Entity Relationship Diagram Approach to Defining Cyber-attacks

Mehdi Kadivar

A thesis submitted to the Faculty of Graduate Studies and

Research in partial fulfillment of the requirements for the degree of

Master of Applied Science

in

Technology Innovation Management

Faculty of Engineering and Design

Carleton University

ABSTRACT

Cyber-attack studies are at the core of cybersecurity studies. Cyber-attacks threaten our ability to use the Internet safely, productively, and creatively worldwide and are the source of many security concerns. However, the "cyber-attack" concept is underdeveloped in the academic literature and what is meant by cyber-attack is not clear.

To advance theory, design and operate databases to support scholarly research, perform empirical observations, and compare different types of cyber-attacks, it is necessary to first clarify the "concept of cyber-attack". In this thesis, the following research question is addressed: How to represent a cyber-attack? Entity Relationship Diagrams are used to examine definitions of cyber-attacks available in the literature and information on ten successful high-profile attacks that is available on the Internet.

This exploratory research contributes a representation and a definition of the concept of cyber-attack. The representation organizes data on cyber-attacks that is publicly available on the Internet into nine data entities, identifies the attributes of each entity, and the relationships between entities. In this representation, Adversary 1 (i.e., attacker) acts to: i) undermine Adversary 2's networks, systems, software or information or ii) damage the physical assets they control. Both adversaries share cyberspace and are affected by factors extrinsic to their organizations. Adversary 2 is comprised of two parts; one includes the organizations that operate the network and the other that is extrinsic to the

organizations that operate the network.

Although this research will be of interest to a broad community, it will be of particular interest to senior executives, government contractors, and researchers interested in contributing to the development of an interdisciplinary and global theory of cybersecurity.

Acknowledgements

I don't have the words to express my full gratitude but I would like to express my deepest appreciation and thanks to my advisor Professor Dr. Tony Bailetti, who has been a tremendous mentor for me. You have done beyond a supervisor's responsibility. It has been such a great honour to be your student. I can write a dissertation on how a wonderful human being you are. This thesis would not have been possible without the guidance and the help of Professor Bailetti. Thank you for being best possible role model I could have hoped for. Working with you has been a most rewarding moment of my life. For your patience, kindness, advice and devotion, thank you.

I would like to express my sincere appreciation to Dan Craigen for his generous sharing of his unique knowledge. I will be forever grateful to him for the many ways he contributed to this thesis.

A special thank to my family, which this journey would not have been possible without the support of them. Words cannot express how grateful I am to my father, Mohammad Hassan, whom has 2 PhDs, which was the biggest motivation for me to do my master's. I understood the real meaning of love when you said that you were proud of me even when I failed. Thank you for working hard to provide for our family. I owe my deepest gratitude to my mother, Nilofar and all of the sacrifices that she has made on my behalf. Your prayer for me was what sustained me thus far. I would like to thank my sister, Ameneh for being a guiding light as I've experienced the ups and downs of life.

At the end I want to dedicate this thesis to the memory of my godmother, Dokhijoon, whom I attribute my success in life to the moral I received from her.

Table of Contents

List of Tables

List of Figures

List of Appendices

1 INTRODUCTION

1.1 Motivation

The main motivation for this thesis is to develop a representation that unifies the knowledge about cyber-attacks. Much is known about various cyber-attacks; however, our understanding of the cyber-attack concept is low (Hathaway et al., 2012, Roscini, 2014). The lack of a coherent unity for cyber-attacks is a barrier to increasing our understanding of the concept. With no coherency in the whole, there will be no coherency in the parts.

Senior corporate executives, government officials, and academics have become aware that there are: i) serious financial and regulatory costs arising from cyber-attacks (Pearson, 2014; Sugarman, 2014; US Securities and Exchange Commission, 2014); ii) vulnerabilities in high-value assets such as supervisory-control and data-acquisition systems (Ashford, 2013; Crawford, 2014; Kovacs, 2014; Nicholson et al., 2012; Weiss, 2014); iii) concerns about the upcoming deployment of the “Internet of Things” (IoT) (NSTAC, 2014); and iv) few constraining mechanisms to inhibit malicious behaviours of threat actors (Castel, 2012; Jowitt, 2014, Scully, 2013; Sugarman, 2014; Weiss, 2014).

This research on cyber-attacks uses the inductive reasoning approach and uses publicly available information on cyber-attacks from sources considered to be reliable. The approach used in this research to clarify what is meant by cyber-attack is similar to the approach researchers followed to clarify what was meant by "security" in the late 1990s (e.g., Baldwin, 1997; Buzan, 1998; Huysmans, 1998). Security researchers

identified essential attributes to make explicit what was meant by security. They eliminated ambiguities and inconsistencies in the different uses of the security concept. Their objective was not to produce another one-sentence definition of security; they set out to identify the essential attributes of security.

A dominant theoretical perspective on cyber-attacks does not exist. Therefore, this research is exploratory.

1.2 Goal, Research Question and Objectives

The goal of the research of which this thesis is a part is to develop a transdisciplinary theory of cyber-attacks and a database to support the theory building effort. The transdisciplinary theory is conceptualized as a unit of intellectual frameworks beyond the disciplinary perspectives (Max-Neef, 2005; Nicolescu, 2005).

The research question addressed is: How to represent a cyber-attack?

The objective is to represent a cyber-attack. The representation should use publicly available information to:

1. Eliminate ambiguities and inconsistencies in the different uses of the cyber-attack concept
2. Develop a transdisciplinary theory of cyber-attacks that can be applied worldwide
3. Develop a cyber-attack data base to support theory development

1.3 Relevance

This research will be of particular interest to senior executives, government contractors, and researchers interested in contributing to the development of a theory of cyber-attacks.

1.4 Contribution

This research makes at least three contributions. This research contributes a set of entities, attributes and relationships as well as a representation and definition of the cyber-attack concept. It does so by examining various definitions published in the literature and information on ten high-profile cyber-attacks. In the representation of a cyber-attack, two adversaries share cyberspace and are affected by factors extrinsic to their organizations. Adversary 1 acts to: i) undermine Adversary 2's networks, systems, software or information or ii) damage the physical assets they control. Adversary 2 is comprised of two parts; one part includes the organizations that operate the network and are responsible for operating the technical aspects of its security and the other part is extrinsic to the internal organizations that operate the network. The definition offered is: a cyber attack is a cyberspace-enabled action executed by Adversary_1 with the intention to damage or undermine assets operated by Adversary_2. Collateral actions, supported by extrinsic capabilities, by Adversary_2 may degrade the ability of Adversary_1 to continue execution.

Second, the research adds fidelity to the concept of cyber-attack by using information from ten scenarios of high-profile cyber-attacks. The representation of a cyber-attack provides a benchmark of what can be known about cyber-attacks without using proprietary information and/or a dominant theoretical perspective on cyber-attacks. Outcomes being produced by personnel who have access to classified information can be benchmarked against the results provided in this thesis. Similarly, outcomes produced using new theoretical perspectives can also be compared against the representation of the cyber-attack concept provided in this thesis.

Third, the representation suggests theories that could be used to help provide a better understanding of cyber-attacks. For example, the inclusion of business models as an attribute of Adversary 1 and Adversary 2 suggest the application of entrepreneurial theories to explain cyberattacks. The inclusion of the attribute Motivation may open the door to psychological and sociological reasoning. Adversarial dynamics suggest game theory and theory of war tactics.

1.5 Organization

The remainder of this thesis is organized into five chapters. Chapter 2 provides the results of reviewing the literature. Chapter 3 describes the method used to carry out this research. Chapter 4 provides the results of the research and Chapter 5 a discussion of the results. Finally, Chapter 6 provides the conclusions of the research, identifies the limitations, and suggests further research.

2 LITERATURE REVIEW

The purpose of Chapter 2 is to provide a literature review of cyber-attacks. This chapter is organized into four sections. Section 2.1 identifies various definitions of cyber-attacks. Section 2.2 describes legal frameworks pertaining cyber-attacks. Section 2.3 reviews the literature on the reasons, motivations and beliefs underpinning cyber-attacks. Section 2.4 provides a summary of Chapter 2.

2.1 Cyber-attack definitions

Journal articles published in the English language by organizations in North America and Europe were reviewed for the purpose of identifying definitions of "cyber-attack." The review of the literature led to the identification of six definitions of "cyber-attack." Table 1 identifies these definitions and their original sources.

Table 1: Cyber-attack Definitions

	Cyber-attack definition	**Source**
1	Any action taken to undermine the functions of a computer network for a political or national security purpose	Hathaway et al., 2012: p. 821
2	Use of deliberate actions – perhaps over an extended period of time – to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or	Owens et al., 2009: p. 10

	transiting these systems or networks	
3	Operations, whether in offence or defence, intended to alter, delete, corrupt, or deny access to computer data or software for the purposes of (a) propaganda or deception; and/or (b) partly or totally disrupting the functioning of the targeted computer, computer system or network, and related computer-operated physical infrastructure (if any); and/or (c) producing physical damage extrinsic to the computer, computer system or network	Roscini, 2014: p. 17
4	An exploitation of cyberspace for the purpose of accessing unauthorized or secure information, spying, disabling of networks, and stealing both data and money	Uma & Padmavathi, 2013: p. 390
5	A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions	US Joint Chiefs of Staff, 2010: p.5
6	Efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them	Waxman, 2011: p. 422

Each definition shown above addresses one or more of the following five questions: i) What types of assets do cyber-attacks target?; ii) What effect do cyber-attacks have on

assets targeted?; iii) What motivates cyber-attacks?; iv) Which actors are involved in cyber-attacks?; and v) What are the durations of cyber-attacks?

2.2 Cyber-attack Legal Frameworks

There are several legal frameworks that can be applied to determine whether a cyber-attack constitutes an armed attack. Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue, and Spiegel (2012) explain that applying the laws of warfare to a cyber-attack is challenging. It is worth noting that the laws of warfare have not been revised since the World War II and therefore were not formed with cyber-attacks in mind. Using these laws to determine if a cyber-attack has occurred is ineffective at best and potentially useless. Additionally, the authors say that it is only possible to use these existing laws to validate cyber-attacks if the cyber-attacks involve property destruction. As summarized in Table 1, however, the best term to use is cyber warfare and not cyber-attacks whenever there is destruction of property.

In the United States of America, legislation allows organizations to use the resources of the Comprehensive National Cyber-Security Initiative. This is defined as a twelve-component program that protects computer networks from cyber-attacks. The program assists in the protection of networks by improving IT processes, reducing the connections between the federal agencies' computers and other computers, and detecting intrusion (Owens, Dam & Herbert, 2009). Owens, Dam and Herbert (2009) explain that the United Nations Charter states that a cyber-attack should be judged

purely by the effect it has, rather than its modality. This means that even though legislation should consider weapons that were used to perform an attack, the effects of the cyber-attack are more important.

Gervais (2012) performed a significant analysis of cyber-attacks and the laws of war. For example, he discusses when, according to international law, it is acceptable to resort to force (*jus ad bellum*) and what wartime conducts (*jus in bello*) are permitted. In the end, Gervais admits that there are numerous difficult questions that arise from trying to adapt existing pre-cyber agreements, into the current cyber-age. However, many of the problems are “of degree” and not “of kind,” thereby implying there is the opportunity to apply current international humanitarian law to cyber-attacks. Consequently, Gervais concludes “States may continue to rely on the existing regime of international law to regulate cyber attacks, while they await the international community’s response to this modern form of waging warfare.”

Alperen (2011) also agrees that the law is insufficient in dealing with cyber-attacks. He explains that domestic laws can be used when the attack is within the country. Conversely, he argues that no laws can be applied when the cyber-attack is launched from one country targeting another. In his view, International laws define crime as “anything that causes physical damage and uses physical weapons.” Contrary to this, cybercrime can cause a lot of physical damage, but does not use physical weapons.

A cyber-attack is a threat source that uses an exploit to take advantage of an existing vulnerability. It causes unintended or unanticipated behaviour to occur in a computer system or network (Rehman, 2014). Cyber-attacks affect the integrity and availability of

systems. The end is beneficial to the threat source and detrimental to other users.

2.3 Reasons, Motivations, and Beliefs Underpinning Cyber-Attacks

Digital infrastructures of governments and institutions are increasingly becoming open for clandestine and malicious activities. Intruders can be organized or act individually when they attack a digital system. Employees and other insiders are also capable of making unauthorized intrusions into their networks (Han & Dongre, 2014).

According to Rehman (2014), the Internet is now a domain for international politics and its structure, spanning beyond country boundaries, makes many national governments feel vulnerable. With the Internet becoming the most common communication tools of the 21st century, it provides a rich source of opportunities for cyber attackers; even though governments are attempting to limit their exposures through both national and international initiatives. The difficulty of attributing actions and the ease by which one can assume an identity on the Internet further enables cyber attackers. Motivations for illicit activities range and include economic espionage, theft of sensitive data, manipulation of systems, and revelation of secret information.

In fact, the exploitability of the Internet is both a blessing and a curse. For example, law enforcement authorities use legalized means to “cyber-attack” and gather evidence about criminal activities.

Cyberspace refers to the Internet and other networks within companies, homes, and institutions. It also relates to electronic devices with computational power linked to any

sort of network. Within cyberspace, there are software and protocols that allow management and transfer of information in connected computers or devices. When talking about cyberspace infrastructure, a person could also be referring to hardware that powers the network, such as telecommunications and operating systems (Han & Dongre, 2014).

The motivations underlying a cyber-attack affect the desired result. For example, an aim to cause economic impact (e.g., theft of intellectual property or denial of service) will have differing reasons for attack than one that is politically inclined (e.g., propaganda or intelligence). Categorizing cyber attackers, as exemplified by Han and Dongre (2014), eases our understanding of common motivations and reinforces the importance of identifying attackers from within and without the organization. Generally, Outsiders are organized attackers, hackers, and amateurs; while Insiders are disgruntled employees, thieves, and unintentional actors (Harris, 2013).

Furthering the discussion on categorization, Han and Dongre (2014) explain that organized attack groups such as terrorists, nation states, and criminal gangs seek to express political statements, gain competitive advantage, steal technical knowhow, or create fear. For hacktivists, the end justifies the means and, as such, a cyber-intrusion would be justified, as long as the target population receives the political message. On the other hand, a predominant outcome for nation state attackers is simply to keep collecting intelligence from other states.

Many attackers are well resourced, especially those that are state-sponsored. Such attackers generally work according to the goals of their sponsors, but may also have additional motivations. Criminals too can have access to significant technologies and complex illicit ecosystems. Despite the potency of state-sponsored and criminal attackers, hackers receive a disproportionate amount of publicity because of their decentralization and motivation to attack the widest variety of computer systems and networks (Han & Dongre, 2014). Cyber-attackers can be explorers, intruders, trespassers, or thieves. Three main categories emerge as motivations for any kind of cyber-attack: political, economic and socio-cultural. The motivations may occur independently or collectively (Han & Dongre, 2014).

Minei and Matusitz (2011) explain that new media enhances the motives of cyber terrorism, which is to frighten and coerce. For such groups, sending the appropriate message could be accomplished by, for example, defacing official law authority websites to show they are capable of doing so and to attract media attention. Such attention advances their cause through fear propagation. In this case, the Internet serves as the main media for propaganda, allowing attackers to gain prominence by vocalizing their activities through Internet-related opportunities for communication. For terrorist propaganda, Minei and Matusitz (2011) explain that the attacks are carefully choreographed. The inspiring factor for such attackers is the need to remain memorable; therefore, all activities revolve around theatrics.

In their research on criminal profiling and insider cybercrime, Nykodym, Taylor and Vilela (2005) show that cybercrime escalated around the world because of existing legislative compatibility gaps. For companies, insiders have been identified as the biggest threat and the best way of dealing with the problem is to have an accurate profile of the insider cybercriminal. By showing how profiling is a critical measure for dealing with cyber criminals, the researchers suggest that the lack of appropriate profiling abilities is a key inspiration for insider cyber-criminal activity (Bayuk, 2012). While profiling is used mainly for solving crimes, it can also be a tool used by criminal gangs to identify potential targets. For criminals, profiling considers the vulnerability of a target, its risk to reward ratio, and the overall cost of conducting an attack.

According to Amoroso (2011), the fundamental institutions of government or commerce are the main targets of cyber attackers. For example, the stock market can be a target because of its potential to make an individual rich. However, other probable reasons for attacking the stock market include destabilization of a country's financial structure. In such an attack, criminals face a number of challenges, which could also explain why elaborate attacks have not (apparently) yet taken place in global stock markets. Criminals have to engineer the needed effect, evade prosecution, and have the confidence to execute their plan. These are not easy to achieve even when the criminals are a group of terrorists or political extremists whose actions are justified by their desire to see changes. Economic rivals, at the nation level, can have the necessary defense against retaliations by the victim nation and use that as a motivation

for cyber war that centers on the crippling of financial institutions. Moreover, military campaigns can motivate such an attack (Amoroso, 2011).

