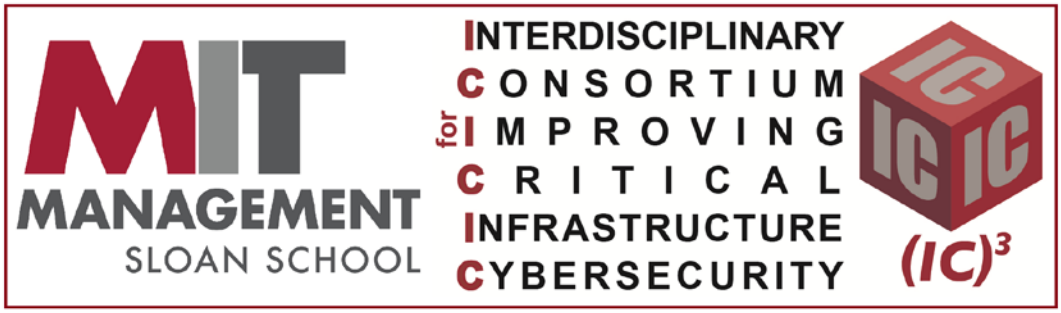

Cyber Warfare Conflict Analysis and Case Studies

Mohan B. Gazula

Working Paper CISL# 2017-10

May 2017

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Cyber Warfare Conflict Analysis and Case Studies

By

Mohan B. Gazula

M.S., Computer Science
Boston University

Submitted to the Systems Design and Management Program
in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology
June 2017

Signature of Author .....

MIT Sloan School of Management
Department of Electrical Engineering and Computer Science
May 12, 2017

Certified by .....

Stuart Madnick
John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management &
Professor of Engineering Systems, MIT School of Engineering
Thesis Supervisor

Certified by .....

Allen Moulton
Research Scientist, Sociotechnical Systems Research Center, MIT
Thesis Supervisor

Accepted by .....

Joan S. Rubin
Executive Director and senior lecturer, System Design & Management

THIS PAGE INTENTIONALLY LEFT BLANK

Cyber Warfare Conflict Analysis and Case Studies

By

Mohan B. Gazula
M.S., Computer Science
Boston University

Submitted to the Systems Design and Management Program
in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Engineering and Management

Abstract

"The supreme art of war is to subdue the enemy without fighting."
- Sun Tsu from "The Art of War" Believed to have lived between 770 and 476 B.C

In the age of code wars, have our lives changed for the better? Are we any safer than the bloody wars or the cold wars from the past? Is there any more guarantee now in a cyber age than in a kinetic age involving human forces? These are the types of questions that have little answers due to the secret nature of the operation. State-sponsored activities are commonplace. Whenever there is involvement by a state, the stakes are higher, and loss of life can never be ruled out.

The objective of this thesis was to research historical cyber-warfare incidents from the past to current and map the relevant cyber-warfare data in a well-known framework called CASCON, which is a history-based conflict analysis and decision-support system. The CASCON-based analysis for cyber incidents revealed a larger picture of the world we live in and how easily that world could change.

The information contained in this thesis is not meant to be conclusive, but a study of state-sponsored cyber cases using MIT's CASCON to map and categorize information for future learning about conflicts involving states. It is the purpose of this thesis to (a) research historical cyber-warfare incidents and (b) map cyber-warfare incidents into a framework.

Thesis Advisor: **Stuart Madnick**
Title: John Norris Maguire Professor of Information Technology, MIT Sloan School of Management & Professor of Engineering Systems, MIT School of Engineering

Thesis Advisor: **Allen Moulton**
Title: Research Scientist, Sociotechnical Systems Research Center

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I was fortunate to have Professor. Stuart Madnick and Allen Moulton as my advisors, and I am profoundly grateful for their support and guidance during the process of writing my thesis. Professor Madnick believed in me and was always available whenever I ran into a trouble spot or had a question about my research or writing. He consistently allowed this paper to be my own work, but steered me in the right direction by motivating me to plan on my thesis early and deliver an excellent product. His expertise and feedback on cyber security has been a guiding light throughout my research work.

Mr. Moulton brought life to my thesis with his expertise on international conflict management, kinetic and cyber warfare along with his experience on various research topics. He being one of the original authors of CASCON helped me tremendously. He also helped me gain momentum towards completing my thesis with a pragmatic approach. I enjoyed having discussions with Allen and benefited from his detailed views on many topics including kinetic warfare and CASCON. Thank you, Professor Madnick and Mr. Moulton in helping me create a robust and quality product. I truly appreciate your advice, time and confidence in me.

Patrick Hale (Former Executive Director of SDM) was always available and provided me with advice and support to work through challenges and believed in me. Thank you, Pat for being available and providing guidance. Thanks to Joan S. Rubin (Executive director and senior lecturer of the Massachusetts Institute of Technology's System Design & Management program) for her tremendous guidance and approachability. Thanks to Triet Nguyen, Bill Foley and Amal Elalam for all their financial, curriculum and administrative advice throughout the duration of the program.

I am grateful to General Dynamics Mission Systems for their support in helping me complete my master's degree program.

Inspiration provided by my parents has enabled me to achieve goals throughout my life. My father, an entrepreneur and visionary, taught me to dream big and think ahead in everything I do. My mother was an exemplary to hard work and patience. My wife, Kavitha, whose inspiration, support and approach to life is second to none. My son, Pratik, and daughter, Kimaya, have been the source of my energy. My two sisters, Kala and Leka, have shown unconditional support for anything I have set out to do in my life.

"The true goal of action is knowledge of the Self."
— The Bhagavad Gita

THIS PAGE INTENTIONALLY LEFT BLANK

Dedicated

To my
Dear Wife - a Noble Family Physician, a Professor and
an
Entrepreneur

Dr. Kavitha Gazula M.D., ABIHM

to my

Dear Son Pratik and Dear Daughter Kimaya

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

List of Figures

List of Tables

1. Motivation

Every new technology presents the possibility of new weapons, and for every new weapon there's a soldier hoping it will yield the ultimate advantage, although few ever do. Many a tome has been dedicated to the power of navies and air forces to change the face of warfare. Nuclear weapons have further complicated the picture, creating a top tier power overshadowing the conventional conflict. Today's net-centric world proffers a new weapon. To many, cyber-warfare represents the 5th battle-space—a new type of warfare in need of further definition. To others, it is merely a new weapon to be integrated into traditional conflict.

It is hardly an overstatement to say that the advent and global expansion of the Internet may prove to become the fastest and most powerful technological revolution in the history of mankind. In just 15 years, the number of individuals actively using the Internet has skyrocketed from an estimated 16 million in 1995 to more than 3.5 billion in 2017[W2]. Today, states, non-state communities, businesses, academia and individuals have become interconnected and interdependent to a point never imaginable before. At the same time, military reliance on computer systems and networks has increased exponentially, thus opening a "fifth" battle-space of war-fighting next to the traditionally recognized domains of land, sea, air and outer space. This trend raises the question: to what extent can existing international laws be transposed to the cyber domain? Without any doubt, as a matter of principle, existing international law governs state activities wherever they are carried out, including in cyberspace. However, applying pre-existing legal rules, concepts and terminology to a new technology may entail certain difficulties in view of the specific characteristics of the technology in question. It seems apparent that we are in that difficult sliding window of deciding which international governing laws apply to cyber-warfare and how much of it really applies. Cyberspace is now considered a subject of high politics[5] due to matters such as national security, core institutions and decision systems critical to the state, its interests and its underlying values.

A number of instances had surfaced over the past 35 years suggesting involvement of one nation in a cyber-attack toward another nation. The recurrences of such instances motivated me to research and capture them as a case and then apply a framework that would help in providing useful insights. CASCON gave me such a framework as it had already captured over 85 cases in kinetic warfare. I started to research cases that fell into the category where actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption, this is also defined as "cyber-warfare".[W1]

1.1 Use of Cyberspace

Cyberspace has become an indispensable part of a state, a society and the life of individuals due to the rapid development and extensive application of information technology. Together

with its convenience, cyberspace has also posed an increasing number of potential risks and challenges. To seek superiority in cyberspace, many countries that are advanced in information and communications technology (ICT) have formulated cyberspace policies and strategies. To understand cyberspace, we could use the layered model as outlined by David D. Clark, namely, (1) the physical foundations and infrastructures that enable the cyber playing field, (2) the logical building blocks that support the physical platform and enable services, (3) the information content stored, transmitted or transformed, and (4) the actors, entities and users with various interest who participate in this arena in various roles.

There is much in this new world that challenges the state, but in the cyber-domain, boundaries are permeable, and information, ideas, interests and the like can circulate with little regard for territory or jurisdiction. This means that the usual instruments of the state are not always transferable for use in the cyber-arena. But the state is adapting. States are developing and deploying new instruments of control, and in many cases they clearly aspire to become the major player in the cyber-arena[5]. Preparations for cyber-warfare have become an important part of army-building in quite a few countries. Besides nation-states, non-state actors have also taken advantage of the vulnerability and interconnectivity of the cyberspace to inflict enormous damage to countries and societies.

The cyber-attacks that Estonia, Georgia and Ukraine suffered, as well as the U.S. PRISM spying scandal exposed in 2013, have demonstrated that there is increasing difficulty in maintaining order and security in cyberspace. However, despite preparations for cyber-warfare by various countries and cyber-intrusions by individuals, there is still a lack of international laws governing cyberspace, especially the law for cyberspace arms control. Since some countries enjoy an advantaged position in information technology, they are unwilling to talk about restraints on cyber-activities. Against such a backdrop, it has become an urgent necessity to formulate international rules and improve the international law system in order to counter cyber threats, maintain order and security in cyberspace, and regulate cyber activities. Cyberspace arms control has also become an important part of the international arms control and disarmament.

Since the early 1970s, the United States has been a leader in information technology. By drawing on its advantaged position in information technology and sufficient funding, it has developed a relatively complete set of policies and strategies for cyberspace and is accelerating its pace in building cyber-forces and carrying out theoretical research on cyber-warfare. As one of the major creators of the international order after World War II, the United States plays an irreplaceable role in international arms control and disarmament. Every single measure and action it takes in cyberspace will inevitably have a bearing on the development of international cyberspace arms control in the future.

