyber Command, that the default position of the VEP was to "disclose", i.e., to disclose vulnerabilities in products and systems used by the US and its allies. This means the VEP has always supposed to prioritize the defensive duty rather than an offensive function. It was further testified

[242] Healey (2020)
[243] Schwartz & Knake (2016)
[244] Hoffman (2019)
[245] President's Review Group (2013)

that “in fact the NSA has always employed this principle”[246]. The New York Times reported that “during the Obama administration, officials said, they shared about 90 percent of the flaws they discovered”[247].

As of January 2020, the VEP policy has been even more clear about giving priority to defence over offence, in spite of the Trump administration’s hawkish cyber position and its secretive cyber war policy[248].

8.3.3 Implementation principles of the VEP

Simply speaking, there are three principles for the implementation of the VEP. First, the majority of VEP decisions should be subject to public debate and scrutiny, although some individual VEP decisions must remain classified. Secondly, not only information like the aggregate number of vulnerabilities discovered, aggregate number of vulnerabilities disclosed, and the length of time during which vulnerabilities are held before disclosure, but also sources and methods of how these vulnerabilities may have been discovered should be released. Thirdly, the information release should be public and official[249].

8.3.4 Priorities of the VEP

There are four major principles that the VEP tries to balance.

To improve US cybersecurity by disclosing major zero-days is the first and most obvious priority. The default of the VEP policy is to disclose. The second priority of the US VEP is to review all high-risk vulnerabilities, so that a small number can be used by intelligence and military with the least impact on US cybersecurity. These first two are of the most importance, as they are “at the centre of the tug-of-war between those wanting to disclose and those pushing to retain”[250]. They emphasize that the primary focus of the VEP is to prioritize public cybersecurity and to protect core Internet infrastructure, information systems, critical infrastructure systems, and the U.S.

[246] Healey (2020)
[247] Barnes & Sanger (2020)
[248] Healey (2020)
[249] Schwartz & Knake (2016)
[250] *Id.*

economy through the disclosure of vulnerabilities discovered by the US government. This overrides the interest in the use of vulnerabilities for lawful intelligence, law enforcement, or national security activities[251].

The other two principles are supposed to provide both internal and external trust.

The third one is to enable internal trust among government departments through interagency coordination. Departments of Treasury and Homeland Security are given a voice in the decision, and typically want to patch as many vulnerabilities as possible and take an opposite position to that of the Department of Defence and intelligence agencies. This critical interagency coordination is allowed by the VEP, which is regarded as "one of few policy levers the White House can adjust to directly favour cyber offence or defence"[252].

The last principle of the VEP is to provide some external assurance. As a process for decision-making about vulnerabilities to underpin the security and economy, the VEP aims to show other nations and industries the mature attitude of the US government on the vulnerabilities[253]. "Public and official release of information about the process with clear oversight" are supposed to enhance public confidence in the government's commitment to core principles[254].

8.3.5 The relevance of VEP in other jurisdictions

So far, no other country worldwide has launched a VEP-like policy of government vulnerability disclosure. In June 2017, the Centre for European Policy Studies (CEPS) formed a Task Force to discuss the implications of software vulnerability disclosure across the EU[255], expecting to "increase the pressure on EU member states to embark on a vulnerability equity process"[256]. However, the focus of the discussion was predominantly on responsible vulnerability disclosure by the private sector rather than the VEP debate across Europe. As of May 2018, only a list of broad "government

[251] *Id.*
[252] *Id.*
[253] *Id.*
[254] Schwartz & Knake (2016)
[255] Pupillo (2017)
[256] Delcheva & Soesanto (2018)

vulnerability disclosure (GVD) characteristics" had been included, pleading for either the EU Commission or the ENISA (European Union Agency for Cybersecurity) to carry out the study of the GVD process implemented by EU member states[257].

It was noted by Robert Hannigan, the former director of Government Communications Headquarters (GCHQ), the British equivalent of NSA, that the UK has its own process running internally within GCHQ and as of November 2017 the UK's intelligence agency had released "over 90% of the vulnerabilities" it knew about. Although the UK process does not have the same involvement of different government agencies as the VEP, Robert Hannigan argued that GCHQ was not doing the disclosure in complete isolation, because the same principles of making judgements were followed and they worked closely with the NSA[258].

In general, little is publicly provided about how other governments handle the knowledge of vulnerabilities in their possession.

8.4 Chapter summary

In this chapter we introduced the dilemma faced by the government: to disclose vulnerabilities for the sake of general cybersecurity or to keep them secret for national security.

Government hacking has been recognized by legal scholars for the purpose of legal enforcement and intelligence, given that more and more advanced encryption and anonymization technologies are used by criminals. Thus, the stockpiling of vulnerabilities by government agencies for temporary use is not necessarily a problem.

The VEP, Vulnerability Equities Process, is the direct product of discussing the dilemma of the government. It is a US balancing policy attempting to explain how the government determines whether to disclose or to retain a zero-day vulnerability. Through this policy, the US government is expressing its attitude on vulnerabilities to the public: The White House gives greater weight to public cybersecurity than to

[257] *Id.*
[258] *Id.*

intelligence gathering. Until recently, European countries have not launched policies similar to the VEP and are deemed to "much less advanced"[259].

In this chapter, I only made a comprehensive introduction to the VEP policy but did not evaluate it. In the next chapter, I will evaluate the VEP policy considering the ever-changing situation with new international challenges.

[259] Delcheva & Soesanto (2018)

Chapter 9: The Role of the Government under New Challenges

In the previous chapter, we introduced the dilemma faced by the government and the VEP policy in response to this. The VEP represents the policy of the US government that was introduced under public pressure and that acts as an open statement of the US government on the issue of state-stockpiled vulnerabilities. The discussion of the VEP in Chapter 8 mostly focused on the normative question of "what should be done", lacking consideration of the ever-changing international background. In order to objectively evaluate the VEP, as well as the role of the government, we need to broaden our vision. As the policy maker and the regulator, a state should also oversee vulnerability issues from a higher strategic level than enterprises or local governments. Therefore, before our evaluation of the VEP policy, it is necessary for us to understand the growth of state-aided hacking and the strategic significance of the vulnerability.

9.1 Covert statecraft: state-aided cyber operations

9.1.1 State-aided hacking as statecraft

The two case studies presented in Chapter 3 are both related to state-aided hackers. In the Stuxnet case, state-aided hackers were accused of being directly involved in cyberattacks. In the WannaCry case, the core component of the malware, the EternalBlue, was stolen from the arsenal of intelligence agency by a foreign hacker group[260].

Today, terms like state-aided hacker, disinformation, and information warfare are familiar to most people. Hacking into other countries' systems is one of the primary ways in which governments can influence and shape geopolitics. Buchanan (2020) studies this issue of the hacker and the state thoroughly and points out that the power and flexibility of hackers are underestimated, especially by those who only focus on visible attacks or an imagined cyber war.

[260] Buchanan (2020)

9.1.2 Disinformation

Disinformation is the most typical state-aided hackers' action, which is not new in international politics, but is a new challenge with the modern cyber background. The popularity of social media allows messages to be spread more broadly and quickly than ever before. A post on modern social media tends to be retransmitted many more times than traditional media at nearly no cost. Much attention has been given to international cases, in which this kind of opportunities are exploited by different actors.

The themes and approaches of disinformation in Ukraine were discussed by the western world, identifying Russian-linked actors as the primary sources of that disinformation[261]. It is argued that the purpose of releasing disinformation is to destabilize the country, suggesting the current government cannot run the country effectively. Another example of disinformation is that the "ongoing conflict in Eastern Ukraine was portrayed as a civil war rather than an external intervention by Russia"[262].

A distinctive feature of disinformation is the manipulation of both the information and the person who receives it. By attacking vulnerabilities on social media platforms and by using fake accounts, governments aim to mobilise and mislead mass opinion. In this case, vulnerabilities are a kind of strategic source for the intelligence agencies in a disinformation campaign. Strategic resources are resources considered crucial to national security concerns and military applications[263]. From the perspective of their utility to intelligence agencies, vulnerabilities like zero-days fully meet this definition. As an intangible resource, the software vulnerability provides state-aided hackers with irreplaceable opportunities. Appendix 1 provides a case of the British Cabinet online meeting in March 2020. If there existed serious vulnerabilities in the software used by the British digital Cabinet, it would not be difficult to understand the potential of vulnerabilities as a strategic resource.

---

[261] Lawson (2019), p.2
[262] *Id.*
[263] https://www.yourdictionary.com/strategic-materials (retrieved on 03 April 2020)

9.1.3 Shaping instead of signalling

Although some scholars and policymakers frequently discuss nuclear or conventional military capabilities as analogies to cyber capabilities, these comparisons are misleading. Cyber capabilities are not as powerful as nuclear weapons or traditional arms, nor do they release deterrence signals as conventional military capabilities. Instead of signalling, which compels a change in the behaviour of the adversary by threatening harm, cyber operations are best conceptualized through shaping subtly, by means of espionage, sabotage, and destabilization, etc.

Cyber operations are showing more and more frequently their shaping effect and cumulative strategic effect. It is government hackers who continually find ways to increase their states' interests and supress those of their adversaries. Buchanan (2020) makes the analogy that the cumulative strategic effect is "like a boxer who wins on points rather than with a knockout blow, … [which] can be effective without being flashy or drawing blood"[264].

9.1.4 Potential threats to democratic elections

It is believed that states who "aggressively mould the geopolitical environment to be more to their liking" reap more benefits than those who "try to hint, coerce, or threaten"[265]. According to CNN, Russia interfered with the 2016 US presidential elections by hacking, claiming that this was an example of a country succeeding in shaping the political environment of another country, at least partially[266]. We have reasons to believe that in future important political events, such as elections in the US or EU, state-aided hackers will continue their hacking attempts to shape public opinion in these democratic countries.

9.2 Evaluation of the VEP or its equivalent in other countries

Based on the previous discussion, we are now ready to evaluate the US VEP[267] or similar policies in other countries within a broader framework of cyberspace

[264] Buchanan (2020), p. 7
[265] Buchanan (2020), p.8; For more notable knowledge, please refer to Fischerkeller & Harknett (2018).
[266] https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html (retrieved on 03 April 2020); https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election (retrieved on 03 April 2020)
[267] For the introduction of the VEP, the Vulnerabilities Equities Process, please refer Chapter 8 of this thesis.

consideration. In the report of CEPS (Centre for European Policy Studies), the European equivalent of the VEP is called GDDP, Government Disclosure Decision Processes. Although by now most EU member states have not yet implemented a government vulnerability disclosure review process, it is a believed that "governments and their agencies have strong policies for reviewing and coordinating the disclosure of vulnerabilities is acritical norm that should be advanced within the EU"[268]. Our evaluation here also applies to those VEP-like policies in other countries.

In general, the VEP policy shows that the central government attaches its biased opinion to cybersecurity to protect its citizens' right in cyberspace. However, we cannot take it for granted that this policy will guarantee what it claims. Some unreliable hidden assumptions could be concluded from this government-disclosure policy.

Unreliable assumption #1:

Intelligence agencies and their adversaries keep overlapping vulnerabilities.

The rationality of this policy only holds if there is a high "collision rate", which refers to a high frequency that the same vulnerability is routinely found by others[269]. In the case of a high collision rate, each vulnerability disclosed to the vendor is "taken directly out of some adversary's arsenal". As Joe Nye, a Harvard international relations scholar, once suggested, "it would perhaps be the sole example in warfare, where disarming yourself also disarms your foes"[270].

In case there is a low collision rate, which means many vulnerabilities are never discovered by others, disclosure actually adds very limited defence. As it was described, "adversaries get a discount on attempts to disarm them"[271].

According to Aitel & Tait (2016), "the prevailing expert opinion is that there is no clear evidence that the operational zero-days of other countries overlap with those of the US".

[268] CEPS Task Force (2018), p. 83
[269] Healey (2020)
[270] *Id.*
[271] *Id.*

Countries are likely to have their own zero-days which are mostly different from each other.

The real collision rate is hard to estimate because each party involved must keep their arsenals secret. Scholars have presented different views. Herr, Schneier & Morris (2017) state that "15% to 20% of vulnerabilities are discovered independently at least twice within a year. For just Android, 13.9% of vulnerabilities are rediscovered within 60 days, rising to 20% within 90 days, and above 21% within 120 days. For the Chrome browser we found 12.57% rediscovery within 60 days……". Ablon & Bogart (2017) focuses on zero-day vulnerabilities, the most critical-severity vulnerabilities. They show in their report of RAND that for a given stockpile of zero-day vulnerabilities, the rate of rediscovery within a year is approximately 5.7%[272]. In recent publications, Healey (2020) estimates an anecdotal figure of 35%.

Roughly speaking, when there exists a collision rate of less than 50%, the disarmament value is small. Let us see an example. There are two countries, A and B. Each country has 100 zero-days, and the collision rate is 40%. Before disclosure, they are evenly matched. If A discloses its zero-days by 100%, A loses its offensive ability completely, while reducing its adversary's arsenal by 40. B has 60 more zero-days than A, as well as absolute strategic advantage. If A discloses its zero-days by 90%, A has 10 zero-days left in hand. B is disarmed by 36 and has 64 in hand. B is still in a position of an offensive advantage.

Absolute offensive advantage normally leads to more intensive attacks. With the existence of adversary B, the disclosure of A can help fix the zero-days known by A, but may lead to more attacks from B targeting the zero-days unknown by A. Healey (2020) argues that "the VEP may provide less actual security than proponents of disclosure expect".

So, the validity of VEP is doubtful when the collision rate of vulnerability discovery is low, for the government agency disarms itself fully yet disarms the adversaries only to

[272] Please refer to section 5.4 in this thesis.

a limited extent. In the EU, it is recommended that "the GDDP (Government Disclosure Decision Process) should be codified into law or other legally binding policy to ensure compliance and permanence"[273]. It is better that a law or policy maker evaluate the real collision rate before a decision is made.

Unreliable assumption #2:

The fault of managing vulnerabilities lies in retaining vulnerabilities.

Retaining vulnerabilities has been criticized for its moral hazard since the Shadow Brokers case, in which NSA's zero-day based tool called "EternalBlue" was stolen from the government agency by a hacker group who named themselves "Shadow Brokers"[274]. Later it was also proved that EternalBlue played a crucial role in both WannaCry and NotPetya, two of the most damaging and disruptive cyberattacks ever[275]. Hoffman (2019) suggests that the government should completely avoid the zero-day supply chain.

However, whether to retain vulnerabilities and how to manage the stockpile of vulnerabilities are two completely different issues. Similarly, an army should not stop possessing missiles only because they can be stolen. Although it was hard to believe, the NSA asserted in the autumn of 2015 that historically 91% of vulnerabilities discovered were disclosed, and the remaining 9%[276] were either kept for national security purpose or already fixed by vendors before NSA's notification[277]. The real problem lies in the management of vulnerabilities after they are acquired, rather than whether these vulnerabilities should be acquired in the first place. If the government agencies cannot keep their cyberweapons secure, they deserve the blame when those exploits are abused by third parties, especially bad ones.

Unreliable assumption #3:

The VEP policy has clear operability.

[273] CEPS Task Force (2018), p. 84
[274] See Chapter 3, section 3.2
[275] Healey (2020)
[276] It is possible that these self-reported numbers are not exact.
[277] Healey (2020)

Instead of a law, the VEP is an administration policy, which does not have very clear operability. When deciding whether to disclose or retain a vulnerability, there are two criteria: a) Is the vulnerability useful to the government agencies? b) Is the vulnerability dangerous to the public?[278]

If the vulnerability cannot be reliably exploited or does not provide a useful capability to the US government, the balance obviously tips towards disclosure. If the vulnerability is too dangerous for the domestic public, for example, a vulnerability in popular software in the US but used rarely by US adversaries, the balance likewise once more tips towards disclosure. However, in reality, it is often quite a subjective decision: How to determine that the US government's need for a vulnerability is crucial? How dangerous is too dangerous?

Unreliable assumption #4:

Software companies have done their best to decrease vulnerabilities.

There will be a negative impact on software companies' motivation to search for vulnerabilities in their products, if they know clearly in advance that the government agencies are to disclose them. After all, searching for vulnerabilities is a money consuming task. Software companies tend to prefer a free ride.

Every disclosure by the government comes at a cost. If the vulnerability is bought from contractors, we know from Chapter 5 that the price level is high[279], especially for the zero-days. If the vulnerability is found by researchers working for government agencies, their regular payments and devoted time are the (taxpayers') costs of disclosure.

In the long run, software companies will decrease their product security standard and their investment to search vulnerabilities. The government should not be constrained by morality and tax money should not be used to subsidize the security problems of big software companies. As for the improvement of vulnerabilities, this should still be left

[278] Aitel & Tait (2016)
[279] See section 5.4

to the enterprise. From the perspective of efficiency, it is the software vendor itself that can improve the quality of its product at the lowest social cost.

9.3 The role of the government

As discussed in section 9.1, the strategic role of vulnerabilities in modern states' playbook and the cumulative shaping effects of cyberattacks in the borderless cyberspace cannot be ignored. Although policies like US VEP, are expected to improve cybersecurity, they may not function as effectively as the original intention. On the one hand, the government may not be sufficiently interested in cooperation. After all, it is in the government's self-interest not to share all knowledge on vulnerabilities. On the other hand, regional unilateral policy constrains the cyber operations of the government and makes the country disadvantaged in the face of borderless cyberattacks. However, the government can play a role in the following aspects to deal with situations of cybersecurity.

1) Reducing liquidity in vulnerability markets

The price model in Chapter 6 implies that the liquidity of the vulnerability markets increases the vulnerability price. This liquidity is related to the dependence of the government to its contractors. If the government must purchase a vulnerability from an outsider, the seller must be legally obligated not to resell it to a third party. The government must have exclusive rights to the vulnerability. Otherwise, it runs the risk that the information could be sold or shared with some actors working against the national security interest of the government[280].

2) From the economic model presented in Chapter 7, I have deduced that the government has an important role in managing its internal digital arsenal and strengthening the related encryption system, thus, to reduce the possibility of leakage of its cyber tools.

3) The economic model in Chapter 7 also shows that increasing the expected penalty for conducting illegal business activities is crucial to the motivation of the seller. The

[280] Schwartz & Knake (2016)

expected penalty depends on two factors: the penalty amount and the probability of detection, which suggests that the government is justified in holding vulnerabilities for law enforcement purposes. Lichtman & Posner (2006) suggests internet service providers should be responsible for helping to identify those individuals who originate illegal activities.

4) The discussions of the vulnerability disclosure policy by the government in Chapter 8 & Chapter 9 explain the limits of this kind of policy. A unilateral disclosure policy can guarantee the government and its nation neither local cybersecurity nor the advantages over its foreign adversaries. Only through strengthening the protection of the whole cyberspace, can digital security and the cyber freedom of citizens within this framework be guaranteed. In this regard, the role of the government is embodied in actively seeking cooperation between governments and abiding by common cybersecurity policies, including the policy of vulnerability disclosure.

9.4 Chapter summary

In the digital age, the vulnerability disclosure policy by the government, like the US VEP or EU GDDP, is much more like a promise of the government to the public: to do the right thing[281]. However, the role of the government can be embodied in other places to improve the overall cybersecurity. For example, when the entire market has insufficient awareness of the risks of software vulnerabilities, the regulative activities of the government may be justified because of the concern of market failure. In next chapter, I will turn to this issue.

[281] Healey (2020)

Chapter 10: Market Failure: Proof from Event Study

After discussing the role of the government, in this chapter, I focus on the market reaction to the cyberattack. It is known that the vulnerability is a by-product of the software, which reflects its quality and reliability. In principle, in a well-functioning product market, users can respond to the quality problem by refusing to buy the affected product and switching to its competitors. However, there are factors that hinder this "invisible hand" of the market mechanism. These factors are referred to as market failures[282] in "first generation" Law and Economics or they are included in a more general and technical concept, transaction cost[283], in the "second generation" Law and Economics[284]. Some characteristics of the software industry have created significant market deficiencies.

The most significant monopolistic trait in the software industry is called "network externalities" or "network effects", which "emerge when the use of one product is more beneficial to a particular user when more people use it"[285]. The most typical example is the use of Microsoft Word. The more popular the software becomes, the more indispensable it becomes to the user. Network effects may increase the costs of market entry, providing first-mover advantage, which is a significant advantage to first comers who may set their own products as the standard in this field[286]. Network effects may lead to market inefficiency because inferior products are protected as long as they have covered the market earlier. When network externalities exist, both the learning cost and the switching cost to users are prohibitively high, and they are locked-in the incumbent software and cannot switch to a new technology[287].

---

[282] The four major types of market failures identified by the Neo-classical school of the economic approach towards law are: 1) Monopolies; 2) Public Goods; 3) Imperfect Information; 4) Externalities. Please refer to Elkin-Koren & Salzberger (2004), Chapter 3 to Chapter 8. Actually, market failure is a term that more generally follows from Economics, rather than only Law and Economics. Please refer to any standard textbook of economics for the concept of market failure, i.g. Microeconomics (5th edition) by Pindyck & Rubinfeld, p.294.

[283] To know more about transaction cost, please refer to Coase (1960), "The Problem of Social Cost (1960)".

[284] Elkin-Koren & Salzberger (2004), p. 90

[285] Elkin-Koren & Salzberger (2004), p. 44

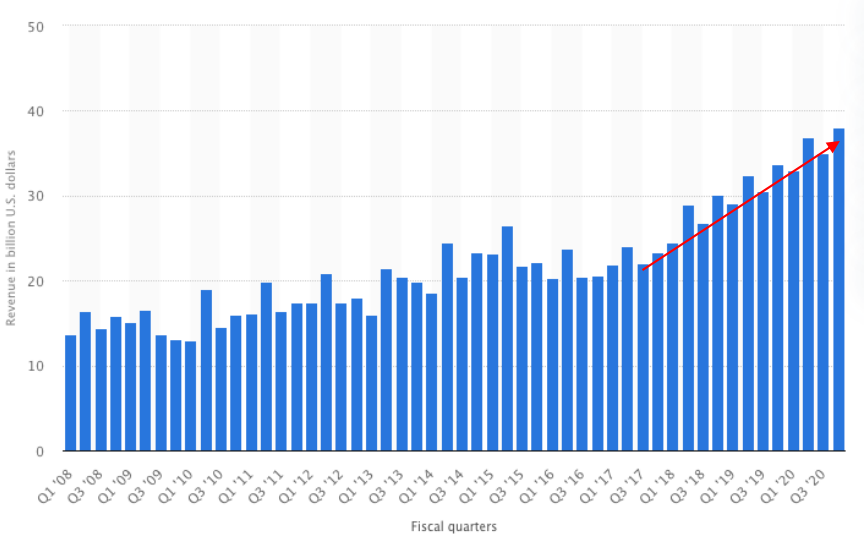
[286] Lemley & McGowan (1998)

[287] Elkin-Koren & Salzberger (2004), p. 45. For a more detailed explanation in economics, please refer to Microeconomics (5th edition, by Pindyck & Rubinfeld, p. 127), or Industrial Organization: Theory and Applications (by Oz Shy, p.254)

Based on the above, we have sufficient reason to doubt that those IT giants will respond properly to the pressure from the product market and make sufficient investment to ensure that their product quality meets the socially optimal requirement.

Data and facts have proved this concern. Although the worldwide cyberattack "WannaCry" exposed that some versions of Microsoft Windows were vulnerable, the quarterly revenue (sales) of Microsoft afterwards was not affected. Instead, the overall trend of revenue (sales) has been climbing up since the third quarter of 2017, the time shortly after the occurrence of WannaCry - May 12, 2017. See the red arrow line in following figure[288].