There is a growing underground market for data that is fuelling increased attacks on networks. Criminals are attacking just for the sake of gaining information that they believe may have financial worth. Therefore, networks with highly valuable data for criminals become highly targeted (“US warns of increased cyber-attacks by Iran”, 2013).

Yunos and Suid (2010) explained that cyber attackers could be differentiated by their actions and motivations. The authors narrow down the motivations of cyber attackers to the availability of technical competency by the attacker, which puts them in an advantaged position of taking on emerging vulnerabilities arising from an ever-changing cyber environment. The tardy response by law enforcement and defense authorities, as well as company security departments, also yield additional reasons for attackers to pounce. Another motivation is the conventional nature of legislation that is inadequate in addressing Internet issues and international cyber-attacks. Moreover, while there are international laws that can cater for criminal activities happening beyond borders, the laws still depend on physical definitions of boundaries (“Alleged MPAA DDoS attacks spark retaliatory cyber attacks”, 2010).

The victims of attacks can also help to explain motivations. As earlier alluded, an attack to a stock exchange market can be fuelled by a need to make a political statement, cause fear and, to a lesser extent, acquire illegal wealth. The last option is unlikely because it is easier for attackers to go directly to a company, rather than attack an entire market for such gains. Thus, for example, if there were a breach in a defense contractor, then the most likely perpetrator of the cyber-attack would be another nation. Even when attackers are individual or organized groups, their motivations and supporters would likely be nations keen on gaining intelligence about defense activities and technologies.

Retail companies can be targets for organized criminals looking for valuable customer information for subsequent trading in the underground market. Attacks can be highly targeted at a specific institution or they can be widespread to a particular industry (Rehman, 2014).

2.4 Summary

Six definitions of the term cyber-attack were identified from the literature. The legal frameworks (both domestically and internationally) are weak both with regards to defining cyber attacks and the enforcement of laws causing retribution. While there are analogs between actions in cyber space and international jurisprudence regarding traditional war-related actions, the International community is in need of updating such jurisprudence to clarify the rules of engagement within cyber space and its impact on the real world.

3 RESEARCH METHOD

This chapter describes the research method used to carry out the research. Chapter 3 is organized into three sections. Section 3.1 describes the motivation for the research; the objective of the research; and the approach used. Section 3.2 describes the research method. Section 3.3 provides a summary of the chapter.

3.1 Motivation, Objectives, and Approach

3.1.1 Motivation

The main motivation of this research is to enable the building of a transdisciplinary theory of cyber-attacks and the development of a database to support this theory building effort.

3.1.2 Research Question and Objective

The research question is: How to represent a cyber-attack? The objective is provide a representation that makes explicit what is meant by the cyber-attack concept. The cyber-attack representation should be able to be characterized using publicly available information. The representation should be used to:

1. Eliminate ambiguities and inconsistencies in the different uses of the cyber-attack concept
2. Develop a transdisciplinary theory of cyber-attacks that can be applied worldwide
3. Develop a cyber-attack data base to support theory development

3.1.3 Approach

This research on cyber-attacks uses the inductive reasoning approach because the study of cyber-attacks is at an early stage and a dominant theoretical perspective does not exist. Therefore, this research is exploratory and open ended.

The research uses definitions of cyber-attacks published in the literature and publicly available information on high-profile cyberattacks to provide examples of entities, attributes and relationships that are relevant to the cyber-attack concept. The intent is to provide strong evidence for the elements included in the representation, not to prove them.

Entity Relationship Diagrams (ERDs) were used to organize data collected into entities and to define the relationship between entities. An ERD is major data modelling tool frequently used by analysts who need to produce a good database structure. An ERD incorporates important semantic information about the real world. Introduced by Chen (1976,2002), the ERD is a data modeling technique and is widely used to produce data designs (Bagui and Earp, 2011; Kendall and Kendall, 2013).

There are three main elements in an ER Diagram: entity, attribute, and relationship.

Entity

An entity is anything real or abstract about which we want to store data. An entity can be a person, place, event, or object that is relevant to a given system and fall into five classes: roles, events, locations, tangible things or concepts.

Attribute

An attribute is a characteristic common to all or most instances of a particular entity. An attribute is a property, trait, or characteristic of an entity, relationship, or another attribute.

Relationship

A relationship describes how entities interact and is a natural association that exists between one or more entities.

3.2 Research method

Table 2 describes the steps carried out to complete this research.

Table 2: Steps Used to Carry Out the Research

Step	Activity	Output
1	Select a sample comprised of 10 high-profile cyberattacks	List of 10 cyber-attacks
2	Collect information on the Internet for each of the	For each cyber attack, a list

	cyber-attacks	of links to news, reports, and articles with information deemed relevant
3	Produce narratives of the cyber-attack scenarios	10 narratives, one for each cyber-attack
4	Identify definitions of cyberattacks and produce an Entity Relationship Diagram (ERD) for these definitions	ERD for cyber-attack definitions
5	Develop ERDs for cyber-attack scenarios	10 ERDs, one for each scenario
6	Produce a spreadsheet with the information required to identify attributes and entities for the 10 scenarios	1 spreadsheet that identifies entities and attributes for all 10 ERDs
7	Develop a rough ERD of the cyber-attack concept	1 rough ERD of the cyber-attack concept
8	Adjust the ERD developed in the previous step to eliminate ambiguities and inconsistencies and identify the fields which are essential to a representation of a cyber-attack	1 final ERD of the cyber-attack concept
9	Provide examples of the fields of the attributes using information from the cyber-attack scenarios	For each entity in the final ERD, a description and examples of the fields of the

		attributes from the cyber-attacks

3.2.1 List of 10 cyber-attack scenarios

At the request of the supervisor of this thesis, a security expert provided the list of the 10 cyber-attacks that were examined in this research. The security expert has 25 years of experience, most of which was spent protecting the critical infrastructure of the Federal Government of Canada.

The supervisor requested that the security expert provide a sample that met the following criteria:

A. Information about the cyber-attacks was published on the internet by media and security firms deemed to be reliable from January 1st, 2006 to December 31, 2013
B. The target of the cyber-attack was deemed to be a high profile organization and/or the attack was deemed to be a high-profile attack
C. Organizations that were attacked operated in different product/markets

The following sources of information were deemed to provide information that was reliable:

1. Articles, books or research papers examined and reviewed by academics
2. Well respected news organizations such as CNN, BBC, Reuters, New York Times, Washington post, Bloomberg, which are well reputable news media

3. Security reports published from well-established security companies such as Symantec Kaspersky and ESET
4. Government documents such as those published by Office of the Privacy Commissioner of Canada
5. Well-established magazine outlets such as Times, Forbes, Foreign Policy is considered to be reliable.

3.2.2 List of links to news, reports, and articles with information deemed relevant to each of the 10 cyber-attacks

For each cyber-attack, the author of this research used the Google search utility to find information prublished bu sources considered to be reliable. A timeline of key events was produced and the information identified was organized using the events in the timeline.

3.2.3 Ten narratives, one for each cyber-attack scenario

A narrative that described each cyber-attack was produced. Each narrative was not to exceed 500 words.

3.2.4 ERD for cyber-attack definitions

An ERD was produced to organize the information in the definitions found in the literature review. Table 3 identifies the steps followed to produce the ERD for the cyber-attack definitions:

Table 3: Steps Used to Produce the Entity Relationship Diagram for the Cyber-attack Definitions

	Step	Description of step
1	Identify cyber-attack definitions	Identify the definitions of the cyber-attack concept found in the literature review
2	Identify entities	Identify the roles, events, locations, tangible things or concepts about which data should be stored
3	Find relationships	Identify the natural associations between pairs of entities
4	Draw a rough ERD	Place entities in rectangles and relationships on line segments connecting the entities
5	Identify attributes	Identify the information details included in the definitions deemed to be essential to the cyber-attack concept
6	Identify cardinality	Determine the number of occurrences of one entity for a single occurrence of the related entity
7	Link ERD to definitions	Produce a table that links each definition to the entities and relationships in the ERD

3.2.5 ERDs for 10 scenarios

For each cyber-attack, an ERD was produced using the steps identified in Table 4.

Table 4: Steps Used to Produce the Entity Relationship Diagram for a Cyber-attack

	Step	Description of step
1	Identify entities	Examine the narrative of a cyber-attack and identify the roles, events, locations, tangible things or concepts about which data should be stored
2	Find relationships	Identify the natural associations between pairs of entities
3	Draw a rough ERD	Place entities in rectangles and relationships on line segments connecting the entities
4	Identify attributes	Identify the information details included in the narrative deemed to be essential to the cyber-attack concept
5	Identify cardinality	Determine the number of occurrences of one entity for a single occurrence of the related entity

3.2.6 Spreadsheet that identifies entities and attributes for ERDs

The author captured the names of the entities and attributes across all ten ERDs. The names of the relationships were kept fixed across the ERDs.

3.2.7 Rough ERD of the cyber-attack concept

Using the ERDs for the ten cyber-attacks a rough ERD for the cyber-attack concept was prepared by the author. The supervisor checked that the rough ERD represented each cyber-attack.

3.2.8 Final ERD of the cyber-attack concept

The security expert who provided the list of high-profiles to examine, the author of this research, and the supervisor validated that the final ERD represented the 10 cyber-attacks.

3.2.9 Definitions and examples of attributes from the cyber-attacks

Definitions and examples of the attributes identified in the 10 cyber-attacks were identified.

3.3 Summary

Chapter 3 provides the research method. The main motivation of this research is to enable the building of a transdisciplinary theory of cyber-attacks and the development of a database to support this theory building effort.

The objective is how to represent a cyber-attack. The representation is to make explicit what is meant by the cyber-attack concept.

The research uses definitions of cyber-attacks published in the literature and publicly available information on high-profile cyber-attacks to provide examples of entities, attributes and relationships that are relevant to the cyber-attack concept.

4 RESULTS

The purpose of Chapter 4 is to provide the results. The chapter is organized into six sections. Section 4.1 identifies the sample and the study period. Section 4.2 provides the narratives, identifies the sources of information for the narratives, and provides the entity relationship diagrams for the 10 cyber-attacks. Section 4.3 provides the entity relationship diagram developed using the definitions of the cyber-attack concept found in the literature. Section 4.4 provides a representation of the cyber-attack concept developed from examining the 10 cyber-attacks. Section 4.5 provides examples derived from the examination of the cyber-attacks. Section 4.6 provides a summary of chapter 4

4.1 Sample and Study Period

Table 5 identifies the alleged attacker and known target for each of the ten scenarios in the sample and provides the rationale for inclusion.

Table 5: Scenarios in the Sample and Rationale for Inclusion

	Scenario		
	Alleged Attacker	Known Target	**Rationale for inclusion in sample**
1	Elderwood Gang	Google	First large attack to gain access to and potentially modify source code that support the supply chain management function of a large number of technology, security and defense companies such as Google, Yahoo, Juniper Networks, Adobe

			Systems and RackSpace.
2	Israel, USA	Natanz Fuel Enrichment Plant	First attack that used malaware to destroy a nation state's physical assets; the incident could have caused a war and elicited retaliation from the nation state that was attacked
3	China military	New York Times	Largest espionage attack on one media company
4	Covert Grove	Chemical company	Largest espionage on chemical and defense firms
5	CyberBunker	Spamhaus Project	Largest distributed denial of service attack to a not-for-profit organization located in Europe
6	Criminal	Target	Second-largest credit card data breach in US history
7	A. Gonzalez	TJX Companies	First largest data heist
8	Aleksandr Andreevich Panin	User with bank accounts	Used a highly innovative Trojan to steal users' credentials and then withdraw money from their bank accounts
9	Evgeniy Bogachev	User of PC with vulnerabilities	Very innovative approach to raise money; attack first encrypts a user's data or system and then demands that the user pay to decrypt
10	Winniti	Gaming company	Uses stolen certificates for a wide variety of purposes

The study period is from May 2006 to December 2013. Three of the 10 cyber-attacks were in progress as of December 2013. These scenarios were: 8 (Aleksandr Andreevich Panin; User with bank accounts), 9 (Evgeniy Bogachev; User of PC with vulnerabilities), and 10 Winniti;Gaming company)

4.2 Narratives, Sources of Information, and Entity Relationship Diagrams for Cyber-attacks

For each cyber-attack, Appendix A provides a narrative that describes the cyber-attack, the references to the information on the Internet that was used to produce the narrative, and the ERD produced for the cyber-attack.

4.3 Entity Relationship Diagram Developed from Definitions

For each of the six definitions identified in the literature review, Table 6 provides the entities, attributes and relationships that were identified to produce the ERD for Definitions shown as Figure 1.

Table 6: Entities, Attributes and Relationships Identified from the Definitions of Cyber-Attacks found in the Literature Review

	Cyber-attack definition	Entities	Attributes	Relationships
1	Any action taken to undermine the functions of a computer network for a political or national security purpose (Hathaway et al., 2012: p. 821)	Action Adversary 1 Net or system	Motivation	Adversary 1 _Executes_Action Action_Undermines_Net or system
2	Use of deliberate actions – perhaps over an extended period of time – to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems	Action Adversary 1 Adversary 2 Net or system Info and SW	Duration	Adversary 1 _Executes_Action Action_Undermines_Net or system Action_Undermines_Info and SW Net or system_Runs_ transits_Info and SW

	or networks (Owens et al., 2009: p. 10)			
3	Operations, whether in offence or defence, intended to alter, delete, corrupt, or deny access to computer data or software for the purposes of (a) propaganda or deception; and/or (b) partly or totally disrupting the functioning of the targeted computer, computer system or network, and related computer-operated physical infrastructure (if any); and/or (c) producing physical damage extrinsic to the computer, computer	Action Adversary 1 Adversary 2 Extrinsic INT Physical Net or system Info and SW	Motivation Objective	Adversary 1 _Executes_Action Action_Undermines_Net or system Action_Undermines_Info and SW Action_Damages_Physical Action_Damages_Extrinsic

	system or network (Roscini, 2014: p. 17)			
4	An exploitation of cyberspace for the purpose of accessing unauthorized or secure information, spying, disabling of networks, and stealing both data and money (Uma & Padmavathi, 2013: p. 390)	Cyberspace Net or system Info and SW	Motivation Objective	Adversary 1_Uses_Cyberspace Action_Undermines_Net or system Action_Undermines_Info and SW
5	A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions (US Joint Chiefs of Staff, 2010: p.5)	Action Adversary 1 Adversary 2 Cyberspace	Motivation Objective	Adversary 1 _Executes_Action Adversary 1_Uses_Cyberspace Action_Undermines_Net or system Action_Undermines_Info and SW
6	Efforts to alter, disrupt,	Action		Adversary 1 _Executes_Action

	or destroy computer systems or networks or the information or programs on them (Waxman, 2011: p. 422)	Net or system Info and SW		Action_Undermines_Net or system Action_Undermines_Info and SW

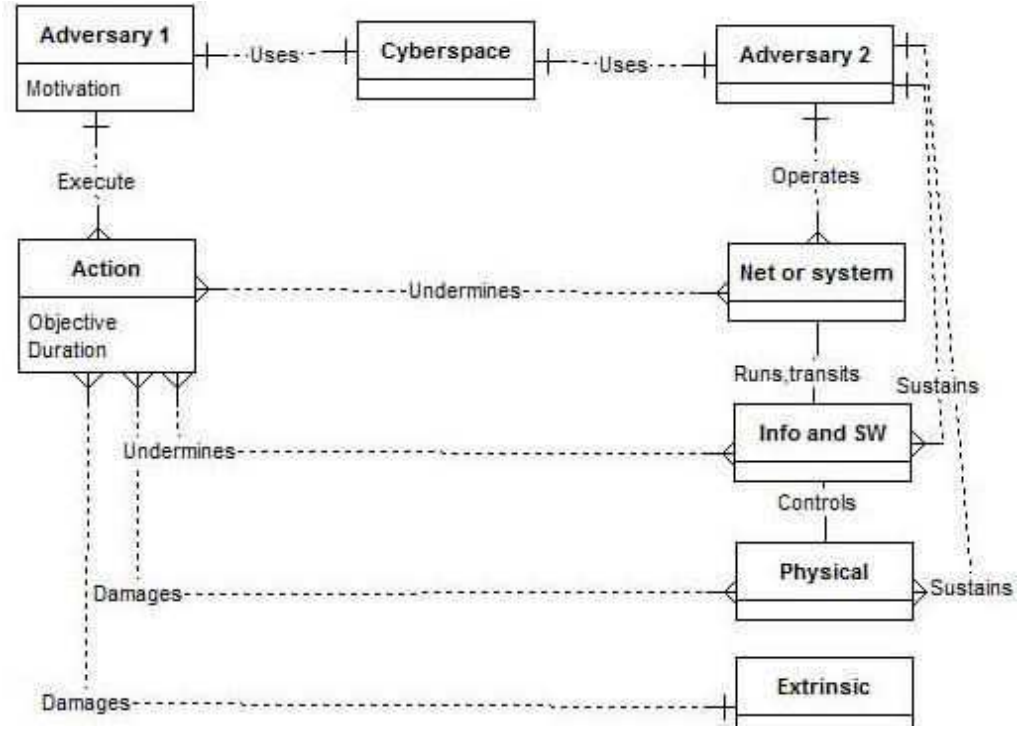
Three relationships were deemed implied by the definitions examined. These are:

- Adversary 2_Uses_Cyberspace
- Adversary 2_Sustains_Info and SW
- Adversary 2_Sustains_Physical

The author implied the cardinality of the relationships.