During my research on cyber-warfare it seemed critical to understand the current situation of cyberspace and then discuss cyber-warfare. Specifically, cyber-warfare's potential to occur in the international community, the restraints on cyber-warfare imposed by existing international laws and, importantly, the potential flaws in these laws. The focus of this thesis however is to collect relevant cyber-warfare information and map it into a framework and hence the governance aspects are not covered. The information collected may help

understand the boundaries that are crossed in cyber-warfare and the abuse of cyberspace that are caused by or result in international conflicts. Although superpower states like the United States and China seemed to be working toward the establishment of a new type major power relationship, cooperation in cyberspace should be an important part of that endeavor.[42][48]

With respect to cyber-war preparedness, cyberspace arms control and the superpower states, whatever methods of production humankind adopts, the corresponding form of warfare will appear. With the development of information technology (IT), cyberspace is becoming another battlefield following the land, sea, air and outer space. The Internet has become an integral and important part of a state, a society and the daily life of individuals. Moreover, it has gained momentum for further development. However, together with the conveniences the Internet has brought, it has also entailed an increasing number of potential risks and challenges. For example, the number of cyber-attacks in 2011 increased by 36% as compared with that in 2010, and the amount of malicious software increased 41% during the same period. A white paper[48] written on national defense in China and around the world, issued in 2013, points out, "Changes in the form of war from mechanization to informationization are accelerating. Major powers are vigorously developing new and more sophisticated military technologies so as to ensure that they can maintain strategic superiorities in international competition in such areas as outer space and cyberspace."

Just as in other domains, to maintain order in cyberspace is becoming the international community's consensus. An American scholar argues that the command of cyberspace in the 21st century is as decisive as the command of the sea in the 19th century and the command of the air in the 20th century. With only about 50 years of history, the Internet is expanding globally at an extraordinary speed. Cyberspace has become a new platform for political, economic, military and cultural interactions, as well as a significant domain that influences social stability, national security, economic development and cultural communication.

1.2 The Cyber-battlefield

There exists a larger problem with the evolution of non-kinetic warfare as a form of low-intensity conflict during peacetime. While non-kinetic warfare offers the potential for impact without loss of life, it also broadens the battlefield in a fashion that has not been seen since the advent of the airplane. Even worse, it has extended the theater of combat to organizations that have never before been responsible for defending themselves against nation-state aggressors. Most conflict around the world is considered "low-intensity," meaning that it takes the form of guerrilla warfare, insurgency, special operations and other such means. Even recent wars between the United States and its enemies in Iraq and Afghanistan may be considered this, from the perspective of its enemies, since they themselves do not engage in large military maneuvers on defined fronts. The days of two large armies amassing their forces to face off on a battlefield with clear battle lines are no more, except between two smaller powers in a regional conflict of only local interest.

What this means in broader terms is that the world's major powers have an incentive and model through which to conduct non-kinetic warfare against potential adversaries, even in peacetime. Between themselves, this category of nation-states typically participate in low-intensity conflict through clandestine operations and special warfare to avoid becoming enmeshed into full-fledged conflict, and the additional deniability that inevitably comes from information warfare makes cyber-warfare an attractive means of conflict. Furthermore, the overwhelming military superiority of the United States—in terms of kinetic warfare—provides an equally overwhelming incentive for smaller nations to adopt cyber warfare for other reasons. Simply put, cyber-warfare provides an economically cheap means of asymmetric warfare that is unlikely to incur a conventional military response from a much larger power.

A cyber-attack and cyber-defense can be conducted at the state level by the military or can be conducted at the personal level by an individual. It can be a simple hacking attack, or a long-term, large-scale and state-launched operation aimed at damaging the infrastructure of an enemy state so as to achieve the strategic purpose of paralyzing the running of that state, or purely an espionage-level activity with an ulterior motive. There is no unequivocal definition of cyber-attack yet, but it generally refers to unauthorized intrusion into a computer or a computer network in such forms as tampering, denial of service, data theft and server infiltration. The emergence and development of the non-state cyber-groups that are obviously politically oriented, such as Anonymous, and other cyber-crime groups also add to the complexity of cyber-attacks.

It is believed that all the top 15 countries around the world in terms of military budget are developing cyber-offensive and defensive capabilities. In 2011, among the 193 UN member states, 68 countries had cyber security projects. However, in 2012, the number of such countries increased to 114, among which 47 countries had military cyber-security projects [42]. These 47 countries are assessing their military capabilities in cyber-security while developing corresponding military theories. Against such a background, cyberspace arms control is becoming an important part of international arms control and disarmament. However, the number of current measures for arms control in this area is almost zero, which further highlights the importance of international negotiations on the code of conduct in cyberspace as soon as possible so as to develop a treaty to regulate international cyber-activities. The developed countries headed by the United States have formulated relatively complete systems of cyber-warfare policies and strategies by making full use of their advanced information technology and sufficient funding. In addition, they are accelerating their pace in building cyber forces and conducting theoretical research on cyber-warfare.

As one of the major creators of the international order after World War II, the United States plays an irreplaceable leading role in international arms control and disarmament. Every single measure and action it takes in cyberspace will inevitably have a bearing on the development of international arms control in cyberspace in the future. Several reports have been published to date that define the rules of engagement in cyberspace and how to prevent international conflict. Unfortunately, the operative mode adapted by states involved in cyber-warfare has been clandestine and this precludes the need for rules of engagement.

Scott J. Shackelford, however, reckons [42] that cyber-attacks are broken down into four categories: cyber-terrorism, cyber-war, cybercrime, and cyber-espionage. Although virtually every terrorist group has a web presence, true cyber-terrorism remains rare, and there has not yet been a genuine cyber-war. He believes that the most pressing problems are cybercrime and cyber-espionage. Michael Glennon observes[42] that any form of cyber-attack is a kind of cyber-intrusion, and the danger of cyber-intrusions should not be underestimated since James Adam, a U.S. military forecaster, once predicted that "the computer would be a weapon in future wartime, and there would be no virtual front line as traditional battles have, and that bits and bytes would replace bombs and bullets as the crucial instrument to seize control of the battlefield." The RAND Corporation also pointed out in one of its reports [43] that "the strategic war in the industrial age is nuclear war, while in the information age, the strategic war is mainly cyber-war." In fact, the United States has prepared for cyber-conflicts for a long time. To confront possible cyber-attacks or cyber-warfare, it has, in recent years, sped up its efforts and pace in forming cyber-forces and given full play to its advantages in technology, policy and management mechanisms.

No longer can we ignore cyber-weapons. Cyber-attacks and cyber-warfare have entered into the arsenal of modern warfare. Where and when the next attack will be launched is anyone's question. The only thing for sure is there will be more.

1.2.1 Operational Boundaries of Cyber-warfare

Battle-space is a term used [w1] to signify a unified military strategy to integrate and combine armed forces for the military theater of operations, including air, information, land, sea and space to achieve military goals. It includes the environment, factors and conditions that must be understood to successfully apply combat power, protect the force or complete the mission. This includes enemy and friendly armed forces, infrastructure, weather, terrain and the electromagnetic spectrum within the operational areas and areas of interest. While we focus on the information to understand the operational boundaries of cyber-warfare, we need to first lay out the landscape of traditional warfare. Military planners have traditionally divided war-fighting capabilities into four domains. These domains are used to develop strategies and tactics, as well as to organize forces. In fact, most modern militaries are organized according to the following domains:

1.2.1.1 Land Operations

The oldest domain in warfare consists of any fighting force on the ground. Land forces include infantry, cavalry, armored vehicles, antiaircraft batteries and artillery. In the U.S. military, the United States Army primarily controls the land domain.

1.2.1.2 Sea Operations

This domain of warfare is fought on oceans, rivers and seas. The sea domain includes all of a nation's naval forces. In the U.S. military, the United States Navy controls the sea domain.

1.2.1.3 Air Operations

This domain of warfare is fought in the sky. The air domain includes fighters, bombers, reconnaissance aircraft, cargo planes and fuel tanker aircraft. After World War II,

responsibility for the air domain in the U.S. military, transferred from the Army to the Air Force.

1.2.1.4 Space Operations

With the advent of space flight, the military added space as a domain of warfare. The primary operations in this domain include satellite operations and the use of intercontinental ballistic missiles. In the U.S. military, the space domain is a mission of the Air Force.

1.2.1.5 Cyber Operations

During the early stages of cyber-warfare, planners struggled with placing the cyber-mission into these domains, and each service claimed responsibility for a portion of the mission. In 2010, a panel conducting the quadrennial defense review for the U.S. Department of Defense (DoD) concluded the following:

Although it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air and space. Cyber is a domain of warfare as significant as the other domains. As the newest domain of warfare, it is the least understood. Military planners specializing in land and sea operations have millennia of military history to draw upon when developing plans and strategies. Air and space have shorter histories as war-fighting domains, but have still existed for over half a century. The cyber-domain is much newer; military plans simply have not adapted fully to this new way of fighting.

Figure1: Cyber, the fifth domain

1.3 The Data Weapon

The concept of attacking a cyber-infrastructure using logical bombs is not difficult to grasp, but simply performing such attacks for their own sake fails to elevate one's effect (or relevance) above that of the chaos-inducing cyber-partisans. The true benefit of any form of warfare lies in its integration with other forms. This is an already established doctrine in terms of kinetic warfare doctrine, whereby troops on the ground move forward after aerial

attacks have severely damaged enemy emplacements, which in turn were first observed using various reconnaissance and intelligence-gathering methods. While attacking, the troops have the ability to call upon artillery strikes, close air support or armor to support their mission. This is known as "combined warfare" and is the norm on today's battlefield. But what happens when the concept of information—both as a weapon and as an objective to be attacked or captured—comes into play?