Figure 9: Microsoft Corporation's quarterly revenue from fiscal year 2008 to 2020 (In billion U.S. dollars)



Source: https://www.statista.com/

The financial market is tightly related to the product market. They are normally complementary. Many issues which cannot be properly responded to in the product

[288] https://www.statista.com/statistics/272746/microsoft-corporations-revenue-by-fiscal-quarters/ (retrieved on 01 June 2020)

market often receive effective and timely market responses in the financial market. The financial market is often considered to be more sensitive and more dynamic. Market information is often reflected more quickly and more comprehensively in the financial market, thereby reflecting the "invisible hand" of the market. When negative information of the quality problem of a listed company is released, investors will sell the company's stocks in the financial market immediately. A rapidly falling stock price signals the reaction of the market, which acts as the market pressure on the affected software company to promote future investment to improve product quality and reduce vulnerabilities.

Next, we will apply a specific empirical method of law and economics, event study, to analyse whether the software vendors with market power are facing sufficient pressure from the financial market in cases of a worldwide cyberattack.

10.1 Some notes before the empirical data

1) Target cases

In the following research we test the impact of the WannaCry cyberattack[289] on the stock of Microsoft, because WannaCry exploited vulnerabilities in different versions of MS Windows system disclosing the quality problems of Windows products. As a comparison, we also test the impact of the Facebook-Cambridge Analytica scandal[290] on the value of Facebook.

2) The task

Software producers have been accused by cybersecurity professionals of not paying enough attention to vulnerability issues. On the one hand, in order to capture the market and gain a first-mover advantage, they bring to the market immature products, which

[289] Please refer to Chapter 3 (section 3.2) of this thesis for detailed introduction of WannaCry case. According to The Economist (2017e), the worldwide cyberattack WannaCry successfully attacked more than 150 countries by exploiting vulnerabilities in Microsoft Windows operating system, including Britain's National Health Service, the Russian interior ministry, Chinese universities, the German state railway, and many individual users.

[290] The Facebook–Cambridge Analytica scandal occurred in 2018 when millions of Facebook users' personal data was collected without consent by Cambridge Analytica for political advertising. It was the largest data breach in the history of Facebook. Cambridge Analytica also sought to sell the data of American voters to political campaigns. In the same year, this event of data breach was disclosed by a former Cambridge Analytica employee, to The Guardian and The New York Times. As a result, Facebook apologized for their role in collecting the data and the CEO Mark Zuckerberg testified in front of Congress. For more reports, please see:
https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html (retrieved on 01 June 2020)

contain a number of vulnerabilities; on the other hand, the switching cost to the user is very high. Even events like cyberattacks that disclose the vulnerabilities in their product, may not harm the value of the company.[291]

The problems of product quality of a listed company will affect investors' expectations of its future market position, thereby directly leading to the decline of the value of the company. This is because from finance theory we know that the market value of a company is the present value of all its future cashflows:

$$stock\ price = sum\ of\ present\ values\ of\ future\ cashflows.$$

The flawed products will lead to a shrinkage in its market share, thus to a decline in future cashflows. If the future cashflows are expected to decline, the stock price will finally decline. The logic herein is intuitive[292].

In some sense, cyberattacks can be regarded as a test from the third party to disclose the quality defects in the affected software or website. More importantly, cyberattacks not only disclose the existence of vulnerabilities, but also reveal their severity. Technically we can estimate the rough number of vulnerabilities based on the length of the program or the website, but we have no clue as to how many of them are fatal[293]. Cyberattacks disclose the severity of these vulnerabilities in a drastic way, exploiting them.

The logic that vulnerabilities, a kind of security risks, will harm the value of a software company does not seem to be applicable. It stands to reason that any kind of severe quality problems will affect the stock price of a listed company, but there seem to be few clear links between them in the software industry, especially for those companies with market power. Our task is to empirically test, using real data from the financial market, whether a severe vulnerability problem disclosed by an unanticipated cyberattack will arouse public attention and influence the affected company's value, which is reflected by the fluctuation in its stock price.

---

[291] The Economist (2017d)
[292] For more introduction, please refer to a finance textbook on the topic of "the time value of money".
[293] Please refer to section 4.2.1.

3) The method

I use event study as my research method[294]. Event study is an empirical method, which is widely accepted in finance to deal with the impact of an unanticipated event on the value of a firm. For example, the announcement of a merger between two business entities can be analysed to see whether investors believe the merger will create or destroy value. Through studying the change of the value of a company, event study presents us with the impact of a sudden shock from the market.

In Appendix 2 of this thesis, I present a comparison of "event study" and another popular empirical method "difference in difference", which explains why event study is the most suitable empirical method in this case. I use statistical software Stata to process data and draw out empirical results and the main commands I used are listed in Appendix 3.

Back to the WannaCry case, it is an unanticipated event, behind which the risk of vulnerabilities in Microsoft's products was exposed. Did the problem of vulnerability influence the value of Microsoft, just like any other quality problem? I start from the observation of Microsoft's daily stock price. As the control group, Facebook's daily stock price is also collected.

10.2 The stock price movements in respective events

Before I begin with the design of our empirical study, I take a look at the absolute price changes in stocks of Microsoft and Facebook in the time of the respective events[295].

[294] The method of event study was invented by Fama, Fisher, Jensen, and Roll (1969) in their paper: The Adjustment of Stock Prices to New Information. The capital market is widely believed to be the fastest-reacting market and can represent the market mechanism. Another classic paper is Jonathan (2008), which applies the method of event study for research of law and economics.

[295] In the following Section 10.3.2 (Step 2), we will see that the object of our research is the rate of change of the stock price, rather than the absolute change of the stock price. Although their movement directions are the same, the former is a more objective index to reflect the fluctuation of stock value influenced by an event. For example, a piece of good news caused both A's and B's stock prices to rise. A's shares rose from 10 euros to 12 euros, while B's shares rose from 1 euro to 3 euros. The absolute increase of the two stocks is the same, both are 2 euros. But A stock rose 20%, while B stock rose 200%. Obviously, using the rate of change of stock price can better reflect the impact of this good news. To objectively evaluate the impact of an event on stock values, we need the rate of change rather than the absolute change in price. However, it is not meaningless to observe the absolute value changes of stock prices at the first stage. This intuitively allows us to see the trend of the relevant stock price.

a) Microsoft case

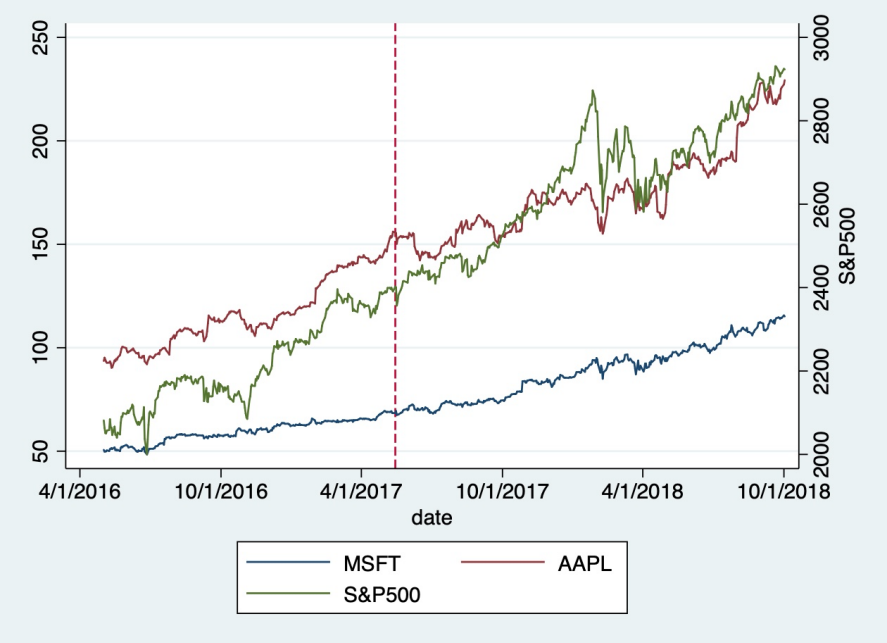
The WannaCry attack happened on 12-05-2017, which is the red dash line on Figure 10[296]. The related stock is Microsoft (MSFT), which is coloured in blue in the figure. I do not see any significant fluctuations in stock price of Microsoft.

Figure 10: Stock price of Microsoft at the time of WannaCry

I further observe the stock price of Microsoft (MSFT) together with the market index, the Standard and Poor's 500 (S&P 500), and one of its main competitors in the same industry, Apple (AAPL). Apple is chosen as one representative in the software industry and the Standard and Poor's 500 (S&P 500) represents the stock market as a whole.

[296] The statistic graph is processed by software Stata and the data source is: https://finance.yahoo.com/ (retrieved on 01 June 2020).

Figure 11[297]: Stock prices of Microsoft, Apple, and S&P 500 at the time of WannaCry



Judging from the observations on Figure 11, it is difficult for us to draw a conclusion that the news of WannaCry did cause the stock price of Microsoft deviate from the trend of its peers or the whole market.

b) Facebook case

The comparison event is the Facebook-Cambridge Analytica scandal, which happened on 18-03-2018. The date is marked as the red dash line in Figure 12. The related stock is Facebook (FB), which is coloured in blue in the figure[298]. We do see significant fluctuations in stock price of Facebook.

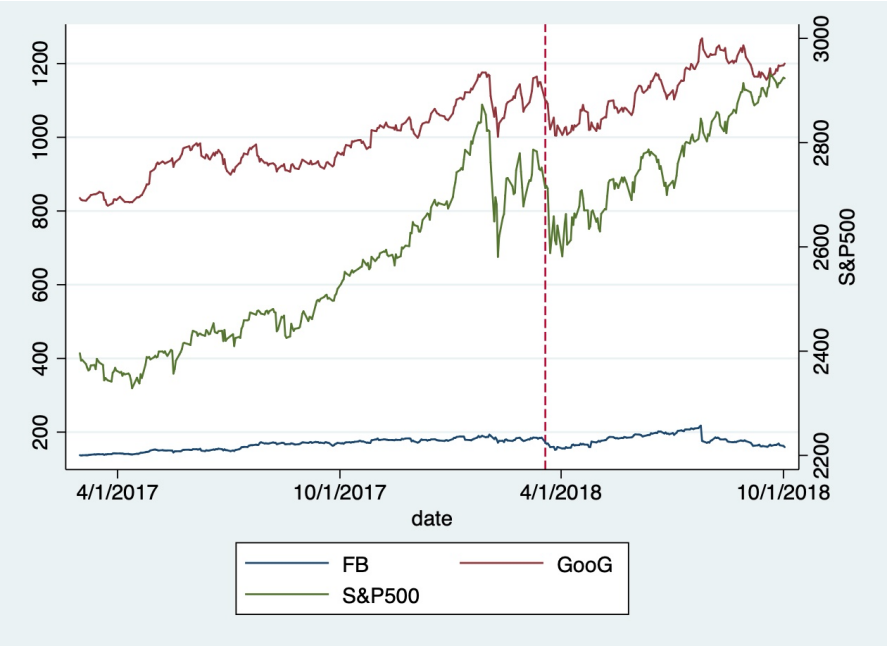
[297] The statistic graph is processed by software Stata and the data source is: https://finance.yahoo.com/ (retrieved on 01 June 2020) and https://www.investing.com/indices/us-spx-500-historical-data (retrieved on 01 June 2020).
[298] The statistic graph is processed by software Stata and the data source is: https://finance.yahoo.com/ (retrieved on 01 June 2020).

Figure 12: Stock price of Facebook at the time of Facebook-Cambridge Analytica scandal

I further observe the stock price of Facebook (FB) together with the market index, the Standard and Poor's 500 (S&P 500), and one of its main competitors in online advertisement, Google (GooG)[299].

[299] Facebook and Google are two main players on the digital advertisement market. According to Reuters, the two tech giants together held nearly 60% of the U.S. internet advertising market in 2018. See, https://www.reuters.com/article/us-alphabet-facebook-advertising-idUSKCN1T61IV (retrieved on 01 June 2020).

Figure 13[300]: Stock Prices of Facebook Google, and S&P 500 at the time of Facebook-Cambridge Analytica scandal



Based on the observations on Figure 13, I see the same declining trend of stocks of Facebook, Google, and S&P 500. The declining trends of Google and S&P 500 are more consistent and both of them look greater than that of Facebook. It is also difficult for us to say that the decline in the stock price of Facebook is due to the impact the news of the scandal or the general trend of the industry or the whole market.

From the discussion above, I see that observing the absolute change of the stock price cannot tell whether this change is merely due to the impact of the event, or only because of the trend of the whole market which has nothing to do with the event, or a result influenced by both. How to strip out the influence from the stock market and highlight the impact of the related event itself? To answer this question, the method of event study

[300] The statistic graph is processed by software Stata and the data source is: https://finance.yahoo.com/ (retrieved on 01 June 2020) and https://www.investing.com/indices/us-spx-500-historical-data (retrieved on 01 June 2020).

is needed. Its research design and the logic behind are presented as follows.

10.3 The design of the research

In the event study, I analyse the impact of an unanticipated event, WannaCry, on the stock of Microsoft. As a comparison, I analyse the impact of another unanticipated event, Facebook-Cambridge Analytica scandal, on the stock of Facebook[301]. To achieve this, we test the significance of the abnormal return of the related stock: $abnormal\ return = actual\ return - expected\ return$[302] . Only the return untangled from the market influence reflects the impact of the event. I calculate the actual return of the stock by collecting data from the open financial market. To have the expected return of the stock, I need to apply the so-called "statistical market model", which presents a linear relationship between the stock return and the market return. The result of the test implies whether the stock return was influenced by the unanticipated event. This thesis follows strictly the assumptions and research design of the method of event study in Jonathan (2008).

10.3.1 Two assumptions

1) Semi-strong version of Efficient capital markets hypothesis (ECMH)[303]

According to ECMH, there are three forms of efficiency: a weak form of efficiency, a semi-strong form of efficiency, and a strong form of efficiency. The weak form means that the price of the stock already contains all the historical information. Investors cannot benefit from having more historical information than others and obtain excess profits. The semi-strong form means that the price of the stock already contains all public information. Investors are only likely to obtain excess profits by gaining insider information. The strong form means that the price of the stock already contains all undisclosed internal information. Even if investors have insider information, they cannot get excess profits. These three forms are progressive. Financial economists

[301] The Facebook-Cambridge Analytica scandal has nothing to do with software vulnerabilities. If the impact of the WannaCry event is not significant, there are two possibilities: 1) failure of market mechanism only in specific case of vulnerabilities; 2) failure of market mechanism in all cases. If the impact of the Facebook-Cambridge Analytica scandal is significant, we can leave out the second possibility.

[302] Please be noted that the "expected return" here is not a concept of average value in statistics. Instead, it means stock returns expected to be in normal market conditions without related events.

[303] The efficient capital markets hypothesis (ECMH) is an important theory in finance, which is about the relationship between information and market price in the capital market. It reflects the market's response to information, thus indicating the effectiveness of the market. To learn more, please refer to Fama (1970) or Shleifer (2000).

generally believe that the stock market is semi-strong efficient[304]. In other words, people who master insider information are still more advantaged than investors who only have public information. This is realistic. The semi-strong efficient market indicates that the market responds quickly to related news or public information.

My event study is based on the hypothesis of semi-strong market efficiency, which means the price of a publicly traded security reflects all public information. Both the cyberattack like WannaCry and the Facebook privacy event are public events. I study how the related stock prices react to this unanticipated public information.

2) Stable market

This hypothesis tells that in the short run the relationship between a security and the market as a whole is relatively stable. With this assumption, I can apply the theoretical model to anticipate the "expected return" of an individual security from the performance of the market.

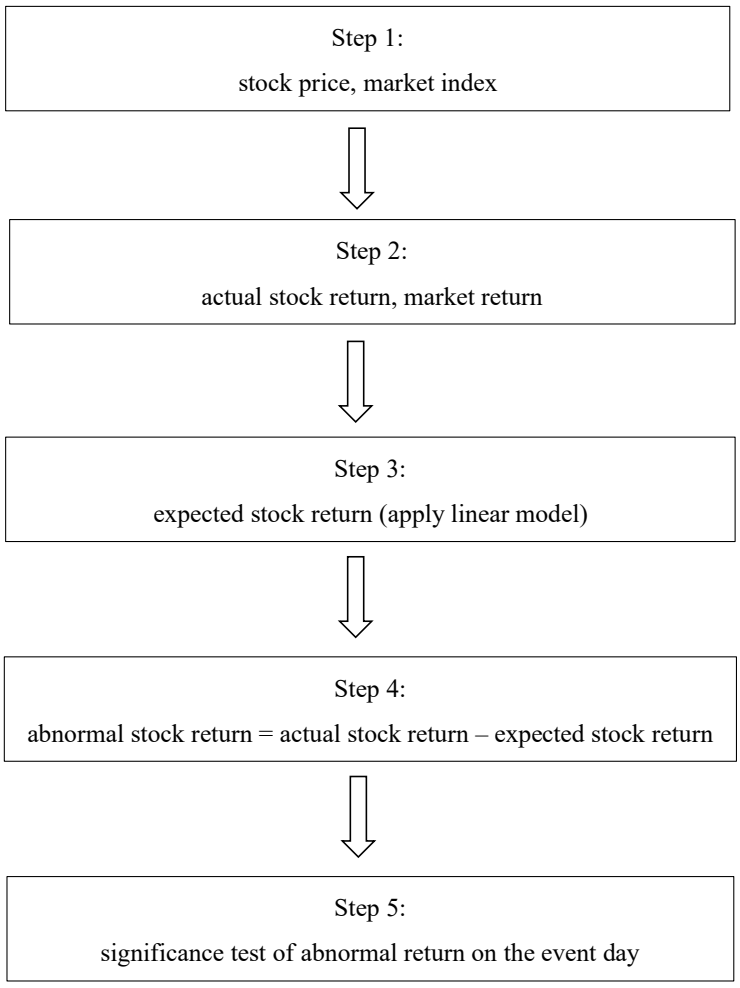
Taken together, these two assumptions imply that it is possible to assess empirically the effect of an unanticipated event on a company's stock price[305].

10.3.2 Five steps

The whole event study will follow in five steps[306]. Figure 14 illustrates the objects I focus on at each step.

[304] Fama (1970) or Shleifer (2000)
[305] Jonathan (2008)
[306] These steps were originally developed by Jonathan (2008).

Figure 14: Illustration of objects at each step



Next, I will explain the logic behind each step and the sequences of these steps.

Step 1: *To identify the event date and the date(s) on which information of the event became public*

My research studies two events:

a) The WannaCry attack happened on 12-05-2017 and the first trading day of the stock market after the information became public is 15-05-2017 (Monday). My study focuses on 15-05-2017. This date will be referred to as the "date of interest" or "event day" in the WannaCry case. WannaCry attacked the vulnerabilities of Microsoft Windows

System, so the related stock is Microsoft (MSFT).
b) The Facebook event happened on 18-03-2018 and the first trading day of the stock market after the information became public is 19-03-2018 (Monday). My study focuses on 19-03-2018. This date will be referred to as the "date of interest" or "event day" in Facebook case. The related stock to this event is Facebook (FB).

I examine the daily closing price data for Microsoft (MSFT) and Facebook (FB) and the market index, the Standard and Poor's 500 (S&P 500). I build two datasets: one for Microsoft and one for Facebook. I will apply the method of event study to each dataset separately. To avoid distortion from stock splits and dividends in my examination of stock prices over time, I use adjusted closing prices provided by NDAQ to establish the dataset.

In this step, the date when the event occurred and when it became public are determined. I assume that the market is semi-strong efficient, which is the semi-strong version of the efficient capital markets hypothesis (ECMH). A semi-strong efficient market means all public information related to a publicly traded security is completely included in its stock price. This is a very important assumption and a prerequisite for my next study. If the public information of the event has been included in the stock price, then I can study how the price fluctuation of the stock is affected by the event. Specifically, by stripping out the price volatility influenced by other factors, for example the market, I can identify the part that is affected merely by the event. This part is the real focus of the event study.

Step 2: *To measure the affected security's actual return on the dates of interest*
I have collected data from the stock market, including the price of the stock and the index of S&P 500. I use S&P 500 to stand for the portfolio of the market. Now I calculate the actual daily return of MSFT (Microsoft) and the daily return of S&P 500 in the dataset of the WannaCry event. Similarly, I calculate the actual daily return of FB (Facebook) and the daily return of S&P 500 in the dataset of the Facebook event. I use the following formula to calculate returns and I pay attention to the actual returns on the dates of interest: 15-05-2017 for the WannaCry event and 19-03-2018 for the Facebook-Cambridge Analytica event.

$$return = \frac{p_t - p_{t-1}}{p_{t-1}} = \frac{p_t}{p_{t-1}} - 1$$

In this step, there is one thing that I must make clear: I am concerned about the rate of return of a stock, not the absolute stock price. I study the volatility of a stock by studying the change in its rate of return. This is because the change in price is an absolute change, and it makes no sense to study the change in the absolute value. In fact, most of the financial models are based on stocks' rate of return. In addition, when I refer to "the stock's rate of return" or "stock return", I am talking about the same thing.

To summarize, after clarifying the effective market assumption and the rate of return of a stock, I enter the main part of the event study. I collect the stock price from the open market. I also use S&P 500 index to stand for the market portfolio. Based on these, I can calculate the daily return of the stock of interest and the daily return of the market. The stock return I get here is called "actual return" because it is directly from the actual data observed from the market.

Step 3: *To estimate the security's expected return on the dates of interest, according to the theoretical relationship between the affected security and the market*

In this step, the most complicated thing is how to untangle the stock return due to the market fluctuation apart from the whole stock return observed. The stock return due to the market influence is the return of a specific stock if there was not an event. This return without the event can be understood as a "normal return" because it is influenced by the market only. In the paper of Jonathan (2008) it is also called "expected return" because it can be expected from a linear relationship if we input the data of the market. Here the word "expected" refers to the expected result from a linear formula. That is, it does not refer to any average value, which is its usual meaning in statistics.

In the paper of Jonathan (2008) a linear formula is introduced to calculate the expected return, which is called "statistical market model":

$$E(r_{it}) = \lambda_i + \phi_i \, Market_t.$$

" $E(r_{it})$ is the expected return for stock i during time period t. λ_i is an i-specific constant, ϕ_i is an i-specific coefficient (i.e., a measure of how the stock i's return has

varied historically in relationship to the market return), and $Market_t$ is the market return over timeframe t. To compute the expected return for stock i, I multiply the market return by ϕ_i and then add λ_i."[307]

From this statistical market model, I see the linear relationship between the return of a stock and the return of the market. I use the data of 250 days before the date of interest as historical data. In step 2, I have calculated the actual daily return of the stock and the daily return of S&P 500. Using the 250 pairs (actual daily return of the stock, daily return of S&P 500), I can find out the constant and coefficient of the linear relationship. Then I multiply the daily market return by the coefficient and add the constant to get the daily expected return of the related stock. The difference between the daily actual return of the stock and its daily expected return is the abnormal return of each day.

The key to understanding this step is to understand the statistical market model. Actually, the statistical market model is a variant of the classic CAPM model in finance together with the second assumption in this chapter. As for these theoretical details, I put the derived results in Appendix 4.

Step 4: *To compute the abnormal return by subtracting the expected return from the actual return*

On the one hand, I get the actual return from step 2, which is calculated directly from the actual market data; on the other hand, I get the expected return from step 3, which is calculated from the statistical market model. Now I call the difference between the "actual return" and "expected return (normal return)" as "abnormal return". Logically this "abnormal return" is caused entirely by the event itself. The idea expressed by the formula is:

$$abnormal\ return = actual\ return - expected\ return.$$

Step 5: *To assess the statistical significance of the abnormal return.*

At this step, I study the distribution of the abnormal return. I suppose these abnormal returns follow a normal distribution[308]. Then I can study the abnormal return on the date

[307] Jonathan (2008)

[308] In the paper of Jonathan (2008), he assumes that the stock return follows a normal distribution. This assumption

of interest. We test its statistical significance using the statistical software Stata[309].