Figure 1 provides a rough ERD titled “ERD for Cyber-attack Definitions.” This ERD includes eight entities, three attributes, and 12 relationships between entities.

Figure 1: Entity Relationship Diagram for Cyber-attack Definitions



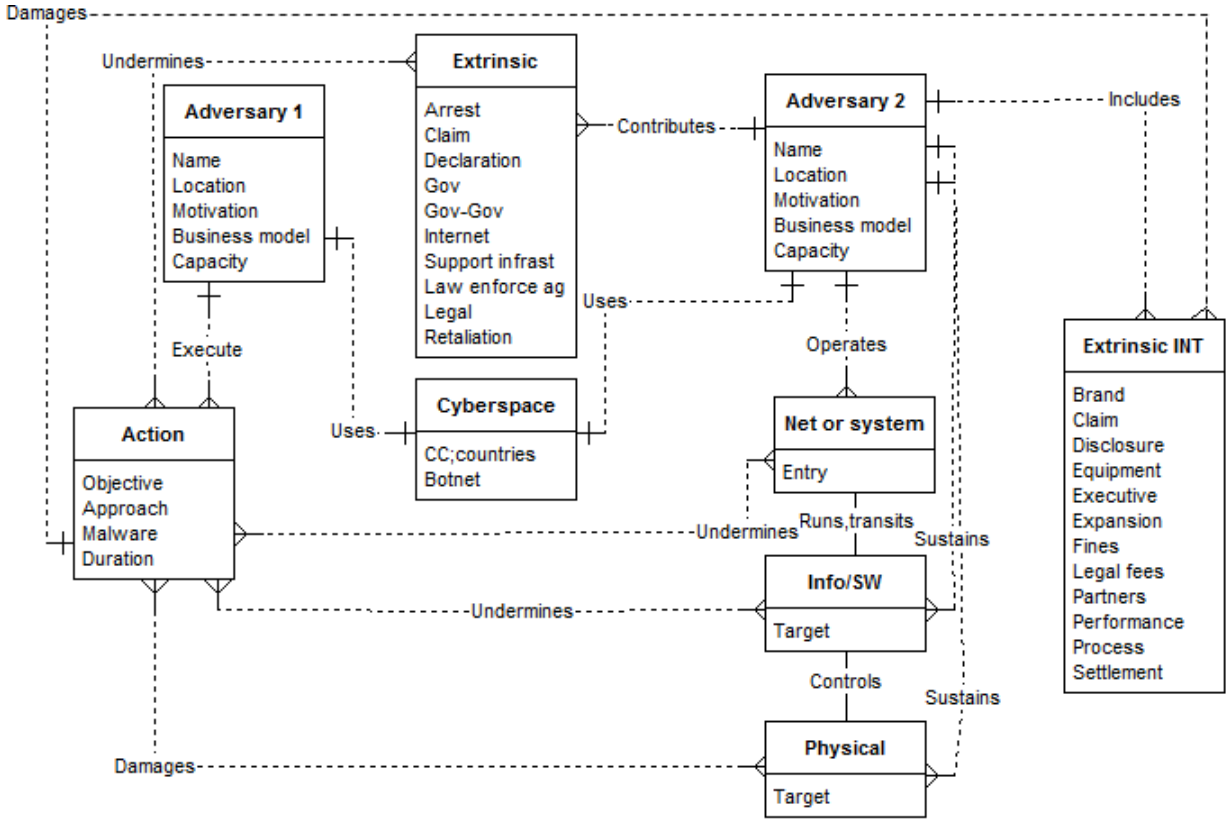
Four of the six definitions included in Table 6, identified motivations for the attack. These motivations are: political or national security purposes (Hathaway et al., 2012: p. 821), propaganda or deception (Roscini, 2014: p. 17), acquiring information and stealing (Uma & Padmavathi, 2013: p. 390), and disrupts or destroy cyber assets (US Joint Chiefs of Staff, 2010: p.5).

4.4 Entity Relationship Diagram Developed from Scenarios

Appendix B provides the spreadsheet that includes the fields for the information collected. Abbreviations were used to name these fields. These abbreviations were used to identify the entities and attributes in the ERD for the Cyber-attack Concept.

Figure 2 provides the ERD developed from scenarios. The intent of Figure 2 is to provide a representation of the cyber-attack concept.

Figure 2: Entity Relationship Diagram for the Cyber-attack Concept



The ERD for the Cyber-attack Concept includes 9 entities, 41 attributes, and 15 relationships.

4.5 Descriptions of Attributes and Examples

This section provides examples of the fields of the attributes included in the representation of the concept of cyber-attack. These examples are organized by entity included in Figure 2.

4.5.1 Descriptions and Examples of Adversary 1 Attributes

Adversary 1 has five attributes: Name, Location, Motivation, Business model, and Capacity.

Name

The attribute “Name” includes basic data on Adversary 1 that is not expected to change frequently (e.g., such as name, addresses, and phone numbers). The fields of “Name” of the entity Adversary 1 can be organized into three types: i) Gang whose members have not been identified (e.g., Elderwood Gang, Covert Grove, Winniti, Criminal group behind the Target Corporation cyber-attack); ii) Nation state alleged to have enabled a cyber-attack (e.g., China, Israel, USA); and iii) Company or individual that one or more law enforcement agencies alleged to be the source of the cyber-attack (e.g., CyberBunker, A. Gonzalez, A. A. Panin, E. Bogachev).

Location

The attribute “Location” refers to the particular place where Adversary 1 operates. The country or the geographical region where Adversary 1 is located is what was reported on the Internet for all ten scenarios. The field and its frequency count (shown in brackets) are: China (4), Israel (1), Netherlands (1), Spain (1), Eastern Europe (2),

United States (2) and Russia (1). Additional details were available for organizations and individuals that one or more law enforcement agencies alleged to be the source of the cyber-attack.

Motivation

The fields of the attribute "Motivation" were inferred by the researcher from the information published on the Internet. The fields of "Motivation" can be organized into five types: i) Make money selling information credentials that were downloaded without authorization from large corporations and consumers (e.g., Unidentified criminal group responsible for the Target Corporation cyber-attack, A. Gonzalez, A. A. Panin, Winniti); ii) Make money by demanding ransom to restore access to files and systems encrypted without authorization (e.g., E. Bogachev); iii) Collect secret information undetected (e.g., Elderwood Gang, Chinese military, Covert Grove); iv) Retaliate (e.g., CyberBunker); and v) Destroy physical assets (e.g., Israel and USA).

Business Model

The attribute "Business model" describes the rationale of how Adversary 1 creates, delivers, and captures value. This definition is consistent with work of business researchers (Chesbrough et al., 2006; Muegge, 2012). Very little is known about the business models used by individuals or organizations that carry out cyber-attacks. The researcher inferred the fields of the Business model attribute. The information available suggests that there are at least six types of business models based on who pays for the cyber-attack action: i) paid by a state actor or an actor that behaves like a state actor (e.g., Elderwood Gang, Israel, USA, Chinese military); ii) paid by the proceeds of the sale of secret information and information credentials; iii) paid by proceeds of ransom

payments (E. Bogachev); iv) paid by proceeds of legitimate business operations and/or personal funds (e.g., CyberBunker); v) paid by a mature cyber-crime organization (e.g., A.A. Panin); and vi. paid by transforming virtual currencies into cash (e.g., Gaming Co.).

Capacity

The attribute “Capacity” refers to Adversary 1’s ability to undertake research and development to carry out cyber-attacks. There at least four fields for this Attribute: i) Ability to carry out research for the purpose of discovering Zero Day vulnerabilities (e.g., Elderwood Gang, Israel, USA, Chinese military, Covert Grove, Criminal organization that carried out the Target cyber-attack); ii) Ability to develop custom code (e.g., Elderwood Gang, Israel, USA, Chinese military, Covert Grove, Criminal organization that carried out the Target cyber-attack, A. Gonzalez); iii) Ability to modify existing code (e.g., A.A.Panin, E. Bogachev, Winniti); and iv) No ability to develop code (e.g., CyberBunker).

4.5.2 Description and Examples of the Attributes of Action

Adversary 1 executes “Action,” an entity that has four attributes: Objective, Approach, Malware, and Duration.

Objective

The attribute “Objective” refers to the aims pursued by an action. Examples of cyber-attack objectives include: i) Copy and download information or code that belongs to Adversary 2 and upload it into an external server (e.g.,Elderwood Gang, Chinese military,Covert Grove, Criminal responsible for cyber-attack on Target Corporation, A.

Gonzalez, A.A. Panin, E. Bogachev, Winniti) ; ii) Damage specific physical assets (e.g., Israel, USA); iii) Take a website offline (e.g., CyberBunker); iv) Withdraw currencies from accounts (e.g., A.A. Panin, Winniti); v) Prevent users from accessing their files and programs (e.g., Evgeniy Bogachev).

Approach

The attribute “Approach” refers to the scheme used during the early phase of the cyber-attack. Examples of these schemes are: i) Spear phishing (e.g., Elderwood Gang, Chinese military, Covert Grove, Winniti); ii) Phishing (e.g., Criminal who carried out the Target Corporation cyber-attack, A.A. Panin, E. Bogachev); iii) Removable disk drives (e.g., Israel, USA), iv) Distributed Denial of Service (e.g., CyberBunker), and v) Wardriving (e.g., TJX Companies).

Spear phishing is a scheme that consists in sending emails that appear to come from a trusted source requesting information such as login IDs and passwords (Parmar, 2012). Spear phishing scams often appear to be from a company's own human resources or technical support divisions and ask employees to update their username and passwords. Once Adversary 1 obtains this data it can gain entry into Adversary 2’s secured networks. Another type of spear phishing attack will ask users to click on a link, which deploys spyware that can copy and download Adversary 2 data to an external server controlled by Adversary 1.

Phishing involved the use of emails and web sites in an attempt to scam the user into surrendering private information to be used for identity theft (Zhang et al., 2007).

A removable disk drive is a high-capacity, self-contained storage device containing a read-write mechanism plus one or more hard disks, inside a sealed unit. They can be used to store malware to penetrate a network to which the computer with the removable disk is connected.

Distributed Denial of Service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers (Taghavi Zargar, S., 2013). Such an attack is often the result of multiple compromised systems in a botnet flooding the targeted system with traffic.

Wardriving entails the search for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (Hurley, 2004). Wardriving can be used to access confidential information of users on a wireless network.

Malware

The "Malware" attribute refers to the malicious code that executes unwanted and possibly dangerous activities on a computer system. Malware is short for malicious software. Malware can be classified based on the characteristics of the malicious software and its possibilities in terms of self-dissemination (and code composition or the methods for bypassing the border security controls and gaining access to the system. (Jasiul et al, 2015). Examples of malware include Hydraq (e.g., Elderwood Gang), Stuxnet (e.g., Israel, US), Poison Ivy (e.g., Covert Grove), Citadel (e.g., Criminal responsible for Target Corporation cyber-attack), Black POS (e.g., Criminal responsible

for Target Corporation cyber-attack), Blabla (e.g.,TJX), SpyEye (e.g., A.A. Panin), Cryptolocker (e.g., E. Bogachev), and PlugX (e.g., Winniti).

Adversary 1 uses malicious software such as Hydraq (Symantec, 2010a), Poison Ivy (Symantec, 2010c), Citadel (Symantec, 2010d), Black Point of Sale (Symantec, 2013a), Blabla (Zetter, 2009), SpyEye (Symantec, 2010e) and PlugX (Symantec, 2010f) to open a back door on the compromised computer and perform actions that have not been authorized by Adversary 2. Citadel, Black Point of Sale, Blabla, and SpyEye copy and upload credit card numbers into external servers controlled by Adversary 1.

Adversary 1 uses Stuxnet to take control of industrial facilities, such as power plants, that are operated by Adversary 2. Stuxnet can self-replicate on computers or via computer networks without Adversary 2 being aware that the network that controls physical devices has become compromised (Symantec, 2010a).

Adversary 1 uses Crytolocker to first encrypt files on the compromised computer and then prompt the user to purchase a password in order to decrypt them (Symantec, 2013b).

Duration

The “Duration” attribute provides the number of weeks from the time the attack was discovered and the time it ended. The duration of the cyber-attacks ranged from 2 to 32 weeks. Note that three cyberattacks were still in progress as of December 2013.

4.5.3 Description and Examples of the Attributes of Adversary 2

Adversary 2 is comprised of two parts; one part includes the organizations that operate the network and are responsible for operating the technical aspects of its security and the other part, referred to as Extrinsic INT. The entity Extrinsic INT is extrinsic to the internal organizations that operate the network but a part of Adversary 2.

The first part of Adversary 2 has five attributes: Name, Location, Motivation, Business model, and Capacity.

Name

The attribute “Name” includes basic data on Adversary 2 that is not expected to change frequently (e.g., such as name, addresses, and phone numbers). The fields of “Name” of the entity Adversary 2 can be organized into three types: names of organizations that were publicly identified as being targets of cyber-attacks (e.g., Google, Natanz Fuel Enrichment Plant, New York Times, Spamhaus Project, Target Corporation, and TJX Companies); names of companies that were attacked but were not publicly identified as having been attacked (e.g., Chemical Company, Gaming Company); and unidentified users of personal computers (e.g., Users of personal computers with bank accounts, users of personal computers with vulnerabilities).

Location

The attribute “Location” can be specified in great detail when Adversary 2 is comprised of organizations than when Adversary 2 is comprised of PC users. The level of detail for Adversary 2 is much greater than the level of detail available for Adversary 1. Examples

of countries where Adversary 2 was located include: China, Iran, Netherlands, and the United States. In two instances, Adversary 2 denotes individuals distributed worldwide.

Motivation

The fields of the attribute "Motivation" were inferred by the researcher from the information published on the Internet. The fields of "Motivation" can be organized into three types: i) Meet quarterly profit targets (e.g., Google, Chemical Company, Target, TJX, Bank, Gaming Company); ii) Advance programs that are core to an organization's mission (e.g., Natanz Fuel Enrichment Plant, Spamhaus Project, New York Times); and iii) Users of personal computers productively (e.g., Users of personal computers with vulnerabilities in their operating systems or applications software).

Business model

The attribute "Business model" describes the rationale of how Adversary 2 creates, delivers, and captures value (Chesbrough et al., 2006; Muegge, 2012). More is known about the business models of Adversary 2 than the business models of Adversary 1. For the purpose of this research, the business model was characterized by the core business of Adversary 2. This can be refined at a later date, if required. Therefore, examples of business models are anchored around the operations of i) Providers of Internet products and services (e.g., Google, Gaming Company); ii) Government agency (Natanz Fuel Enrichment Plant); iii) Not-for profit (e.g., Spamhaus); iii) Discount retailers (e.g., Target Corporation, TJX Companies); iv) Daily newspaper (e.g. New York Times); v) Banking services (e.g. Bank); vi) Profits from intellectual property (e.g., Chemical); and vii) Consumers (e.g., User of personal computer with vulnerabilities).

Capacity

The attribute “Capacity” refers to Adversary 2’s ability to undertake research and development to prevent and respond to cyber-attacks. Examples can be categorized into two groups based on whether Adversary 2 has internal capability to carry out security related research and development. Examples of organizations with internal capability to carry out security related research and development include Google and Gaming Company.