There exist two primary objectives that compete for primacy in the context of information warfare. One is the control of information, either in the sense of gaining access to it or denying access to it. The other is influence over that information. The two concepts may sound vague and unrelated to warfare until one considers the way in which they can be applied. For example, denying access to information could take on the form of using logical attacks to cause an air defense system's radar to show data that may not be accurate; if the enemy cannot perceive the intrusion into its airspace of an invading force, that becomes a tactical advantage to the invader as it would provide obscure the scale and composition of the attack while maintaining total surprise until the last possible minute. If the same effect were to be sought using kinetic warfare, such as bombing the radar installations, then the element of surprise would be lost, and the only benefit would be denial of information about how the attack was progressing at the early stages.

The influence factor applied against the information would cause the radar systems to register false positive at times, showing things that are not there. Eventually, the information produced by the radar systems would be considered so unreliable as to be nearly worthless, thus degrading the quality of decisions made based upon that data. This seems like the lesser of the two approaches until one recognizes that it is far easier to make fake objects show up on a screen than it is to selectively hide the ones that you wish to keep hidden.

It is not considered a more aggressive act to attack a bank or other civilian target (counter-value) than it would be to restrict the scope of an attack on military targets (counterforce), for example. In fact, the result of this aspect of doctrine tends to favor attacks against private organizations for the numerous reasons listed earlier. Furthermore, this reality has been acknowledged by leading members of the Chinese cyber-warfare community on many occasions.

1.4 Evolution of Cyber-warfare and Cyber-conflict

Throughout history, civilian commercial entities have not been the primary targets of warfare and have even been avoided as targets. In the earliest days, groups existed that did not make feasible targets in and of themselves. Such organizations existed within the physical boundaries of nation-states, such that attacks upon them could only be conducted within the scope of much larger, comprehensive attacks upon the nation-states themselves, or the castles and cities in which they were located. The concept of weakening an enemy by focusing on causing economic impact exclusive of significant loss of life simply did not exist, and even if one were to focus military efforts on disruption of commercial activity, it inevitably involved a focus on killing civilians. In those days, the only means of warfare was

kinetic warfare using spears, swords, ballistic weapons, explosives and so on. Non-kinetic warfare, also known as cyber-warfare, was not an option as there simply was no digital infrastructure through or against which to leverage attacks.

Trade, both between and within nation-states and cities, was conducted using material goods, which in and of themselves were transported by people. As a result, the notion of warfare, even for the specific purpose of halting or impeding such trade, necessarily involved direct attacks on civilians. This fact remained in effect from the feudal era on until the late twentieth century, a time when warfare (especially aerial warfare in general and bombing in particular) allowed for the capability to target commercial entities. The Fourth Geneva Convention, abbreviated as GCIV, one of the four treaties of the Geneva Conventions and adopted in August 1949, primarily defined humanitarian protections for civilians in a war zone. There have been exceptions to the degree with which nations have followed the Geneva Conventions, but these exceptions have tended to stand out as just that: exceptional events, accidents (such as a bomber crew targeting the wrong building through genuine human error), or the misbehavior of nation-states that were judged to be barbaric for their actions. Despite these outlying events, the general fact has been that nations have sought to target counterforce (military) targets and avoid damage to counter- value (civilian) targets.

As kinetic warfare has evolved, this differentiation has only grown. The advent of precision-guided munitions has reduced the civilian death toll from bombing raids to numbers so low as to be unimaginable during earlier conflicts. Where once entire neighborhoods would be bombed in the course of attacks on a single building of military value, it is now considered a tragedy if a single civilian building is destroyed as a result of human error or incorrect information. In a sense, the protection of civilian industry was a beneficial side effect of the Geneva Conventions, given the fact that one could not deliberately attack a commercial enterprise without physically harming or killing its employees. Such organizations also experienced reduced risk from their geographic distance from theaters of warfare, and their attack surface was relatively small compared to that of the military itself. A shop owner need not fear the destruction of his business by a war that was fought thousands of miles away.

In the late twentieth century, this began to change. Now, as the methods, processes and doctrine around cyber-warfare have evolved, the above-described world has nearly reversed itself. Attacks using non-kinetic means are nonlethal in nature and do not even incur physical harm; as such, the Fourth Geneva Convention does not apply. Furthermore, while the IT infrastructure of the military is often sequestered (with varying success, admittedly) into enclaves, private industry is heavily interconnected with a great deal of exposure to the digital world and all of its inhabitants.

There are several things about cyber-warfare that differentiate it from hacking related to other motivations. Originally, hackers (or "vintage hackers") were people with extraordinary expertise and talent, but typically altruistic motivations. It was not uncommon for a hacker to notify the sysadmin of a compromised system as soon as a hack was successful, both informing them of the way they gained access and of how to prevent it in the future. The key motivation was a quest for knowledge and greater expertise, combined with a lack of a legitimate outlet for their skills. While their actions were unquestionably illegal, there

nonetheless existed a consistent morality to these individuals, and they rarely caused the havoc they were capable of.

Later came the time of the "script kiddie." Once Internet access became commonplace, hacking tools became more widespread, and a far lesser degree of skill was needed to break into vulnerable systems. These individuals lacked the expertise or moral fiber found in their predecessors, typically defacing websites with profane messages just to gain bragging rights. Dealing with this group has been little more than a matter of implementing best practices for security, because the threat posed by them has not proven to be particularly sophisticated. Most recently, criminal organizations have adopted hacking as a means toward generating revenue through extortion, embezzlement or identity theft. This threat has been gaining in sophistication and scope and still poses an evolving challenge to both individual people and private organizations.

A nation-state leveraging offensive cyber warfare with hostile intent, however, embodies the worst aspects of all three groups: the sophistication and expertise of the vintage hacker, the indiscriminate scope of the script kiddie and the targeted, hostile intent to maximize damage of the cybercriminal. In addition, cyber-warfare units of military and intelligence organizations are furnished with unprecedented resources. The vintage hackers and script kiddies both did their work on a shoestring budget and, while criminal organizations are better funded, they still have limited resources, plus a significant need to avoid capture and prosecution. A nation-state's offensive cyber-warfare assets, however, have plentiful resources and training, and no fear of criminal prosecution for their acts. They operate within save enclaves from which they have little fear of facing retribution for whatever they may do. The morality of their acts is typically limited to that of the government they serve. As two of the more sophisticated cyber-warfare actors are North Korea and China, this is a chilling thought indeed.

1.5 Cost and Scale of Cyber-warfare

Bill Woodcock, a research director at the Packet Clearing House, a nonprofit organization that tracks Internet traffic, once said, cyber-attacks are so inexpensive and easy to mount, with few fingerprints; they will almost certainly remain a feature of modern warfare. “It costs about 4 cents per machine,” Mr. Woodcock said [w9] “You could fund an entire cyber-warfare campaign for the cost of replacing a tank tread, so you would be foolish not to.”

In developing a strategy to counter these dangers, the Pentagon is focusing on a few central attributes of the cyber-threat. First, cyber-warfare is asymmetric. The low cost of computing devices means that U.S. adversaries do not have to build expensive weapons, such as stealth fighters or aircraft carriers, to pose a significant threat to U.S. military capabilities. A dozen determined computer programmers can, if they find a vulnerability to exploit, threaten the United States' global logistics network, steal its operational plans, blind its intelligence capabilities or hinder its ability to deliver weapons on target. Knowing this, many militaries are developing offensive capabilities in cyberspace, and more than 100 foreign intelligence organizations [w7][w10] are trying to break into U.S. networks. Some governments already have

the capacity to disrupt elements of the U.S. information infrastructure.

In cyberspace, the offense has the upper hand. The Internet was designed to be collaborative and rapidly expandable and to have low barriers to technological innovation; security and identity management were lower priorities. For these structural reasons, the U.S. government's ability to defend its networks always lags behind its adversaries' ability to exploit U.S. networks' weaknesses. Adept programmers will find vulnerabilities and overcome security measures put in place to prevent intrusions. In an offense-dominant environment, a fortress mentality will not work. The United States cannot retreat behind a Maginot Line of firewalls, or it will risk being overrun. Cyber-warfare is like maneuver warfare, in that speed and agility matter most. To stay ahead of its pursuers, the United States must constantly adjust and improve its defenses.

It must also recognize that traditional Cold War deterrence models of assured retaliation do not apply to cyberspace, where it is difficult and time-consuming to identify an attack's perpetrator. Whereas a missile comes with a return address, a computer virus generally does not. The forensic work necessary to identify an attacker may take months, if identification is possible at all. And even when the attacker is identified, if it is a non-state actor, such as a terrorist group, it may have no assets against which the target nation can retaliate. Furthermore, what constitutes an attack is not always clear. In fact, many of today's intrusions are closer to espionage than to acts of war. The deterrence equation is further muddled by the fact that cyber-attacks often originate from co-opted servers in neutral countries and that responses to them could have unintended consequences.

Given these circumstances, deterrence will necessarily be based more on denying any benefit to attackers than on imposing costs through retaliation. The challenge is to make the defenses effective enough to deny an adversary the benefit of an attack, despite the strength of offensive tools in cyberspace. Traditional arms control regimes would likely fail to deter cyber-attacks because of the challenges of attribution, which make verification of compliance almost impossible. If there are to be international norms of behavior in cyberspace, they may have to follow a different model, such as that of public health or law enforcement.

The scale of a state sponsored cyber-attack could be devastating given the possibilities. Some of the strikes are serious enough to wound individuals or companies, but happen below the threshold that would trigger a forceful government response. A few such instances have also been researched as part of this thesis because an attack on a state's companies with anti-state slogans becomes an attack on the industrial infrastructure of the state, no matter how it is considered. Here are a few statistics [44] for the U.S., which illustrate how tricky this problem is.

- The Department of Homeland Security has classified 1,700 of the 33,000 entities in the national asset database as nationally critical.
- Just one natural gas supplier has over 35,000 miles of distribution pipeline.
- The electricity industry added 21 gigawatts of new generating capacity in 2004.
- Just one electrical utility has over 21,000 miles of distribution lines.
- There are nearly 10,000 airports in the country.