In practice, after I study the abnormal returns on 250 days before the date of interest, I can conclude the concrete parameters of this normal distribution. Then I can test whether the abnormal return of the stock on the day of interest is significant or not. If it is significant, the unanticipated event is regarded as having a strong impact on the price of the related stock and the market mechanism is sensitive to the event. If it is not significant, the unanticipated event has little or no impact on the price of the related stock and the market mechanism is not sensitive to the event.

10.4 The empirical results

Figure 15 shows the results run by software Stata. The red "**" stands for the meaning of significance. It is seen that the impact of the WannaCry cyberattack on Microsoft stock is not significant, whereas the impact of Facebook-Cambridge Analytica scandal on Facebook stock is significant. On the picture of the Microsoft case, my interested day 15-05-2017 is not marked with red "**", which means the fluctuation of Microsoft's stock return was not significant. On the picture of the Facebook case, my interested day 19-03-2018 and several of its following days are marked with red "**", which means the fluctuation of Facebook's stock return was highly significant.

is consistent with the conventional assumptions in the finance. In finance, it is generally believed that stock prices are log-normal distributed. Since the quotient of a log-normal distributed variable and another log-normal distributed variable follows a normal distribution in mathematics, the stock return follows a normal distribution. This assumption is reasonable.

[309] For operational commands in Stata to complete the task, please refer to Appendix 3.

Figure 15: Illustration of Microsoft case (result from Stata)

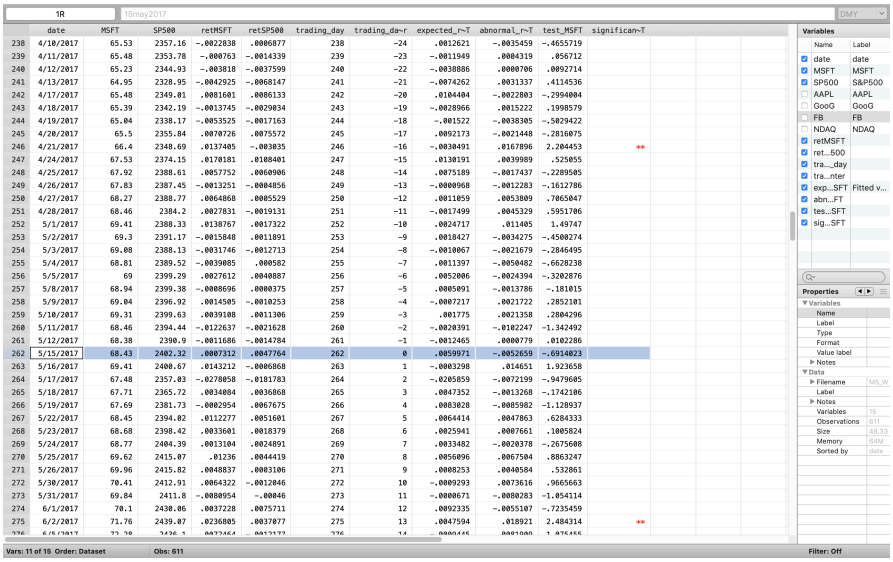
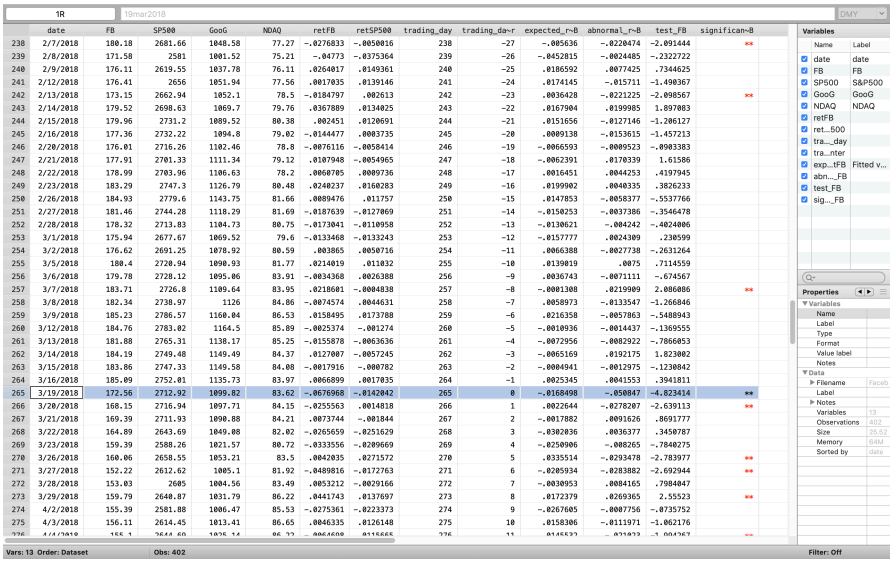


Figure 16: Illustration of Facebook case (result from Stata)



10.5 Analysis of the empirical results

The reactions of the market in the two cases are seen different. The impact of the vulnerability-related cyberattack is not significant in the stock fluctuation of Microsoft,

whereas the impact of a privacy-related scandal is apparently reflected in the fluctuation of the stock of Facebook.

As a reference event, the Facebook-Cambridge Analytica case presents a well-functioning market, in which the market reaction is fast and drastic. The problem of privacy releasing was very intuitive and there were concrete data. The mass responded quickly to the event and readjusted the value of the company correspondently.

In contrast, the WannaCry case discloses that the market is quite insensitive to the problem of software vulnerabilities, even when a large-scale cyberattack alarmed the public how serious the security risks could be.

The above findings suggest that Microsoft's value was not affected by large-scale exploiting of its product vulnerabilities. The market appeared to be insensitive, or at the least the mass did not respond to the problem of vulnerabilities, to a great extent, due to an ineffective recognition. In reality, it is difficult for common users to intuitively link technical details like "ports" or "SMB (service message block)" to their real feeling or emotion, even when they are told that some ports in their systems are open or vulnerable. Thus, the mass is not sensitive to cyberattacks or the things behind them. Insufficient attention has been paid to cyberattacks and risks of vulnerabilities[310]. It frequently happens that the same vulnerability has been attacked repeatedly. In August 2018, one year after the worldwide attack of WannaCry in 2017, Taiwan Semiconductor Manufacturing Company - the world's largest makers of semiconductors and processors - was forced to shut down several of its chip-fabrication factories for two days after being hit by WannaCry. The negative impact accounted for nearly $256 million[311]. The cognitive problem caused by high technology will become more serious with the development of the Internet of Things.

Technical barriers like imperfect information leads to cognitive inefficiency, which prevents the market from effectively turning cyber risks to users into market pressure

[310] In the year 2020, cybercrime seems to have been more widely recognized than some years before because of international political wrestling. Further analysis can be done to test whether this still holds after 2020.
[311] https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html (retrieved on 01 June 2020).

and passing it on to software vendors, forcing them to improve the product quality. If the value of Microsoft would change due to vulnerabilities passively disclosed by a large-scale cyberattack like WannaCry, for sure the management of Microsoft would be forced to be more careful and take actions to improve its product quality.

In short, the market is sensitive and seems to function well in general, which is proven by my event study on the Facebook-Cambridge Analytica case. However, the market failed to turn security problems of vulnerabilities into market pressure on Microsoft in my study on WannaCry. Technical barriers and cognitive inefficiency are deterring the market or the mass from responding properly.

10.6 Chapter summary

The monopoly market position of some software giants protects them from market competition. Because of network effects and high switching costs, users have to stick to the flawed products.

The financial market is widely believed to be more effective than the product market. Cyberattacks can be regarded as a way of disclosing the severity and existence of vulnerabilities of the affected software. The event study presented in this chapter aimed to test whether there is pressure from the financial market on the listed software vendor after a large-scale cyberattack.

The result of my event study suggests that there is no significant pressure from the financial market on the affected software vendor even if vulnerabilities in its product were exploited in a severe cyberattack. However, the financial market appears to function well in other cases, which is reflected in my study on privacy violation. This proves that the financial market also cannot exercise sufficient pressure on those software giants[312].

[312] So far, since there have not been many cyberattacks of the similar scale of WannaCry, we cannot collect more cases to test the relevant response from the financial market. This work can be improved in the future as and when more cases of cyberattack are collected.

Cyberspace, on the one hand, eliminates some of the common market failures; on the other hand, it creates some new market deficiencies[313]. This chapter proves the existence of market failures in cyberspace. Technical barriers and cognitive inefficiency could be the main reasons. Vulnerabilities are generally not familiar to the public and the technical barriers deter people from making proper decisions. The observation of this chapter can act as a bridge to further research. Since dominant software vendors are not subject to market pressure, I will study what will influence them to improve the situation of vulnerabilities in the following chapters.

[313] Elkin-Koren & Salzberger (2004), p. 107

Chapter 11: Tort Law and the Combination of Legal Tools

My empirical analysis in the previous chapter showed that the market mechanism does not put sufficient pressure on the affected software vendor in the case of a wide-reaching cyberattack. The inability of the market to respond appropriately can be considered as a market failure. Possible avenues to correct market failure could be the options provided by private law, administrative law, or other central intervention.

In private law, remedies to claim compensation from the software vendor could be sought under contract law, tort law, or both. In other words, when a wrong is committed (by an individual or an entity) and results in harm (to someone else), the harmed party is entitled to claim monetary compensation on the basis of a breach of contract law or tort wrong-doing.

From a law and economics perspective, regulation can be justified when market failure exists. The meaning of regulation can be understood in a narrow sense and a broad sense. In the narrow sense, regulation is part of administrative law, which can be of two kinds: ex-ante and ex-post. Ex-ante regulation imposes all kinds of duties irrespective of the occurrence of harm, for example safety regulation. Ex-post regulation can consist of a sanction if harm incurs, such as a public (administrative) fine. These two kinds of regulation are not part of private law. In the broad sense, regulation can mean every intervention of the government. In this sense, torts liability also falls into the scope of regulation. In this thesis, I will use the narrow definition.

Private law and administrative regulation are complementary to each other. Private law (in particular when compensation is used as a remedy, as in tort law) is often considered as an ex-post mechanism, whereas many regulations are ex-ante mechanisms[314]. However, under particular circumstances, ex-post regulations, such as administrative fines, may also be required. This will be reflected in the discussion in this chapter. A good set of policy tools often combines these measures to maximize the welfare of

[314] Regarding the extent to which legal commands should be promulgated as rules (ex-ante) or standards (ex-post), i.e., the "rules versus standards" debate, please refer to Kaplow (1992).

society[315].

In this chapter, I will examine whether legal tools in contract or tort law, or regulation, could be a desirable solution to the risk of vulnerability. In the discussion below, the concept of "software vendor" or "vendor" refers to the developer of the software, such as Microsoft. Those licensed resellers or other participants on the supply chain of the software are referred to as distributors. The focus will be on safety-critical COTS[316] software and software embedded in COTS products[317] ("software embodiment" hereinafter). The word "software" will be used to refer to both the software and the software embodiment. Furthermore, the focus of this chapter is on cyberattack accidents, where software vulnerabilities are exploited.

The chapter outline is as follows. In section 11.1, the barriers to apply contract law in vulnerability accidents will be introduced. In section 11.2, the question "whether software should be defined as a product or a service" will be raised and analysed from a positive legal perspective. Its legal implications are related to tort law. Sections 11.3 and 11.4 are the part of normative analysis in this chapter. Liability rules in tort law are discussed from the perspective of law and economics. Through the analysis from section 11.5 to section 11.7 I will discuss the desirable legal rules. I will recommend a solution of using jointly liability rules and safety regulation backed by a public fine (regulation backed by an administrative fine) for the harm caused by a vulnerability. It is a combination of torts and regulation (ex-ante and ex-post), which is in line with the suggestions made in Shavell (1984), and Faure, Visscher & Weber (2016).

[315] For further information about smart mixes of different types of regulatory and policy instruments and different levels of governance, please refer to Van Erp, Faure, Nollkaemper & Philipsen (2019).

[316] COTS refers to "commercial off-the-shelf". A COTS (commercial off-the-shelf) product is one that is used "as-is." COTS products are designed to be easily installed and to inter-operate with existing system components. Almost all software bought by the average computer user fits into the COTS category: operating systems, office product suites, word processing, and e-mail programs are among the myriad examples. One of the major advantages of COTS software, which is mass-produced, is its relatively low cost.
Retrieved from https://searchdatacenter.techtarget.com/definition/COTS-MOTS-GOTS-and-NOTS; (March 23, 2021).

[317] Goertzel (2016) explains it as "software used in commercial aircraft, motor vehicles, unmanned aerial vehicles, medical devices, physical security systems, automated teller machines, commercial robots and industrial control systems, a wide variety of COTS diagnostic and sensor systems, and the whole growing panoply of cyber-physical devices and systems that collectively comprise the Internet of Things". Artificial intelligence algorithms are not included here.

11.1 Barriers in contract law

In contract law, the premise of the claim for compensation is the existence of a contract, which reflects the legally binding consent and agreement between two or more parties. Anyone who is not a party to the contract is prevented from having rights conferred or obligations imposed upon them. In common law systems, like the US and England &Wales, it is called "the privity principle of contract[318]". The duty, which is breached but protected by contract law, is the duty established by the parties in their agreement.

Here, we distinguish between customized software, which is developed under contract for a specific customer, and COTS software, which is mass-produced. In the case of the customized software, a software contract (licence) is made directly between the user and the software vendor, which satisfies the requirement of the privity principle. Furthermore, unlike mass-produced software, which is transferred to unknown buyers, the customized software is tailor-made for specific requirements and the known buyer. The software vendor and the buyer (the potential victim in a cyberattack) can optimize their respective benefits through negotiations and formulate a contract tailored to their specific wishes, including compensation in the case of accidents. In addition, buyers of customized software are frequently businesses or organizations [319] rather than individuals, having more bargaining power in a negotiation with the vendor. From the perspective of law and economics, transaction costs for the vendor and the buyer are relatively small, and thus many conflicts can be effectively solved through negotiation. Furthermore, the buyer can sue the vendor for breach of contract under contract law without any barrier.

The number of users of COTS software is much larger than that of customized software. COTS software users face three legal barriers when resorting to contract law.

---

[318] The privity principle prevents anyone who is not a party to the contract from being conferred rights or imposed obligations upon. Retrieved from https://uk.practicallaw.thomsonreuters.com/8-107-7056?transitionType=Default&contextData=(sc.Default)&firstPage=true on 11 February 2021.

[319] For example, United Kingdom National Health Service (NHS) has long-term customized contracts with Microsoft for system security and digitalization. For more information, please refer to:
https://news.microsoft.com/en-gb/2020/06/15/nhs-chooses-microsoft-365-to-create-a-truly-joined-up-national-health-service/ (retrieved on 11 February 2021), or
https://nhsprocurement.org.uk/nhs-strikes-200m-deal-with-microsoft-to-patch-cyber-holes/
(retrieved on 11 February 2021)
The NHS itself was also one of the victims during the cyberattack WannaCry in 2017. However, we have not found any legal disputes reported publicly between the NHS and Microsoft.

a) Requirement of privity

The privity principle requires that the software contract (licence) is made directly between the vendor and the user (victim). This requirement cannot always be satisfied because privity does not exist when software is licensed to a reseller, an equipment manufacturer (OEM) or integrator, who make a resale to the end user[320]. Thus, only the reseller has the contract with the victim, where the requirement of privity is satisfied. The requirement of privity in this scenario is a barrier for the victim to sue the vendor under breach of contract.

b) Validity of warranties

In addition to the requirement of privity, an additional barrier might be the specifications of contract warranties. Software contract (licence) usually includes "express warranties about the product or its performance or implied warranties"[321]. The warranties of software vendors are often applicable only for a limited period. If the versions of the software are outdated, the warranties are no longer valid and all the support and service from the software vendor stop. Table 10, as an example, shows us when the supportive service ends for various versions of Microsoft Windows 10.

Table 10: Service duration for different versions of Windows 10 (full version)

Windows 10 version history	Date of availability	End of service for Home, Pro, Pro Education, and Pro for Workstations editions	End of service for Enterprise and Education editions
Windows 10, version 2004	May 27, 2020	December 14, 2021	December 14, 2021
Windows 10, version 1909	November 12, 2019	May 11, 2021	May 10, 2022
Windows 10, version 1903	May 21, 2019	December 8, 2020	December 8, 2020
Windows 10, version 1809	November 13, 2018	November 10, 2020	May 11, 2021
Windows 10, version 1803	April 30, 2018	November 12, 2019	May 11, 2021
Windows 10, version 1709	October 17, 2017	April 9, 2019	October 13, 2020

[320] Goertzel (2016)
[321] *Id.*

Windows 10, version 1703	April 5, 2017	October 9, 2018	October 8, 2019
Windows 10, version 1607	August 2, 2016	April 10, 2018	April 9, 2019
Windows 10, version 1511	November 10, 2015	October 10, 2017	October 10, 2017
Windows 10, released July 2015 (version 1507)	July 29, 2015	May 9, 2017	May 9, 2017

Source: Microsoft Official Website[322]

The problem of using the extinct versions of a software in a cyberattack constitutes, at least in part of the cases, a barrier for the user to claim for compensation from the software vendor under breach of warranties.

c) Exemption clauses of limited liability

The mass-produced software (COTS software) is "commercially produced and sold in a retail store or online, ready to use without any form of modification by the user, and accessible to everyone"[323]. This kind of software is typically supplied under a licence transaction together with a digital licensing agreement, which is thoroughly formulated and made with every unknown user. In this formulated agreement, exemption clauses are frequently seen that preclude the purchaser from either any liability or recovering more than the original purchase price. For instance, Microsoft's licence terms for the Windows operating system clearly stipulate that "(the user) may not under this limited warranty, under any other part of this agreement, or under any theory, recover any damages or other remedy, including lost profits or direct, consequential, special, indirect, or incidental damages"[324]. Even though the local law allows the user to recover damages from Microsoft, the user cannot recover more than what he has paid for the software, or up to $50 USD if the user acquired the software for no charge[325]. Literally, Software vendors like Microsoft enjoy a strong immunity from breach of contract, even in accidents like WannaCry[326].

[322] https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet (retrieved on 01 September 2020)
[323] https://study.com/academy/lesson/what-is-commercial-off-the-shelf-cots-software.html (retrieved on 11 February 2021)
[324] See Microsoft Software License Terms, term 9, paragraph d – Damages, https://www.microsoft.com/en-us/Useterms/Retail/Windows/10/UseTerms_Retail_Windows_10_English.htm (retrieved on 01 September 2020)
[325] *Id.*
[326] https://www.cybersecurity-insiders.com/microsoft-not-to-entertain-lawsuits-on-wannacry-related-cyber-attack/ (retrieved on 01 September 2020)

Many countries have a special legislation for standard contracts, allowing courts to annul unilateral exemption clauses. Experience from case law may prove that unilateral exemption clauses in the standard contract are possibly deemed invalid. For example, in Kingsway Hall Hotel Ltd. v. Red Sky IT (Hounslow) Ltd. (2010), the England & Wales High Court held that 1) the exemption terms in the software license agreement of Red Sky IT were unreasonable, and thus invalid; 2) Red Sky IT was liable for damages beyond the software price[327]. However, it should be noticed that the software in this case was customized rather than mass-produced, and the plaintiff was a four-star hotel, rather than an individual.

Due to these barriers, contract law is not always applicable. In contrast with contract law, no agreement or contract is needed between the parties in tort law, which is based on the premise that people should be liable for their actions or non-actions. In the next section, I will analyse the question - whether software is a product or a service, before my study on tort law starts.

11.2 Is software a product or service?

When discussing vulnerable software, it is important to first address the question of whether the software is a product or a service. This question is important because we need to find out which liability regime applies. Defining software as a product would imply that strict product liability in tort law may be applicable.

11.2.1 From the perspective of product liability

In the U.S. and the EU, the incumbent product liability regimes have their own ways to define a product. The American Law Institute's Restatement (Third) of Torts: Product Liability (1998) adopts a tangibility-intangibility dichotomy to determine the meaning of "product", which defines a product as "tangible personal property distributed commercially for use or consumption"[328]. Other items, such as real property and electricity, are also defined as products, as long as "the context of their distribution and

[327] Refer to: England and Wales High Court (Technology and Construction Court) Decisions, Neutral Citation Number: [2010] EWHC 965 (TCC), Case No: HT-08-111. Retrieved from https://www.bailii.org/ew/cases/EWHC/TCC/2010/965.html (on 30 March 2021).
[328] Restatement (Third) of Torts: Product Liability §19 (1998)

use is sufficiently analogous to the distribution and use of tangible personal property that it is appropriate to apply the rules stated in this Restatement"[329]. However, whether software or software embodiment would be regarded as product is left unclear.

Different from the American wording of "tangible", the keyword used in the European Product Liability Directive (EPLD), the uniform system of no-fault product liability adopted in the EU in 1985, is "movable". According to the EPLD, "a 'product' includes all movables which can be the subject of economic activity…… Immovable goods and services are excluded"[330]. Although the EPLD does not mention the distinction between "tangible" and "intangible", electricity is explicitly stated to be a product in Article 2. Apart from this, other intangible things like software are left unspecified in this EU directive[331].

11.2.2 From the perspective of contract law

Contract law distinguishes between "services" and "goods". It is not self-evident under the US regime whether software should be regarded as goods or a service. The Uniform Commercial Code (UCC), which interprets the civil contract law in the US, defines "goods" as "all things (including specially manufactured goods) which are movable at the time of identification to the contract for sale……"[332]. The two key prerequisites of being regarded as goods under the UCC are: 1) mass-produced 2) transferred to unknown buyers. Software complies fully with both[333]. However, unlike other tangible products, software is typically supplied under a licence transaction and protected by intellectual property laws. A software vendor like Microsoft has licensing agreements with a huge number of software customers. When a customer buys the software, he gets only the right to use it. There is no transfer of ownership from the vendor to the customer and the right of a customer to use the vendor-owned product is not exclusive. By contrast, in a real ownership transfer case, the related right should be exclusive. In this sense, the software is much like the delivery of service, rather than a product. With the popularity of computer clouds, much software is subscriber-based, e.g., Microsoft

[329] *Id.*
[330] Article 2, EU Council Directive 85/374
[331] Alheit (2001)
[332] The Uniform Commercial Code (UCC) § 2-105
[333] Goertzel (2016)

365. There is also increasing reliance on the data-processing functions of the cloud[334].

In May 2019, the European Commission proposed two directives, the directive on contracts for the supply of digital content and digital services (DIRECTIVE (EU) 2019/770) and the directive on contracts for the sale of goods (DIRECTIVE (EU) 2019/771). These two directives are supposed to complement each other[335]. In the directive on contracts for the sale of goods, the European Commission has clearly extended the definition of "goods" by including "goods with digital elements". It is stated that "the term 'goods' should be understood to include 'goods with digital elements', and therefore also referring to any digital content or digital service that is incorporated in or interconnected with such goods, in such a way that the absence of that digital content or digital service would prevent the goods from performing their functions"[336]. Operating systems, applications, and any other software are referred to as digital content, whereas "software-as-a-service" offered in the cloud computing environment is included into digital service[337].

Apart from the functional digital content and digital services discussed above, there are other informative digital content and digital services, whose absence does not prevent goods from performing their functions. They fall within the scope of Directive (EU) 2019/770 concerning contracts for the supply of digital content and digital services[338].