4.5.4 Description and Examples of the Attributes of Network or System

The attribute “Network or System” refers to the entry point of the attack. Examples of these entry points include i) vulnerability of a single purpose server operated by Adversary 2 (e.g., Google, New York Times, Chemical Company, TJX, Gaming Company); ii) vulnerability of server linked to Adversary 2’s supply chain (e.g., Natanz Fuel Enrichment Plant, Target); iii) vulnerability of operating system or software application of a personal computer (e.g., User of PC with vulnerabilities); iv) use of stolen credentials to enter the network (e.g., PC user with bank account); and v) server flooding (e.g., Spamhaus).

4.5.5 Description and Examples of the Attributes of Information and Software

The attribute “Information and Software” identifies the digital assets targeted by Adversary 1 that run on the computers operated by Adversary 2. Examples of these digital assets include: i) Source code (e.g., Google, Gaming Company); ii)

Programmable logic controllers (e.g., Natanz Fuel Enrichment Plant); iii) Passwords (e.g. New York Times); iv) Information about debit and credit cards and bank accounts; v) Digital certificates used to secure exchange of information over the Internet using the public key infrastructure (e.g. Gaming Company); vi) Industrial secrets and proprietary information (e.g., New York Times, Chemical Company); and vii) Regular user files (e.g., User of personal computer with vulnerabilities).

4.5.6 Description and Examples of the Attributes of Physical Assets

The attribute “Physical” refers to physical assets that are controlled by the network or system operated by Adversary 2. There is only one example of physical assets: centrifuges that were damaged at the Natanz Fuel Enrichment Plant.

4.5.7 Description and Examples of the Attributes of Extrinsic INT

The entity Extrinsic INT is extrinsic to the internal organizations that operate the network but is a part of Adversary 2.

The examination of the 10 cyber-attacks led us to conclude that factors that are not directly related to the operations of data networks but are integral to the organizations dealing with a data breach play major roles during a cyber-attack. A total of 12 attributes were identified. These are: Brand (e.g., Target Corporation, TJX); Claims against assets (e.g., Target Corporation); Disclosure (e.g., Target Corporation, TJX); Equipment (e.g., Natanz Fuel Enrichment Plant, Target Corporation); Executives (e.g., Target Corporation); Expansion (e.g. Google, Target Corporation); Fines (e.g., TJX

Companies); Legal fees (e.g. TJX Companies); Partners (e.g., New York Times); Performance (e.g., Natanz Fuel Enrichment Plant, Target Corporation, TJX Companies); Process (e.g., Target Corporation), and Settlement (Target Corporation).

4.5.8 Description and Examples of the Attributes for Cyberspace

In the proposed representation, Adversary 1 and Adversary 2 share the use of a common resource named cyberspace. However, the “Cyberspace” attribute is not well defined because, unfortunately, the concept of cyberspace is underdeveloped. There are at least 28 definitions of the term cyberspace (Kramer, 2009). Instead of accepting the limitation that this ambiguity poses to carrying out research, it was decided to use the term to denote the technical infrastructure shared by the two adversaries. However, it was limited to only two attributes: Botnets and Command and Control servers.

Botnet

The Botnet attribute refers to the network of computers infected with malicious software and controlled as a group without the owners’ knowledge. A "bot" is a type of malware that allows an attacker to take control over an affected computer. Also known as “Web robots”, bots are usually part of a network of infected machines, known as a “botnet”, which is typically made up of victim machines that stretch across the globe

Eight of the ten cyber-attacks examined relied on botnets. The two cyber-attacks that did not rely on botnets included the attacks on the Natanz Fuel Enrichment Plant and TJX Companies.

Command and Control Servers

The attribute denoted “Command and Control” refers to the servers that issue commands to the computers that are part of the botnet and accept reports back from the compromised computers. A Command and Control server (C&C) is a computer used to coordinate the actions of computers infected by a bot, rootkit, worm or other forms of malicious software (malware) that rely on another computer for instructions and updates.

The information on these attacks highlighted three aspects of these servers: i) communications architecture of the command and control servers; ii) the number of command and control servers used by Adversary 1; and the location of the command and control servers.

Public information on these three aspects of Command and Control servers is not of high quality. Command and control servers have been reported to be located from one to 20 countries.

4.5.9 Description and Examples of the Attributes for Extrinsic

Extrinsic is an entity that is extrinsic to both Adversary 1 and Adversary 2 and affects both of them.

The examination of the 10 cyber-attacks identified 10 attributes for Extrinsic. These are: Arrests (e.g., Spamhaus Project, TJX, Bank, User of PC with vulnerabilities); Claims (e.g., Target Corporation); Government (Chemical Company, Target Corporation), Gov-Gov (e.g., China-US involving Google, New York Times); Internet (e.g., Spamhaus

Project); Support infrastructure (e.g., Spamhaus Project); Law enforcement agencies (e.g., Google, Spanhaus Prject, Target Corporation, Users of PCs with vulnerabilities); Legal (e.g., Target Corporation); Retaliation (Natanz Fuel Enrichment Plant).

4.6 Summary

Chapter 4 provides the results of the research. The results include:

- Narratives, links to sources of information used to produce the narratives, and the entity relationship diagrams for each of the ten cyber-attacks
- One entity relationship diagram developed from the definitions of the cyber-attack concept identified in the literature review
- One entity relationships diagram developed from the information on the 10 cyber-attacks
- Examples of the attributes of the nine entities included in the representation of the cyber-attack concept

In the representation of a cyber-attack, two adversaries share cyberspace and are affected by factors extrinsic to their organizations. Adversary 1 acts to: i) undermine Adversary 2's networks, systems, software or information or ii) damage the physical assets they control. Adversary 2 is comprised of two parts; one part includes the organizations that operate the network and are responsible for operating the technical aspects of its security and the other part is extrinsic to the internal organizations that operate the network.

Many factors that are not directly related to the data breach, which is at the core of the cyber-attack, were found to affect the behaviors of the two Adversaries.

5. DISCUSSION OF RESULTS

The purpose of Chapter 5 is to relate the results presented in chapter 4 back to the goal and objectives provided in Chapter 1. This chapter is organized into six sections. Section 5.1 discusses the representation of the cyber-attack concept. Section 5.2 is a discussion about the fidelity this research adds to the cyber-attack concept. Section 5.3 is a discussion of two entities, “Cyberspace” and “Extrinsic,” that are part of the representation of the cyber-attack concept. Sections 5.4 and 5.5 discuss the intra-, cross- and multi-disciplinary perspectives of cyber-attacks. Section 5.6 provides a summary of Chapter 5.

5.1 Representation of the Cyber-attack Concept

The ERD shown in Figure 2 provides a representation of the cyber-attack concept. The ERD includes 9 entities, 41 attributes and 15 relationships.

In the representation shown as Figure 2, two adversaries share cyberspace and are affected by factors extrinsic to their organizations. Adversary 1 acts to: i) undermine Adversary 2’s networks, systems, software or information or ii) damage the physical assets they control. Adversary 2 is comprised of two parts; one part includes the organizations that operate the network and are responsible for operating the technical aspects of its security and the other part is extrinsic to the internal organizations that operate the network.

The representation in Figure 2 can be used to examine adversarial perspectives. For example, the representation is biased towards the impact on Adversary 2 through the choice of relationship names. For example, "Undermines" properly describes the relationship between the actions of Adversary 1 and Adversary 2's networks, systems, information, and software given the definitions and information that was used to produce it. However, Adversary 1 probably views this relationship as a successful operation. Moreover, Adversary 2 in Figure 2 is shown as being comprised of two parts, while Adversary 1 as being comprised of only one part. An adversarial perspective would require symmetry between the way Adversary 1 and Adversary 2 are represented. The representation in Figure 2 reflects the biases in the current definitions of cyber-attack and the lack of information about the attackers relative to the information available for their targets.

5.2 Adding Fidelity to the Cyber-attack Concept

The research adds fidelity to the concept of cyber-attack by using information from ten scenarios of high-profile cyber-attacks.

The representation of a cyber-attack in Figure 2 provides a benchmark of what can be known about cyber-attacks without using proprietary information and/or a dominant theoretical perspective on cyber-attacks. Outcomes produced using new theoretical perspectives can also be compared against the representation of the cyber-attack concept provided in this thesis. Similarly, outcomes being produced by personnel who

have access to proprietary information can be benchmarked against the results illustrated in Figure 2.

Figure 2 suggests the importance of complementors, particularly for Adversary 2. It also suggests that the study of complementors of Adversary 1 is in area that deserves further study.

5.3 Cyberspace and Extrinsic Entities

The representation shown in Figure 2 suggests that the adversary that better understands the “Cyberspace” and “Extrinsic” entities may have an advantage. However, this representation is limited in the sense that it does not benefit from a suitable definition of what is meant by cyberspace and does not properly distinguish between what is in the “Cyberspace” entity relative to what is in the “Extrinsic” entity. For example, arguments can be made for including the attributes Botnet and Malware as part of the Extrinsic entity. Similarly, arguments can be made for including the “Internet” as an attribute of the “Cyberspace” entity.

Two of the six definitions of cyber-attack found in the literature include the word cyberspace (Uma & Padmavathi, 2013: p. 390; US Joint Chiefs of Staff, 2010: p.5). However, there are at least 28 definitions of the term cyberspace (Kramer, 2009). For the purpose of carrying out this research, it was decided to use the term cyberspace to denote the technical infrastructure shared by the two adversaries. However, this decision is controversial and warrants further investigation.

5.4 Intra-, Cross- and Multi-disciplinary Perspectives

The representation provided as Figure 2 suggests theories that could be used to help provide a better understanding of cyber-attacks. For example, the inclusion of “Business Model” as an attribute of both Adversary 1 and Adversary 2 suggests the application of entrepreneurial theories to explain cyber-attacks. The inclusion of the attribute “Motivation” opens the door to cross-disciplinary reasoning anchored on psychological and sociological perspectives. Adversarial dynamics suggest multi-disciplinary perspectives that support game theory and theory of war tactics.

5.5 Trans-disciplinary Perspective

The goal is to develop a trans-disciplinary perspective of the cyber-attack concept, one that provides a unity of intellectual frameworks beyond those offered by disciplinary perspectives (Max-Neef, 2005; Nicolescu, 2005).

This is a suitable goal because at this time what is needed the most is the unification of the knowledge that exists about cyber-attacks.

5.6 Summary

The purpose of this chapter is to discuss the results. This research has developed a representation of cyber-attacks for the purpose of unifying the knowledge about cyber-attacks. This representation includes 9 entities, 41 attributes, and 15 relationships.

In the cyber-attack representation that was developed, Adversary 1 and Adversary 2 share the use of cyberspace, an entity for which at least 28 definitions exist and both adversaries are affected by 10 factors that are extrinsic to both organizations. Adversary 2 is conceptualized as being comprised of two parts, one that is responsible for the security of a network and the other that is not.

The representation developed can be used as a benchmark to assess theoretical contributions as well as applications using proprietary data.

The attributes and relationships identified add details to what is referred to as cyber-attacks.

The unification of the knowledge about cyber-attacks can be used to identify theories that are relevant to better understand the cyber-attack concept as well as to advance a trans-disciplinary perspective of cyber-attacks.

6. CONCLUSIONS, LIMITATIONS, AND SUGGESTIONS FOR FURTHER RESEARCH

Chapter 6 is organized into three parts. Section 6.1 provides the conclusions of the thesis. Section 6.2 identifies the limitations of the research. Finally, Section 6.3 provides suggestions for future research initiatives.

6.1 Conclusions

This research developed a representation of the cyber-attack concept for the purpose of unifying six cyber-attack definitions found in the literature and the information published about ten high-profile cyber-attacks. The goal is to enable the development of a trans-disciplinary theory of cyberattacks and a database that can support theory development.

The following definition is advanced: A cyber attack is a cyberspace-enabled action executed by Adversary_1 with the intention to damage or undermine assets operated by Adversary_2. Collateral actions, supported by extrinsic capabilities, by Adversary_2 may degrade the ability of Adversary_1 to continue execution.

The cyber-attack representation is not symmetric in terms of the representation of the Adversary 1 and Adversary 2 entities and uses an ambiguous entity referred to as cyberspace. The separation between two entities “Cyberspace” and “Extrinsic” is not as well defined as the author would like it to be.

6.2 Limitations of the Research

This research has at least five limitations. First, the cyber-attack representation developed includes “Cyberspace” as an entity. The many definitions of cyberspace

create confusion about what is really meant by the term cybersecurity making it difficult to identify the components of the Extrinsic and Cyberspace entities.

Second, the narratives prepared from the information found on the Internet result in biases against Adversary 2. Most of these biases are introduced by the names selected for the relationships between entities.

The third limitation is that the information found on the Internet for Adversary 2, the target of the attack, was much greater than the information found for Adversary 1. This resulted in an undesirable asymmetry between the representations of Adversary 1 and Adversary 2.

The fourth limitation is that the sample size was small with only 10 cyber-attacks examined. Finding information, organizing it around time-lines, and then producing narratives was very time consuming. Adding many more other cyber-attacks to the sample was for all practical purposes not possible.

Fifth, since mass media are typically owned and run by American corporations, most of available data which can be found on-line are pivoting around Eastern European and Chinese attacks on American organizations; this is why most studies may reflect a pro-America bias.

6.3 Suggestions for Future Research

Three initiatives for future research are identified. First, is the development of a representation of the cyber-attack concept with the representations of the two entities, Adversary 1 and Adversary 2, have the same parts and the same attributes.

The second research initiative is to develop a characterization for cyberspace that allows a clear separation between the “Cyberspace” and “Extrinsic” entities used in Figure 2.

The third research initiative is to define the relationships between the two parts that constitute Adversary 2.

6.4 Contribution to theory development

This research provides a representation that can enable the advancement of theory. The inclusion of the attribute Motivation may open the door to psychological and sociological reasoning. Adversarial dynamics suggest game theory and theory of war tactics.

This research provides the first step to the design and development of a database that can support scholarly research.

REFERENCES

Alperen, M. 2011. Foundations of homeland security: Law and policy. New York, NY: Wiley.

Amoroso, E.G. 2011. Cyber Attacks: Awareness. Network Security, Volume 2011, Issue 1:10-16, January 2011.

Ashford, W. 2013. US Researchers Find 25 Security Vulnerabilities in SCADA Systems.*ComputerWeekly.com,* October 18. http://www.computerweekly.com/news/2240207488/US-researchers-find-25-sec...

Baldwin, D. A. 1997. The Concept of Security. Review of International Studies. 23:5-26 http://www.princeton.edu/~dbaldwin/articles.html

Bagui, S., & Earp, R. 2011. Database Design Using Entity-Relationship Diagrams: Foundations of Database Design, (2th Edition). Auerbach Publications.

Buzan, B., Waever, O., & De Wilde, J. 1998. *Security: A New Framework for Analysis.* Boulder, CO: Lynne Rienner Publishers.

Castel, M. E. 2012. International and Canadian Law Rules Applicable to Cyber Attacks by State and Non-State Actors. *Canadian Journal of Law & Technology*, 10(1): 89-120. https://ojs.library.dal.ca/CJLT/article/view/4833/4353

Chen, P. 1976. The entity-relationship model--Toward a unified view of data. ACM Transactions on Database Systems, 1(1): 9–36. http://www.comp.nus.edu.sg/~lingtw/papers/tods76.chen.pdf

Chen, P. P. 2002. Entity-relationship modeling: Historical events, future trends, and lessons learned. In Broy, M., & Denert, E. (eds.), SpringerSoftware pioneers: Contributions to software engineering, Berlin: Springer: 296-310. http://bit.csc.lsu.edu/~chen/pdf/Chen_Pioneers.pdf

Chesbrough, H.W. 2006. Open Business Models: How to Thrive in the New Innovation, (1th Edition). Harvard Business Review Press.

Crawford, J. 2014. The U.S. Government Thinks China Could Take Down the Power Grid. *CNN,*November 20. http://www.cnn.com/2014/11/20/politics/nsa-china-power-grid/

Colored Petri Nets. Computer Science and its Applications. Lecture Notes in Electrical Engineering, 330: 475-482.

ESET Virus Radar. 2015.Command and Control Server. January. http://www.virusradar.com/en/glossary/command-and-control-server

Gervais, M. Cyber Attacks and the Law of War. Berkeley Journal of International Law, Volume 30, Issue 2, 2012. http://scholarship.law.berkeley.edu/bjil/vol30/iss2/6.

Han, C., & Dongre, R. 2014. Q&A. What Motivates Cyber-Attackers? Technology Innovation Management Review, 4(10): 40–42. http://timreview.ca/article/838

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. 2012. The Law of Cyber-Attack. *California Law Review*. 100(4): 817-885. http://www.californialawreview.org/articles/the-law-of-cyber-attack

Hurley, C. 2004. WarDriving: Drive, Detect, Defend: A Guide to Wireless Security. Syngress (1th Edition). Syngress.