- There are approximately 1.5 million miles of gas pipe.
- There are nearly 7,000 bridges in the National Highway System inventory.
- There are nearly 10,000 high-hazard dams.
- In the U.S., about 80% of critical infrastructure is privately owned.

1.6 A Historical Glimpse of Cyber-warfare

Following is a snapshot view of the major cyber-warfare cases that have surfaced in the past four decades.

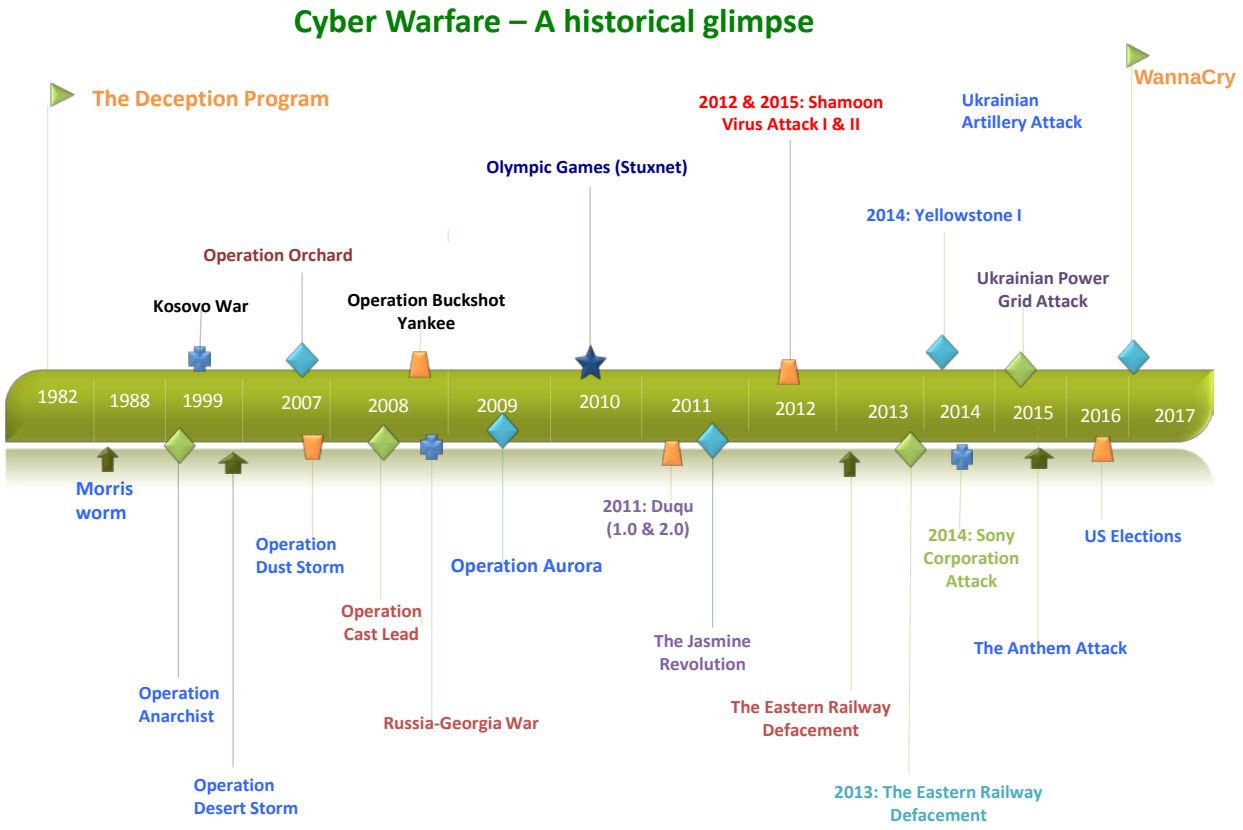

Figure2: Historical Glimpse of Cyber Warfare Cases

2. A Framework for Cyber-Warfare

The use of CASCON for Cyber-Warfare data has helped tremendously in this project. Since warfare has historically consisted of kinetic elements, the CASCON database of cases and its various phases provide a unique perspective into conflicts and their outcomes. This thesis leveraged the kinetic warfare framework to build the cyber warfare framework so it is easier to visualize and infer from the information.

3.1 Typical Phases in Cyber-warfare

Cyber Warfare is mission focused and the success is largely based on the superiority and sophistication of technology used in the planning phase. The criteria for the mission have to be defined in this phase. Compared to kinetic warfare, where a dispute is the basis for the warfare that escalates to become a conflict, cyber-warfare could originate with or without a conflict.

A planning phase is when a cyber-weapon is tailored to the opponent's cyber environment (Target). Knowledge about the target is key during the planning phase. Knowing specific vulnerabilities and scenarios on which vulnerabilities could be seized constitutes a major part of the planning. This phase is also called the intelligence gathering and evaluation phase. The triggers to the planning phase include a new dispute that surfaces between states or an ongoing dispute that had existed. After thorough planning has been achieved the weapon is released into the target environment. The entry point, what vulnerabilities to seize and how it exits the target is determined in the planning phase.

Actors: Status quo, non-status quo, dispute, mission

The Reconnaissance phase is where the Cyber weapon has been released by the non-status quo side and has found a way to enter the target environment to be able to take control and proceed with its mission. The weapon is scanning the target to take its full form.

Actors: Status-quo side, target, weapon, entry

During the Replicate phase, one or more vulnerabilities in the target environment have been identified and acted upon. The footprint of the weapon has grown significantly and has taken form. The weapon is still in the stealth mode but is in control.

Actors: Status-quo side, target, weapon, vulnerability

The Assault or Hostilities phase is where the weapon is unleashed and it carries out the mission in the target environment. This could be followed by a counter assault in the form of a defense weapon or a separate and hence exchange of hostilities happen in this phase. The weapon could still remain in stealth mode during this phase and attacks the target. It has a much bigger footprint than when it first entered the target, it has identified the vulnerabilities and knowledgeable about the target. In comparison with the Hostilities phase of CASCON kinetic warfare, the weapon might not reside in the target although it could attack it in stealth mode.

Actors: Non-Status-quo, Status quo, target, weapon, damage

The Obfuscation phase is where the mission has been accomplished to the extent to which it was successful and then the Cyber weapon hides or self-destroys.

***Actors*: Status-quo side, target, weapon, damage**

The Withdraw phase is when the parties go into an agreement phase with or without the help of a third party. There is no active weapon on either side.

***Actors*: Non-Status-quo, Status quo, target, agreement**

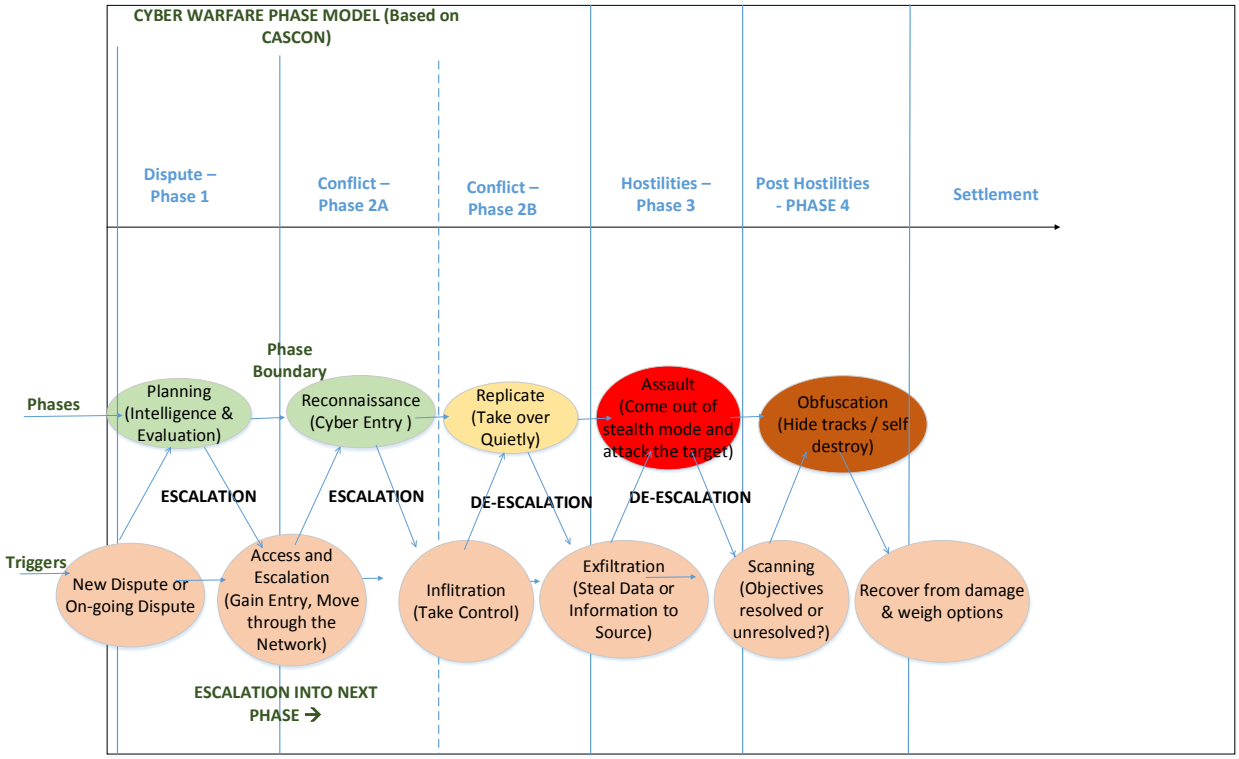

Figure3: Cyber-Warfare Phase Model

3.2 Cyber Warfare: Factor coding

The coding factors for cyber warfare will apply from CASCON's list of coding factors for kinetic warfare, it is to be noted that states could use Cyber-warfare in conjunction with kinetic. This thesis will extend the list of kinetic coding factors and categories by a few specific categories and factors that are specific to Cyber-Warfare, these are described below:

Factor	Phase1	Phase2	Phase3
R – Previous or General Relations	All CASCON coding factors apply	All CASCON coding factors apply	All CASCON coding factors apply
G – Great Power	All CASCON coding factors apply	All CASCON coding factors apply	All CASCON coding factors apply
X – External Relations Generally	All CASCON coding factors apply	All CASCON coding factors apply	All CASCON coding factors apply
M – Military-Strategic	All CASCON coding factors apply	All CASCON coding factors apply	All CASCON coding factors apply

U–International Organizations (UN)	All CASCON coding factors apply	All CASCON coding factors apply	All CASCON coding factors apply
E– Economic/Resources	All CASCON coding factors apply	All CASCON coding factors apply	All CASCON coding factors apply
I – Internal Politics	All CASCON coding factors apply	All CASCON coding factors apply	All CASCON coding factors apply
C – Communication and Information	All CASCON coding factors apply	All CASCON coding factors apply	All CASCON coding factors apply
D – Actions in Disputed Area	All CASCON coding factors apply	All CASCON coding factors apply	All CASCON coding factors apply

Table1: CASCON: Coding Factors (Kinetic)

Factor	Phase1	Phase2	Phase3
O – Open Internet Regulations	1. Net Neutrality : No discrimination on data 2. General and wide availability of broadband access 3. No Paid Prioritization: broadband providers may not favor some lawful Internet traffic over other lawful traffic in exchange 4. No Throttling: broadband providers may not impair or degrade lawful Internet traffic on the basis of content, applications, services, or non-harmful devices. 5. No Blocking: broadband providers may not block access to legal content, applications, services, or non-harmful devices.	1. Access to status-quo government documents 2. Access to status-quo technology to non-status quo state 3. Business presence of non-status quo state within status quo state 4. Ability to influence non-status quo principles within status quo states	1. Ability for non-status quo state to go undetected during hostilities 2. Ability of status quo state to decipher the attack 3. Ability of status quo state to quickly determine the Cyber nature of the attack 4. Ability of status quo state to recover from the hostilities 5. Ability of the status quo state to articulate the attack publicly without regulatory restrictions or fear of being self-blamed

B – Internet Infrastructure Backbone	1. Number of ISPs 2. Access to global information 3. Social Media awareness and influence 4. Government promotion of global information through internet 5. government-led efforts to restrict online speech 6. Government promotion of state sponsored Cyber Organizations 7. Ability for non-status quo state to conduct remote surveillance through modern technology	1. Non-status quo side learns enough information and decides to quit 2. Non-status quo side has unleashed a weapon that cannot be withdrawn 3. Non-status quo side has pressure from other supporting states 4. Status-quo side has detected the weapon 5. Status-quo side has all its vulnerabilities covered	1. Inability of the status quo state to quickly respond with a counter cyber-attack 2. Inability of status quo state to detect the source of the cyber-attack. 3. Inability of Status Quo state to be prepared for an Adversary attack
W - Weapons Cyber Command	1. Cyber Capability to Attack and Defend 2. Global Awareness of Cyber Capabilities 3. Cyber Experience in Warfare 4. Cyber Alliances	1. One side has bought technological infrastructure from companies sourced in another side 2. One side has far better knowledge on technological side than the other 3. One side has knowledge of zero day vulnerabilities 4. One side can influence the other side's technological decision	1. One side will send a strong message by using a Cyber weapon 2. One side will avoid a major threat by using Cyber weapon to the other side 3. One side will gain inside details about the other side with espionage 4. Superpower (US) involved in the status quo side

Table2: CASCON: Coding Categories and Factors (Cyber)

The above factors are analyzed and applied to the Cyber case to identify how they exert an influence over the dynamics of the conflict by steering it either towards the next phase or away from it. The following nine factor coding choices will be used for Cyber cases:

T3	Major influence toward use of Cyber force
T2	Some influence toward use of Cyber force
T1	Little influence toward use of Cyber force
N	Neutral, present in the case but no influence in either direction
A1	Little influence away from use of Cyber force
A2	Some influence away from use of Cyber force
A3	Major influence away from use of Cyber force
F	False, or not present in the case
--	No information available, or not yet coded

Table3: CASCON coding factor

4. Cyber Warfare: Case Studies

Cyber-Warfare incidents from the past were researched for this thesis, included are a number of prominent and publicized Cyber-warfare cases that involving states. Each case has been researched, analyzed and written using the model of the CASCON framework as used in kinetic warfare in the realm of international conflict management. The general format for each of the case studies is to begin with a short background of the conflict to understand the parties involved. The parties are then differentiated into status quo and non-status-quo sides based on the historical application of conflict management. The status-quo state is the victim and the non-status quo state is the one that initiated the warfare. The different phases for Cyber-Warfare have been identified given the kinetic post-World War II data from the CASCON model. Case detail provides basic information including region, dates, type of conflict etc. The case précis is provided with Identify the parties, the locale, the issues in dispute, and the dates that mark the thresholds between phases. Finally a set of coding factors is identified for the conflict. Visual indications of the region and conflict are included as appropriate.

4.1 Olympic Games (a.k.a Stuxnet)

Conflict Background:

Iran and the US have no formal or direct diplomatic relationship[w1]. Iran's democratically elected leader was ousted by a COO orchestrated by the US and British intelligence agencies in 1953[w1]. 26 years later US Backed Iranian President leaves after mass demonstrations. Successor Islamic leader takes over US hostages and seizes US embassy in Tehran (1979-1981). Relationship deteriorated further when in 1988 a US warship shot down Iranian plane. In 2002 denounced Iran as part of an axis and evil, accusing it of having a secret nuclear weapons program. Iran's president accused US for the 9/11 attacks in 2001. Change of Iranian Government happens in 2013 and they have a first phone call between heads of state after 30 years. [W1]

Figure4: Olympic games: Region of conflict

Figure5: Map showing Natanz where the secret nuclear program was hosted (courtesy: Institute for science and security)

Cyber Case Detail	
Case Code Name	Olympic Games
Status Quo States	US, Israel
Non Status Quo States	Iran
Region	Middle East
Conflict Type	Interstate
Motive	Sabotage
Phase 1	6/1/2008 (1st) & 6/2/2009 (2nd)
Phase2	January 2010
Phase3	June 2010
Phase4	2011
Phase5	2011

Table: Case Detail for Olympic Games (a.k.a Stuxnet)

Phase	Activity
Dispute	Phase1 01/30/2002: In 2002 an Iranian opposition group reveals that Iran is developing nuclear facilities including a uranium enrichment plant at Natanz and a heavy water reactor at Arak. The US accuses Iran of a clandestine nuclear weapons program, which Iran denies.
Conflict 2A (Reconnaissance)	Phase2a 2006 – 2010: A decade of intermittent Iranian engagement with the UN's nuclear watchdog and diplomatic activity follows. The UN ratifies four rounds of sanctions on Iran between 2006 and 2010 over the nuclear issue. Weapon targeted Zero day vulnerabilities on Microsoft Windows machines and networks, repeatedly replicating it. Weapon sought out Siemens Step7 software, which is also Windows-based and used to program industrial control systems that operate equipment, such as centrifuges.
Conflict 2B (Replicate)	Phase 2b 2010: About 13 days after infection, the virus turned itself on and was able to spread via USB interface. Operationally it was able to speed up or slow down the centrifuges causing them to destroy themselves. The sabotage was so sophisticated it was able to unfold without showing any signs of problems on monitoring systems used by officials at the Iranian facility.
Hostilities (Assault)	Phase 3 2010: Weapon compromised the programmable logic controllers. The worm's authors could thus spy on the industrial systems and cause the fast-spinning centrifuges to tear themselves apart, unbeknownst to the human operators at the plant. DDOS attacks on US Financial Websites are launched allegedly by non-status quo state.
Post Hostilities (Obfuscation)	Phase 4 2010: Stuxnet hides itself from plant personnel by installing rootkits on infected Windows computers and on infected PLCs, in order to hide its files. By installing a driver on Windows computers, it hid itself by manipulating requests sent to devices. Stuxnet modifies some routines on the PLCs, preventing a safe shutdown even if the operator finds out that the system is not operating normally.
Post Hostilities (Withdraw)	Phase 5 2010: Uranium enrichment of the Nuclear program was withdrawn and sanctions were withdrawn.

Table: Case Precis for Olympic games

Coding Factors

The CASCON methodology to code the Stuxnet case will be applied here. The following table indicates three categories identified earlier in this thesis. For example '**.1O**' indicates whether 'Net Neutrality or No discrimination on Data' exerted influence within the Open Internet Regulations category towards or away from the conflict. If it did influence to what

extent it did. The nine factor coding choices will be used below. Each box to the right will represent a single factor identified for Cyber. In the table below O represents - Open Internet Regulations, B represents Internet Infrastructure Backbone and W Cyber Weapon Capability.

.1O	T2	T3	T1	N	T3		
.1B	T1	T3	A2	N	T3	T3	T1
.1W	T3	T3	T1	N			
.2O	A1	N	T3	N			
.2B	N	A1	T2	T3	T1		
.2W	T1	T1	T3	T2			
.3O	A1	T2	T3	N	A2		
.3B	T2	T3	T1				
.3W	T3	T2	T3	T3			

Table: Stuxnet: Coding Factors

4.2 Ukranian Power Grid

Conflict Background:

Russia and Ukraine trace their roots back to the first East Slavic state, Kievan Rus, which stretched from the Baltic to the Black Sea from the 9th century to the mid-13th century[wc1]. There were both part of the Union of Soviet Socialist Republic that formed in 1922 and Ukraine was controlled by Moscow, then and now the capital of Russia. The two neighboring countries have been intertwined for over 1,000 years of tumultuous history. Today, Ukraine is one of Russia's biggest markets for natural gas exports, a crucial transit route to the rest of Europe, and home to an estimated 7.5 million ethnic Russians who mostly live in eastern Ukraine and the southern region of Crimea. About 25 percent of Ukraine's 46 million people claim Russian as their mother tongue. Russia lacks natural borders like rivers and mountains along its western frontier, it is believed that the Russian leaders have traditionally seen the maintenance of a sphere of influence over the countries around it as source of security and especially true of Ukraine, which Russia regards as its little brother.