11.2.3 The legal implication

Although the definition of goods and services for software is becoming clearer in the legislation of contract law (especially in the EU), the "good" determined by contract law cannot be identified automatically as the "product" in tort law. The distinction between good and service determines whether the related software contract is a product sales contract or a service delivery contract, which is pertinent to how breach of warranty liability can be applied under contract theory[339]. By comparison, to define software as a product is important in the decision of whether the strict product liability

[334] Varadi, Gultekin, and Kertesz (2019)
[335] DIRECTIVE (EU) 2019/770, L 136/4, para. 20
[336] DIRECTIVE (EU) 2019/771, L 136/30, para. 14
[337] *Id.*
[338] DIRECTIVE (EU) 2019/770, L 136/4, para. 22
[339] Goertzel (2016)

rule in tort law can be applied to software. To be precise, the application of strict liability is based on the solid premise that the software is a product, rather than a service[340]. Any doubt on this point will limit the application of strict product liability to mass-produced software. In cases where damage consists of personal injury and injury to personal property, the strict product liability regime places the injured user in the favourable position of 1) not having to prove the software vendor's fault regarding the defective software; 2) being able to claim for compensations against a wider circle of liable persons; 3) regardless of the exemption clause contained in the standard form contract[341]. Considering the legal implications of "product", legislators are very hesitant to extend the meaning of "product" to software or software embodiment without a case-by-case study, even when they are defined as "goods" in contract law or in case law[342].

In short, the dichotomy standard of tangible-intangible or movable-immovable is only the appearance, not the essence. The classification of the software or the software embodiment as a product should be based on the strong causality between the operation of these digital items and the accidental harm. However, the causation may not be that easy to establish. Thus, this issue should be determined on a case-by-case basis. Since strict product liability in tort law cannot be automatically applied to the problem of software vulnerabilities, the following part will first discuss the different possible liability rules in tort law from a (theoretical) law and economics perspective.

11.3 The duty and economic essence of tort law

Unlike the duty under contract law, which originates from the contract agreed by the parties, the duty under tort law originates from the defective product or service per se, rather than the agreement. The duty violated in a tort is not the duty stipulated by a contract but imposed by legal principle. When some duty, especially relating to social welfare, is not stated in the contract, it often requires the intervention of tort law or

[340] According to the American Law Institute's Restatement (Third) of Torts: Products Liability, §19, product liability is traditionally limited to products in the form of tangible personal property.
[341] Alheit (2001)
[342] For example, in the case of Computer Associates (UK) Ltd (Respondent) v The Software Incubator Ltd (Appellant) (2018), the judge held that a sale of electronically supplied software was a sale of "goods" within the meaning of the Commercial Agents (Council Directive) Regulations 1993/3053. Retrieved from https://laweuro.com/?p=13546 and https://www.edwincoe.com/blogs/main/software-goods-or-services/ on 26 March 2021.

default rules that originate from regulation[343].

11.3.1 The duty under tort law

Lichtman & Posner (2006) clearly express the opinion that software vendors should be held liable for their flawed products, because the overall probability of accidental occurrence is statistically influenceable by them. In a cyberattack scenario, although software vendors are not the attackers who initiate cyberattacks, they are the ones who can influence statistically the probability and severity of potential harm. More vulnerable software will incur more attacks. The decision by the software vendor to invest less or more in searching for vulnerabilities in the software is deliberate, and the result of this decision is statistically predictable – resulting in higher or lower potential risks. Therefore, the software vendors should be held liable for accidental harm directly or indirectly caused by software defects.

The goal of tort law according to Calabresi (1970) is to minimize the total social costs of accidents. Calabresi categorised social costs into a) precaution costs; b) harm caused by accidents; c) administrative costs and litigation costs.

To minimize the social costs, both the precaution costs and the harm should be taken into consideration by the software vendor. The vendor is always balancing his precaution costs and the compensation he has to pay for the harm, to achieve the lowest sum of both. If the vendor chooses a high investment level to control the software quality, few risks (vulnerabilities) are released, and thus his expected costs (in terms of damages to be paid in tort law) are low. If the investment level is kept low, the users are likely to be harmed, and thus his expected costs are high. When there is no sufficient legal intervention, the vendor's liability will not be completely internalized into his cost function. Then the vendor is very likely to choose the low level of investment in precaution, which is not favoured by society. To some extent, the question of "how many vulnerabilities are allowed to go to the public?" only reflects how much software vendors are willing to invest in precaution.

[343] For a simple reference, see Cooter & Ulen (2014), p. 291-299

As explained before, most software users use mass-produced software rather than customized software, which makes them risk-bearers of negative impacts from defective software. If the accidental harm suffered by these users will not be incorporated in the decision-making by software vendors, their behaviour will not meet the goal of optimizing social welfare, which is a standard externality problem. After all, all harm will be borne by society.

11.3.2 The economic essence of tort law

In some situations, externalities can be internalized by parties (injurer and victim) themselves. Such successful negotiations between parties only work well if transaction costs are low enough. The Coase Theorem treats all obstacles to bargaining as transactions costs – including bargaining costs, strategic behaviour, cognitive imperfections, information asymmetry, emotions[344]. Contracts involve relationships among people for whom the transaction costs of private agreements are relatively low, whereas tort law governs relationships among people for whom transaction costs of private agreements are relatively high[345]. From the analysis in the previous section, it is seen that the transaction costs are high in the context of users and software vendors, if an individual victim tries to sue the software vendor relying on contract law. The economic essence of tort law is the availability of liability rules to internalize negative externalities which are created by high transaction costs. When bargaining cannot enable cooperative behaviour concerning harm that one party imposes on another, tort law is conventionally thought of as an option to internalize the costs of harm, which occurs from failing to take care, by making the injurer compensate the victim. The logic behind this is simple: if the potential wrongdoer is required to internalize the costs of the harm he causes, he will have an incentive to invest in and improve the safety of the product/service to a level optimal for him. The liability rules in tort law provide us with an alternative possibility to protect victims and improve the overall social welfare. The discussion in the following is mainly based on Brown (1973), Shavell (1980), Parisi (2013), Cooter & Ulen (2014), and Faure (2016).

[344] Cooter & Ulen (2014), p. 177

[345] For a deeper understanding of liability rules from the perspective of law and economics, readers can refer to Shavell (1980), Cooter & Ulen (2014), and Calabresi & Melamed (1972).

11.4 Lessons from the economic analysis of liability rules

11.4.1 A short review of different liability rules

a) No liability and strict liability

In the absence of liability rules, the victim bears all the accident costs. Under a strict liability rule, the injurer bears all costs. These two rules are direct opposites.

A victim can rely on the strict liability rule to request compensation, if two requirements are satisfied: 1) The injuries and losses suffered by the victim are causally related to the product; 2) It is clear who is the producer of the defective product. Other issues are not for the victim to prove. This is because victims are generally in a disadvantaged position compared with producers, while producers are in the best position to control their product's quality at the lowest social cost. Therefore, the law does not require victims to bear the burden of proof for product defects.

Furthermore, the no liability rule and the strict liability rule have one feature in common: Only one party is to bear the liability. For a unilateral accident, where only one party can influence the probability and magnitude of an accident, no liability rule and strict liability rule are applicable. As long as the liability is imposed on the party who can influence the accident, the social welfare is to be improved. But for a bilateral accident, where both parties can influence the accident simultaneously, these two rules are not sufficient. To encourage both the injurer and the victim to take precautions in advance, the negligence rules are introduced.

b) Negligence rules

There are several different forms of the negligence rule. In each of them, the court judges who is (are) negligent and who should bear the costs of accidental harm by observing the precautions taken by the injurer and the victim.

- Simple negligence

The simplest form of all negligence rules can be termed "simple negligence". The injurer is held "liable for accidents that he or she causes if, and only if, precaution is

below the legal standard, regardless of the victim's level of precaution"[346]. In other words, by satisfying the requirements of the legal standard, the injurer can avoid the liability. As long as the injurer's precaution has reached the legal standard, the victim has to bear the costs of an accident.

- Negligence + contributory negligence

The rule of "negligence + contributory negligence" allows the injurer a defence of contributory negligence on the basis of simple negligence. By proving the insufficient precaution taken by the victim, the negligent injurer can escape liability. In a case where both parties are negligent, the injurer is liable under "simple negligence", but not liable under "negligence + contributory negligence".

- Comparative negligence

In contrast to "simple negligence" and "negligence + contributory negligence", the rule of "comparative negligence" divides the harm between the parties in proportion to the contribution of their negligence to the accident[347].

- Strict liability + contributory negligence

Under the rule of "strict liability with a defence of contributory negligence", the injurer is strictly liable and should bear all the costs of accidental harm, unless he can prove that the victim was at fault, i.e., if the victim's precaution did not reach the related legal standard.

11.4.2 Economic analysis of liability rules

a) Four variables

Grady (1983) and Shavell (1980) group the factors affecting the likelihood of an accident under the headings of "care level" and "activity level", including the quality and quantity of the precautions taken by injurers and victims as well as the intensity and duration of their activities.

[346] Cooter & Ulen (2014), p. 196
[347] Parisi (2013), p.65

The care level refers to the "observable precautions[348] used by courts to ascertain negligence and indicates the extent of parties' precautionary efforts in carrying out their activities". Other factors which "are not taken into account by courts to ascertain negligence and which indicate the intensity and duration of the parties' activities" fall into the scope of activity level[349].

Law and economics scholars regard both care level and activity level as relevant variables. Since both the injurer and the victim have their respective care levels and activity levels, the impacts of different liability rules on their incentives can be studied according to these four variables.

b) The impacts of different liability rules

The impacts of different liability rules on the incentives of both the injurer and the victim are summarized in the following table, on the assumption that a legal standard of care level is equal to the efficient (optimal) care level, which is in compliance with the requirements of maximizing social welfare.

Table 11: Efficiency of incentives created by liability rules

Legal Rule	Care Level		Activity Level	
	Victim	Injurer	Victim	Injurer
#1 No liability	yes	0	yes	no
#2 Strict liability	0	yes	no	yes
#3 Simple negligence	yes	yes	yes	no
#4 Negligence + contributory negligence	yes	yes	yes	no
#5 Comparative negligence	yes	yes	yes	no
#6 Strict liability + contributory negligence	yes	yes	no	yes
Notes: - "yes" indicates efficient incentives. - "no" indicates inefficient incentives.				

[348] Some precautions are non-observable ex post. Dari-Mattiacci and Parisi (2005) researched this question and pointed out that "investment in non-observable precautions may reduce the probability of an accident but would not reduce the likelihood of being found negligent if an accident did occur. For this reason, the incentives to invest in non-observable precautions generally follow the activity level incentives of the parties".

[349] Parisi (2013), p.2

- "0" indicates no incentive.
- The legal standard of care level is assumed to be equal to the efficient care level.
- Perfect compensation is assumed.

Source: Cooter & Ulen (2014), p.192

Polinsky (1980) and Shavell (1980) independently pointed out that the distinction between care level and activity level is irrelevant in regimes of no liability and strict liability. Under these two rules, the liability is borne by only one party - the victim under the "no liability" rule, or the tortfeasor under strict liability. The one who is to bear the liability will be incentivized to take efficient actions, i.e., both efficient care level and efficient activity level, to avoid the occurrence of the accident. The counterparty has no incentive to take any efficient actions. The results are seen in the first two liability rules in Table 11.

The remainder of Table 11 shows that the distinction between care level and activity level becomes relevant under negligence rules. When the criterion of negligence is used to establish liability, the court determines negligence by observing the care level(s) rather than the activity level(s) of the injurer and the victim. Both of them are supposed to be rational. Under each form of the negligence rule, one party can escape liability by satisfying the legal standard for him. Consequently, the counterparty will have to internalize the cost of the harm from the accident. Expecting this, the counterparty has incentives for efficient precautions in order to avoid the occurrence of harm. In the end, both the (potential) tortfeasor and the (potential) victim are incentivized to satisfy their respective requirements of efficient care. From Table 11, different forms of the negligence rule are seen to lead to similar outcomes, which give both the (potential) victim and the (potential) tortfeasor efficient incentives for their care levels.

An efficient remedy in tort law is supposed to incentivize efficient care levels and efficient activity levels for both the (potential) tortfeasor and the (potential) victim. However, these four variables (victim's care level, victim's activity level, tortfeasor's care level, and tortfeasor's activity level) cannot all be optimized at the same time. Shavell (1980) proves that under negligence-based regimes this ideal goal is not

achievable. Although negligence rules can incentivize both sides of an accident to adopt efficient (optimal) care levels, they cannot push both to take their efficient (optimal) activity levels simultaneously. In fact, under each form of negligence, the activity level of only one side is optimized, i.e., only one party will take the efficient activity level. In other words, no matter under which liability rule, at most only three variables can be optimized. It is obvious that only one party bears the residual cost of the accident if the other party demonstrates his due care and proves his non-negligence. This party is called the bearer of residual liability and has incentives to exercise an optimal activity level and to invest in non-observable precautions. Shavell's theorem shows that no negligence rule can incentivize optimal activity levels for both parties. This is because the bearer of residual liability tries the best (including the optimal care level and the optimal activity level) to avoid the accident (thus the accidental harm), whereas the non-bearer of residual liability only tries to avoid liability (for which only the sufficient care level is needed).

11.4.3 Care level and activity level in vulnerability accidents

In the case of vulnerability accidents, whether the software vendor or the user has achieved due care (the standard of care level) can be observed. For the vendor, the observable precaution is embodied in aspects like whether the patch for the vulnerability is released in time, whether the vendor has used effective ways to inform the users in good time, or whether the requirements of safety regulation are met, etc. The court can judge whether the vendor has exerted sufficient due care according to these facts[350]. For the user, the judgemental criteria of the court could be whether the patch released has been installed in time, or whether the software has been used in the right way. All these observable precautions taken by the vendor or the user fall into the scope of care level because they can be used by the court to ascertain negligence.

However, there are precautions that cannot be observed by the court to ascertain negligence. Typical examples are the investments in quality control by the vendor, and the inputs in cyber security and data backup by the user. Since investing in non-

[350] Obviously, if there exists a zero-day vulnerability, the care level of the software vendor is not in compliance with the due care standard. This is because the vendor does not know the existence of the vulnerability and could not develop patches for it.

observable precautions would not reduce the likelihood of being found negligent by the court, the non-residual bearer of the accidental harm would rationally limit his investment in these precautions. Only the one who finally bears the accidental harm would have incentives to invest in non-observable precautions. These non-observable precautions fall into the scope of activity level. Although investing in non-observable precautions would not reduce the likelihood of being found negligent if an accident did happen, doing so may reduce the probability and severity of an accident.

Other factors, which also affect the likelihood of an accident, are not related to the type of precaution. They fall into the scope of the activity level too. Typical examples are the market coverage of an item of software, or the time span of an item of software from its R&D (Research and Development) to its market availability.

The larger the market coverage of an item of software, the more the users may be negatively affected by the same vulnerability, and the higher the probability of an accident occurring. Similarly, the shorter the time left for R&D and testing before software is available on the market, the less mature or stable it could be, which increases the probability of corresponding accidents. These activities of the vendor can affect the likelihood of an accident but cannot be relied on by the court to ascertain negligence. They are classified as the activity level of the vendor. For the user, the frequency of his usage of the software as well as how professional he is in cybersecurity fall into the scope of the user's activity level. Although investing in these factors will reduce the likelihood of an accident and benefit the overall social welfare, the party who is not the ultimate bearer of the accidental harm will not do so. This is because all these investments are his own costs, while they do not generate any benefits.

11.5 Designing legal solutions

11.5.1 Distinguishing between two types of accidents

Before applying liability rules to vulnerability issues, it is necessary to distinguish between two types of accidents that occur due to software defects. One includes accidents caused by defective software per se, which is the scenario without outside hackers. I use "defect accident(s) or type I accident(s)" to refer to these scenarios. The other includes accidents caused by cyberattacks, in which hackers exploit defects

(vulnerabilities) in the software. I use “vulnerability accident(s) or type II accident(s)” to refer to them.

I mainly focus on the cyberattack scenario, the ‘vulnerability accident’ (type II), but this does not mean that the ‘defect’ accident (type I) scenario will be ignored. These two types of accidents are different in nature. For ‘defect’ accidents, the relationship between the defective software and the accidental damage is simpler. If causality can be proven and harm is observed, liability can be determined. However, the causality cannot be proven easily in ‘vulnerability’ accidents because it is the third party - the hacker - who initiates cyberattacks exploiting vulnerabilities and his criminal actions cause harm. Although the hidden risks of vulnerabilities play a supportive but decisive role in and contribute to the success of cyberattacks, the causality between the vulnerabilities and the harm could be indirect.

In addition to the causality relationship, it is helpful to understand these two different accidents using the following aspects.

a) The software user can influence the accident risk

The user has an important role in mitigating the risks of these two types of accidents, although different technical skills are required. An unskilled user can take an active role and make up for his lack of technical skills through good software usage habits. For example, a user can minimize the risk of data getting lost in system crashes by a good backup habit. Similarly, the user’s precaution also cannot be ignored to reduce the probability and magnitude of a ‘vulnerability’ accident. Although it seems that more professional knowledge and skills are needed in case of a cyberattack, the user is in the best position to know his own system or machine, and his daily habits, in order to prevent a type I accident also help in a type II accident.

b) The vendor is in the best position to fix vulnerabilities

In no matter which scenario, the software vendor is in the best position to fix the software. By investing in observable and non-observable precautions, a vendor can reduce the overall vulnerability risks faced by both software users and society. Let us suppose an item of vulnerable software with ten thousand users. If some vulnerabilities

can be fixed by the vendor before the software becomes available on the market, the social costs should be far less than that of fixing them ten thousand times by individual users in the future. Furthermore, technically it is possible that a software vendor takes remote actions to push his users to install the latest patch within a specified period. For example, if a user does not keep the patch version up to date, his system will keep reminding him. This intrusive way to push users to install patches in time is compared by Lichtman & Posner (2006) to "mandatory vaccinations for school children"[351].

11.5.2 Liability rules versus safety regulation

To control the risks of accidents, liability in tort and safety regulation are two different approaches. Table 12 presents the comparison of them.

Table 12: Comparison of liability in tort and safety regulation

	Tort liability	Safety Regulation
Nature	private in nature	public in nature
Influence	by deterrent effect to risky actions	by social command stipulating to do and not to do
Time Employed	ex-post: employed only after accident's occurrence	ex-ante: employed beforehand
Forms	strict liability, non-liability, and different forms of negligence rules	standards, prohibitions, and other forms
Initiator	private parties	public authority

Source: Information summarized from Shavell (1984)

Shavell (1984) states that liability in tort is socially desirable when private parties have more information than public authorities or when liability has a significant administrative cost advantage over regulation in controlling the risks of typical torts. When the injurer can escape a court case or is unable to pay the compensation, a combination of regulation and liability rules is often needed.

[351] Lichtman & Posner (2006), p. 257

I apply Shavell's theory to analyse the two types of accidents mentioned before. In the case of a type I accident ('defect' accident), the advantage of differential knowledge by the private parties is significant. It seems unnecessary for the public authority to be involved. The stipulations of regulations will also incur higher administrative costs because these costs happen ex-ante, independently of the occurrence of accidents. These two determinants are strongly in favour of using liability rules to alleviate risks. Further, the possibility of escaping prosecution works with only moderate or even less force against applying liability rules, considering the existence of some exemption clauses which may hinder the user to sue. Thus, theoretically the preferred solution to the problem of type I accident ('defect' accident), which is related to the familiar category of risks of the typical tort, is liability rules.

When the focus is turned to type II accidents ('vulnerability' accidents), things are different. In a cyberattack case, victims find it difficult to sue the vendor of the affected software, which makes the dilution of the deterrent effect of liability rules significant. The first reason is that it is difficult to attribute accidental harm to the vendor because it is not the vendor but the hacker who initiated cyberattacks. Secondly, the incapability of hacking knowledge makes it difficult for individual victims to collect evidence necessary for a successful action. Shavell (1984) argues that if victims are allowed to initiate class actions, this concern can be offset to a degree. However, there have only been few class actions against software vendors after a cyberattack[352]. Thus, tort liability alone as the solution to type I accidents ('defect' accidents) may not work well in case of type II accidents ('vulnerability' accidents), which is related to the unique risks of cyberattack. Besides the tort liability, some complementary tools initiated by a public authority are needed to strengthen the deterrence effect of tort liability in hand[353].

Shavell (1984), Faure, Visscher & Weber (2016) and other scholars have discussed this. Tort liability should be combined with regulation. Even if all indicators point towards regulation over liability rules, regulation will rarely be perfectly enforced (so accidents do happen). Moreover, regulation is often not perfect because it is subject to lobbying and not very flexible in circumstances where markets change quickly.

[352] Refer to: https://www.jdsupra.com/topics/data-breach/cybersecurity/class-action/ (retrieved on 08 April 2021)
[353] Faure, Visscher & Weber (2016)

The type of desirable regulation should incorporate both ex-ante and ex-post elements.

a) Ex-ante regulation should be backed by ex-post regulation

Ex-ante regulation, like safety regulation, may be unspecific, expensive, and difficult to carry out. Cyberattacks are specific events, which are the minority points on the timeline. It would be a waste of society's resources to monitor the daily behaviour of the software vendor. The administration cost of an ex-ante regulation, such as safety regulation, is high. The software industry changes fast. It is not reasonable to impose a very detailed list of "to do" or "not to do" on an industry which needs innovation.

b) Ex-post regulation should be linked to ex-ante regulation

Ex-post regulation needs to be linked to some type of ex-ante regulation, i.e., a public (administrative) fine can only be imposed if there is a breach of a particular rule, e.g., on the safety of software (safety regulation). According to the definition of ex-post regulation at the beginning of this chapter, which is basically a punishment if harm incurs, a public (administrative) fine[354] can be imposed if harm in a severe cyberattack incurs. Thus, a public (administrative) fine needs to be linked to a safety regulation. In the contexts of cyberattacks, the public (administrative) fine is a kind of social control. The public authority should collect information of damages in cyberattacks at society level and publish the fine amounts if different scales of harm incur. The fine for vulnerabilities exploited in cyberspace is similar to fining pollutants in physical space. If a fine is necessary for the event in which crude oil spills from an offshore drilling platform in public waters, the same logic applies to the risky vulnerabilities exploited in cyberspace. Although the regulator does not have sufficient knowledge about the actual number of existing vulnerabilities, cyberattacks disclose the riskiest ones. The public (administrative) fine is the public intervention after the cyberattack, in which the social administrative costs only happen when the event incurs.

To summarize, for both types of accidents, neither tort liability nor regulation could be exclusively dominant as the solution of reducing social risks. I recommend a solution of jointly using liability rules and safety regulation backed by a public fine (regulation

[354] The fine is not a criminal fine, so it has to be an administrative one.

backed by an administrative fine). The liability rules and the regulation backed by public (administrative) fine are not mutually exclusive, but complementary. The joint use of them as a comprehensive solution reflects the goal of optimising social welfare.