Huysmans, J. 1998. Security! What Do You Mean? From Concept to Thick Signifier. *European Journal of International Relations*, 4(2): 226-255. http://dx.doi.org/10.1177/1354066198004002004

Jasiul, B., Szpyrka, M., & Sliwa, J. 2015. Formal Specification of Malware Models in the Form of Colored Petri Nets. Computer Science and its Applications. Lecture Notes in Electrical Engineering, 330: 475-482.

Jowitt, T. 2014. White House Advisory Group: Governments Have Five Years To Secure IoT.*TechWeek Europe*, November 20. http://www.techweekeurope.co.uk/e-regulation/governments-secure-iot-156149

Kendall, K.E. , &Kendall, J.E. 2013. Systems Analysis and Design (9th Edition). Prentice Hall.

Kovacs, E. 2014. U.K. Invests Heavily in ICS Cyber Security Research. *Security Week*, October 3. http://www.securityweek.com/uk-invests-heavily-ics-cyber-security-research

Kramer, F.D. 2009. Cyberpower and National Security:Policy Recommendations for a Strategic Framework, in , Kramer, F.D., Starr, S., and Wentz, L.K. (Ed.), Cyberpower and National Security, National Defense University Press, Washington.

Max-Neef, M. A. 2005. Foundations of Transdisciplinarity. Ecological Economics, 53(1): 5-16. http://dx.doi.org/10.1016/j.ecolecon.2005.01.014

Minei, E. and Matusitz J. 2011. Cyberterrorist Messages and Their Effects on Targets: A Qualitative Analysis. Journal of Human Behavior in the Social Environment, Volume 21, Issue 8: 995-1019.

Muegge, S. 2012. Business Model Discovery by Technology Entrepreneurs. April: 5-16. http://timreview.ca/article/545

National Security Telecommunications Security Advisory Committee. 2014. *Draft Report to the President on the Internet of Things,* November. Washington, DC: Department of Homeland Security.

Nicolescu, B. 2005. Transdisciplinarity – Past, Present, and Future. II Congresso Mundial de Transdisciplinaridade, 6-12 September, 2005, Brazil. http://cetrans.com.br/textos/transdisciplinarity-past-present-and-future.pdf

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. 2012. SCADA Security in the Light of Cyber-Warfare. *Computers & Security*, 31(4):418-436. http://dx.doi.org/10.1016/j.cose.2012.02.009

Nykodym, N., Taylor, R. Vilela, J. Criminal Profiling and Insider Cyber Crime. Computer Law & Security Review, 2005

Norton by Symantec. 2015. Bots and Botnets - A Growing Threat. January. http://ca.norton.com/botnet

Owens, W. A., Dam, K., & Lin, H. S. 2009. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber-attack Capabilities.* Washington, DC: National Academies Press.

Pearson, N. 2014. A Larger Problem: Financial and Reputational Risks. *Computer Fraud & Security*, 2014(4): 11-13. http://dx.doi.org/10.1016/S1361-3723(14)70480-4

Parmar, B. 2012. Protecting against spear-phishing. Computer Fraud & Security, January 1 : 8–11.

Rehman, A.U. 2014. Understanding the significance of cyber security threats. *VFAST* Transactions on Educational and Social Sciences, 4(2): 21-26.

Roscini, M. 2014. *Cyber Operations and the Use of Force in International Law.* Oxford: Oxford University Press

Schmitt, M.N. 2012. The Laws of Cyber Warfare: Quo Vadis? Stanford Law and Policy Review, Volume 25:269-300. https://journals.law.stanford.edu/sites/default/files/stanford-law-policy-review/print/2014/06/schmitt_25_stan._l._poly_rev._269_final.pdf.

Scully, T. 2013. The Cyber Security Threat Stops in the Boardroom. *Journal of Business Continuity & Emergency Planning*, 7(2):139-147. http://www.ncbi.nlm.nih.gov/pubmed/24457325

Sugarman, E. 2014. Cybersecurity is a Severe and Growing Challenge for Government Contractors. *Forbes,* August 24. http://www.forbes.com/sites/elisugarman/2014/08/26/cybersecurity-is-a-se...

Symatec. 2010. Trojan.Hydraq. Accessed January 1, 2015 http://www.symantec.com/security_response/writeup.jsp?docid=2010-011114-1830-99

Symatec.2010. Poison IVY Backdoor Activity. Accessed January 1, 2015 http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=24379

Symantec. 2010. W32.Stuxnet. Accessed January 1, 2015 http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

Symantec. 2010. System Infected: Citadel C&C Activity. Accessed January 1, 2015 http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=26434

Symantec. 2010. Trojan.Spyeye. Accessed January 1, 2015 http://www.symantec.com/security_response/writeup.jsp?docid=2010-020216-0135-99

Symantec. 2010. System Infected: PlugX Remote Access Tool Activity. Accessed January 1, 2015 http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=27409

Symantec. 2013. Infostealer.Reedum.B. Accessed January 1, 2015 http://www.symantec.com/security_response/writeup.jsp?docid=2013-121909-3813-99

Symantec.2013. Trojan.Cryptolocker: Accessed January 1, 2015 http://www.symantec.com/security_response/writeup.jsp?docid=2013-091122-3112-99

Taghavi Zargar, S. 2013. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE Communications Surveys & Tutorials, 15(4): 2046–2069.

Uma, M., & Padmavathi, G. 2013. A Survey on Various Cyber Attacks and their Classification.*International Journal of Network Security*, 15(5): 390-396.

United States Joint Chiefs of Staff. 2010. Memorandum: Joint Terminology for Cyberspace Operations. Washington, DC: United States Department of Defense.

US Securities and Exchange Commission. 2014. Form 8-K (001-15935): Community Health Systems, Inc. *United States Securities and Exchange Commission,* August 18. http://www.sec.gov/Archives/edgar/data/1108109/000119312514312504/d77654...

Waxman,.M,.C.2011. Cyberattacks and the Use of Force: Back to the Future of Article 2(4). Yale Journal of International Law, 36(2). : 421-458 http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf

Weiss, M. 2014. Do We Need a CDC for Cybersecurity? *CIO Insight,* October 30. http://www.cioinsight.com/security/do-we-need-a-cdc-for-cybersecurity.html

Yunos, Z., Suid, S. Protection of Critical National Information Infrastructure (CNII) against cyber terrorism: Development of strategy and policy framework. Proceedings of IEEE Conference on Intelligence and Security Informatics, 2010.

Zetter,K.2009. TJX Hacker Was Awash in Cash; His Penniless Coder Faces Prison.Wired, Accessed May 2, 2014. http://www.wired.com/2009/06/watt/

Zhang, Y., Hong, J. I., Cranor, L.F. 2007. Cantina: A Content-based approach to detecting phishing Web Sites. Proceedings of the 16th International Conference on World Wide Web: 639-647.

Appendices

Appendix A. Narratives of Ten High-Profile Cyber-Attacks

Appendix A includes narratives of the ten high-profile attacks examined in the thesis.

The narratives describe the following cyber-attacks:

	Cyber-attack	
	Alleged Attacker	**Known Target**
1	Elderwood Gang	Google
2	Israel, USA	Natanz Fuel Enrichment Plant
3	China military	New York Times
4	Covert Grove	Chemical company
5	CyberBunker	Spamhaus Project
6	Criminal	Target
7	A. Gonzalez	TJX Companies
8	Aleksandr Andreevich Panin	User with bank accounts
9	Evgeniy Bogachev	User of PC with vulnerabilities
10	Winniti	Gaming company

1. Elderwood Gang_Google

On January 12, 2010 Google announced that:

- It had detected a highly sophisticated and targeted attack on its corporate infrastructure that had originated from China and had resulted in the theft of intellectual property from Google
- Accounts of dozens of U.S.-, China- and Europe-based Gmail users who were advocates of human rights in China had been routinely accessed by third parties in attacks that were not related to the attack on Google

As a result of the attack, Google announced that it was reviewing the feasibility of its business operations in China, was no longer willing to continue censoring search results on Google.cn, and recognized that it may have to shut down Google.cn and its offices in China (Drummond, 2010).

Theft of Google's intellectual property

Attackers:

- Stole the source code behind Google's search engine (Zetter,2010)
- Accessed a database that flagged Google's Gmail accounts marked for court-ordered wiretaps

The information on the database that was accessed could have provided Chinese operatives advanced warning about specific operations being carried out by various law enforcement agencies. The advanced warning would have enabled Chinese intelligence

agencies to destroy or insert false information (Schwartz, 2013). The information gained by the attackers would have given them insight into active investigations being conducted by the FBI and other law enforcement agencies that involved undercover Chinese operatives (Schwartz, 2013).

Access to Activists' email accounts

Activists' email accounts were accessed via phishing scams or malware placed on the users' computers, not through any security breach at Google (Drummond, 2010).

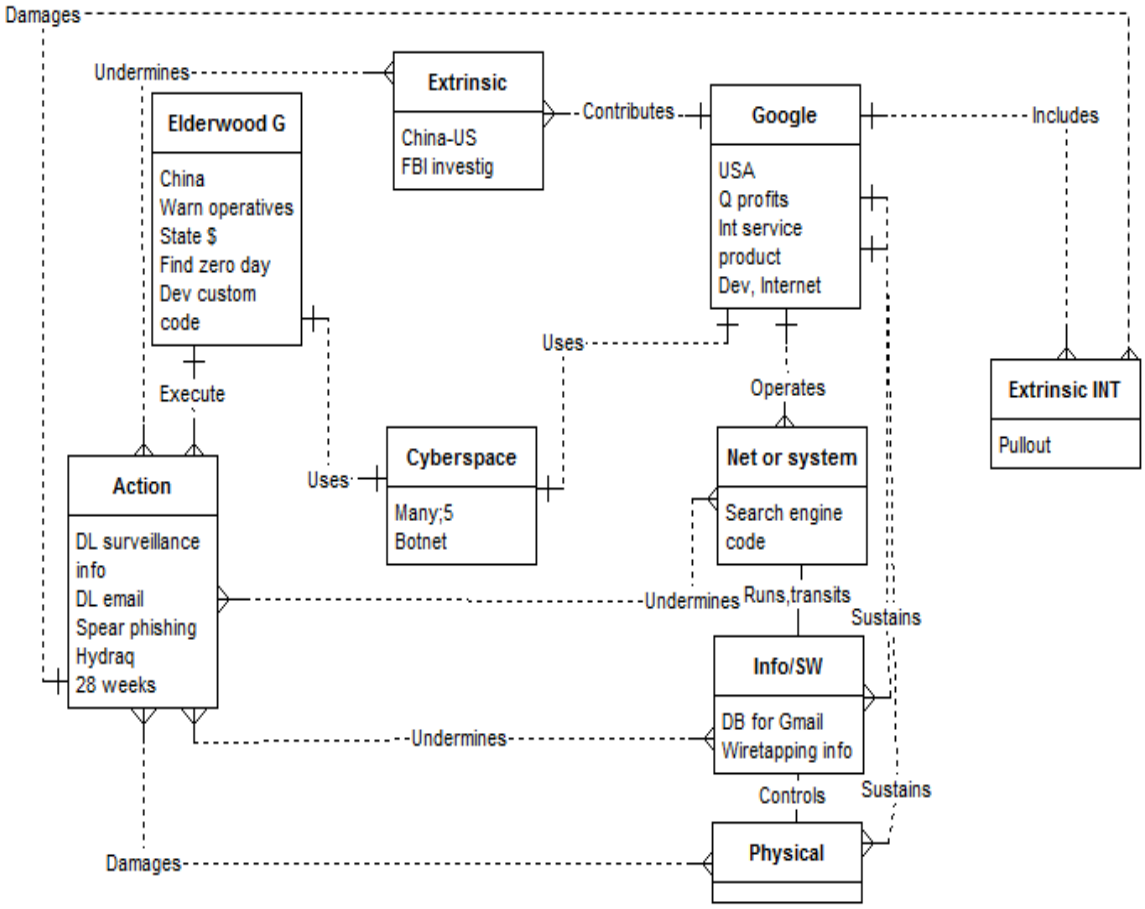
Believing they had received an email or instant message from a trusted source, users were fooled into clicking on a link, which would open up an infected Internet site using Internet Explorer. This website would download a Javascript onto the user's computer which would send an encrypted message to a remote server where it would activate and run as an executable. The file would then place 10 different malware files into the infected computer.

The botnet the Chinese used to obtain information from users had command and control servers in the United States, China, Germany, Taiwan and the United Kingdom.

Other companies targeted

At least 34 companies were targeted. Some of the targeted companies included: Adobe, Juniper, Rackspace, Symantec, Northrop Gruman, Morgan Stanley and Yahoo (Schwartz, 2013).

Figure 3. A.1. Entity Relationship Diagram for Elderwood Gang_Google



References:

DAMBALLA. 2010. The Command Structure of the Aurora Botnet. https://www.damballa.com/downloads/r_pubs/Aurora_Botnet_Command_Structure.pdf

Drummond, D. 2010. A New Approach to China. http://googleblog.blogspot.ca/2010/01/new-approach-to-china.html

Schwartz, M. 2013. Google Aurora Hack Was Chinese Counterespionage Operation. May. http://www.darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060?

Zetter,K. 2010. Google Hack Attack Was Ultra Sophisticated, New Details Show. Wired, http://www.wired.com/2010/01/operation-aurora/

2. Israel, USA_Natanz Fuel Enrichment Plant

In 2007, Israel and the US discovered that Iran was able to design and develop nuclear weapons (Maclean, 2010; Shubert, 2011). To destroy or delay Iran's nuclear program, Israel and the USA developed the Stuxnet worm between November 2007 and June 2010 (Khandelwal, 2013). The Stuxnet worm was malicious software designed to damage the nuclear centrifuges at Iran's Natanz Fuel Enrichment Plant by sending them out of control (Broad & Sanger, 2010).

The Stuxnet worm exploited well-known flaws in the PLC system as well as zero-day bugs (Naraine, 2010). The Stuxnet worm increased the revolving speed of nuclear equipment motors and shifted them up and down. These fluctuations damaged the centrifuges (Maclean, 2010).

The Stuxnet program had four command and control servers hosted in commercial hosting providers (Symantec Security Response, 2013).

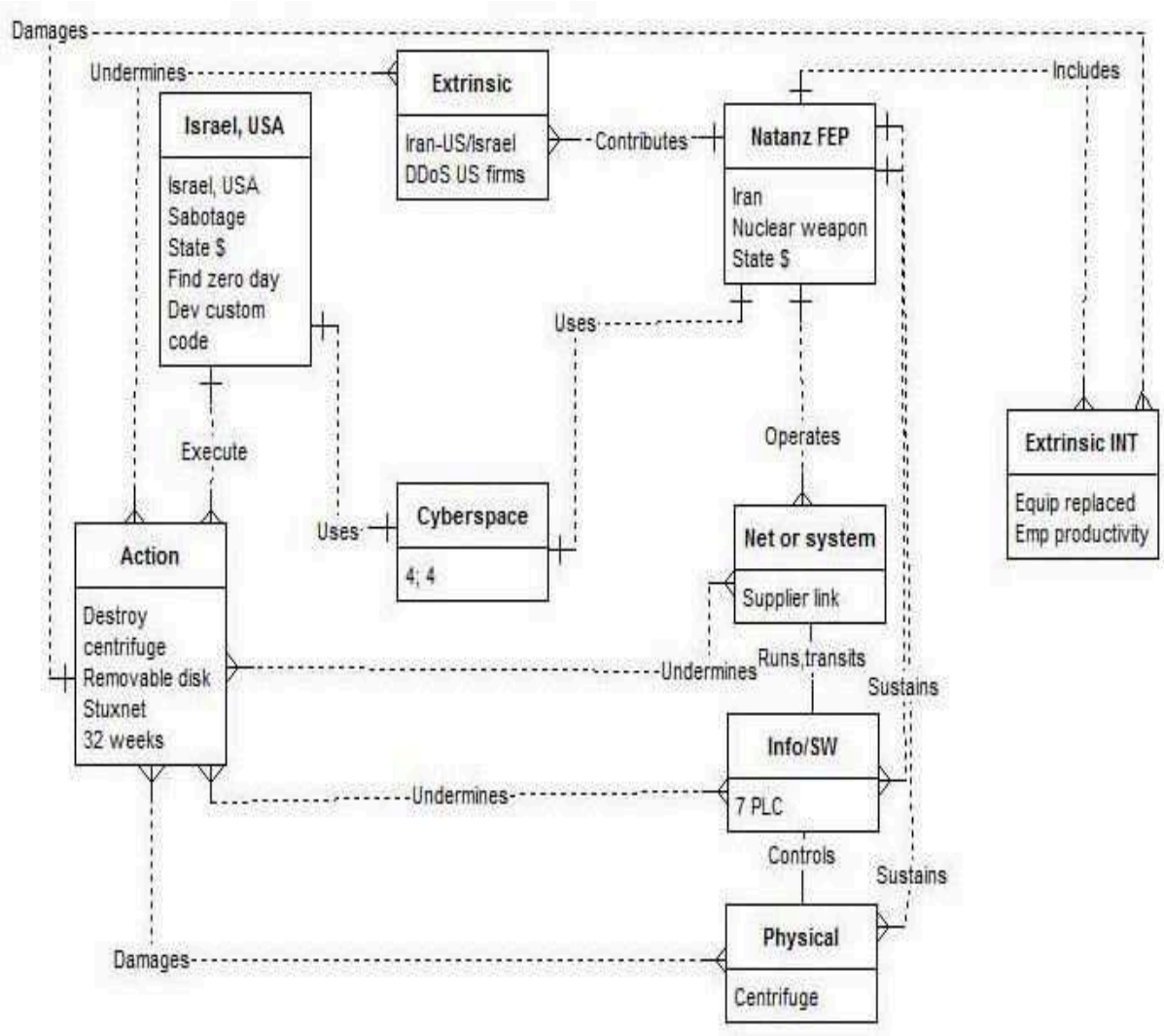
The Stuxnet worm first infected a network system that was separate from the Natanz facility and then gained access to the Natanz's internal network. The worm spread undetected infecting the Step 7 (Programmable Logic Controller – PLC) program used to operate the Siemens controllers. The Stuxnet worm took control of the physical systems (Kushner, 2013; Shubert 2011).