Cyber Case Detail	
Case Code	Ukrainian Power Grid Attack
Status Quo States	Ukraine
Non Status Quo States	Russia
Region	Europe
Conflict Type	Interstate

Motive	Territory
Phase1	Prior to December 2015
Phase2	Spring 2015 through December 2015
Phase3	December 23, 2015
Phase4	December 23, 2015
Phase5	December 2015 through April 2016

Ukrainian Power Grid: Case Detail

Figure6: Russia and Ukraine: Region of Conflict

Phase	Activity
Dispute	Phase 1 Prior to December 2015: The attacks began last spring with a spear-phishing campaign that targeted IT staff and system administrators working for multiple companies responsible for distributing electricity throughout Ukraine. The phishing campaign delivered email to workers at three of the companies with a malicious Word document attached. When workers clicked on the attachment, a popup displayed asking them to enable macros for the document. If they complied, a program called BlackEnergy3—variants of which have infected other systems in Europe and the US—infected their machines and opened a backdoor to the hackers. Over many months they conducted extensive reconnaissance, exploring and mapping the networks and getting access to the Windows Domain Controllers, where user accounts for networks are managed. Here they harvested worker credentials, some of them for VPNs the grid workers used to remotely log in to the SCADA network. Once they got into the SCADA networks, they slowly set the stage for their attack.
Conflict 2A (Reconnaissance)	Phase 2 Spring 2015: Over many months they conducted extensive reconnaissance, exploring and mapping the networks and getting access to the Windows Domain Controllers, where user accounts for networks are managed. Here they harvested worker credentials, some of them for VPNs the grid workers used to remotely log in to the SCADA network. Once they got into the SCADA networks, they slowly set the stage for their attack. The Operation-specific malicious firmware updates [in an industrial control setting] had never been done before. From an attack perspective, it was a job well done by them.
Conflict 2B (Replicate)	Phase 3 Spring 2015: Each company used a different distribution management system for its grid, and during the reconnaissance phase, the attackers studied each of them carefully. Then they wrote malicious firmware to replace the legitimate firmware on serial-to-Ethernet converters at more than a dozen substations (the converters are used to process commands sent from the SCADA network to the substation control systems). Taking out the converters would prevent operators from sending remote commands to re-close breakers once a blackout occurred. . The Operation-specific malicious firmware updates [in an industrial control setting] had never been done before. From an attack perspective, it was a job well done by them.
Hostilities (Assault)	Phase 5: December 23 2015: Armed with the malicious firmware, the attackers were ready for their assault. Sometime around 3:30 p.m. on December 23 2015, they entered the

	SCADA networks through the hijacked VPNs and sent commands to disable the UPS systems they had already reconfigured. Then they began to open breakers. But before they did, they launched a telephone denial-of-service attack against customer call centers to prevent customers from calling in to report the outage. TDoS attacks are similar to DDoS attacks that send a flood of data to web servers. In this case, the center's phone systems were flooded with thousands of bogus calls that appeared to come from Moscow, in order to prevent legitimate callers from getting through. Investigators noted that this move illustrates a high level of sophistication and planning on the part of the attackers. Cybercriminals and even some nation-state actors often fail to anticipate all contingencies.
Post Hostilities (Obfuscation)	Phase 4: December 23 2015: After the assault had completed all of this, they then used a piece of malware called KillDisk to wipe files from operator stations to render them inoperable as well. KillDisk wipes or overwrites data in essential system files, causing computers to crash. Because it also overwrites the master boot record, the infected computers could not reboot.
Post Hostilities (Withdraw)	Phase 5: December 2015 through April 2016: The fact that the hackers could have done much more damage than they did do if only they had decided to physically destroy substation equipment as well, making it much harder to restore power after the blackout. The power wasn't out long in Ukraine: just one to six hours for all the areas hit. But more than two months after the attack, the control centers are still not fully operational

Table: Ukrainian Power Grid: Case Precis

Code Factors

.1O	T3	T2	N	A1	A3		
.1B	A2	T1	T3	T2	T2	T2	T3
.1W	T2	T1	T3	A1			
.2O	T1	A1	T3	T2			
.2B	T1	T2	T3	T3	T1		
.2W	T2	T1	T3	T2			
.3O	A1	T2	T1	T2	N		
.3B	T1	T2	T3				
.3W	T3	T3	T3	T2			

Table: Ukranian Power Grid: Coding Factors

4.3 Kosovo War

Conflict Background:

Kosovo is a disputed territory and a partially recognized state. Long-term ethnic tensions between Kosovo's Albanian and Serb populations left the territory ethnically divided,

resulting in inter-ethnic violence, culminating in the Kosovo War of 1998–99, part of the wider regional Yugoslav Wars. The war ended with a military intervention of NATO, which forced the Federal Republic of Yugoslavia to withdraw its troops from Kosovo, which became a UN protectorate under UNSCR 1244. [W1]

Cyber Case Detail	
Case Code	Kosovo War
Status Quo States	Kosovo
Non Status Quo States	Federal Republic of Yugoslavia
Region	Europe
Conflict Type	Interstate
Motive	Sabotage
Phase1	1999
Phase2	1999
Phase3	7 May 1999
Phase4	1999
Phase5	1999

Figure7: Kosovo War: Region of Conflict

Phase	Activity

Dispute	**Phase1 1980s:** Tensions on Kosovo started in 1980s with discrimination of both ethnic groups where they were minority. In 1989, president of Serbia, Slobodan Milosevic, vastly reduced the autonomy of Kosovo. In response, Albanians in Kosovo organized referendum in 1991 and proclaimed independence. Independence was recognized only by Albania. However, Albanians started to ignore state and federal structures and started to create parallel institutions. In the mid-1990s, UCK was created, an Albanian militant force. There were no major conflicts until 1998. UCK by that time was building up, mainly through organizing underground network in the western Europe. This network was using drug and human trafficking to fund UCK with equipment and weapons. In 1998, major attack on Yugoslav police and army had started. As no state would stand still having a terrorist attacks on their police and soldiers, FR Yugoslavia fought back and as it was heavily equipped with an army and police of a country, they sometimes used their force too much. Because some of attacks had some consequences in civilians, international society (NATO) started to get involved.
Conflict 2A (Reconnaissance)	**Phase2A Early July 2008:** After the NATO air campaign started, many people in Serbia felt it their duty to help defend their country or somehow to disrupt or stop NATO operations. They formed Cyber groups and attacked NATO websites, servers or any infrastructure of NATO or countries that were part of NATO and are exposed on the internet.
Conflict 2B (Replicate)	**Phase2B Early July 1999:** Modern Black Hand was a hacker group that was quite successful in their attacks. Firstly they started with Kosovo and Albanian websites that spread propaganda. They took down and defaced websites like kosova.com and Swiss based Albanian news portals zik.com
Hostilities (Assault)	**Phase3: 20 July 2008;** Hosting company put down website after the attack and unregistered domain, because attacker who said he was from Poland threatened the company that he will delete all the content from the hard drives of the hosting company. Also website of UCK got defaced by Black Hand. They were claiming that each NATO tomahawk missile would destroy at least one server. By the beginning of the NATO aggression over Yugoslavia, Yugoslav hackers were aided with Russian hackers who performed attacks on US military websites and internet infrastructure. After NATO bombed China embassy in Belgrade, claiming it was a mistake, China hackers joined combined forces of Yugoslav and Russians hackers. Here the things became serious. NATO server was shot down because of denial of service attacks over it. US Navy website was hacked by the Russians. NATO mail servers were nonfunctional because they were daily they were receiving more than 20 000 emails with malware in attachment. After these 78 intense days conflict ended. With it cyber war ended as well. Although, no army was officially involved in cyber-attacks, it cannot be said that it was not a real cyber war.
Post Hostilities (Obfuscation)	**Phase4 Early July 2008:**

	There was a lot of back and forth in the form of Cyber-attacks between the status quo and non-status quo state. The only obfuscation involved was the coup organized by the Yugoslavian military involving several allies.
Post Hostilities (Withdraw)	**Phase5 Early July 2008:** The ceasefire was signed on June 9th 1999, in Kumanovo in Macedonia. This ceasefire and following UN resolution ended conflict between NATO and FR Yugoslavia. NATO had archived most of the goals in physical war, since it was stronger. However, in cyber space NATO was a novice. NATO leaders claimed that they did not wanted to start Cyber Warfare because of undefined international regulations. However, it is more likely that NATO at that time was not prepared for the attacks in the Cyber domain.

Table: Kosovo War: Case Precis

4.4 Russia-Georgia War

Conflict Background:

The relations between Georgia and Russia date back hundreds of years and remain complicated despite certain religious and historical ties that exist between the two countries and their people[W1]. The first formal alliance between Georgia and Russia took place in 1783 when, as a last attempt to deal with repeated Persian invasions, king Heraclius II of Eastern Georgia (Kartlinia-Kahetia) signed the Treaty of Georgievsk with the Russian Empire, which the Georgian monarchy viewed as a replacement for its long-lost Orthodox ally, the Eastern Roman Empire. Having spent more than a century as part of the Russian Empire, in 1918 Georgia regained independence and established the First Republic. In 1921 Georgia was invaded and occupied by Bolshevik Russia to form the Soviet Union in 1922. When the country regained independence in 1991, the bilateral Russo-Georgian ties were once again strained due to Moscow's support of the separatist regions within Georgia, Georgia's independent energy policies and most recently, its intentions to join NATO.