11.6 Comparative negligence as the preferred tort rule for cyberattacks

11.6.1 Why not strict liability?

a) Only two variables optimized

From our normative analysis before, it could be concluded that the rule of strict liability provides incentives for efficient precautions (care level + activity level) by only one side, the vendor (tortfeasor) side, but not both. In other words, only two variables can be optimized. Compared to strict liability, negligence rules provide incentives for one more variable, which is relevant in bilateral accident settings where both the injurer and victim can influence the accident risk. Various forms of negligence create incentives for efficient care levels of both the vendor and the victim, as well as the efficient activity level of one of the two parties. The residual liability bearer, who must bear the cost of accident harm in the end, will have incentives to optimize his activity level under any form of negligence rule[355]. As we discussed before, to reduce the negative influence of cyberattacks, precautions from both the software vendor and the user are required. Thus, negligence rules have sufficient reasons to be preferred.

b) The premise of being a product

The application of strict liability is based on the solid premise that the software is a product. Section 11.2 showed that in some of the major product liability regimes in the world, like the U.S. and the EU, there is no conclusive answer whether software should be treated as a product under strict product liability. The American Law Institute's Restatement (Third) of Torts: Product Liability (1998) adopts a tangibility-intangibility dichotomy to determine the meaning of "product", which defines a product as "tangible personal property distributed commercially for use or consumption"[356]. Unlike the American wording of "tangible", the wording used in the European Product Liability Directive (EPLD), the unitary product liability regime in EU issued in 1985, is "movable". According to the EPLD, "a 'product' includes all movables which can be

[355] Diamond (1974); Shavell (1980)
[356] Restatement (Third) of Torts: Product Liability §19 (1998)

the subject of economic activity…… Immovable goods and services are excluded"[357]. With vague terms like "tangible" and "movable", it remains unclear whether software with material effect would be subject to strict liability[358].

c) The causality between vulnerability and damage

Both the European Product Liability Directive (EPLD) and the American Law Institute's Restatement (Third) of Torts: Product Liability (1998) have the same requirement of causality[359]. The application of strict liability is only justified when the causality between defect and damage is proven. In addition, in the U.S. product liability regime, only manufacturing defects are subject to strict liability, whereas design defects and warning defects are subject to negligence[360]. In case of a cyberattack, it is the hacker who exploits the vulnerability and brings about damage or harm to society. Although a strong correlation is found between the vulnerability and the accidental result, the causality between them is not as obvious as the difference between black and white.

d) Vendor's innovation and user's precaution

In fact, for vulnerability (cyberattack) accidents, it is very risky to impose strict liability on software vendors without necessity proofs based on significant statistical results. Innovation in the software industry, which affects the social welfare fundamentally in the long run, should be well promoted and protected. Without the consideration of insurance, if strict liability is used improperly, it can easily lead to bankruptcies of many companies, especially those new entrants, and suppress the industry's motivation to adopt new technologies and innovate new products. On the other hand, due to the expectation of strict liability upon the vendor side, cautious behaviour from the user side may change. When the user is placed in a favourable position, inefficient precautions may result on his side. There also exists a possibility that some users may abuse the protection of strict liability to sue, leading to a waste of social resources.

---

[357] Article 2, EU Council Directive 85/374

[358] If a software is defined as a product in product liability law, the legal implication is significant. According to EPLD §8(1), "Without prejudice to the provisions of national law concerning the right of contribution or recourse, the liability of the producer shall not be reduced when the damage is caused both by a defect in product and by the act or omission of a third party", a software vendor should be subject to strict liability in cyberattacks initiated by third parties.

[359] Article 4 of the European Product Liability Directive (EPLD) and ALI's Restatement (Third) of Torts: Product Liability (1998), §1&§2

[360] The American Law Institute's Restatement (Third) of Torts: Product Liability (1998), §2

11.6.2 Comparative negligence

Different from other negligence rules under which only one party bears all of the damage, under the rule of "comparative negligence" any harm caused by an accident is divided between the parties in proportion to the contribution of their negligence to the accident. Applying comparative negligence means that the user and the vendor share the accidental burden according to the weight of their respective negligence.

First, it is observed that the role of the user is important in the prevention of accidents. Although the user cannot stop the attacks targeting the vulnerabilities in his system or machine, he is in the best position to install patches, protect data, etc. Normally the user knows his system or machine much better than others and can do these at a relatively lower cost. This is like having the driver fasten the seat belt by himself which is much cheaper than to design an automatic system for this by the manufacturer. In this sense, to push the user to install a patch should be given the same weight as to push the software vender to develop the patch. According to the efficiency argument in law and economics[361], efficiency requires choosing the party whose activity level affects accidents most to be the residual liability bearer. In other words, the one who has more influence on the accident or ability to avoid the accident should be chosen as the residual liability bearer. Considering that the vendor's activity level can be influenced through other means like public fine, which will be introduced in the next section, the user is more appropriate as the residual liability bearer under comparative negligence rule.

Secondly, the negligence of the vendor side should not be overlooked or misunderstood. As long as the defective software is sold, the vendor should be held liable for those harmful vulnerabilities inside it. If the due care standard is set as the availability of the vulnerability patch(es), by fulfilling this requirement the vendor can only avoid the liability for the time after patches are released. In other words, the vendor is still liable for the risks he has bought to the user during the time period when no patch or remedy is available.

[361] Shavell (1987, 2004), Miceli (1997), Cooter and Ulen (2004), Posner (2011)

To illustrate, we take a look at an example. On the first day, the vendor sold the user the software. After 90 days, the vendor announced the patch for the software. Afterwards, the user forgot to install the patch due to negligence. On the 100th day, accidents happened due to the existence of software defects, and the user suffered losses. In this example, the user should bear the liability for his negligence for the last ten days, whereas the vendor should bear the liability for his negligence for the time when there was no patch available. Thus, under comparative negligence, the user should bear 10% liability and the vendor should bear 90% liability.

It seems reasonable to allocate liability like this between the victim and the vendor. "Ship now, patch later" is one of the most common philosophies in the commercial software industry. In order to occupy the market early, the software vendor has the incentive to launch software with vulnerabilities first and then provide patches in the future[362]. Suppose an extreme situation in which the patch is released just one minute before the accident. Obviously, it seems unreasonable to exempt the vendor from liability because of his fulfilment of due care one minute ago. The comparative negligence rule helps allocate liability fairly between the vendor and the user.

In addition, the basis relied on by the court to judge negligence needs to be improved continuously. The availability of patches is merely a demonstration in our example, which should not be the only standard considered by the court[363]. The more reasonable the design of the standard of due care, the more effective the application of comparative negligence rule.

Under the comparative negligence rule, three variables from Table 11 will be optimized. As the residual liability bearer, the user (victim) has incentives to take an optimal care level and an optimal activity level to reduce the accidental impacts to the minimum. At the same time, the care level of the vendor is also optimized, because he wants to avoid his liability by setting his care level to the stipulated standard. As for his activity level, other legal tools outside tort law, e.g., safety regulation backed by a public fine, can be

[362] Goertzel (2016)
[363] Some safety regulations are possible to take on this role.

applied to control.

Comparative negligence also has its disadvantages. The court needs a clear basis and reliable proofs for judging who is paying for what, thus the related costs will increase accordingly[364]. In this case, safety regulation may become the criterion for the court to rely on. How to design such safety regulation is one possible direction of future research.

11.7 Public fine as a supplement

11.7.1 Arguments from Lichtman and Posner

Lichtman and Posner (2006) argue that software vendors like Microsoft should be liable because "the vulnerabilities in the Windows operating system are akin to the design defects……"[365]. This means an affected software vendor should be held liable for the vulnerabilities exploited in cyberattacks, even though the cyberattack has been launched by the third-party hackers. Furthermore, they point out that private parties cannot reach the optimal solution on their own because of two main reasons[366]:

1) The party directly responsible for the bad act is beyond the effective reach of the law:
Cyber-attackers are quite often not subject to the effective reach of the law. Cyberspace knows no borders. Those cyber-attackers are frequently both thousands of kilometres away physically and hiding behind firewalls virtually. They are relevant direct actors, but they are outside the reach of the laws where the victims are located. Their risk of being apprehended is rather small, but the magnitude of loss they can cause is rather large[367]. In most cases, cyber-attackers lack sufficient assets to pay for the harm they cause, especially for those who are from developing areas.

2) The high transaction costs make contract negotiations implausible.
The victims also cannot avoid being attacked through the negotiation with those attackers. Transaction costs are high, and the private parties cannot create a contract as the efficient solution.

---

[364] Parisi (2013) p.65
[365] Lichtman & Posner (2006), p.257
[366] Lichtman & Posner (2006), p.233
[367] This is also the reason why criminal liability cannot be an ideal deterrent. Criminal punishments cannot reach such severity that the expected punishment of the cyber-attackers, which is the product of the probability of being apprehended and the punishment amount, will be significantly influenced.

Based on the considerations above, Lichtman and Posner (2006) recommend explicitly to impose legal incentives on the party who has the ability to "deter or detect the bad acts" and will be encouraged to "internalize some significant negative externality associated with its activities"[368].

11.7.2 Vulnerabilities as the pollutants of cyberspace

As pollutants bring risks to the environment, vulnerabilities bring risks to cyberspace. Both of them are dangerous by-products in the production process. In this sense, software vendors who release vulnerabilities outside should be treated in a similar manner as producers of environmental pollutants. Cyberattacks just reveal the existence of those dangerous vulnerabilities.

It is recommended that a public fine is imposed on the affected software vendor after a wide influencing cyberattack if liability rules or safety regulations are absent. This means that the software vendor will have to pay a fine to the government or some public institute. Unlike comparative negligence, which is the remedy from the micro perspective of individuals, imposing a public fine is the remedy from the macro perspective of society. Because of the anticipation of this sanction, the software vendor will be incentivized to optimize his activity level in accordance with social welfare requirements. The dilution of the deterrent effect of tort liability (private in nature) could be made up by social control (public in nature).

In Chapter 10, the result of our empirical study has shown that in the case of a large-scale cyberattack, the market does not pass reasonable pressure on the vendor of relevant software. If market failure exists, public intervention as the corresponding remedy is justified. In addition, widely used software is getting more and more like a public good. Once there is a problem, many people will be negatively influenced. These arguments in my view justify the introduction of a public fine for cyberattacks.

The public authority may suffer an informational disadvantage compared to the micro

[368] Lichtman & Posner (2006), p.233

level but may have better skills and knowledge to evaluate the risks related to vulnerabilities and cyberattacks on a macro level, especially when there are economies of scale in acquiring such information. When the threat of tort liability provides an insufficient deterrence against improper release of risks - due to barriers faced by victims wanting to sue the vendor or to establish causality in the accident - the public fine could be held as a backup solution to create incentives to reduce risks by making the software vendor pay the fine.

In addition, a public fine essentially functions like an order to pay damages in tort proceedings, which means that the vendor has to make a cost-benefit analysis on the risk of vulnerabilities. To improve the overall cybersecurity, the role and responsibility of the software vendor is self-evident. Software vendors are in a good position to influence and deter the bad actions. Although software vendors cannot directly detect or monitor cyberattacks, they can effectively influence the possibility of their occurrence as a whole. This means that the software vendors can affect the frequency and severity of cyberattacks. An easy-to-compromise system often incurs more attacks than a hard-to-compromise system. The larger the total number of vulnerabilities, the greater the probability that there are zero-day vulnerabilities. The attitude of the software vendor today – whether he has taken due care and been responsible for the risk of vulnerabilities – will directly influence the occurrence and magnitude of harm of cyberattacks in the future. This kind of influence spans time. Logically there is a strong relationship between the security status of a piece of software and the subsequent attacks on it. Although the attackers' motivations cannot be easily influenced, their incentives to attack can be deterred and influenced. Furthermore, software vendors can also learn experience from past cyberattacks of how vulnerabilities are exploited and make the software more robust under extreme conditions of cyberattacks.

To summarize, the imposition of a public fine has the following merits. First, the software vendor will be incentivized to consider the significant negative externalities unavoidably associated with his activities. Thus, he will invest in and improve the security processes (activity level), which will lead to less vulnerabilities and cyberattacks. Second, due to the existence of a public fine, the total costs of the vendor will increase accordingly. As a result, the price level of the software will increase to a

level at which it should be[369]. The price advantage of low-quality software is weakened. This seems fair because the resulting price reflects better the relative value of his product compared to other competing alternatives. A vendor of a defective product should not get a price advantage over his competitors, merely because they are more careful and invest more into their products. And this will also help mediate the adverse selection problem that the inferior software crowds the good software out of the market by its relative low price, especially for those software giants with monopolistic characteristics and economies of scale[370]. Thirdly, such a social control will prompt software vendors to improve their own efficiency in security processes or outsource the task to those who are more efficient (or at a lower social cost), such as the legal bug hunters. In this case, the overall social costs are the lowest[371].

However, a public fine also has its own disadvantage due to its public nature. The victims do not benefit automatically when the fine is collected. How to establish a reasonable mechanism to get victims compensated indirectly is a direction that needs to be further studied.

11.8 Chapter summary

Users of mass-produced software often encounter barriers when they try to sue the software vendor under breach of contract.

Unlike contract law, the duty violated in tort law is not based on a contract but on the premise that people should be liable for their actions or non-actions.

The legal analysis of whether software could be defined as a "product" in tort law showed us that strict product liability was not automatically applicable. Although the European Commission has developed some clues to this question in its directives on contracts, the answer is still unclear in tort law because of its related legal implication – the application of strict product liability. Thus, strict product liability is not automatically applicable and should be based on the causation analysis case by case.

---

[369] Lichtman & Posner (2006)

[370] In microeconomics, "economies of scale" means the cost per unit of output decreases with an increasing amount, which is one of the reasons that form monopoly – one typical market failure.

[371] We will discuss this in the next chapter by using an economic model.

From the perspective of law and economics, it was shown that no single liability rule can optimize all four variables (care and activity levels of the tortfeasor and the victim) commonly used in liability rules in tort law at the same time. The difficulty lies in controlling the activity level of the non-bearer of residual liability.

To optimize the four variables at the same time, a combination of comparative negligence and safety regulation backed by a public (administrative) fine is advocated. In other words, the user will be incentivized to optimize his care level and activity level by the adoption of comparative negligence, where the software vendor will have incentives to optimize his care level. Due to the existence of regulation backed by an administrative fine for risky vulnerabilities, the vendor will also be incentivized to optimize his activity level. As a result, the four variables can be optimized simultaneously through the combination of different legal tools. To put it more precisely, this combination of legal tools guarantees a kind of legal certainty. My recommendation fits Shavell's framework. An agency is needed to enforce the public (administrative) fine if harm occurs in a wide scale cyberattack.

The next chapter will study how to design the public (administrative) fine through an original economic model, assuming liability rules are absent.

Chapter 12: The Design of the Public Fine

In this chapter the focus shifts from legal discussions to quantitative analysis. By establishing an economic model, it is going to study how to design the public (administrative) fine ("public fine" hereinafter) to achieve an optimal amount of care taken by the software vendor to prevent vulnerability accidents (i.e., prevention of harm).

As seen in the previous chapter, the public fine belongs to the combination of legal tools which includes the liability rule. To see the pure impact of the public fine on the decision of the software vendor, I set the assumption under which liabilities in contracts or torts are absent[372] (or do not work). This fits the situation in which the victim is unable to sue the software vendor for harm in a cyberattack, where only the public fine can be imposed. By relaxing this assumption, future research can be developed based on the implications of this chapter.

12.1 Model introduction and specification

Consider two players in the model, the software vendor (or "1" hereinafter) and the white cap bug hunter (or "white hunter" or "2" hereinafter)[373]. I will first study the cost functions of the software vendor[374] and the white hunter, and then consider the total social welfare (costs of the two players to hunt bugs as well as possible harm to society arising from cyberattacks). To maximize social welfare, I search for the suitable public fine. The following symbols are used in the model.

Table 13: Symbol systems in the model

x_1	the investment level by the software vendor to hunt bugs
x_2	the investment level by the white hunter to hunt bugs

[372] It is worth noting that my suggestion is consistent in this chapter and in the previous chapter, i.e., a solution of jointly using liability rules and safety regulation backed by a public fine (regulation backed by an administrative fine) for the risk of vulnerability. In other words, I attach importance to both, not only the public fine but also the private law. The absence of the role of private law in the model is merely for constructing the model.

[373] The white cap bug hunter can be either an individual or a company, who/which reports vulnerabilities to the software vendor for receiving bounties. Please refer to Chapter 5 in this thesis for more information.

[374] The reputation loss of the affected software vendor is ignored because the empirical results in Chapter 10 present the conclusion that there is no significant negative reputational influence on the software vendor after a cyberattack event.

c_1	the vendor's unit cost for every improved investment level
c_2	the white hunter's unit cost for every improved investment level
C_{sv}	the cost of the software vendor
C_{wh}	the cost of the white hunter
TC	the total cost of social welfare
H	the monetary value of the harm in a cyberattack
B	the bounty offered by the software vendor to the white hunter
F	the amount of public fine
$p(x)$	the probability of finding a vulnerability given the investment level of x, assuming the vulnerability exists. Suppose $p(x) = \frac{x-1}{x}$, satisfying $\lim_{x\to\infty} p(x) = 1$ and $x \geq 1$.

12.2 Cost functions

12.2.1 The cost function of the software vendor

The utility function of the software vendor on the issue of the vulnerability is a cost function because the vulnerability will not bring any revenues to the software vendor. In form, the cost function includes three parts: 1) the cost of the investment by the vendor to prevent vulnerabilities from being released outside; 2) the bounty paid by the vendor to the white hunter for reporting vulnerabilities; 3) the public fine faced by the vendor when facing accidents caused by the released vulnerabilities. I use "C_{sv}" to stand for the total cost of the software vendor. Then the cost function is expressed as:

$$C_{sv} = c_1x_1 + p(x_2)[1 - p(x_1)]B + [1 - p(x_1)][1 - p(x_2)]F$$

For the first part of the expression, I assume a linear function c_1x_1. x_1 is the investment level chosen by the software vendor, where $x_1 \geq 1$ and $x_1 \in \mathbb{R}^+$. A higher investment level x_1 corresponds to fewer vulnerabilities to be released, and vice versa. c_1 is the unit cost for every investment level increased, where $c_1 \in \mathbb{R}^+$. c_1 reflects the cost efficiency of the software vendor in searching vulnerabilities. A low value of c_1 means that the vendor can carry out the task of vulnerability hunting at a low unit cost, reflecting the overall high efficiency. So, c_1x_1 is the cost of the investment by the vendor to prevent vulnerabilities from being released, or simply the cost of avoiding damage.

The second part of the expression, $p(x_2)[1-p(x_1)]B$, is the bounty paid by the vendor to the white hunter. Here $p(x_1)$ is the probability that a vulnerability is found by the software vendor at the investment level of x_1. If the software vendor increases his investment level x_1, $p(x_1)$, the probability that a vulnerability will be found, will increase. The subscript "1" stands for the software vendor. Accordingly, $1-p(x_1)$ is the probability that the vulnerability is missed by the software vendor. $p(x_2)$ is the probability that a vulnerability will be found by the white hunter, when an investment level x_2 is chosen to search for vulnerabilities. If the investment level x_2 increases, $p(x_2)$, the probability that a vulnerability will be found by them, will also increase. The subscript "2" here stands for the white hunter. Therefore, the product $p(x_2)[1-p(x_1)]$ is the probability that the white hunter finds a vulnerability missed by the software vendor. I use B to stand for the bounty amount. Thus, $p(x_2)[1-p(x_1)]B$ is the expected bounty paid by the vendor, which is also one part of his costs.

The third part of the expression, $[1-p(x_1)][1-p(x_2)]F$, is the expected public fine faced by the vendor in an accidental scenario. For simplicity[375], I suppose an accident occurs, if the vulnerability was found neither by the vendor nor by the white hunter. I use F to stand for the public fine.

12.2.2 The cost function of the white hunter

The utility function of the white hunter is the profit from activities of searching for and reporting a vulnerability, which can be expressed as: $P_{wh}=p(x_2)[1-p(x_1)]B-c_2x_2$. I focus on the cost part c_2x_2, because the revenue part $p(x_2)[1-p(x_1)]B$ has no impact on total social welfare. This revenue consists of revenues going to the white hunter, which are costs for the software vendor. The cost part c_2x_2 is one part of the total social costs, thus:

$$C_{wh}=c_2x_2$$

12.2.3 The total cost function of social welfare

The total cost of social welfare includes three parts: 1) the investment cost by the vendor

[375] To understand how realistic such "simplification" is, please refer to Chapter 5 for the realistic existence of bad players in vulnerability markets.

to search for vulnerabilities: c_1x_1; 2) the investment cost by the white hunter to search vulnerabilities: c_2x_2; 3) the harm if vulnerabilities are released out of control: $[1-p(x_1)][1-p(x_2)]H$. As I have discussed, the bounty amount paid by the vendor is only a cost to the vendor himself, rather than one part of the social costs. Thus, the cost function of social welfare is:

$$TC = c_1x_1 + c_2x_2 + [1-p(x_1)][1-p(x_2)]H$$

12.3 Assumptions

Assumption #1:

I assume the form of probability function $p(x)$, which is determined by people, is the same for the vendor and the white hunter. As discussed in Chapter 5, an engineer working for a vendor today may become a freelancer white hunter tomorrow. People are the same, but their roles can change. That is why I use the same probability function $p(x)$ for them.

Assumption #2:

I assume the probability function $p(x)$ satisfying conditions: $p'(x) > 0 \; and \; p''(x) < 0$. This assumption has two layers of progressive meanings here: 1) As the input – the investment level x – increases, the output – the probability $p(x)$ – increases; b) As the input increases, the output increases at a decreasing rate. In other words, every unit of increment in the low range of x has a better output than the same unit of increment in the high range of x. This is in line with the law of diminishing marginal utility[376]. The effect of improvements in output decreases, as investment level increases.

Assumption #3:

Based on the two assumptions above, I set $\frac{x-1}{x}$ ($\lim_{x\to\infty} p(x) = 1$ and $x \geq 1$) as the form of $p(x)$, because $p(x) = \frac{x-1}{x}$, satisfying $p'(x) > 0 \; and \; p''(x) < 0$, i.e., $p(x_1) = \frac{x_1-1}{x_1}$ and $p(x_2) = \frac{x_2-1}{x_2}$.

[376] See any textbook of microeconomics for an explanation of this concept, for example, Microeconomics: Global Edition (The Pearson series in economics) by Robert S. Pindyck.

Assumption #4:

For every investment level increased, the software vendor and the bug hunter have their own unit costs c_1 and c_2. The respective unit costs c_1 and c_2 reflect their respective efficiency in the use of resources other than human resources. I suppose a linear function form of cx, given the investment level x[377]. For the software vendor, the total investment cost is c_1x_1, given his investment level x_1. Similarly, for the white hunter, the total investment cost is c_2x_2, given his investment level x_2.

12.4 Analysis of the model

12.4.1 The requirement of social welfare

I start from minimizing the total cost of social welfare, which reflects the requirement from the standpoint of overall social welfare. The related expression is:

$$TC = c_1x_1 + c_2x_2 + [1 - p(x_1)][1 - p(x_2)]H$$

Substituting the $p(x_1)$ and $p(x_2)$ by their concrete forms, $p(x_1) = \frac{x_1 - 1}{x_1}$ and $p(x_2) = \frac{x_2 - 1}{x_2}$, I get the new expression:

$$TC = c_1x_1 + c_2x_2 + \frac{1}{x_1}\frac{1}{x_2}H$$

To minimize the total cost of social welfare, I find the solution[378]:

$$x_1 = \sqrt[3]{\frac{c_2H}{{c_1}^2}},\ x_2 = \sqrt[3]{\frac{c_1H}{{c_2}^2}}$$

They are the optimal investment levels, required by social welfare, of the software vendor and the white hunter.

Accordingly, the minimum total cost of social welfare is:

---

[377] Note that the linear function is for each investment level to find vulnerabilities, rather than each vulnerability. From Assumption #2, we notice that the probability of finding vulnerabilities increases at a decreasing rate, as we increase the investment level. This means that it is more and more difficult to find vulnerabilities for every subsequent investment level. Assumptions #2 and #4 together, inform us that for a certain amount of financial input, more vulnerabilities are found in the beginning than in the later stages. In other words, the unit cost to one vulnerability is lower in the beginning and the marginal cost to find one more vulnerability is increasing. Our assumptions are in line with the intuition that "low hanging fruits" are easy to take, in which the cost per unit of fruit is lower in the first stage.