The Stuxnet worm also issued a restore command to revert motors to their normal operating frequency to make it difficult for operators to discover the damage had been done. While the centrifuge motors span abnormally too fast and damaged the centrifuges, the available monitoring tools showed adherence to normal operations. This

allowed for prolonged adverse effects to centrifuges to occur before preventive action could be taken.

The Stuxnet attack caused several problems for Iran and other countries (Broad & Sanger, 2010). Approximately 1,000 centrifuges at the Natanz facility had to be replaced (Katz, 2010) and work on the nuclear program declined (Maclean, 2010). Stuxnet disseminated and infected at least 100,000 additional computers. Iran retaliated against Saudi Arabia and the US (Capaccio, 2013), and Iran had to fight the Stuxnet worm to safeguard its centrifuge plants (Broad & Sanger, 2010).

Figure 4 . A.2 Entity Relationship Diagram for Israel, USA_Natanz Enrichment Plant



References:

Broad, W.J., & Sanger, D.E. 2010. Worm Was Perfect for Sabotaging Centrifuges. *The New York Times.* November 19. http://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html?pagewanted=all&_r=1&

Capaccio,T,2013. Iran's Cyber Threat Potential Great U.S. General Says.Bloomberg, January 17. http://www.bloomberg.com/news/2013-01-17/iran-s-cyber-threat-potential-great-u-s-general-says.html

Katz,Y. 2010. Stuxnet may have destroyed 1,000 centrifuges at Natanz. The Jerusalem Post, December 2010. http://www.jpost.com/Defense/Stuxnet-may-have-destroyed-1000-centrifuges-at-Natanz

Khandelwal,S. 2013. Super 'Stuxnet' Malware development in progress to destroy Iran's nuclear program. The Hack News December 3. http://thehackernews.com/2013/12/Stuxnet-2-Saudi-Arabia-Israel-Iran-nuclear-plant-virus.html

Kushner, D. 2013. The Real Story of Stuxnet.Febuary 2013. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Maclean, W. 2010. Analysis - Stuxnet: A new weapon for cyber insurgents? Reuters,November 28. http://uk.reuters.com/article/2010/11/28/uk-security-cyber-conflicts-idUKTRE6AR0CC20101128

Naraine, R.2010. Stuxnet attackers used 4 Windows zero-day exploits. September 2010. http://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits

Shubert, A. 2011. Cyber warfare: A different way to attack Iran's reactors, CNN, Novemebr 8. http://www.cnn.com/2011/11/08/tech/iran-stuxnet/

Symantec Security Response. 2013. Stuxnet 0.5: The Missing Link. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf

3.China military_ New York Times

On October 25, 2012, the New York Times (The Times) published an online article that claimed that the family of Wen Jiabao, then Premier of the People's Republic of China, had accumulated billions of dollars and that this amount was in hiding. The Times had alerted AT&T, its network security provider, of potential cyber-attacks given that it had been warned that its investigation of the Jiabao family had angered the Chinese government.

On October 25, 2012, behavior that was consistent with other attacks believed to have been perpetrated by the Chinese military was noticed on the New York Time's servers. On November 7, security breaches had not ceased despite efforts from AT&T and the FBI. The Times hired Mandiant to monitor their systems. Mandiant found that hacking of The Times' servers started at around 8am, Beijing time, and would continue for a standard workday. Hacking would occasionally stop for two-week periods. The reason for this was not clear (Perlroth, 2013).

The attacks on The Times were routed from the same university computers the Chinese military had previously used to attack US military contractors.

The hackers developed custom malware to retrieve the usernames and passwords of 53 employees of The Times. The malware was traced back to China. Since the custom malware was not on the list of forbidden software maintained by Symantec, the provider of antivirus software for The Times, it was allowed to pass through the network undetected (Goldman, 2013).

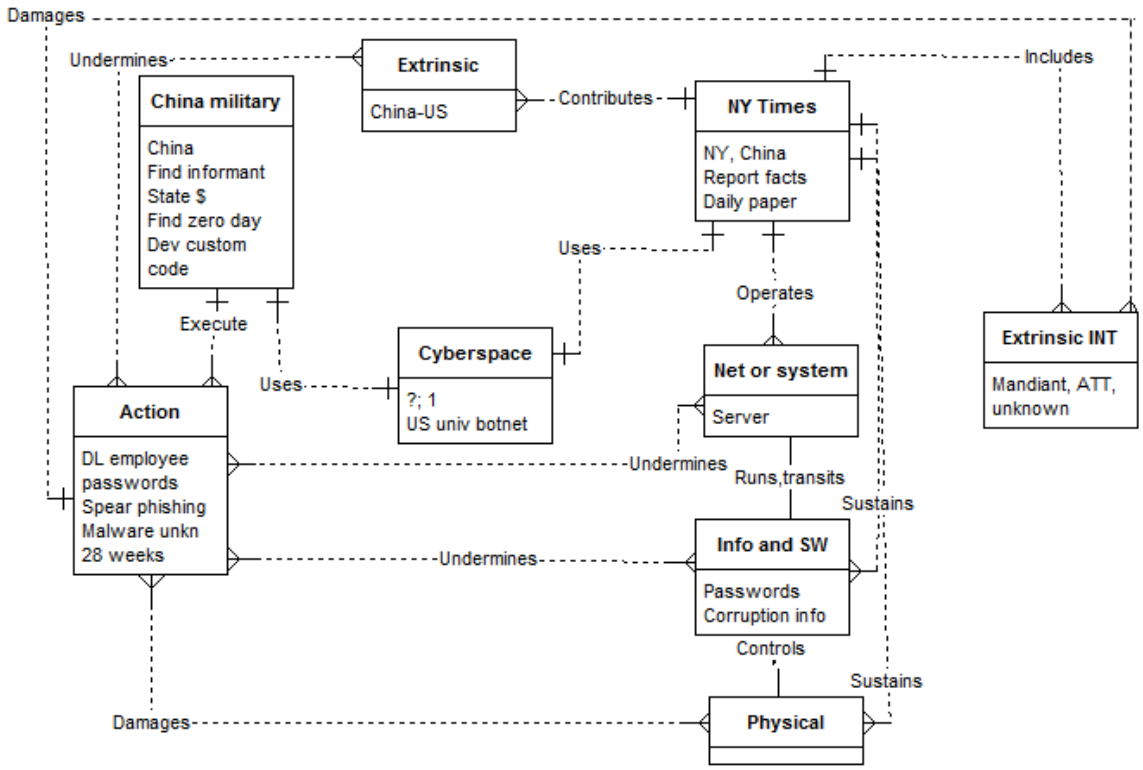
.

The hackers used these employees' passwords to remotely enter the network and seek information about the Wen family and the sources providing the information. No sensitive e-mails or files from employees were "accessed, downloaded or copied."

The New York Times uses the Symantec antivirus software. Of the 45 pieces of malware installed by attackers on the New York Times' network, the company's antivirus missed 44 (Goldman, 2013).

Symantec has claimed that the New York Times was not using its most advanced solutions (Goldman, 2013).

Figure 5. A.3. Entity Relationship Diagram for China military_New York Times



References:

Goldman,D. 2013. Your Antivirus Software Probably Won't Prevent a Cyberattack.CNN,January.
http://money.cnn.com/2013/01/31/technology/security/antivirus/

Perlroth,N. 2013. Hackers in China Attacked The Times for Last 4 Months, The New York Times,January.
http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0

4. Covert Grove_Chemical Company

In 2011, at least 29 chemical and 19 defense companies in the United States, Bangladesh and the United Kingdom were victims of cyber-attack industrial espionage (Homeland Security News Wire, 2014). These cyber-attacks, denoted “Nitro,” were traced to a man in China (Symantec Corporation, 2011) who exploited Java Zero-Day vulnerability (Prince, 2011).

PoisonIvy is a Remote Access Tool that is placed on computers systems to steal data and information undetected. PoisonIvy was used to hijack design documents, formulas as well as details on manufacturing processes. Although the targeted companies have not been identified, many of them are believed to be Fortune 100 corporations that develop compounds and advanced materials (Finkle, 2011).

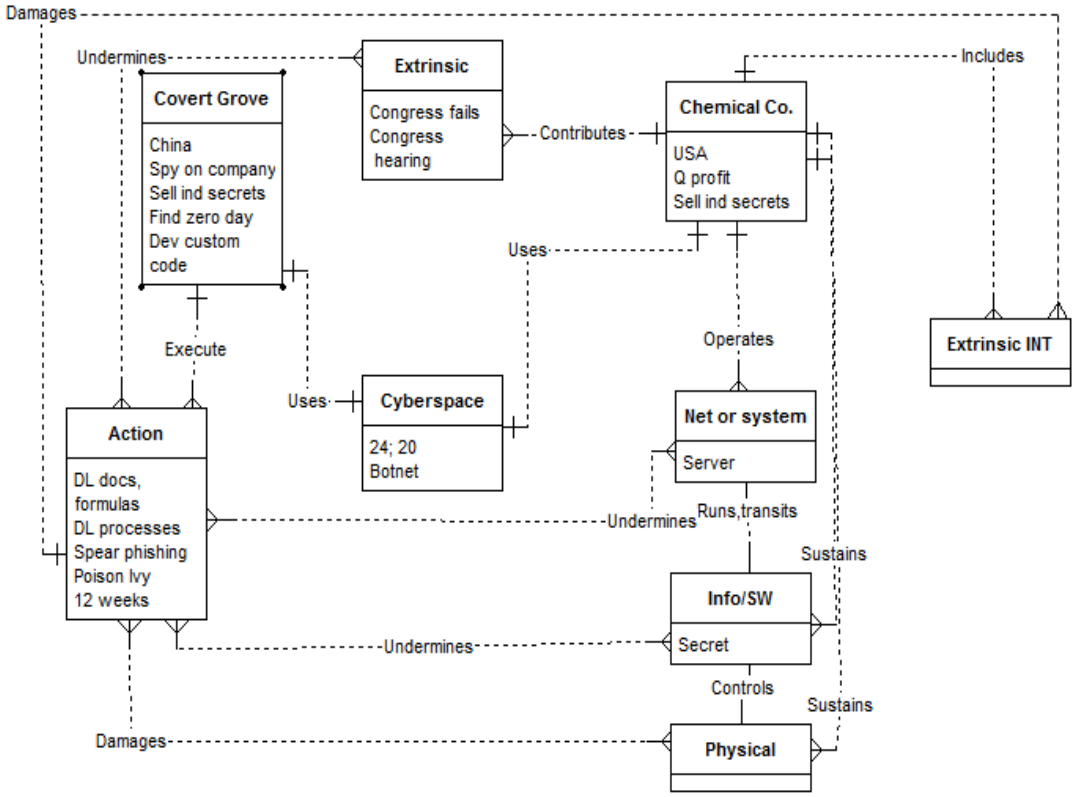
The Nitro attacks took place over a period of two and half months (Symantec, 2011). In total, 52 different IP addresses, belonging to organizations in over 20 countries, contacted a command control server with traffic consistent with malware. Data accessed during the Nitro attacks include, but are not limited to, information on compounds and advanced materials used primarily for military vehicles. A total of 24 command and control servers in different locations were used; most of the servers were located in the United States.

Malicious emails were sent to approximately 500 individuals. These emails came in the form of either a meeting invitation from an established business partner or a request for a necessary security update (Chien & O’Gorman, 2011). The emails contained an

executable attachment file. To the recipient of the email, the attached file either appeared to be a text file, based on the file's name and icon, or a password protected archive file which had a password provided in the email. In both cases, the executable file was a self-extracting executable containing PoisonIvy, a common backdoor Trojan.

The attacker knew familiar ploys to that would result in specific members of target organizations opening up compromised files.

Figure 6. A.4. Entity Relationship Diagram for Covert Grove_Chemical Company



References:

Chien,E., & O'Gorman,G. 2011. The Nitro Attacks: Stealing Secrets from the Chemical Industry,November 2011.

http://securityresponse.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

Finkle,J. 2011. 'Nitro' Attacks: China-Based Hacker Targeted Chemical Firms, Symantec Reports. October 2011.

http://www.huffingtonpost.com/2011/10/31/nitro-attacks-china-hacker-chemical-firms-symantec_n_1067978.html

Homeland Security News Wire. 2014. China syndrome: Chemical, defense companies subject to Chinese Nitro attacks, Homeland Security News Wire, February.

http://www.homelandsecuritynewswire.com/dr20140204-chemical-defense-companies-subject-to-chinese-nitro-attacks

O'Gorman,G., & Millington.T. 2011. Nitro attackers have some gall, December 2011.

http://www.symantec.com/connect/blogs/nitro-attackers-have-some-gall

Prince,B. 2011. Coordinated Cyber Attacks Hit Chemical and Defense Firms.October 2011.

http://www.securityweek.com/coordinated-cyber-attacks-hit-chemical-and-defense-firms

Symantec Security Response. 2011. The Nitro Attacks: Stealing Secrets from the Chemical Industry. Accessed January4, 2015:

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

5. CyberBunker_ Spamhaus Project

The Spamhaus Project (Spamhaus), a not-for-profit organization based in London and Geneva, compiles several widely used anti-spam lists. Many Internet service providers and email servers use the lists to reduce the amount of spam they accept.

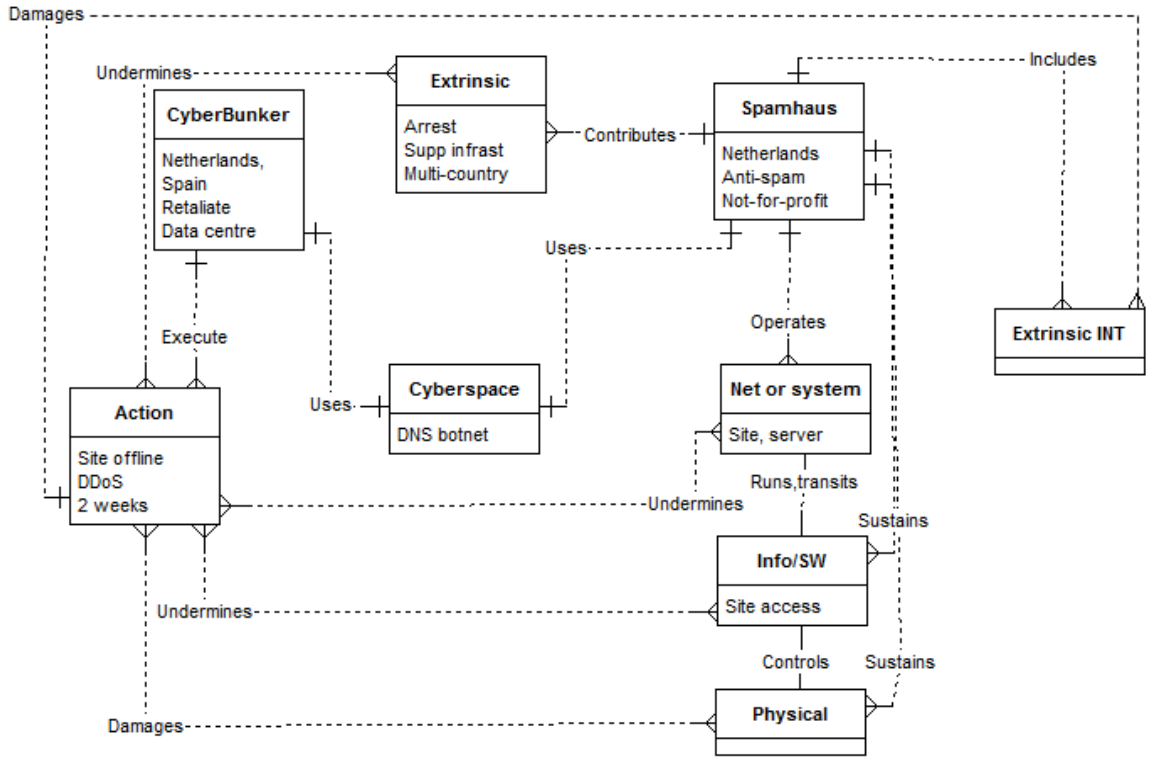
In March 2013, CyberBunker, a Dutch data centre, was added to the Spamhaus blacklist used by email providers to weed out spam. Starting March 18, Spamhaus was the target of a distributed denial of service (DDoS) attack exploiting a long-known vulnerability in the Domain Name System (DNS). The DDoS attack caused widespread congestion and jamming of crucial infrastructure around the globe. Millions of Internet users experienced delays in services and were unable to access websites (Perlroth & Markoff, 2013).