Cyber Case Detail	
Case Code	Russia-Georgia War
Status Quo States	Georgia
Non Status Quo States	Russia
Region	Europe
Conflict Type	Interstate
Motive	Sabotage
Phase1	Early July 2008
Phase2	Early July 2008
Phase3	20 July 2008; 5 Aug 2008, 9 Aug 2008, 10 Aug 2008, 11 Aug 2008

Phase4	14 August 2008
Phase5	15 August 2008

Table: Russia-Georgia War: Case Detail

Figure 8: Russia-Georgia War: Map of Georgia

Figure9: Russia-Georgia War: Detailed region of Conflict

Phase	Activity
Dispute	Phase1 April 21, 2008 Status quo side accuses non-status quo side of shooting down an unmanned drone over Abkhazia on April 20 2008. Non-status quo side denies the claim and sends more troops to Abkhazia to counter what it says are status quo side plans for an attack. A UN investigation concludes that a missile from a non-status quo side's fighter jet struck the drone shot down on April 21. Non-status quo side sends several hundred unarmed troops to Abkhazia, saying they are needed for railway repairs. Status quo side accuses non-status quo side of planning a military intervention. [W1]
Conflict 2A (Reconnaissance)	Phase2A Early July 2008: The attacks originally starting to take place several weeks before the actual "intervention" with the Status-quo side President's web site coming under DDoS attack from Non-Status quo state's hackers in July 2008. At the strategic level the (alleged) Russian cyberspace reconnaissance and probing attacks began weeks prior to the actual inception of virtual and physical combat. Russian web sites, chat rooms, and networks also discussed the upcoming attacks for several weeks.
Conflict 2B (Replicate)	Phase2B Early July 2008: Georgia's Internet infrastructure began as early as July 20, with coordinated barrages of millions of requests - known as distributed denial of service, or D.D.O.S., attacks - that overloaded and effectively shut down Georgian servers. As it turns out, the July attack may have been a dress rehearsal for an all-out cyber war once the shooting started between Georgia and Russia. According to Internet technical experts it was the first time a known cyber-attack had coincided with a shooting war. These extensive preparatory actions imply a strategic planning process that began long before July 2008.
Hostilities (Assault)	Phase3: 20 July 2008; 5 Aug 2008, 9 Aug 2008, 10 Aug 2008, 11 Aug 2008: The attack modalities included: Defacing of Web Sites (Hacktivism), Web-based Psychological Operations (Psyc-Ops), a fierce propaganda campaign (PC) and of course a Distributed Denial of Service Attacks (DDoS).
Post Hostilities (Obfuscation)	Analysts tracking the RBN, released data claiming to show that visits to Georgian sites had been re-routed through servers in Russia and Turkey, where the traffic was blocked. The traffic was restored slowly back to normal by August 15 2008
Post Hostilities (Withdraw)	Georgian President Mikheil Saakashvili signs a cease-fire agreement with Russia. French President Nicolas Sarkozy brokers the deal.

Table: Russia-Georgia War: Case Precis

4.5 Operation Cast Lead

Conflict Background:

Israel and the PLO (Palestine Liberation Organization) began to engage in the late 1980s and early 1990s in what became to be the Israeli–Palestinian peace process, culminated with the

Oslo October 2012 accords in 1993. Shortly after, the Palestinian National Authority was established and during the next 6 years formed a network of economic and security connections with Israel, being referred to as a fully autonomous region with self-administration. In the year 2000, the relations severely deteriorated with the eruption of the Second Intifada – a rapid escalation of the Israeli–Palestinian conflict. The events calmed down in 2005, with only partial reconciliation and cease fire. The situation became more complicated with the split of the Palestinian Authority in 2007, the violent split of Fatah and Hamas factions, and Hamas' takeover of the Gaza Strip. The Hamas takeover resulted in a complete rift between Israel and the Palestinian faction in the Gaza Strip, cancelling all relations except limited humanitarian supply[w1].

Cyber Case Detail	
Case Code	Operation Cast Lead
Status Quo States	Palestine
Non Status Quo States	Israel
Region	Middle East
Conflict Type	Espionage
Motive	Sabotage
Phase1	December 2008
Phase2	October 2012
Phase3	November 2012
Phase4	November 2012
Phase5	November 21 2012

Table: Operation Cast Lead: Case Detail

Figure 10: Region of conflict (Israel and Palestine)

Phase	Activity
Dispute	**<u>Phase1December 2008:</u>** Israel began a military assault on Hamas's infrastructure in Gaza on December 27, 2008, called "Operation Cast Lead." A cyber backlash by Arabic hackers targeted thousands of Israeli government and civilian Web sites. When the government of Israel publicly threatened to sever all Internet and other telecommunications into and out of Gaza they crossed a line in the sand. As the former dictator of Egypt, Mubarak learned the hard way - we are ANONYMOUS and NO ONE shuts down the Internet on our watch. To the IDF and government of Israel we issue you this warning only once. Do NOT shut down the Internet into the "Occupied Territories", and cease and desist from your terror upon the innocent people of Palestine or you will know the full and unbridled wrath of Anonymous.
Conflict 2A (Reconnaissance)	**<u>Phase 2A Early November 2012:</u>** Most of the Non-State Arabic hackers involved do not have the technical skill to carry out sophisticated network attacks, opting instead for small to mid- scale denial of service attacks and mass website defacements. There were no zero day vulnerabilities exploited in these attacks. Instead, most attackers focused on old Web site vulnerabilities that had not been patched. [40]
Conflict 2B (Replicate)	**<u>Phase2A Early November 2012:</u>** This is the first instance of a voluntary botnet ("Help Israel Win") used in a Cyber conflict where individuals voluntarily passed control of their own computers to the botnet host server.

Hostilities (Assault)	**Phase3 November 2012:** Hackers in Gaza have leaked 35,000 credit card numbers of "Zionist civilians" as a "response from the lions to the aggression of the Jews." On 16NOV12 at the Arab hacker group Oujda-Tech Group defaced 40 Israeli websites (non-government) to protest Gaza missile strikes. Later Hamas-friendly websites including ".qassam.ps"and "hamasinfo.net" went down. Unlike other instances of cyber conflicts (Chechnya, Estonia, Lithuania, Georgia, India), this conflict involved both State (Israel and possibly Iran) and Non-State hackers.
Post Hostilities (Obfuscation)	**Phase4 November 2012:** The attack into Israel was carried out by ANONYMOUS.
Post Hostilities (Withdraw)	**Phase 5 November 21 2012:** Israel and the Hamas militant group agreed to a cease-fire Wednesday to end eight days of the fiercest fighting in nearly four years, promising to halt attacks on each other and ease an Israeli blockade constricting the Gaza Strip.EndFragment

Table: Operation Castlead: Case Precis

4.6 The Tulip Revolution

Conflict Background:

Kyrgyzstan had more often wished for more attention and support from the Soviet Union than it has been able to obtain. For all the financial support that the world community has offered, Kyrgyzstan remains economically dependent on Russia, both directly and through Kazakhstan. In early 1995, Askar Akayev, the then President of Kyrgyzstan, attempted to sell Russian companies controlling shares in the republic's twenty-nine largest industrial plants, an offer that Russia refused[W1].
In the months of unrest leading up to Kyrgyzstan's second Tulip revolution, the technical unit of Kyrgyzstan intelligence cracked the email account of Gennady Pavlyuk, a leading dissident journalist, to obtain specific data on a project of his, then lured him to Kazakhstan under the pretense of meeting angel invesors and killed him. Pavlyuk's assassination was the beginning of an escalating series of attacks to shutter opposition websites until April 8, 2010 when the second Tulip revolution occurred.

Cyber Case Detail	
Case Code	The Tulip Revolution II
Status Quo States	Kyrgyzstan
Non Status Quo States	Russia
Region	Europe
Conflict Type	External intervention

Motive	Sabotage
Phase1	February 2005 through 2010
Phase2	Feb 2005
Phase3	January 18, 2009
Phase4	2009 through 2010
Phase5	2010

Table: The Tulip Revolution: Case Detail

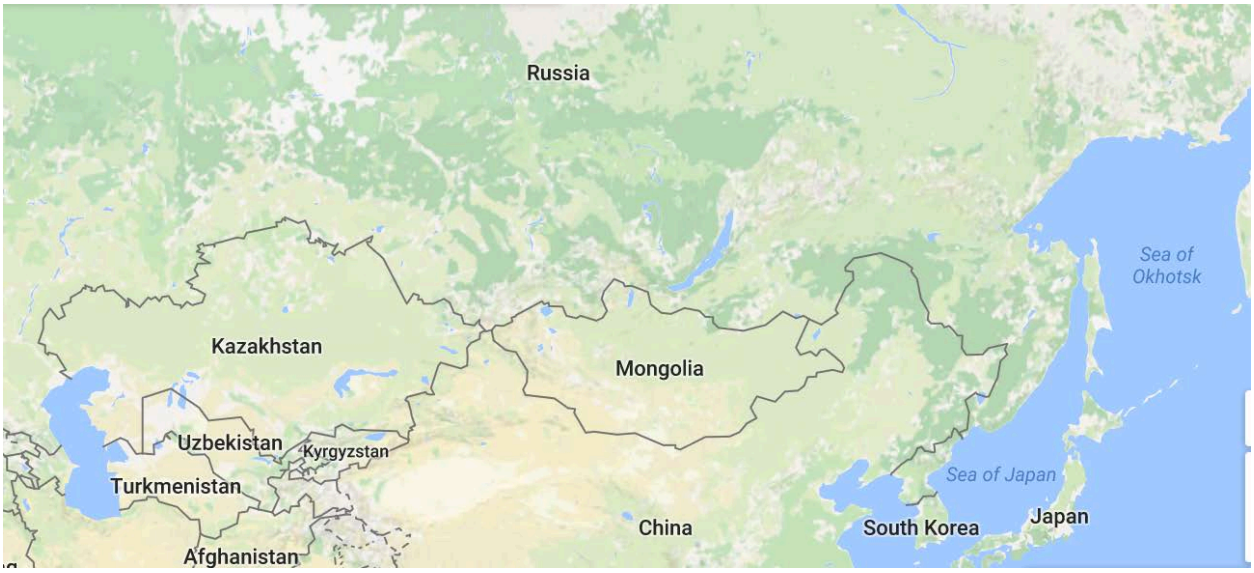

Figure11: The Tulip Revolution: Map of the Conflict Region

Phase	Activity
Dispute	Phase1 Prior to Feb 2005: Websites belonging to political parties and independent media were subject to unexplained technical failures and deliberate hacking during Kyrgyzstan's recent Parliamentary elections. Researchers from the Open Net Initiative documented a pattern of failures that suggest a deliberate attempt to interfere with the functioning of the Internet during election period. The January 2009 denial of service attacks against Kyrgz Internet service providers are an example of one of the most common applications of cyber-attacks; that used by a ruling party against opposition groups inside their own country.
Conflict 2A (Reconnaissance)	Phase2 Prior to Feb 2005: The entire operation was secretly planned to overthrow the presidential.
Conflict 2B (Replicate)	Feb 2005: Insufficient data.