[378] For detailed calculations, please refer to Appendix 5, #1.

$$TC_{min} = 3\sqrt[3]{c_1 c_2 H}$$

12.4.2 The incentive of the software vendor

The cost function of the software vendor is:

$$C_{sv} = c_1 x_1 + p(x_2)[1 - p(x_1)]B + [1 - p(x_1)][1 - p(x_2)]F$$

The software vendor has an incentive to minimize his costs. Notice the relationship between B and F, i.e., $B \leq p(x_2)[1 - p(x_1)]F$. If $B > p(x_2)[1 - p(x_1)]F$, the software vendor will choose to pay the expected public fine rather than the bounty. Thus, the existence of B makes no sense. For simplicity of the calculation, I choose $B = p(x_2)[1 - p(x_1)]F$. Substituting B with $p(x_2)[1 - p(x_1)]F$, I get the expression of C_{sv}:

$$C_{sv} = c_1 x_1 + p^2(x_2)[1 - p(x_1)]^2 F + [1 - p(x_1)][1 - p(x_2)]F$$

The incentive of the software vendor is to minimize his cost, i.e., to satisfy the first order condition[379] of the cost function: $\frac{\partial(C_{sv})}{\partial(x_1)} = 0$. Accordingly, when the software vendor minimizes his cost, the following expression of F should be satisfied[380]:

$$F = \frac{c_1 {x_1}^2}{2\frac{1}{x_1}\left(\frac{x_2 - 1}{x_2}\right)^2 + \frac{1}{x_2}}$$

12.4.3 Combining the social requirement and the vendor's incentive

In section 12.4.1, I have concluded the requirement to minimize the social cost:

$$x_1 = \sqrt[3]{\frac{c_2 H}{{c_1}^2}},\ x_2 = \sqrt[3]{\frac{c_1 H}{{c_2}^2}} \qquad ①$$

In section 12.4.2, I have concluded the expression of the public fine when the software vendor managed to minimize his total cost:

$$F = \frac{c_1 {x_1}^2}{2\frac{1}{x_1}\left(\frac{x_2 - 1}{x_2}\right)^2 + \frac{1}{x_2}} \qquad ②$$

To make the vendor's incentive in line with the social requirement, I combine these two

[379] We don't have to calculate the second order condition to prove the existence of minimum, because this cost function includes three non-negative parts. In the extreme, the minimum exists and is equal to zero. So, the second order condition is automatically satisfied.

[380] For detailed calculations, please refer to Appendix 5, #2.

conditions together and get the expression of F_{min}[381]. By substituting $\sqrt[3]{\frac{c_2H}{{c_1}^2}}$, $\sqrt[3]{\frac{c_1H}{{c_2}^2}}$ with x_1, x_2 in ②, I can get the form of F_{min} expressed only by c_1, c_2, and H[382]

$$F_{min} = \frac{c_1\left(\sqrt[3]{\frac{c_2H}{{c_1}^2}}\right)^2}{\frac{2}{\sqrt[3]{\frac{c_2H}{{c_1}^2}}}\left(1-\frac{1}{\sqrt[3]{\frac{c_1H}{{c_2}^2}}}\right)^2+\frac{1}{\sqrt[3]{\frac{c_1H}{{c_2}^2}}}}$$

In the next section, I will use specific values of c_1, c_2, and H to simulate the design of this public fine.

12.5 The simulation

12.5.1 The constraints

To satisfy a) the inequalities $0 \le p(x_1) \le 1$ and $0 \le p(x_2) \le 1$, while $x_1 = \sqrt[3]{\frac{c_2H}{{c_1}^2}}$, $x_2 = \sqrt[3]{\frac{c_1H}{{c_2}^2}}$, $p(x_1) = \frac{x_1-1}{x_1}$ and $p(x_2) = \frac{x_2-1}{x_2}$, and b) $TC_{min} = 3\sqrt[3]{c_1c_2H} < H$ simultaneously, the constraints for c_1, c_2, and H are expressed in ③[383]:

$$c_1H \ge {c_2}^2 \; and \; c_2H \ge {c_1}^2 \; and \; H^2 > 27c_1c_2 \qquad ③$$

12.5.2 Six scenarios

In this section, I will carry out a simulation by assigning six sets of c_1, c_2, and H with concrete values which satisfies ③. Then I will calculate the six values of F_{min} in these six scenarios. The simulation results are summarized in the following table.

Table 14: Different minimum public fine requirements in different scenarios

scenario	c_1	c_2	H	F_{min}	F_{min}/H
#1	1	1	8	5.33	66.67%
#2	1	1	27	14.29	52.94%

[381] This public fine amount is in line with the requirement of minimizing total social cost.
[382] For detailed calculation, please refer to Appendix 5, #3.
[383] For detailed calculation, please refer to Appendix 5, #4.

#3	1	8/27	8	1.57	19.63%
#4	1	8/27	27	4.58	16.96%
#5	8/27	1	8	7.71	96.38%
#6	8/27	1	27	23.52	87.15%

12.5.3 Observations

Observing the formula of F_{min} and the simulation results above, the following points can be concluded:

a) In theory, a quantitative relationship can be established between the harm and the public fine. According to different values of c_1 and c_2, this quantitative relationship is reflected in a certain degree of proportional relationship. This implies that the regulator can determine the amount of the public fine by the statistical data of different scales of harm in cyberattacks in history.

b) When c_1 and c_2 are very close, which are scenarios #1 and #2 in Table 14, F_{min} does not need to cover all the harm, counting for only part of it (66.67% and 52.94%). This reflects that the existence of the white hunter has a leverage effect - the public fine imposed on the software vendor only needs to cover part of the harm, not all of it. Objectively the white hunter takes part of the duty to reduce the overall social risks because the task of bug hunting can be outsourced by the software vendor. By making the vendor internalize some of the harm, i.e., imposing a public fine, the total social costs can be minimized.

c) When c_2 is much smaller than c_1, i.e., the white hunter is much more efficient than the software vendor, the leverage effect is much more significant (19.63% and 16.96%), referring to scenarios #3 and #4 in Table 14. This is because when the white hunter is more efficient, efficiency requires him to undertake more tasks to reduce the social risks of cyberattacks. The software vendor can also save costs by outsourcing tasks of bug hunting. In this case, it is unnecessary for the regulator to impose a high amount of public fine. However, to impose a public fine on the software vendor is still necessary because this helps to make the software vendor outsource tasks of bug hunting.

d) When c_1 is much smaller than c_2, i.e., the software vendor is much more efficient

than the white hunter, the leverage effect is greatly weakened (96.38% and 87.15%), referring to scenarios #5 and #6 in Table 14. This is because the efficiency requires the software vendor to undertake the task of reducing the overall risks. A higher proportion of the harm should be internalized to incentivize the software vendor to solve the problems of vulnerabilities. The role of the white hunter is weak because of his lower efficiency and higher unit cost to do the same thing.

12.5.4 Implications

a) It is necessary to impose a public fine on the software vendor to incentivize him to internalize the externalized social costs in cyberattacks. The concrete expressions of x_1 and x_2 in section 12.4.1 are the optimal investment levels, required by social welfare, for the software vendor and the white hunter. The public fine in this chapter is designed to achieve this goal through the cost-minimization process of the software vendor and his outsourcing activities.

b) The regulator can determine the amount of such a public fine based on the statistical data of harm resulting from cyberattacks in the past. Based on the expectation of such public fine, the software vendor will internalize the possible harm caused by vulnerabilities and increase his investment level in bug hunting. Fewer vulnerabilities will reduce the possibility of cyberattacking.

c) The regulator should analyse the real value of c_1 and c_2, the (average) unit cost of the software vendor (group) and the (average) unit cost of the white hunter (group). Intuitively, c_1 and c_2 may be close, or c_2 may be a bit smaller than c_1[384]. If this is the case, the regulator can set the public fine as a medium proportion of the corresponding harm level. If c_2 is much smaller than c_1, the public fine can be set as a small proportion of the correspond harm level. If c_2 is much bigger than c_1, the public fine can be set as a big proportion of the corresponding harm level. All these are reflected by the column of ratios "F_{min}/Hin" in Table 14.

d) The role of the white hunter is important. How to make good use of their professional

[384] Otherwise, it will be difficult for a white hunter with high unit cost to stay in the business.

capabilities thus eliminate cyber risks is the key. Recall one of the conclusions in Chapter 7, increasing the penalty for the illegal market transactions is the most effective way to get them to trade in the white market. Policy makers need to always keep them in mind and effectively guide their behaviour by making policy tools from a macro perspective.

12.6 Chapter summary

In this chapter, I studied the design of a public fine without the consideration of contracts or torts by establishing an economic model. Such a public fine was recommended in the previous chapter as a tool to control the activity level of the non-bearer of residual liability, especially in cyberattacks, in case liabilities in contracts and torts do not function well.

Based on an analysis of minimizing total social costs, the suitable amount the public fine was found, which is a function of the harm and the cost efficiencies of the software vendor and the white hunter. A regulator should set the public fine according to a) the historical different level of harm caused by cyberattacks and b) the relative efficiency of the investments by the software vendor and the white hunter in hunting bugs.

Thus, this chapter is a supplement to the previous chapter, by providing recommendations to regulators to formulate relevant regulatory policies. The premise of the design of such a public fine is that there are no liabilities from contracts and torts. In case either of them works, the amount of public fine should be adjusted accordingly or regarded just as a reference. Otherwise, a double burden will be imposed on the software vendor, which will restrict his innovation and development.

Finally, it is worth noting that my recommendation is consistent with the previous chapter, i.e., a solution of jointly using liability rules and safety regulation backed by a public fine for the risk of vulnerability. In short, I attach importance to both the private law and the public fine.

Chapter 13: Conclusion

Our world is increasingly interconnected via various software applications. Meanwhile, potential threats in the cyberspace are growing and becoming more challenging than ever. Cyberattacks, initiated from thousands of kilometres away, are seen to cross physical national borders and negatively influence countries' economy, social life, politics, and other aspects. These remote attacks target vulnerabilities in software and try to compromise the associated computer systems, networks, and applications. As software is implanted into every aspect of our life, the negative externality of software vulnerabilities is significant and cannot be ignored. Although our thorough understanding of the vulnerability risk is crucial to improve cybersecurity from its roots, currently there is little literature that contributes to this topic. This thesis aims to fill the gap.

13.1 Review of previous chapters

My research question was how to understand vulnerabilities and their relevance to cybersecurity, the role of the government, as well as the role of law and regulation thereof. Chapter 1 was set as the prologue of the whole thesis. After showing the facts and statistics of recent cyberattacks, I introduced the research question of my thesis, seven research sub-questions, and the structure of this thesis. Sub-topics like the vulnerability's role in cyberattacks, its intrinsic value and related markets, the dilemma of the government, the concern of market failure in case of vulnerability and cyberattack, and the possible legal (or regulative) solutions for the risk of vulnerability and cyberattack were introduced as well.

Chapter 2 reviewed the existing literature on software vulnerability and cybersecurity. Although scholars agree that vulnerabilities are crucial to cybersecurity and cybercrime, few of them have discussed important aspects of the issue, such as the liabilities related to such software flaws in cyberattack cases. Among those articles discussing the dilemma faced by governments - whether they should disclose or retain vulnerabilities for legal or military purposes, few contributions were found that comprehensively and systematically considered both the role of a vulnerability for public security and the vulnerability itself as a kind of strategical resource.

Chapter 3 answered the first sub-question by directing readers' attention to the impacts of vulnerabilities on cybersecurity. Two real cases - Stuxnet and WannaCry - were studied. Both were landmarks in history and unveiled the mysterious veil of cyberattacks. The Stuxnet case (2010) revealed that by exploiting existing vulnerabilities, virtual codes can cause physical damage to the real world. And the WannaCry case (2017) was the beginning of the ransomware attacking vulnerabilities in connected networks worldwide. These two cases reflected the significance of vulnerabilities to cybersecurity.

Chapter 4 answered the second sub-question by focusing on the economic nature of vulnerabilities. It analysed the life cycle of a vulnerability, its intrinsic value, and explained why vulnerabilities are inevitable. The link and difference between a vulnerability and its related exploit(s) were clarified. The zero-day, which is the most dangerous and socially destructive type of vulnerability, was also emphasized because of its impacts on cybersecurity.

Chapter 5 responded to the third sub-question by examining people who search vulnerabilities - the bug hunters and the markets for vulnerabilities. I showed, using various data sources, that bug hunters are distributed all over the world and that financial incentives constitute the main motivation for their activities. In other words, the assumption of profit maximization in traditional economics is applicable to them. Then three markets for vulnerabilities - white, grey, and black - were studied and compared. The competitive nature of the white market vis-à-vis the grey or black market was found. Further, complementarity was found between the grey market and the black market, because the respective buyers in the two markets may require vulnerabilities of different risk levels. Government agencies are the main buyers in the grey market, and they need high-risk and secretive vulnerabilities such as zero-days. Criminal organizations are usually the buyers in the black market, and they often need a vulnerability toolkit which is affordable and easy to operate.

Chapter 6 applied an auction model to derive a vulnerability's price in the black market, in response to the fourth sub-question. Theoretically, three factors were found to

influence this price: a) the price level in the white market; b) the number of players in the black market; c) the buyer's historically highest willingness to pay for the risk premium in the black market. An increased bounty price (white market price) results in a similar price increase in the black market, constituting a barrier to criminals because of higher crime costs. However, the high price in the black market does not pose a problem for some hackers funded by the military or the state. As long as the black market exists, they can obtain the vulnerabilities they need by merely increasing their biddings. The key points to consider in policy or law making are reducing the liquidity of the black market (limiting the number of participants), increasing the costs of illegal transactions, and promoting the reasonable bounty price (white market price).

The answer to the fifth sub-question was the theme of Chapter 7 to Chapter 9. In these three chapters, the focus was on the role of the government, discussing its involvement in vulnerability transactions and the relevant policy to retain or to disclose vulnerabilities. The participation of governments in the black market was discussed in Chapter 7. The dilemma of the government, i.e., whether it should keep vulnerabilities in its arsenal, was discussed in Chapter 8 and Chapter 9.

Chapter 7 expanded the analytical framework of Chapter 6 and emphasized the following points on the governments' participation in the black market:

a) Governments hacking for the purpose of legal enforcement or intelligence should be acceptable, given the booming advanced encryption and anonymization technologies used by criminals. From a static or short run perspective, the governments' participation in the black market to some extent decreases the probability of risky vulnerabilities flowing to criminals, as long as no third party can get the same vulnerability. This exclusivity of transactions should be the prerequisite for government agencies to purchase vulnerabilities from outside.

b) From a dynamic or long-term perspective, the governments' participation in the black market may increase the number of total active market players, as well as the anticipation of the highest possible valuation of vulnerabilities. Both will lead to a more active black market, jeopardizing cybersecurity.

c) Paying attention to the seller (the bug hunter) is more effective than paying attention to the buyer (the government agency). Increasing sellers' anticipation of penalties in

illegal transactions will, to a greater extent, weaken the probability of vulnerabilities flowing into the wrong hands. This finding is in line with the theory of criminal law formalized in Becker (1968).

Chapter 8 and Chapter 9 presented the dilemma faced by the government, whether to disclose the vulnerabilities in its stockpile for the sake of general cybersecurity or to retain them for the sake of national security. The corresponding policies (VEP in the US and GDDP in the EU) were evaluated, considering the strategic role of vulnerabilities in cyberattacks. The following conclusions were made as a result:

a) Cyberspace has no borders. The regional unilateral policy constrains the cyber operations of the government and makes the country disadvantaged in the face of borderless cyberattacks. In other words, without effective international cooperation, a unilateral disclosure policy by the government can guarantee neither local cybersecurity nor the advantages over its foreign adversaries. Cybersecurity can only be guaranteed through strengthening the protection of cyberspace as a whole. In this regard, the role of the government should be embodied in actively seeking cooperation between governments and abiding by common cybersecurity policies.

b) Government agencies should give the utmost attention to how to protect their vulnerability stockpiles from being stolen and manage their channels and suppliers for transactions. This should be valued more than the question of immediate disclosure of their vulnerabilities in hand.

Just at the time I was finalizing this thesis, an interesting news item appeared that strongly supports my conclusions from Chapter 7 to Chapter 9: the FBI got Colonial Pipeline's bitcoin ransom back by exploiting the criminals' password storage[385]. Although the FBI would not explain exactly how the private key for the bitcoin wallet was retrieved, it is likely that the government agency exploited vulnerabilities in the server and got access to where the criminals had stored the key[386]. An alternative possibility is that the bitcoin had security vulnerabilities, which has not been confirmed

[385] See CNBC, https://www.cnbc.com/2021/06/08/fbi-likely-exploited-sloppy-password-storage-to-seize-colonial-ransom.html; The Wall Street Journal, https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981 (retrieved on 09 June 2021)

[386] *Id.*

by crypto experts[387]. This recent case confirmed my answer to the fifth sub-question. Government hacking for the purpose of legal enforcement or intelligence should to some extent be acceptable, given the booming advanced encryption and anonymization technologies used by criminals. One result in Chapter 7 showed that in the short run, the governments' participation in the black market to some extent decreases the probability of risky vulnerabilities flowing to criminals, as long as the exclusivity of transactions can be ensured. From the conclusions in Chapter 9, it was seen that in the short run it is better for the government agency to keep vulnerabilities, rather than to disclose them, for the purposes of law enforcement and investigation.

Vulnerabilities are a by-product of software. When looking for solutions to them, it is impossible to bypass the software and its developer, the software vendor. The subsequent cyberattacks disclose how dangerous these vulnerabilities are, or how flawed the affected software is. Correspondingly, the software vendor is supposed to be in the best position to reduce the risks of vulnerability at the lowest social cost.

Chapter 10 answered the sixth sub-question by empirically studying the reaction of the market to cyberattacks and more specifically whether the market exerts pressure on a software vendor if vulnerabilities in his software were exploited in a large-scale cyberattack. The empirical result proved that at least to some extent market failure exists in reaction to vulnerabilities. There was no significant market pressure upon the software vendor even when the software had been proven seriously risky by a severe cyberattack. Comparatively, the market mechanism functioned well in other cases. The following reasons were given as explanations:

a) Technical barriers and cognitive inefficiency deter the public from recognizing the root of the problem or being familiar with the risks of vulnerabilities.

b) Due to the existence of network effect and high switching costs, users have to stick to the flawed software, even if they have known about the possibility of cyberattacks.

c) The dominant position or market power of software giants protects them from the market pressure.

[387] https://www.cnbc.com/2021/06/08/fbi-likely-exploited-sloppy-password-storage-to-seize-colonial-ransom.html (retrieved on 09 June 2021)

The empirical result in Chapter 10 paved the way for further research. Since market failure was proven, solutions without external intervention are often inefficient to solve problems caused by software vulnerabilities. Chapter 11 focused on this and discussed the possible options of central intervention through private and public law, covering contracts, liabilities in torts, and regulation.

Chapter 11 and Chapter 12 responded to the last sub-question. At the beginning of Chapter 11, the question "whether software should be defined as a product or a service" was raised and discussed. Doing so is meaningful because its legal implication is related not only to contract law but also to tort law, especially the application of strict liability laws. In the following steps, barriers to applying contract law in vulnerability accidents were discussed and the different liability rules in tort law were analysed from the perspective of law and economics. After considering liability rules in torts (and the related four variables) within the law and economics analytical framework, I proposed a solution of jointly using comparative negligence rule and safety regulation backed by a public (administrative) fine for the harm caused by vulnerabilities. It is a combination of torts and regulation (ex-ante and ex-post), which is in line with the principles in Shavell (1984) and Faure, Visscher & Weber (2016).

Chapter 12 was a supplement to Chapter 11, studying how to design the public (administrative) fine under the assumption that private laws and regulations are absent. To maximize total social welfare, the optimal investment level by the software vendor was deduced. Furthermore, the most effective public fine, which can incentivize the software vendor to internalize the negative externalities of vulnerabilities at the lowest social cost, was found. Conclusions in this chapter were reflected in the following aspects:

a) It is necessary to impose a public (administrative) fine on the software vendor to incentivize him to internalize the externalized social costs in cyberattacks.

b) Based on an analysis of minimizing total social costs, the suitable amount of the public fine can be found, which is a function of the harm and the cost efficiencies of the software vendor and the white hunter. A regulator should set the public fine according to the statistical data of harm resulting from cyberattacks in the past, as well as the relative efficiency of the investments by the software vendor and the white hunter

in bug hunting. Due to the anticipation of such a public (administrative) fine, the software vendor will internalize the possible harm caused by vulnerabilities and increase his investment level in bug hunting accordingly.

c) The role of white hunters is important to the overall cybersecurity. How to make good use of their professional capabilities to eliminate cyber risks is the key. Policy makers need to always keep them in mind and effectively guide their behaviour by making policy tools from a macro perspective. On the one hand, the bounty amount should be raised; on the other hand, the deterrence of illegal transactions should be strengthened.

d) As mentioned before, the public fine should be considered as complementary to laws or safety regulation.

13.2 Policy recommendations

Software vulnerabilities are risky to cybersecurity, as well as an obstacle to the development of cyberspace and cyber welfare. To deal with this challenging obstacle, it is necessary to implement both short-term solutions and long-term strategies. To this end, the following policy recommendations follow from my findings.

13.2.1 Short-term solutions

1) A combination of legal tools

As I explained in Chapter 11, it is meaningful to implement a combination of legal tools, i.e., a toolbox of liability rules and regulations. In this thesis, it is recommended to jointly use comparative negligence and safety regulation backed by a public fine. As a result, not only will the software vendor be incentivized to optimize his care level and activity level according to the requirement of social welfare, but also the user will increase his cybersecurity awareness (care level) and improve his behaviour patterns (activity level) in cyberspace.

2) Regulations (ex-ante and ex-post) are necessary

If the regulator or court needs to set the legal requirement for the (minimum) investment level in bug hunting (i.e., the level of care) for the software vendor, the results of the model in Chapter 12 could be referenced. In case private law is difficult to apply, the public fine is the alternative for incentivizing the software vendor to perform his

responsibility to society and internalize the negative impacts of vulnerabilities. In a sense, vulnerabilities in cyberspace are like environmental pollutants in real living space, both of which should be regulated at least to some extent, based on the law and economics literature.

3) To establish a database on cyberattacks

As I explained in Chapter 12, a regulator should set the public fine according to the statistical data of different levels of harm that resulted from cyberattacks in the past, as well as the relative efficiency of the investments by the software vendor and the white hunter in bug hunting. Based on this, to obtain objective data to formulate effective regulation, a database on large-scale cyberattacks must be established. Furthermore, an in-depth investigation, into the efficiency in bug hunting by the software vendor (group) and the bug hunter (group), should be made. Related datasets are also necessary to establish for the purpose of policy making.

4) To induce more legal transactions

Based on the conclusions of Chapter 5 and Chapter 6, on the one hand, the bounty amount and the accumulated reputation by legally reporting vulnerabilities are two attractions in the white market. In addition, the expected punishment in the black market is a deterrence for a bug hunter on illegal trade. On the other hand, high bidding in the black market lures a bug hunter to enter into illegal transactions. To influence the decision of the bug hunter to trade legally or not, the policy maker should take these four factors into account. In other words, as long as the weight of "the accumulated reputation in the white market together with the punishment in the black market" is greater than the weight of "the highest bidding in the black market minus the bounty amount", i.e., the price premium in the illegal transaction, the bug hunter will spontaneously choose the white market and stay away from the black market. To treat these four factors as a whole to incentivize bug hunters to contribute their skills to cybersecurity is one suggestion for policy makers.