The DDoS attack overloaded Spamhaus' servers by flooding them with data. The attack was intended to take Spamhaus offline and put an end to its spam-blocking service.

The attackers conducted IP address spoofing. Whenever an Internet query was conducted, the victim's server was flooded with results, more data than it could handle. The amount of data being flooded at the website grew so large that it "threatened to clog up the Internet's core infrastructure and make access to the rest of the Internet slow of impossible" (Mimoso, 2014).

A 16-year-old southwest Londoner and the owner of CyberBunker, a 35-year-old Dutchman, were arrested in connection with the cyber-attacks (Bentham, 2013).

Figure 7. A.5. Entity Relationship Diagram for CyberBunker_Spamhaus Project



References:

Bentham, M. 2013. London schoolboy secretly arrested over 'world's biggest cyber attack'. Yahoo News, September 2013.

http://www.standard.co.uk/news/crime/london-schoolboy-secretly-arrested-over-worlds-biggest-cyber-attack-8840766.html

Mimoso, M. 2014. High-Volume DDoS Attacks Top Operational Threat to Businesses, Service Providers .January 29.

http://threatpost.com/high-volume-ddos-attacks-top-operational-threat-to-businesses-service-providers/103933

Perlroth,N., & Markoff,J. 2013. Firm Is Accused of Sending Spam, and Fight Jams Internet.The New York Times, March.

http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?pagewanted=all

6. Criminal_ Target

Attackers stole approximately 40 million credit card numbers and 70 million pieces of customer data (e.g., contacts) from the Target Corporation during the Christmas season of 2013 (Bill, 2014).

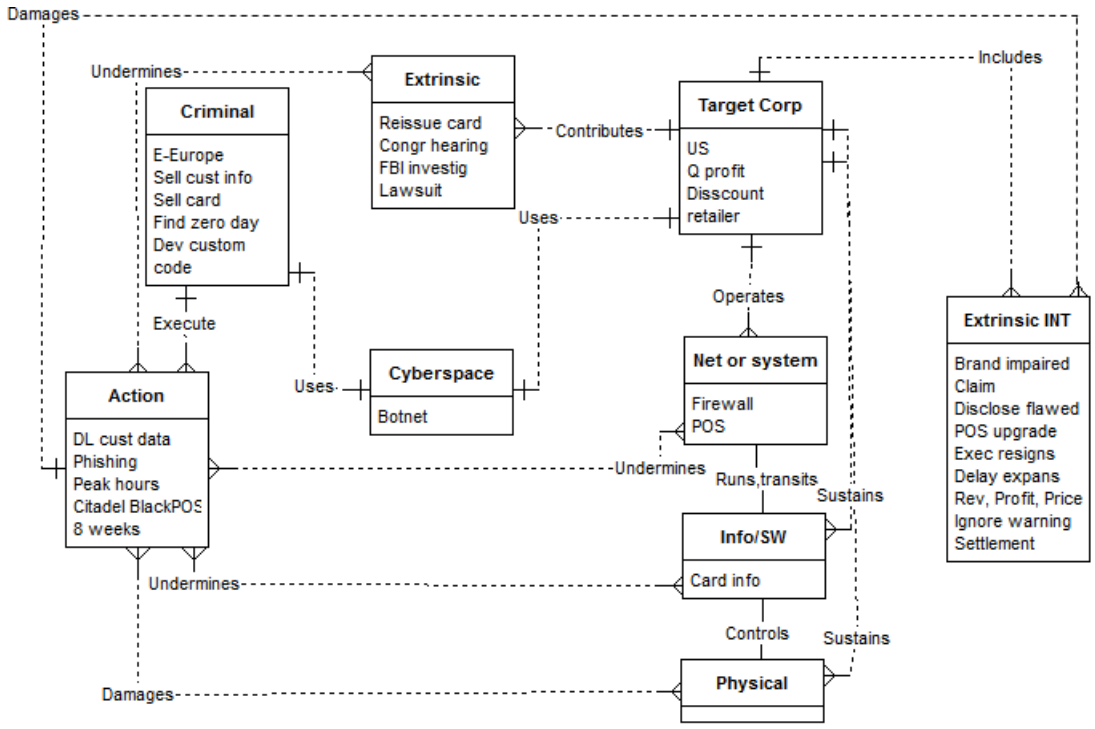
The malware used in the Target Corporation attack contained bits of Russian words. Therefore, the attackers are believed to be from Eastern Europe (RT, 2014). The attackers first breached the firewall using a phishing technique and then installed random access memory (RAM) scrapping malware on the point of sale terminals of the Target Corporation for the purpose of tapping data off its systems (Kerbs, 2014). Cybercriminals accessed customer data that was on transit in the computer memory. In memory the data shows as plain text, instead of encrypted data (Kerbs, 2014).

The code used in the attack was custom developed to execute the attack in the stores of the Target Corporation located in Canada and the US.

The data breach resulted in the delay of Target's expansion to Canada, reported losses of approximately US $1 billion, Target's share price dropping by 3.5%, the ousting of the CEO, and loss of consumer and investor confidence in the retailer (Finkle & Hosenball, 2014; Taylor et al., 2014).

The attack occurred during peak business hours – from 10 am to 5 pm, when malicious activities are hard to detect. Intruders were communicating with botnets through their command and control servers in order to upload stolen data from POS terminals (Tsukayama, 2014).

Figure 8. A.6. Entity Relationship Diagram for Criminal_Target



References:

Bill, K. 2014. Organizations Struggle with Evolving Cyber Threats. Business Insurance, May.
http://www.businessinsurance.com/article/20140511/NEWS07/305119988

Finkle. J. & Hosenball, M. 2014. More Well-known U.S. Retailers Victims of Cyber attacks – sources. Reuters, Business Insurance, January 12.
http://in.reuters.com/article/2014/01/12/target-data-breach-retailers-idINDEEA0B00W20140112

Kerbs,B.2014. A First Look at the Target Intrusion, Malware. January .
http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/

RT. 2014. Target Part of a Broader Cyber-Attack, Russian Hackers Allegedly Involved.January 17.
http://rt.com/usa/retailers-hacker-attack-russian-750/

Taylor, S., Cavale, S., & Finkle,J. 2014. Target's Decision to Remove CEO Rattles Investors. Yahoo News, May 2014.
http://news.yahoo.com/target-ceo-stepping-down-wake-devastating-cyber-attack-120451886--sector.html

Tsukayama, H. 2014. Security Firm IntelCrawler Says it has Identified Target Malware Author. Washington Post, January.
http://www.washingtonpost.com/business/technology/security-firm-intelcrawler-says-it-has-identified-target-malware-author/2014/01/17/258efa48-7fa4-11e3-9556-4a4bf7bcbd84_story.html

7. Gonzalez_TJX Companies

TJX Companies (TJX) announced that 94.5 million credit and debit card numbers of its customers were stolen in the U.S., Canada, and Puerto Rico between May 2006 and January 2007 (Roberts, 2007; Vijayan, 2007). The company network that handled credit card, debit card and other transactions had been breached (Roberts, 2007).

On March 25, 2010, Albert Gonzalez, a 28 year old Cuban-American was sentenced to 20 years in federal prison for gaining access to roughly 180 million payment-card accounts from the customer databases of TJX and some of the most well-known corporations in America (Verini, 2010). Gonzalez was working with 10 associates located in the United States, Eastern Europe, and China (Vijayan, 2007).

In November 2006, it was estimated that the security breach could cost TJX between $4.5 and $8.6 billion including fines, legal fees, notification expenses and brand impairment (Gaudin, 2007).

Gonzalez hired people to look for “war driving” targets. To identify vulnerable Wi-Fi networks, Gonzalez had individuals sit in cars or vans in the parking lots of big-box stores with laptops and high-power radio antennae. Once vulnerable networks were identified, Gonzalez would do the rest.

Gonzalez used associates to sell fake credit cards to buyers across the globe, in order to infiltrate their bank accounts at ATMs. The money collected at ATMSs through a third party, was either directly wired to Miami or sent to a PO box. To cover his money-laundering scheme, Gonzalez set up dummy companies in Europe, and opened e-gold

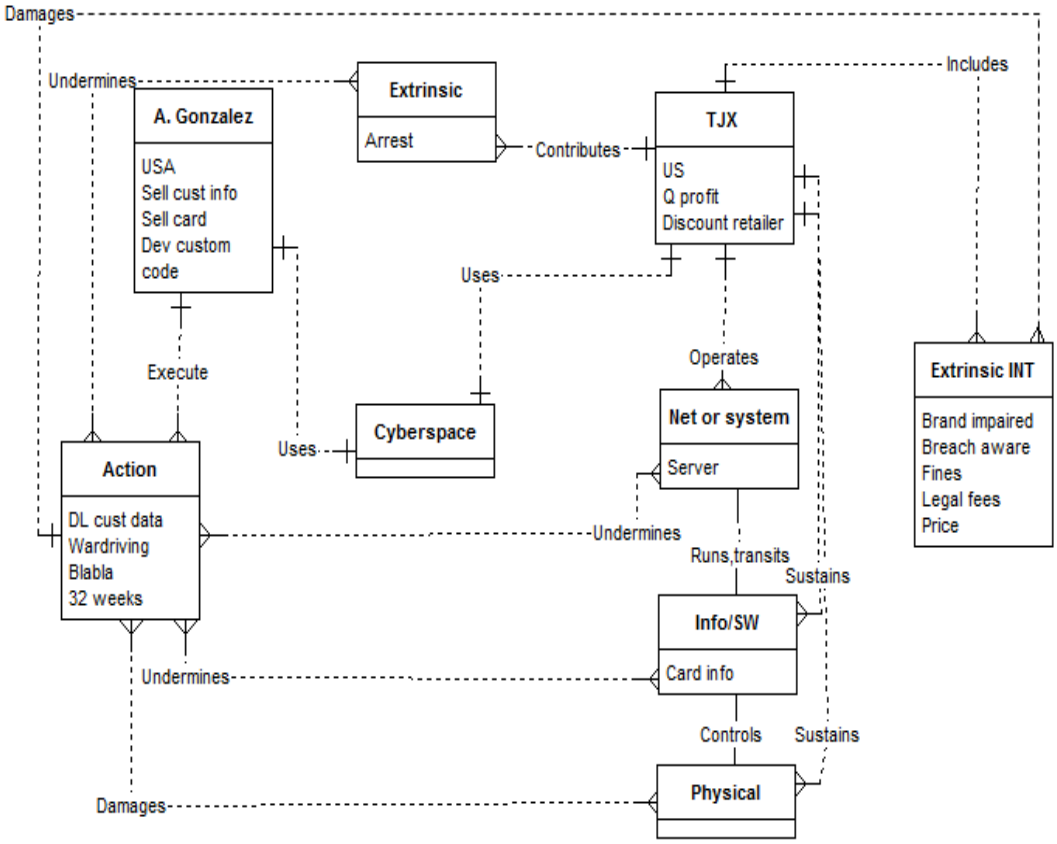
and WebMoney accounts. Gonzalez's hacking software and credit card data were stored on servers located in Europe.

At the time of the breach, TJX operated a wireless network that was less secure than a home network. Gonzalez was able to access TJX's servers due to the fact that the retailer used the Wired Equivalent Privacy (WEP) standard (The Office of the Information and Privacy Commissioner (OIPC) of Alberta, 2007). For 8 months the company had no idea that hackers had penetrated its network to steal approximately 98 million visa and master card accounts (Pepitone, 2014; Pereira 2007).

Even though the WEP was in the process of being converted into a more secure protocol at the time of the breach, WEP is an old protocol for wireless local networks, which can easily be intercepted by hackers.

Gonzalez's cyber gang motto was "Operation Get Rich or Die Trying." The main purpose for hacking into the TJX 's network was to make money.

Figure 9. A.7.Entity Relationship Diagram for Gonzalez_TJX Companies



References:

Gaudin, S. 2007. Estimates Put T.J. Maxx Security Fiasco At $4.5 Billion. InformationWeek. February http://www.informationweek.com/estimates-put-tj-maxx-security-fiasco-at-$45-billion/d/d-id/1054704?

Pepitone, J. 2014. TJX: 94 million. CNN, January. http://money.cnn.com/gallery/technology/security/2013/12/19/biggest-credit-card-hacks/3.html

Pereira.J. 2007. TJX in Security-Breach Deal. The Wall Street Journal, December. http://www.wsj.com/articles/SB119664612876511238

Roberts,P. 2007. Retailer TJX Reports Massive Data Breach. InfoWorld,January. http://www.infoworld.com/article/2661052/security/retailer-tjx-reports-massive-data-breach.html

The Office of the Information and Privacy Commissioner (OIPC) of Alberta. 2007. TJX Companies Inc. /Winners Merchant International L.P. September. https://www.priv.gc.ca/cf-dc/2007/TJX_rep_070925_e.asp

Verini,J. 2010. The Great Cyberheist. The New York Times,November. http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html?pagewanted=all&_r=1&

Vijayan, J. 2007. TJX Data Breach: At 45.6M card numbers, it's the biggest ever. ComputerWorld,March. http://www.computerworld.com/article/2544306/security0/tjx-data-breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html

8. Panin_User with Bank Accounts

SpyEye is a malicious software that enables criminals to first obtain victims' financial and identification files stored on their computers and then use this information to transfer money out the victims' back accounts into external accounts.

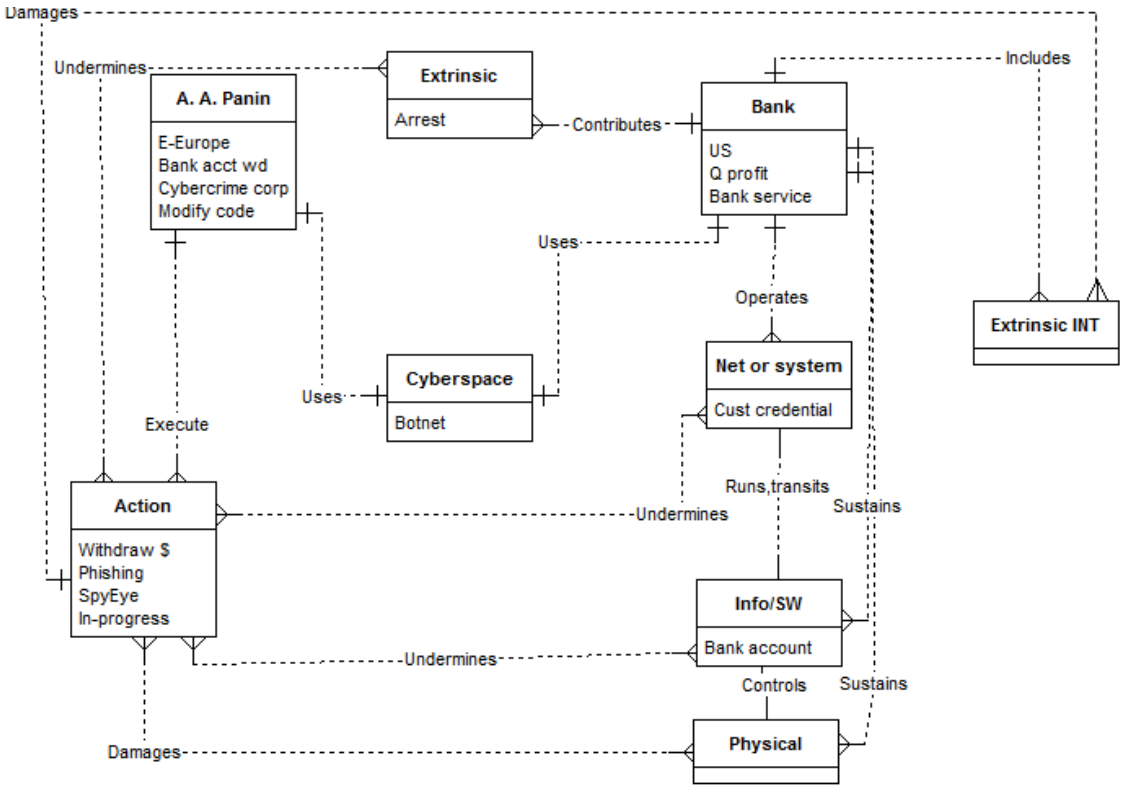
SpyEye was discovered in March 2011and it is was operated by criminals in Eastern Europe (Kirk, 2011). Aleksandr Andreevich Panin led the criminal group. Most of the victims were users in the United States. However, other victims were observed in countries such as the United Kingdom, Mexico, Canada, and India (Irinco, 2011).

SpyEye's cybercriminals are said to have generated revenue of $17,000 per day or $3.2 million dollars in 6 months (Irinco, 2011). SpyEye affected 253 financial institutions (Smythe & Beasley, 2014).

The main method that SpyEye uses to infect a user system is phishing attacks. These attacks result in the installation of SpyEye on a user's system, guaranteeing direct access to the individual's system. Once the malicious software is installed, it starts stealing banking credentials and information from websites such as Facebook, Twitter, Yahoo!, Google, eBay, and Amazon (Irinco, 2011). In order to steal additional information, SpyEye is capable of taking screenshots.

SpyEye is growing due to a botnet with a network of command-and-control servers in different countries (Kirk, 2011). According to SpyEye Tracker, a website which gathers information regarding SpyEye, 46 command-and-control servers are still online (Kirk, 2011).

Figure 10.A.8. Entity Relationship Diagram for Panin_User with Bank Accounts



References:

Irinco, B. 2011. Trend Micro Researchers Uncover SpyEye Operation. http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/87/trend-micro-researchers-uncover-spyeye-operation

Kirk,J. 2011. SpyEye Trojan defeating online banking defenses , ComputerWorld,July http://www.computerworld.com/article/2509482/security0/spyeye-trojan-defeating-online-banking-defenses.html

Smythe, C. & Beasley, D. 2014. SpyEye Russian Creator Pleads Guilty in Software Case. Bloomberg,January 2014. http://www.bloomberg.com/news/2014-01-29/spyeye-russian-creator-pleads-guilty-in-software-case.html

9. Bogachev_User of PC with vulnerabilities

Ransomware is malware that stops people from using their PCs and holds the PCs, or its files, for ransom (Microsoft Malware Protection Center, 2014). Since September 2003, ransomware named CryptoLocker has affected users of personal computers that operate Windows Vista, Windows 7, and Windows 8. CryptoLocker exploits vulnerabilities to hijack users' systems (Abrams, 2013). Most of the users affected are owners of personal computers who are located in the United States, the United Kingdom, and Australia.

The Federal Bureau of Investigation charged Evgeniy Bogachev, a Russian, for orchestrating the cybercriminal gang associated with CryptoLocker (Ward, 2014).

CryptoLocker first encrypts certain files on a personal computer and then displays a page on the screen that prompts the user to send a $100 to $300 ransom payment to decrypt the files (Gilbert, 2013). The screen also displays a timer stating that the user has 72 hours, or 4 days, to pay the ransom or the encryption key will be deleted. If the key is deleted the user has no way to decrypt his or her files. This ransom must be paid using MoneyPak vouchers or Bitcoins. Once the user makes the payment and it is verified, the program will decrypt the files that it encrypted.

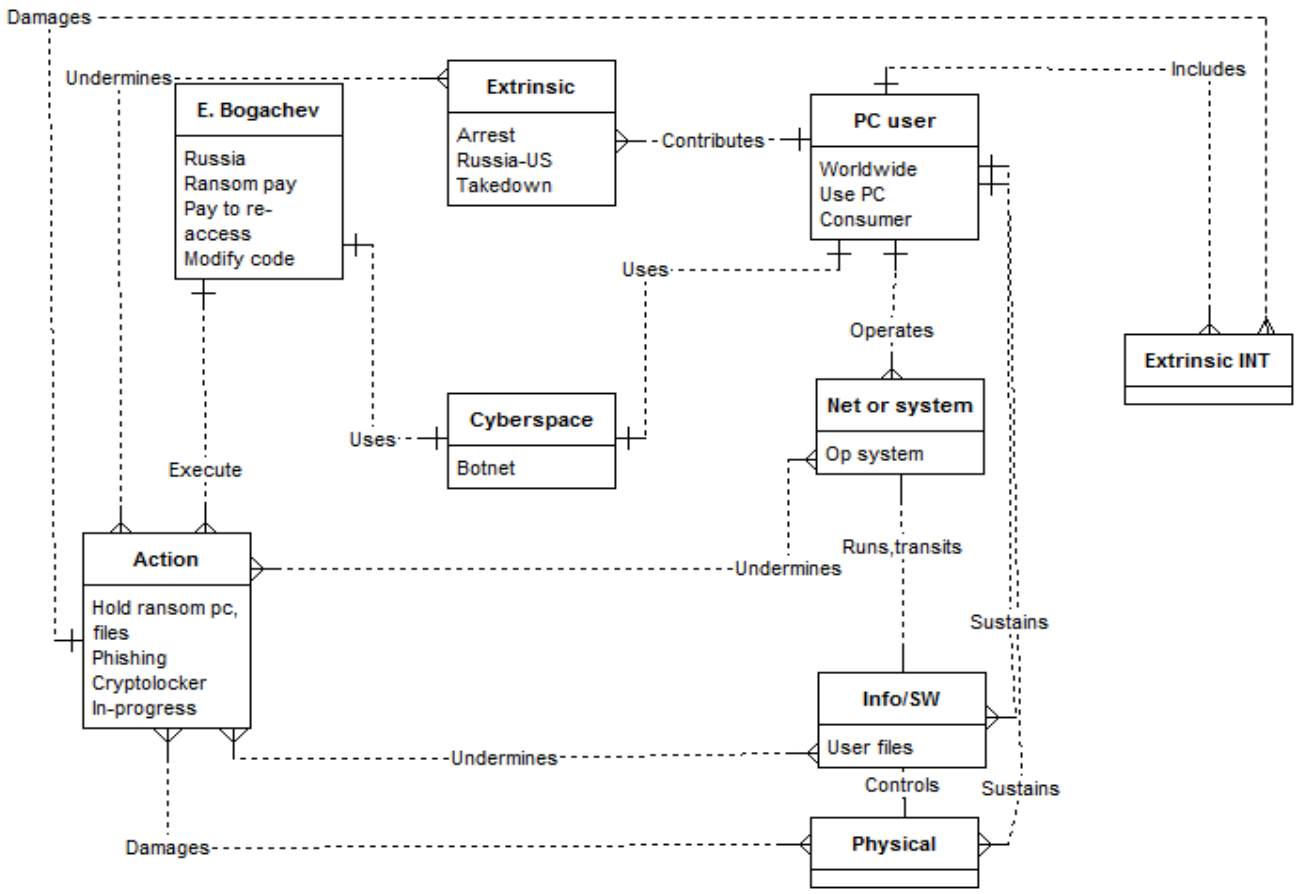
CryptoLocker has affected 200,000 to 250,000 systems (Jarvis, 2013).

The cybercriminals behind CryptoLocker use social engineering schemes to infect individuals' systems (Abrams, 2013). Messages are sent from accounts claiming to be

DHL, FedEx or UPS customer support asking users to open an attachment, which is usually in the form of Portable Document Format (PDF.)

Once a user opens the attachment, the system becomes infected and files on the system are encrypted (Abrams, 2013).

Figure 11 .A.9. Bogachev_User of PC with vulnerabilities



References:

Abrams, L. 2013. CryptoLocker Ransomware Information Guide and FAQ. October. http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

Gilbert, D. 2013. CryptoLocker Gang Earns Millions in Just 10 Days.International Business Times, December. http://www.ibtimes.co.uk/cryptolocker-criminals-earn-30-million-100-days-1429607

Jarvis, K. 2013.CryptoLocker Ransomware.December. http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/

Microsoft. 2015. Ransoware. Malware Protection Centre. http://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx

Ward, M. 2014. Cryptolocker Victims to Get Files Back for Free. BBC,August . http://www.bbc.com/news/technology-28661463

10. Winniti_Gaming company

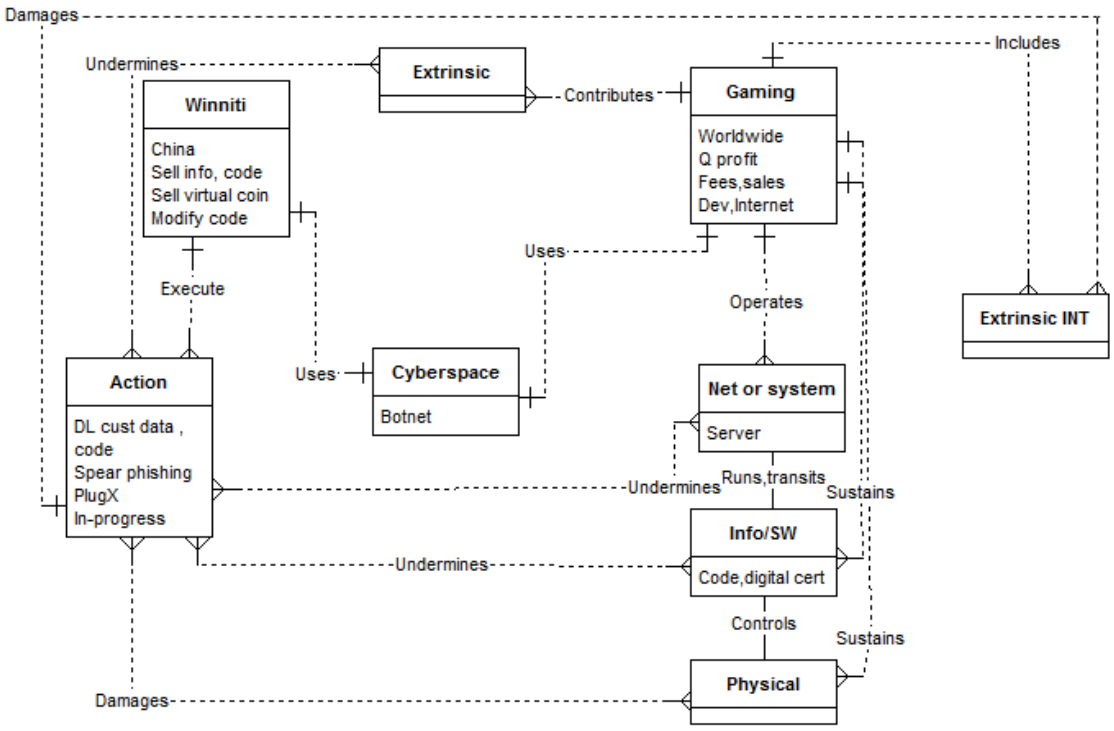
The cybercriminal group named “Winniti” has attacked at least 35 online gaming companies since 2009 (Kaspersky Lab Research, 2011). The Winniti group is based in China and it steals digital certificates and source codes from online gaming companies (Great, 2013).

To attack, Winniti uses spear phishing -- a targeted email scam designed to obtain unauthorized access to sensitive data and installation of malicious programs on the servers.

Criminals operate a large number of command and control servers and botnets to infect the servers.

Profit making motives drive the Winniti group to carry out cyber-attacks (Great, 2013). For example, Winniti profits from the collection of in game currency (gold) in online games, converting it to gold (virtual money) and then into real money (Great, 2013).

Figure 12. A.10. Entity Relationship Diagram for Winniti_Gaming Company



References:

Enzer, G. 2013. Cyber-criminal Gang Targets Online Gaming Industry. April. http://www.itp.net/mobile/593061-cyber-criminal-gang-targets-online-gaming-industry

Kaspersky Lab. 2013. Winniti. More than Just a Game. Kaspersky Lab Accessed January 4. http://securelist.com/analysis/internal-threats-reports/37029/winnti- more-than-just-a-game/

Appendix B. Information used to produce Entity Relationship Diagrams for Cyber-attacks

1-10 scenarios	1 Google	2 Natanz Fuel Enrichment Plant	3 NY Times	4 Chemical company	5 Spamhaus Project	6 Target	7 TJX Companies	8 User with bank accounts	9 User of PC with vulnerabilities	10 Gaming Company
Adversary 1										
Name	Elderwood Gang	Israel, USA	Chinese military	Covert Grove	CyberBunker	Criminal	A. Gonzalez	Aleksandr Andreevich Panin	Evgeniy Bogachev	Winniti
Location	China	Israel, USA	China	China	Netherlands, Spain	E-Europe	USA	E-Europe	Russia	China
Motivation	Warn operatives	Sabotage	Find informant	Spy on company	Retaliate	Sell cust info	Sell cust info	Bank account WD	Ransom pay	Sell info, code
Business model	State $	State $	State $	Sell ind secrets	Data centre	Sell card	Sell card	Cybercrime corp	Pay to re-access	Sell virtual coin
Capacity	Find zero day	Find zero day	Find zero day	Find zero day		Find zero day				
	Dev custom code	Dev custom code	Dev custom code	Dev custom code		Dev custom code	Dev custom code	Modify code	Modify code	Modify code
Action										
Objective	DL surveillance info	Destroy centrifuge	DL employee password	DL docs, formulas	Site offline	DL cust data	DL cust data	Withdraw $	Hold ransom PC, files	DL cust data, code
	DL email			DL processes						
Approach	Spear phishing	Removable disk	Spear phishing	Spear phishing	DDoS	Phishing	Wardriving	Phishing	Phishing	Spear phishing

						Peak hours				
Malware	Hydraq	Stuxnet	Unidentified	Poison Ivy		Citadel,BlackPOS	Blabla	SpyEye	Cryptolocker	PlugX
Duration	28 weeks	32 weeks	28 weeks	12 weeks	2 weeks	8 weeks	32 weeks	In-progress	In-progress	In-progress
Extrinsic										
Arrest					Arrest		Arrest	Arrest	Arrest	
Claim						Reissue card				
Declaration				Congress fails						
Gov				Congr hearing		Congr hearing				
Gov-Gov	China-US	Iran-US/Israel	China-US						Russia-US	
Internet					Net clogged					
Support infrast					Supp infrast					
Law enforce ag	FBI investig				Multi-country	FBI investig			Takedown	
Legal						Lawsuit				
Retaliation		DDoS US firms								
Cyberspace										
CC; countries	Many; 5	4; 4	?; 1	24; 20						
Botnet	Botnet		US univ botnet	Botnet	DNS botnet	Botnet		Botnet	Botnet	Botnet
Adversary 2										
Name	Google	Natanz FEP	New York Times	Chemical	Spamhaus Proj	Target Corp	TJX	Bank	PC user	Gaming company
Location	USA	Iran	NY, China	USA	Netherlands	US	US	US	Worldwide	Worldwide

Motivation	Q profits	Nuclear weapon	Report facts	Q profit	Anti-spam	Q profit	Q profit	Q profit	Use PC	Q profit
Business model	Int service product	State $	Daily paper	$ from IP	Not-for-profit	Discount retailer	Discount retailer	Bank service	Consumer	Fees, sales
Capacity	Dev, Internet									Dev, Internet
Net or system										
Entry	Search engine code	Supplier link	E-mail server	Server	Site, server	Supplier link	Server	Cust credential	Op system, application	Server
						POS				
Info/SW										
Target	DB for Gmail	7 PLC	Passwords	Secrets	Site access	Card info	Card info	Bank account	User files	Code, digital cert
	Wiretapping info		Corruption info							
Physical										
Target		Centrifuge								
Extrinsic INT										
Brand						Brand impaired	Brand impaired			
Claim						Claim				
Disclosure						Disclose flawed	Breach awareness			
Equipment		Equip replaced				POS upgrade				
Executive						Exec resigns				

Expansion	Pullout			Delay expans	
Fines					Fines
Legal fees					Legal fees
Partners			Mandiant, ATT, FBI		
Performance		Emp productivity		Rev, Profit, Price	Price
Process				Ignore warning	
Settlement				Settlement	