5) To protect the stockpile of vulnerabilities from being stolen

Combining the discussions in Chapter 7 and Chapter 9, government should be supervised to better manage their stockpiles of vulnerabilities. While ensuring their

capabilities of law enforcement or intelligence, government agencies also assume the duty to protect their vulnerabilities from being hacked. If they fail to keep their vulnerabilities or equivalent tools properly, criminals will not only buy them from the black market, but also steal them from the government agencies' arsenals. At the same time, those sellers who supply vulnerabilities to government agencies should also be well supervised to ensure that they will not sell vulnerabilities to any third party.

13.2.2 Long-term strategies

1) International cooperation

Cyberspace knows no borders. Therefore, cybersecurity needs the cooperation of countries or coordinated cyberspace regulations. As I discussed in Chapter 8 and Chapter 9, in the long run, a unilateral policy like the VEP can guarantee a country neither local cybersecurity nor advantages over other malicious adversaries in cyberspace. Only through strengthening the protection of cyberspace as a whole, the digital security and cyber freedom of citizens within this framework can be guaranteed. In this regard, the role of the lawmaker or regulator is embodied in actively seeking cooperation between countries and abiding by common cybersecurity policies.

2) Integration with competition law

Software vulnerabilities impose negative externalities on society, but Chapter 10 showed that the market may not respond properly to this externality problem. This lack of market response is likely to be caused also by the market power of the software vendor and the network effect of the software. Competition law considers exactly how to eliminate the negative effects of market failure and the concentration of market power. Therefore, laws and regulation dealing with vulnerabilities should be formulated in conjunction with competition law, considering the market share and market power of the related software vendor.

3) Government agencies should avoid vulnerability transactions

In the long run, government agencies should leave vulnerability business, even if they can guarantee the exclusivity of transactions. Regular financial inflows into the non-white market will raise the anticipation of income from vulnerability business. The black market will become more attractive, and the market liquidity will therefore be

strengthened, which ultimately lead risks to increase in social welfare in the long term. Government agencies can maintain and improve their capabilities of law enforcement and intelligence by strengthening their own technical teams and cooperating with the software industry.

13.3 Directions for further research

Like most research, this thesis has some limitations, caused by the necessarily restricted scope of the study and the availability of data. Here I would like to point out some possible directions for further research.

First, the event study in this thesis was focused on the WannaCry cyberattack. When there are more and more cyberattacks of similar scale and wide influence, future research can be updated based on new data of those attacks.

Second, as for the application of comparative negligence, the court needs a clear basis and operable standards to determine negligence objectively. How to design these standards is another possible direction of future research.

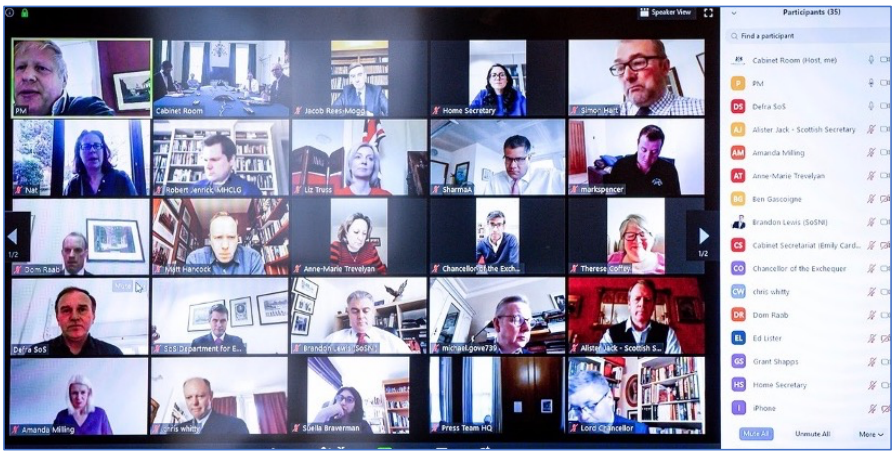
Thirdly, the public fine recommended in this thesis has its own disadvantage due to its public nature. The victims do not benefit automatically when the fine is collected. How to establish a reasonable mechanism for victims to obtain compensation for harm suffered is a topic that merits further study.

Last but not least, the problem of software vulnerabilities should be viewed from a dynamic perspective and thus related laws and regulation should be formulated in conjunction with competition law, considering the market share and market power of the related software vendor. This area is yet another direction worthy of future research.

Appendix 1: British Cabinet's Online Meeting

In the morning of 31 Mar 2020, Boris Johnson, the British prime minister who was self-isolating after confirmed positive for coronavirus, together with his top team had their "first-ever digital Cabinet" on the video meeting platform. At 11:20 on the same day, he tweeted a picture of their online cabinet meeting forgetting to cut the meeting ID number 539-544-323, as well as the usernames of some participating ministers.

Online meeting ID 539-544-323



Source: https://twitter.com/BorisJohnson

Although in most cases the meeting owner should set a password and the Downing Street spokesman expressed their confidence in and satisfaction with the security[388], all those necessary security procedures cannot completely guarantee there is no possibility of unauthorized access during the meeting, if there exist hidden vulnerabilities in the software.

Security experts are suggesting those particularly high-risk users, with their highly sensitive discussions, to find more secure methods of communication. For they might potentially be the target of cyberattacks[389].

[388] https://metro.co.uk/2020/03/31/boris-johnson-sparks-security-concerns-revealing-zoom-id-cabinet-meeting-12489236/ (retrieved on 31 March 2020)
[389] https://www.bbc.com/news/technology-52133349 (retrieved on 2 April 2020)

In history a tiny piece of information often becomes the last straw that breaks a camel's back, not to mention in today's big data era. In the Battle of Middle way in World War II, a message intercepted by U.S. Navy intelligence personnel, which reported "AF" was running out of fresh drinking water, leaked Japan's combat intention, leading to a decisive victory for the U.S.[390] Today, to a great extent those genius brains of intelligence personnel have been replaced by algorithms of big data. What the intelligence agencies need is all types of data as inputs for big data algorithms to process. In most cases these data maybe tiny, fragmented, or even neglectable. Although there is the GDPR (General Data Protection Regulation[391]) in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA), it is not binding on other countries.

Being able to monitor meetings of the British Cabinet must be an extreme temptation to many intelligence agencies. Nowadays not only the British Cabinet carries its meeting on a commercial conference platform; many companies do the same. Secrets are potentially straightforward to be known by third parties. Furthermore, in an era of big data, even several fragmented information together can splice out a piece of sensational information. These fragmented inputs can be achieved either from an illegal access to the email, a monitored video conference, or data traces left undeleted. To many intelligence agencies, crucial vulnerabilities are the key to access to those databases. Intelligence agencies are not likely to give up stockpiling vulnerabilities as strategic resource.

[390] https://www.history.com/news/battle-midway-codebreakers-allies-pacific-theater (retrieved on 2 April 2020)
[391] Regulation (EU) 2016/679 (General Data Protection Regulation), https://gdpr-info.eu/ (retrieved on 2 April 2020)

Appendix 2: “Event Study” VS. “Difference in Difference”

Here we discuss why we use event study in our study rather than difference in difference. It is about the comparison of these two empirical methods. In the following I use “ES” standing for “Event Study” and “DD” for “Difference in Difference”.

1) One dimension VS. Two dimensions

ES does only one difference: the difference between without-event and with-event. There is no control group in ES. So, the comparison is only from one dimension. In the real practice, it refers to the “abnormal return”, which is the difference between “actual return” (with-event) and “expected return” (without-event). We test the statistical significance of this “abnormal return”.

DD does two differences: the difference between pre-policy and after-policy (time dimension), as well as the difference between treatment-group and control-group (treatment dimension). So, the comparison is from two dimensions: the time dimension and the treatment dimension. In the real case, we create the interaction term which is the product of the time dummy and the treatment dummy, meaning the impact of time dummy and the impact of treatment dummy function at the same time. After we incorporate this interaction term into our regression model, we can recognize the “untangled” or “clean” average impact of the related policy after being applied by reading directly the coefficient from result table of regression.

2) Time point Vs. Time period

ES studies the impact of an event, which is usually a sudden event or news. So, it focuses on the reaction of the market or the stake holders at the moment when the sudden event or news becomes public. It focuses on the time point or a very short period of time after the event or news. In real practice, normally we use the data of the stock market on the first day after the event. The event happens only once, and it will not happen every day after it happens. So, the ES is a method for a sudden event at some time point. The time frame of ES is: without-event → with-event →without-event. In addition, after the event, the “abnormal return” or “abnormal signal” may become as normal as before the event. Because of its attribute of “time point”, we usually build

the dataset of ES as a daily time series dataset.

DD studies the effectiveness of a policy or a regulation, which refers to two time periods --- pre-policy period and after-policy period. The influence of the policy will last once the policy is imposed. So, the DD is a method for time periods. The time frame of DD is "before the policy → after the policy". Because of its attribute of "time period" and it needs a relative longer period to study the effect of a policy, we usually build the dataset of DD as a yearly panel dataset.

3) The data on event day

We can use ES to test the sudden impact of the event on the related day(s). But in the DD, the data on this day will be treated as an outlier if it is abnormal. This is because DD focuses on time period and the event in ES will not last as long as a policy or a regulation.

4) The essence of Event Study

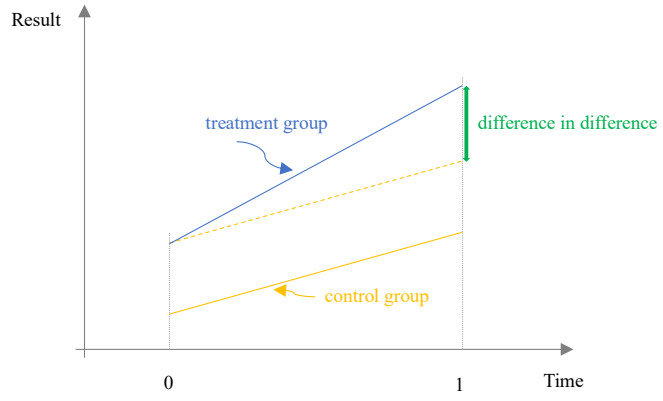
The ES and DD are very similar. In DD, graphically we draw a line parallelly to the line of the control group to have the "difference in difference" (see the graph of "difference in difference" below). In ES, graphically we draw a line (line② on the graph of "event study" below) using a statistical market model, which is a transformation of CAPM model assuming the linear relationship between the expected return of a specific stock and the return of the market as a whole. On the graph as well as in real practice, we use S&P500 standing for the market. After a simple calculation of taking the expected return from the actual return, we have the abnormal return. Then we can test whether the abnormal return is due to the event itself.

The parallel dash line in the graph of DD and the dash line② on the graph of ES have the same function: to help untangle the impact of another factor, which is control group in DD and S&P500 (market) in ES. This is to make the final difference clean. Although we don't say any "control group" in ES, the S&P 500 is the "control group in logic". Like in DD, we also take the impact of this "control group in logic" (expected return of the specific stock) away from the observation of our target group (the actual return of the stock on the event day). Because we use the linear model to calculate the expected

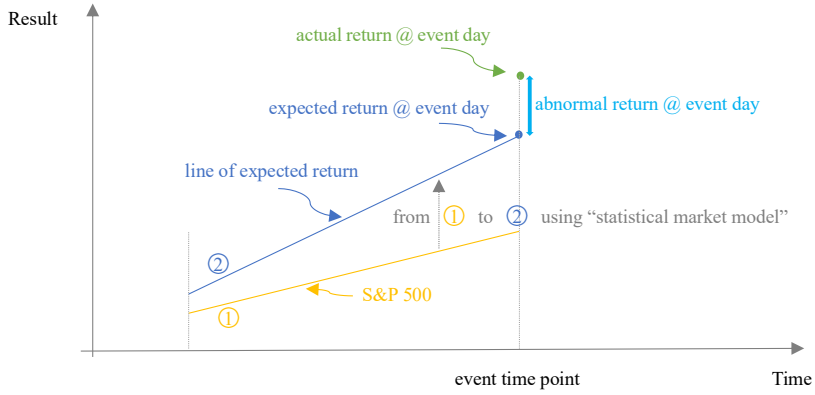
return, we don't have to calculate the difference between "treatment before policy" and "control before policy", which is calculated in DD. We have only one difference in ES, the difference in time dimension. The other difference of "controlled vs. treated" in DD, is replaced by the CAPM linear model in ES.

Please note, on the graph of ES, line②, the line of the expected return of a specific stock, is not necessarily parallel to line①, the line of the return of the market or S&P 500. This is because the expected return is a linear function of the return of the market, rather than a constant plus the return of the market.

Graph of "Difference in Difference"



Graph of "Event Study"



Appendix 3: STATA Commands

1) WannaCry case

```
tsset date, daily
twoway(tsline MSFT), tline(15may2017, lpattern(-))
twoway(tsline MSFT AAPL, yaxis(1)) (tsline SP500, yaxis(2)), tline(15may2017,
lpattern(-))

gen retMSFT = MSFT/MSFT[_n-1]-1
twoway(tsline retMSFT), tline(15may2017, lpattern(-))

gen retSP500 = SP500/SP500[_n-1]-1

gen trading_day=_n
gen trading_day_center=trading_day-262
reg retMSFT retSP500 if trading_day_center<=-1 & trading_day_center>=-250

predict expected_retMSFT
gen abnormal_return_MSFT = retMSFT-expected_retMSFT
sum abnormal_return_MSFT if trading_day_center<=-1 & trading_day_center>=-250
gen test_MSFT= abnormal_return_MSFT/.0076162
gen significance_MSFT="**" if abs(test_MSFT)>=1.96
```

Notes:

The attack of WannaCry occurred on Friday, May 12, 2017, so we focus on the share price on Monday, May 15, 2017, which is the 262nd record in the database for WannaCry case.

2) Facebook-Cambridge Analytica case

```
tsset date, daily
twoway(tsline FB), tline(19mar2018, lpattern(-))
twoway(tsline FB GooG, yaxis(1)) (tsline SP500, yaxis(2)), tline(19mar2018,
lpattern(-))

gen retFB = FB/FB[_n-1]-1
twoway(tsline retFB), tline(19mar2018, lpattern(-))

gen retSP500 = SP500/SP500[_n-1]-1

gen trading_day=_n
gen trading_day_center=trading_day-265
reg retFB retSP500 if trading_day_center<=-1 & trading_day_center>=-250

predict expected_retFB
gen abnormal_return_FB = retFB-expected_retFB
sum abnormal_return_FB if trading_day_center<=-1 & trading_day_center>=-250
gen test_FB= abnormal_return_FB/.0105417
gen significance_FB="**" if abs(test_FB)>=1.96
```

Notes:

The Facebook-Cambridge Analytica scandal occurred on Friday, March 16, 2018, so we focus on the stock price fluctuations on and after March 19, 2018, which is the 265th record in the database for Facebook-Cambridge Analytica case.

Appendix 4: Proof of "Statistical market model = CAPM + second assumption"

In fact, the statistical market model is a variant of the classic CAPM model in finance, which is expressed as the following for one period:

$$E(r_i) = r_f + \beta_i\,(Market - r_f)$$

Where $E(r_i)$ is the expected return for stock i. r_f is the risk-free rate, which is customarily the yield on government bonds like U.S. Treasuries. The risk-free rate in the formula represents the time value of money. $\beta_i\,(Market - r_f)$ as a whole represents the amount of compensation the investor needs for risk. β_i is the coefficient between $E(r_i)$ and $(Market - r_f)$, measuring how risky stock i is compared to overall market risk. $(Market - r_f)$ is the market premium, or the market return in excess of the risk-free rate. Normally the S&P 500 index is used to represent the market.

The deduction from CAPM model to the statistical market model is as follows:

$$\begin{aligned} E(r_i) &= r_f + \beta_i\,(Market - r_f) \\ &= r_f + \beta_i\,Market - \beta_i r_f \\ &= r_f - \beta_i r_f + \beta_i\,Market \\ &= r_f(1 - \beta_i) + \beta_i\,Market \end{aligned}$$

Let $\lambda_i = r_f(1 - \beta_i)$ and $\phi_i = \beta_i$, then $\lambda_i = r_f(1 - \beta_i)$ is an i-specific constant and $\phi_i = \beta_i$ is an i-specific coefficient. Now we can write the model as:

$$E(r_i) = \lambda_i + \phi_i\,Market.$$

We notice that the transformation of CAPM model $E(r_i) = \lambda_i + \phi_i\,Market$ and the statistical market model $E(r_{it}) = \lambda_i + \phi_i\,Market_t$ in Jonathan (2008) are very similar. The only difference is the subscript period t. CAMP model is for one period and the statistical market model is for different periods. Now we add the second assumption in Chapter 10 here: In the short run the relationship between an individual security and the market as a whole is relatively stable. This means, in the short run, λ_i and ϕ_i will not change for every period, i.e., $\lambda_i = \lambda_{i,t-1} = \lambda_{i,t}$ and $\phi_i = \phi_{i,t-1} = \phi_{i,t}$. The only change is the $E(r_{it})$ and $Market_t$ in every period. With this assumption of same λ_i and ϕ_i of each period in the short run, together with the transformation of CAPM model $E(r_i) = \lambda_i + \phi_i\,Market$ for one period, we can write out a combination form: $E(r_{it}) = \lambda_i + \phi_i\,Market_t$, which is the same as the statistical market model in the paper of Jonathan (2008). In my dataset, each period is

daily basis. The 250 days which I retrospect are still in the short run.

Back to the statistical market model: $E(r_{it}) = \lambda_i + \phi_i \, Market_t$, for every time period t, the expected return of a stock $E(r_{it})$ has the same linear relationship with the market return $Market_t$. So, every $(E(r_{it}), Market_t)$ will be on a line.

In addition, because of the second assumption, a stable relationship between an individual security and the market, we notice that it is possible to retrospect the data in past periods to find out the λ_i and ϕ_i, then apply them with $Market_t$ to get the $E(r_{it})$.

Appendix 5: Some Detailed Calculations

#1 The mimimal cost of social welfare

a) to find out (x_1, x_2)

the cost function $TC = f_{(x_1,x_2)} = c_1x_1 + c_2x_2 + \frac{1}{x_1}\frac{1}{x_2}H$

$$f_{x_1} = \frac{\partial(f_{(x_1,x_2)})}{\partial(x_1)} = c_1 - \frac{1}{{x_1}^2}\frac{1}{x_2}H$$

$$f_{x_2} = \frac{\partial(f_{(x_1,x_2)})}{\partial(x_2)} = c_2 - \frac{1}{x_1}\frac{1}{{x_2}^2}H$$

$$\begin{cases} f_{x_1} = 0 \\ f_{x_2} = 0 \end{cases} \Longrightarrow \begin{cases} c_1 - \frac{1}{{x_1}^2}\frac{1}{x_2}H = 0 \\ c_2 - \frac{1}{x_1}\frac{1}{{x_2}^2}H = 0 \end{cases} \Longrightarrow \begin{cases} x_1 = \sqrt[3]{\frac{c_2H}{{c_1}^2}} \\ x_2 = \sqrt[3]{\frac{c_1H}{{c_2}^2}} \end{cases}$$

b) to test whether (x_1, x_2) is the solution to minimize social welfare

$$A = f_{x_1x_1} = \frac{\partial(f_{x_1})}{\partial(x_1)} = \frac{H}{x_2}\frac{2}{{x_1}^3} = \frac{2H}{x_2{x_1}^3}$$

$$B = f_{x_1x_2} = \frac{\partial(f_{x_1})}{\partial(x_2)} = \frac{H}{{x_1}^2}\frac{1}{{x_2}^2} = \frac{H}{{x_1}^2{x_2}^2}$$

$$C = f_{x_2x_2} = \frac{\partial(f_{x_2})}{\partial(x_2)} = \frac{H}{x_1}\frac{2}{{x_2}^3} = \frac{2H}{x_1{x_2}^3}$$

$$\because AC - B^2 = \frac{3H^2}{{x_1}^2{x_2}^2} > 0 \; and \; A = \frac{2H}{x_2{x_1}^3} > 0$$

$\therefore$ *There exists the minimal* $f_{(x_1,x_2)}$.

Thus, the solution $\left(x_1 = \sqrt[3]{\frac{c_2H}{{c_1}^2}}, x_2 = \sqrt[3]{\frac{c_1H}{{c_2}^2}}\right)$ is the solution to minimize the social welfare.

c) the minimal total cost of social welfare

$$TC_{min} = c_1\sqrt[3]{\frac{c_2H}{{c_1}^2}} + c_2\sqrt[3]{\frac{c_1H}{{c_2}^2}} + \frac{1}{\sqrt[3]{\frac{c_2H}{{c_1}^2}}}\frac{1}{\sqrt[3]{\frac{c_1H}{{c_2}^2}}}H = 3\sqrt[3]{c_1c_2H}$$

#2 The first order condition of the software vendor

$\frac{\partial(C_{sv})}{\partial(x_1)} = 0$, where $C_{sv} = c_1 x_1 + p^2(x_2)[1-p(x_1)]^2 F + [1-p(x_1)][1-p(x_2)]F$

$$\frac{\partial(C_{sv})}{\partial(x_1)} = c_1 - 2p^2(x_2)F[1-p(x_1)]p'(x_1) - [1-p(x_2)]Fp'(x_1) = 0$$

$$\therefore p'(x_1) = \frac{c_1}{F\{2p^2(x_2)[1-p(x_1)] + [1-p(x_2)]\}}$$

$$\therefore F = \frac{c_1}{p'(x_1)\{2p^2(x_2)[1-p(x_1)] + [1-p(x_2)]\}}$$

$\because p(x_1) = \frac{x_1-1}{x_1},\ p(x_2) = \frac{x_2-1}{x_2},\ p'(x_1) = \frac{1}{{x_1}^2},\ 1-p(x_1) = \frac{1}{x_1},\ 1-p(x_2) = \frac{1}{x_2}$

$$\therefore F = \frac{c_1 {x_1}^2}{2\left(\frac{x_2-1}{x_2}\right)^2 \frac{1}{x_1} + \frac{1}{x_2}} = \frac{c_1 {x_1}^2}{2\frac{1}{x_1}\left(\frac{x_2-1}{x_2}\right)^2 + \frac{1}{x_2}}$$

Thus, according to the first order condition of the software vendor, the following expression should be satisfied:

$$F = \frac{c_1 {x_1}^2}{2\frac{1}{x_1}\left(\frac{x_2-1}{x_2}\right)^2 + \frac{1}{x_2}}$$

#3 The expression of F_{min}

$F = \frac{c_1 {x_1}^2}{2\frac{1}{x_1}\left(\frac{x_2-1}{x_2}\right)^2 + \frac{1}{x_2}}$, substituting $x_1 = \sqrt[3]{\frac{c_2 H}{{c_1}^2}},\ x_2 = \sqrt[3]{\frac{c_1 H}{{c_2}^2}}$, we get the expression of F_{min}:

$$F_{min} = \frac{c_1\left(\sqrt[3]{\frac{c_2 H}{{c_1}^2}}\right)^2}{\frac{2}{\sqrt[3]{\frac{c_2 H}{{c_1}^2}}}\left(1 - \frac{1}{\sqrt[3]{\frac{c_1 H}{{c_2}^2}}}\right)^2 + \frac{1}{\sqrt[3]{\frac{c_1 H}{{c_2}^2}}}}$$

#4 The constraints for c_1, c_2, and H

To satisfy the inequalities $0 \le p(x_1) \le 1$ and $0 \le p(x_2) \le 1$, while $x_1 = \sqrt[3]{\frac{c_2 H}{{c_1}^2}}$,

$x_2 = \sqrt[3]{\frac{c_1 H}{{c_2}^2}}$, $p(x_1) = \frac{x_1 - 1}{x_1}$ and $p(x_2) = \frac{x_2 - 1}{x_2}$, we can find the constraints.

$$p(x_1) = \frac{x_1 - 1}{x_1} \geq 0 \Longrightarrow x_1 \geq 1, i.e., \sqrt[3]{\frac{c_2 H}{{c_1}^2}} \geq 1 \Longrightarrow c_2 H \geq {c_1}^2,$$

$$p(x_1) = \frac{x_1 - 1}{x_1} \leq 1, the\ inequality\ always\ holds\ because\ x_1 \geq 1\ (\because\ p(x_1) \geq 0)$$

$$p(x_2) = \frac{x_2 - 1}{x_2} \geq 0 \Longrightarrow x_2 \geq 1, i.e., \sqrt[3]{\frac{c_1 H}{{c_2}^2}} \geq 1 \Longrightarrow c_1 H \geq {c_2}^2,$$

$$p(x_2) = \frac{x_2 - 1}{x_2} \leq 1, the\ inequality\ always\ holds\ because\ x_2 \geq 1\ (\because\ p(x_2) \geq 0)$$

So far, we get the constraints to assign concrete values to c_1, c_2, and H in our simulation:

$$c_1 H \geq {c_2}^2\ and\ c_2 H \geq {c_1}^2$$

References

Ablon, Lillian; Libicki, Martin; Golay, Andrea (2014), Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar, *RAND CORPORATION (Mar. 2014),* Retrieved on 20 November 2020, from http://www.rand.org/pubs/research_reports/RR610.html

Ablon, Lillian; Bogart, Andy (2017), Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits, *RAND Corporation,* Santa Monica, CA, p. xii., Retrieved on 20 November 2020, from www.rand.org/t/RR1751

Aitel, Dave; Tait, Matt (2016), Everything You Know About the Vulnerability Equities Process Is Wrong, *Lawfare,* Aug 18, 2016, Retrieved on 20 November 2020, from https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong

Albright, David; Brannan, Paul; Walrond, Christina (2010), Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment, *ISIS (Institute for Science and International Security) Report,* Retrieved on 20 November 2020, from https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/

Algarni, Abdullah; Malaiya Yashwant (2014), Software Vulnerability Markets: Discoverers and Buyers, *World Academy of Science, Engineering and Technology, International Journal of Computer, Information Science and Engineering,* Vol. 8, No. 3, pp. 480-490

Alheit, K. (2001), The applicability of the EU Product Liability Directive to software, *The Comparative and International Law Journal of Southern Africa*, Vol. 34, No. 2, pp. 188-209

Allodi, Luca; Shim, Woohyun; Massacci, Fabio (2013): Quantitative assessment of risk reduction with cybercrime black market monitoring, *Security and Privacy Workshops (SPW), IEEE,* Retrieved on 20 November 2020, from https://ieeexplore.ieee.org/document/6565246

Althuis, Jente; Haiden Leonie (2018), Fake News: A Road Map, *NATO Strategic Communications Centre of Excellence and King's Centre for Strategic Communications, Riga,* Retrieved on 20 November 2020, from https://www.stratcomcoe.org/download/file/fid/78539

Anthony, Sebastian (2015), The first rule of zero-days is no one talks about zero days (so we'll explain), *Ars Technica (Oct. 20, 2015),* Retrieved on 20 November 2020, from https://arstechnica.com/information-technology/2015/10/the-rise-of-the-zero-day-market/

Baezner, Marie; Robin, Patrice (2017), *Hotspot Analysis: Stuxnet*, Center for Security Studies (CSS), ETH Zürich, Retrieved on 05 December 2020, from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf

Barnes, Julian; Sanger, David (2020), N.S.A. Takes Step Toward Protecting World's Computers, Not Just Hacking Them, *The New York Times (Jan. 14, 2020),* Retrieved on 20 November 2020, from https://www.nytimes.com/2020/01/14/us/politics/nsa-microsoft-vulnerability.html

Becker, Gary (1968), Crime and Punishment: An Economic Approach, *Journal of Political Economy,* Vol. 76, No. 2 (Mar. - Apr. 1968), pp. 169-217, The University of Chicago Press

Bellovin, Steven; Blaze, Matt; Clark, Sandy; Landau, Susan (2014), Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet, *Northwestern Journal of Technology & Intellectual Property*, Vol. *12*, Issue 1, pp. 1-63

Broad, William J.; Markoff, John; Sanger, David E. (2011), Israeli Test on Worm Called Crucial in Iran Nuclear Delay, *N.Y. TIMES,* Jan. 15, 2011, Retrieved on 05 December 2020, from http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=a

Brown, John Prather (1973), Toward an Economic Theory of Liability, The Journal of Legal Studies, Vol. 2, No. 2, pp. 323-349

Buchanan, Ben (2020), *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Harvard University Press

Calabresi, Guido (1961), Some Thoughts on Risk Distribution and the Law of Torts, *The Yale Law Journal*, Vol. 70, No. 4, pp. 499-553

Calabresi, Guido (1970), *The Costs of Accidents: A Legal and Economic Analysis*, New Haven: Yale University Press

Calabresi, Guido; Melamed, Douglas (1972), Property Rules, Liability Rules, and

Inalienability: One View of the Cathedral, *Harvard Law Review,* Vol. 85, No. 8, pp. 1089-1128

CEPS Task Force (2018), Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges, *Centre for European Policy Studies (CEPS),* Retrieved on 20 November 2020, from https://www.ceps.eu/system/files/CEPS%20TFRonSVD%20with%20cover_0.pdf

Chen, Thomas (2010), Stuxnet, the real start of cyber warfare*? IEEE Network. Vol. 24, No.6, pp. 2–3,* Retrieved on 20 November 2020, from *https://doi.org/10.1109/MNET.2010.5634434*

Chen, Thomas; Abu-Nimeh, Saeed (2011), Lessons from Stuxnet, *Computer,* Vol. 44, No. 4, pp. 91–93, Retrieved on 20 November 2020, from https://doi.org/10.1109/MC.2011.115

Coase Ronald (1960), The Problem of Social Cost, *The Journal of Law & Economics,* Vol. 3, October 1960, pp. 1-44

Collins, Sean; McCombie, Stephen (2012), Stuxnet: the emergence of a new cyber weapon and its implications, *Journal of Policing, Intelligence and Counter Terrorism*, Vol. 7, No. 1, pp. 80-91

Cooter, Robert; Ulen, Thomas (2014), *Law and Economics (6th edition),* Pearson Education Limited

Corera, Gordon (2020), Coronavirus: Cyber-spies hunt Covid-19 research, US and UK warn, May 05, 2020, *BBC News,* Retrieved on 20 November 2020, from https://www.bbc.com/news/technology-52551023

Daniel, Michael (2014), Heartbleed: Understanding When We Disclose Cyber Vulnerabilities, *White House Blog,* 28th April 2014 ("Daniel Blog Post"), Retrieved on 30 November 2020, from https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities

Dari-Mattiacci, Giuseppe; Parisi, Francesco (2005), The economics of tort law: a precis, in Backhaus, Jürgen (ed.): *The Elgar Companion to Law and Economics*, 2nd Edition, pp. 87-102, Cheltenham: Edward Elgar

De Falco, Marco (2012), Stuxnet Facts Report: A Technical and Strategic Analysis, *NATO Cooperative Cyber Defence Centre of Excellence,* Tallinn, Retrieved on 30

November 2020, from https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf

Delcheva, Teodora; Soesanto, Stefan (2018), Time to talk: Europe and the Vulnerability Equities Process, *European Council on Foreign Relations,* 21 March 2018, Retrieved on 30 November 2020, from https://www.ecfr.eu/article/commentary_time_to_talk_europe_and_the_vulnerability_equities_process

Egelman, Serge; Herley, Cormac (2013), Markets for zero-day exploits: ethics and implications, *NSPW '13: Proceedings of the 2013 New Security Paradigms Workshop,* pp. 41-46, Retrieved on 05 December 2020, from https://doi.org/10.1145/2535813.2535818

Elkin-Koren, Niva; Salzberger, Eli (2004), *Law, Economics and Cyberspace: The Effects of Cyberspace on the Economic Analysis of Law*, Edward Elgar Publishing Limited (UK) & Edward Elgar Publishing, Inc (USA)

Fama Eugene (1970), Efficient Capital Markets: A Review of Theory and Empirical Work, *The Journal of Finance,* Vol. 25, No. 2, pp. 383-417

Farwell, James P.; Rohozinski, Rafal (2011): Stuxnet and the Future of Cyber War, *Survival,* Vol. 53, No. 1, pp. 23-40

Faure, Michael (2016), Economic Analysis of Product Liability, in Machnikowski, Piotr (ed.), *European Product Liability. An Analysis of the State of the Art in the Era of New Technologies*, Antwerp, Intersentia, pp. 619-665

Faure, Michael; Visscher, Louis; Weber, Franziska (2016), Liability for Unknown Risks - A Law and Economics Perspective, *Journal of European Tort Law*, Vol. 7, No. 2, pp. 198-228

Fidler, Mailyn (2015): Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis, *I/S: A Journal of Law and Policy for the Information Society,* Vol. 11.2, 406-483

Fischerkeller, Michael; Harknett, Richard (2018), Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace, *Lawfare blog,* 9 November 2018, Retrieved on 05 December 2020, from https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace

Frei, Stefan (2013), *The known unknowns: empirical analysis of publicly unknown*

security vulnerabilities, NSS Labs, Austin

Friedman, Allan; Moore, Tyler; Procaccia, Ariel (2010), Cyber-Sword v. Cyber-Shield: The Dynamics of US Cybersecurity Policy Priorities, *Center for Research on Computation & Society,* Harvard University, Retrieved on 05 December 2020, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.455.4819&rep=rep1&type=pdf

Ganim, Narmeen Al (2020), *Is software a product? A comparative study of EU and US law*, Master Thesis, Tilburg University, Retrieved on 05 December 2020, from http://arno.uvt.nl/show.cgi?fid=149658

Goertzel, Karen (2016), Legal liability for bad software, *CrossTalk,* Sep./Oct. 2016, Vol. 29, No. 5, pp. 23-28, Retrieved on 05 December 2020, from https://www.researchgate.net/publication/310674753

Goodin , Dan (2017), NSA-leaking Shadow Brokers just dumped its most damaging release yet, *Arstechnica*, Retrieved on 01 December 2020, from https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

Goodin, Dan (2019), Zero-day exploit prices are higher than ever, especially for iOS and messaging apps, *Ars Technica,* Jan. 7, 2019, Retrieved on 05 December 2020, from https://arstechnica.com/information-technology/2019/01/zeroday-exploit-prices-continue-to-soar-especially-for-ios-and-messaging-apps/

Gossart, Cédric (2014), Can Digital Technologies Threaten Democracy by Creating Information Cocoons?, In book: *Transforming Politics and Policy in the Digital Age* (Chapter 10, pp.145-154), Center for Research into Online Communities and E-Learning Systems, Belgium,

Grimes, Roger A. (2017), *Hacking the Hacker: Learn from the Experts Who Take down Hackers,* Wiley & Sons

Gross, Michael Joseph (2011), A Declaration of Cyber-War, *VANITY FAIR,* 02 March 2011, Retrieved on 05 December 2020, from https://www.vanityfair.com/news/2011/03/stuxnet-201104

Hannigan Robert (2017), How Britain's GCHQ Decides Which Secrets to Share with You, *The Cipher Brief,* Nov. 19, 2017, Retrieved on 05 December 2020, from https://www.thecipherbrief.com/column/strategic-view/britains-gchq-decides-

secrets-share

Healey, Jason (2020), Vulnerabilities, the Search for Buried Treasure, and the US Government, *OODA Network,* Retrieved on 05 December 2020, from https://www.oodaloop.com/ooda-original/2020/01/14/vulnerabilities-the-search-for-buried-treasure-and-the-us-government/

Herr, Trey (2017), Countering the Proliferation of Malware: Targeting the Vulnerability Lifecycle, *Belfer Center for Science and International Affairs (Harvard Kennedy School),* Retrieved on 05 December 2020, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3005616

Herr, Trey; Schneier, Bruce; Morris, Christopher (2017), Taking Stock: Estimating Vulnerability Rediscovery, *Belfer Center for Science and International Affairs (Harvard Kennedy School),* Retrieved on 05 December 2020, from https://www.belfercenter.org/publication/taking-stock-estimating-vulnerability-rediscovery

Herzog, Michel; Schmid, Jonas (2016): Who pays for zero-days? Balancing long-term stability in cyber space against short-term national security benefits, In book: Karsten, Friis; Ringsmose, Jens (2016): *Conflict in cyber space: theoretical, strategic and legal perspectives,* Routledge, pp.95-116

Hoffman Alex (2019), Moral Hazards in Cyber Vulnerability Markets, *The IEEE Computer Society*, Dec. 2019, Retrieved on 05 December 2020, from https://ieeexplore.ieee.org/document/8909925

Householder, Allen D.; Wassermann, Garret; Manion, Art; King, Chris (2017), The CERT Guide to Coordinated Vulnerability Disclosure, *Software Engineering Institute, Carnegie Mellon University,* Retrieved on 20 November 2020, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330

Howells, Geraint; Twigg-Flesner, Christian; Willett, Chris (2017), Product liability and digital products. In: Synodinou, T. E. and Jougleux, P. and Markou, C. and Prastitou, T. (eds.): *EU Internet Law*, Springer, Cham, pp. 183-195

Huang, Keman; Siegel, Michael; Stuart, Madnick (2018), Systematically Understanding the Cyber Attack Business: A Survey*, Working Paper CISL# 2018-08, July 2018,* Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan School of Management, Massachusetts Institute of Technology Cambridge

Hurley, John; Chen, Jim (2018), *ICCWS 2018 13th International Conference on Cyber*

Warfare and Security, Academic Conferences and Publishing International Limited, Mar 2018, UK

Jonathan Klick (2008): Agency Costs, Charitable Trusts, and Corporate Control: Evidence from Hershey's Kiss-off*, Columbia Law Review*, Vol. 108, No.4

Jougleux, Philippe; Synodinou, Tatiana-Eleni; Markou, Christiana; Prastitou, Thalia (Eds.) (2017), *EU Internet Law - Regulation and Enforcement*, Springer International Publishing AG

Kaplow, Louis (1992), Rules Versus Standards: An Economic Analysis, *Duke Law Journal*, Vol. 42, pp. 557-629, Retrieved on 05 December 2020, from https://scholarship.law.duke.edu/dlj/vol42/iss3/2

Kennan George (1948), *The Inauguration of Organized Political Warfare*, Redacted Version, Wilson Center Digital Archive, Retrieved on 05 December 2020, from https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=941dc9ee5c6e51333ea9ebbbc9104e8c

Knapp, Eric D.; Langill, Joel Thomas (2015), Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems (2nd Edition), *Syngress Publishing,* Elsevier, Waltham

Kobayashi, Bruce (2005), Private versus social incentives in cybersecurity: Law and economics, *The Law and Economics of Cybersecurity*, Cambridge University Press 2006, pp. 13-28

Kumar, Mohit (2018), TSMC Chip Maker Blames WannaCry Malware for Production Halt, *The Hacker News*, Retrieved on 01 December 2020, from https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html

Kshetri, Nir (2017), Should spies use secret software vulnerabilities?, *The Conversation*, Retrieved on 01 December 2020, from https://theconversation.com/should-spies-use-secret-software-vulnerabilities-77770

Landes, William M.; Posner, Richard A. (1987), *The Economic Structure of Tort Law*, Cambridge, MA: Harvard University Press.

Lawson, Ewan (2019), *Conference Report: Roundtable Discussion on Disinformation in Ukraine,* Royal United Services Institute for Defence and Security Studies, UK

Lemley, Mark; McGowan, David (1998), Legal Implications of Network Economic Effects, *California Law Review,* No. 86, pp. 479 ff.

Libicki, Martin; Ablon, Lillian; Webb, Tim (2015), *The Defender's Dilemma: Charting a Course Toward Cybersecurity*, RAND Corporation, Santa Monica

Lichtman, Doug; Posner, Eric (2006), Holding Internet Service Providers Accountable, *Supreme Court Economic Review,* Vol. 14, pp. 221-259

Lindsay, Jon R. (2013), Stuxnet and the Limits of Cyber Warfare, *Security Studies*, Vol. 22, No. 3, pp. 365-404

Maurushat, Alana (2013), *Disclosure of Security Vulnerabilities: Legal and Ethical Issues,* London Heidelberg New York Dordrecht: Springer

Mayer, Jonathan (2018), Government Hacking, *The Yale Law Journal,* Vol. 127, No. 3, pp. 490-787

McConnell, Steve (2004), *Code Complete: A practical handbook of software construction*, Microsoft Press, Redmond, Washington

Nader, Ralph (1965), *Unsafe at Any Speed: The Designed-In Dangers of The American Automobile*, Grossman Publishers, New York

Nakashima, Ellen; Warrick, Joby (2012), Stuxnet Was Work of U.S. and Israeli Experts, Officials Say. *Washington Post*, Retrieved on 05 December 2020, from https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Perlroth, Nicole; Sanger, David (2017), Hacks raise fear over N.S.A.'s hold on cyber-weapons, *NY Times*, 28 June 2017, Retrieved on 05 December 2020, from https://www.nytimes.com/2017/06/28/technology/ransomware-nsa-hacking-tools.html

Philp, Catherine (2020), State-sponsored hackers 'trying to steal coronavirus vaccine secrets', *The Times,* 05 May 2020, Retrieved on 05 December 2020, from https://www.thetimes.co.uk/article/state-sponsored-hackers-trying-to-steal-coronavirus-vaccine-secrets-mrmrlzcst

Picker, Randal (2004), Cyber Security: Of Heterogeneity and Autarky, In Book: Grady, Mark F.; Parisi, Francesco (2004): *The Law and Economics of Cybersecurity,* Cambridge University Press, pp. 115-140

Pindyck, Robert; Rubinfeld, Daniel (2001), *Microeconomics (5th edition),* Prentice Hall International Inc.

Polinsky, A. Mitchell (1980), Strict liability vs. negligence in a market setting, American Economic Review, Vol. 70, pp. 363-370

Polinsky, A. Mitchell; Che, Yoen-Koo (1991), Decoupling liability: optimal incentives for care and litigation, *RAND Journal of Economics*, Vol. 22, pp. 562-570

President's Review Group (2013), *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, Retrieved on 05 December 2020, from https://obamawhitehouse.archives.gov/blog/2013/12/18/liberty-and-security-changing-world

Pupillo Lorenzo (2017), *Software Vulnerabilities Disclosure: The European Landscape*, CEPS, 31 July 2017, Brussel, Retrieved on 05 December 2020, from https://www.ceps.eu/ceps-publications/software-vulnerabilities-disclosure-european-landscape/

Radianti, Jaziar; Rich, Eliot; Gonzalez, Jose J. (2009): *Vulnerability Black Markets: Empirical Evidence and Scenario Simulation*, 42nd Hawaii International Conference on System Sciences, IEEE, Retrieved on 05 December 2020, from https://ieeexplore.ieee.org/document/4755606

Rosenzweig, Paul (2013), *Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare*, The Great Courses, Chantilly

Sanger, David (2014), Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say, *New York Times,* 12 April 2014, Retrieved on 05 December 2020, from https://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html

Schaefer, Hans-Bernd; Mueller-Langer, Frank (2008), *Strict liability versus negligence*, MPRA Paper No. 40195, Retrieved on 05 December 2020, from https://mpra.ub.uni-muenchen.de/40195/1/MPRA_paper_40195.pdf

Schneier, Bruce (2017), Who are the shadow brokers?, *The Atlantic*, May 23, 2017, Retrieved on 20 April 2020, from https://www.theatlantic.com/technology/archive/2017/ 05/shadow-brokers/527778/

Schwartz, Ari; Knake, Rob (2016), *Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Retrieved on 05 December 2020, from https://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf

Shavell, Steven (1980), Strict Liability versus Negligence, *The Journal of Legal Studies*, Vol. 9, No. 1, pp. 1-25

Shavell, Steven (1984), Liability for Harm versus Regulation of Safety, *The Journal of Legal Studies*, Vol. 13, No. 2, pp. 357-374

Shavell, Steven (2005), *Liability for Accidents,* Discussion Paper No. 530, Harvard Law School, Cambridge, Retrieved on 05 December 2020, from http://www.law.harvard.edu/programs/olin_center/papers/pdf/Shavell_530.pdf

Shavell, Steven (2013), A Fundamental Enforcement Cost Advantage of the Negligence Rule over Regulation, *The Journal of Legal Studies*, Vol. 42, No. 2

Shleifer, Andrei (2000), *Inefficient Markets: An introduction to behavioral finance*, Oxford University Press; 1 edition (April 20, 2000)

Shy, Oz (2008), *How to Price*, Cambridge University Press, Cambridge

Shy, Oz (2001), *The Economics of Network Industries,* Cambridge University Press, Cambridge

Shy, Oz (1995), *Industrial Organization: Theory and Applications*, The MIT Press

Skybox (2020), *2020 Vulnerability and Threats Trends*, Skybox Security Research Report, Retrieved on 05 December 2020, from https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/2020-VT-Trends_Executive-Summary.pdf

Swire, Peter (2004), A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?, *Journal on Telecommunications and High Technology Law*, Vol. 3, pp. 163-208

The Economist (2013): The digital arms trade, *The Economist*, Mar 30th, 2013, Retrieved on 05 December 2020, from https://www.economist.com/business/2013/03/30/the-digital-arms-trade

The Economist (2017a): Cyber-crime: Electronic bandits, *The Economist*, May 20th, 2017, pp. 67-68

The Economist (2017b): The exploits of bug hunters, *The Economist*, May 20th, 2017, Retrieved on 05 December 2020, from https://www.economist.com/science-and-technology/2017/05/18/the-exploits-of-bug-hunters

The Economist (2017c): The worm that turned, *The Economist*, May 20th, *2017,* Retrieved on 05 December 2020, from https://www.economist.com/leaders/2017/05/20/the-wannacry-attack-reveals-

the-risks-of-a-computerised-world

The Economist (2017d): Why everything is hackable?*, The Economist*, April 8th, 2017, Retrieved on 05 December 2020, from https://www.economist.com/science-and-technology/2017/04/08/computer-security-is-broken-from-top-to-bottom

The Economist (2017e): Electronic bandits, *The Economist*, May 20th-26th 2017

Trautman, Lawrence J.; Ormerod, Peter C. (2018), Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things, *University of Miami Law Review,* Vol. 72, pp. 761-826

Triaille, Jean-Paul (1990), The EEC directive of july 25, 1985 on product liability and its application to databases and information, *International Computer Law Adviser*, Vol. 5, No. 2, pp. 7-20

Varadi, Sz.; Gultekin Varkonyi, G.; Kertesz, A. (2019), Legal Issues of Social IoT Services: The Effects of Using Clouds, Fogs and AI, in Hassanien, Aboul Ella; Bhatnagar, Roheet; Khalifa, Nour Eldeen M.; Taha, Mohamed Hamed N. (2019): *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*, Springer, pp. 123-138

van Erp, Judith; Faure, Michael; Nollkaemper, André; Philipsen, Niels (2019), *Smart Mixes for Transboundary Environmental Harm*, Cambridge University Press

Volz, Dustin (2020), Microsoft Releases Patch to Severe Windows Flaw Detected by NSA, *The Wall Street Journal,* Jan. 14, 2020, Retrieved on 05 December 2020, from https://www.wsj.com/articles/microsoft-releases-patch-to-severe-windows-flaw-detected-by-nsa-11579030780

Zetter, Kim (2011), How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History, *WIRED*, July 11, 2011, Retrieved on 05 December 2020, from https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/