Hostilities (Assault)	Phase3: Feb 2005: Attacks included flooding journalist e-mail accounts with large amounts of spam, and spoofing of e-mail from Kyrgyz websites located in the US. Several political websites were deliberately defaced. In one case, a domain address belonging to an opposition group was apparently de-registered as a result of the organization having no legal status under Kyrgyz electoral law. On February 26th an apparent Distributed Denial Of Service Attack (DDOS) temporarily disabled all websites hosted by major Kyrgyz ISPs (Elcat and AsiaInfo). These ISPs host the websites of many Kyrgyz political parties, media outlets and NGOs. The spike in traffic associated with the failure of Elcat's and AsiaInfo's hosting services led upstream ISPs in Russia and Europe to block access to Elcat's and AsiaInfo's IP addresses, so that web sites hosted by these ISPs are no longer accessible outside of Kyrgyzstan.
Post Hostilities (Obfuscation)	2009 through 2010: Sufficient data was not available.
Post Hostilities (Withdraw)	The response to Bakiyev's presidency was mixed and in April 2010, he was ousted in a second revolution. He was replaced by the popular politician and another leader of the Tulip Revolution, Roza Otunbayeva

Table: The Tulip Revolution: Case Precis

4.7 The Jasmine Revolution

Conflict Background:

In 2011 thousands of Tunisians have taken to the streets to call for extensive economic and social change in their country. Among the fundamental changes the protesters have been demanding is an end to the government's repressive online censorship regime and freedom of expression. That battle is taking place not just on the country's streets, but in internet forums, blogs, Facebook pages and Twitter feeds.

The Jasmine Revolution made history as Tunisia became the first nation in the Arab world to have its leader removed through a popular uprising of its citizens or, more precisely, its web activists thanks to Tunisia's modern communications infrastructure, pervasive Internet access and a completely digitized mobile phone network.

Tunisia's Jasmine Revolution, which resulted in the overthrow of a corrupt government, included violent protests and the hacking of user names and passwords for the entire online population of Tunisia by AMMAR, the country's government-run Internet Services Provider (ISP). Anonymous involved itself by launching Denial of Service attacks at AMMAR and other government websites.

Cyber Case Detail	
Case Code	The Jasmine Revolution

Status Quo States	Tunisian Government
Non Status Quo States	Tunisian & International Web Activists
Region	Middle East
Conflict Type	External intervention
Motive	Sabotage
Phase1	2010
Phase2	2010
Phase3	Jan 2011
Phase4	2011
Phase5	2011

Table: Jasmine Revolution: Case Detail

Figure12: The Jasmine Revolution: Map of the Conflict

Phase	Activity
Dispute	<u>Phase1 2010:</u> Civil unrest in Tunasia for fundamental rights including government's repressive online censorship regime and freedom of expression.
Conflict 2A (Reconnaissance)	<u>Phase 2a 2010:</u> Planning done using social media.
Conflict 2B (Replicate)	<u>Phase 2b 2010:</u> Social media was used to spread the word.
Hostilities (Assault)	<u>Phase 3 2011:</u>

	That battle took place not just on the country's streets, but in internet forums, blogs, Facebook pages and Twitter feeds. The Tunisian authorities have allegedly carried out targeted "phishing" operations, stealing user's passwords to spy on them and eradicate online criticism. Websites on both sides have been hacked.
Post Hostilities (Obfuscation)	Phase4 2011: Insufficient data.
Post Hostilities (Withdraw)	Phase 5 2011: The Jasmine Revolution or uprising in Tunisia that protested against corruption, poverty, and political repression resulted in a forced step down of Pres. Zine al-Abidine Ben Ali in January 2011. The success of the uprising, which came to be known in the media as the "Jasmine Revolution," inspired a wave of similar protests throughout the Middle East and North Africa.[W18]

Table: The Jasmine Revolution: Case Precis

4.8 DuQu (1.0 & 2.0)

Conflict Background:

DuQu, was an espionage tool. Duqu looks for information that could be useful in attacking industrial control systems and reported the sensitive data back to the mother ships. DuQu was found to be a child of Stuxnet since its' executables seem to have been developed after Stuxnet because they use the same Stuxnet source code. Central to DuQu was its' ability to capture keystrokes and computer system and network information. Like Stuxnet, Duqu attacks Microsoft Windows systems using a zero-day vulnerability. [W1]

This spy virus was discovered and linked to several countries, duqu 1.0 was first installed in 2011 and updated to duku 2.0, it affected over 400 million computers. There were three computers in different hotels that hosted Iran Nuclear talks were targeted by the Duku Virus. We will discuss the specific aspect of the nuclear discussion attack for our case study. This was a direct espionage on the nuclear talks with intent to spy on several countries

Cyber Case Detail	
Case Code	DuQu (1.0 & 2.0)
Status Quo States	Iran
Non Status Quo States	Israel
Region	Middle East
Conflict Type	Interstate
Motive	Keylogger, Espionage, Spyware
Phase1	Nov 2010
Phase2	Apr 2011
Phase3	Oct 2011
Phase4	Oct 2011
Phase5	No data found.

Table: Duku 1.0 & 2.0: Case Detail

Figure13: Duku1.0/2.0: Map of the conflict region where Duku attacks occurred

Phase	Activity
Dispute	Phase1: 10 November 2010: A collection of computer malware discovered on 1 September 2011, thought to be related to the Stuxnet worm. The Laboratory of Cryptography and System Security (CrySyS Lab) of the Budapest University of Technology and Economics in Hungary discovered the threat, analyzed the malware, and wrote a 60-page report naming the threat Duqu. Duqu got its name from the prefix "~DQ" it gives to the names of files it creates. Per reports, this spy virus was discovered and linked to Israel, duqu 1.0 was first installed in 2011 and updated to duku 2.0.
Conflict 2A (Reconnaissance)	Phase2A: 11 April 2011: This was an incredibly sophisticated virus with 100 modules; each module could do a task. For example there was a video module, a Wifi module, a phone module etc. Each module collects information from its task. It affected over 400 million computers.
Conflict 2B (Replicate)	Phase2B: 11 April 2011: Replicates very similar to the Stuxnet weapon as discussed in the Olympic Games case, except that the attack was a spying effort to gather information without causing damage along the way.
Hostilities (Assault)	Phase3: 11 October 2011: The 3 computers in 3 hotels that hosted Iran talks targeted by Virus linked to Israeli spies. This was a direct espionage on the nuclear talks with an intent to spy on several countries

Post Hostilities (Obfuscation)	Phase4: Late 2011: Duku is zero day vulnerability so its obfuscation is intrinsic to the platform. The attackers also appear to have used at least three zero-day exploits to conduct their attack, as well as a clever technique to surreptitiously extract data remotely and communicate with infected machines. [W19]
Post Hostilities (Withdraw)	Phase5: Late 2011: No information found.

Table: Duku1.0/2.0: Case Precis

4.9 The Eastern Railway Website Defacement

Conflict Background:

Relations between India and Pakistan have been complex due to a number of historical and political events. Relations between the two states have been defined by the violent partition of British India in 1947, the Kashmir conflict and the numerous military conflicts fought between the two nations. Consequently, even though the two South Asian nations share linguistic, cultural, geographic, and economic links, their relationship has been plagued by hostility and suspicion.

On December 24, 2008, the Whackerz Pakistan Cr3w defaced India's Eastern Railway website with the following announcement:

"Cyber war has been declared on Indian cybers[ace by Whackerz-Pakistan[1]."

Cyber Case Detail	
Case Code	Eastern Indian Railway Website Defacement
Status Quo States	India
Non Status Quo States	Pakistan
Region	South East Asia
Conflict Type	Interstate
Motive	Sabotage
Phase1	12/2008 – 08/2014
Phase2	No Data Found.
Phase3	No Data Found.
Phase4	No Data Found.
Phase5	No Data Found.

Table: Cyber Warfare/Attack on Eastern Indian Railway: Case Detail

Figure14: Eastern Railway Attack: Map of conflict Region

Figure15: Eastern Railway Defacement: cyber-attacks in Assault phase

Phase	Activity
Dispute	Phase1 12/2008 through 8/2014:

	India and Pakistan have a long history of dispute. With Cyber capabilities both countries have displayed potential to sabotage each other's web infrastructure. The Hack was performed against the shameful action of Pakistani troops, entered Indian territory along the Line of Control in the Poonch sector in Jammu and Kashmir and ambushed a patrol killing five Indian soldiers.
Conflict 2A (Reconnaissance)	No data found.
Conflict 2B (Replicate)	No data found.
Hostilities (Assault)	Phase1 12/2008 through 8/2014: The Indian group Guards of Hindustan hacked into the Oil and Gas Regularity Authority of Pakistan website and placed their organization's logo and the Indian national symbol on the site. The Pakistani organization Pakistan Cyber Army soon answered the attack by hacking the websites of the Indian Institute of Remote Sensing, the Centre for Transportation Research and Management, the Kendriya Vidyalaya of Ratlam and the Oil and Natural Gas Corporation of India. Following this a Pakistani group calling itself Zombie_KSA hacked and defaced the Criminal Investigation Department website, a cyber security unit of the Andhra Pradesh state police, and removed the site's information about 10 most wanted criminals. Soon after the Eastern railways attack, another Pakastani group, which is yet to be identified, hacked an Indian television station and State Bank of India. The website of Bank of India, one of the largest banks in India, was completely down on Christmas Eve.
Post Hostilities (Obfuscation)	No data found.
Post Hostilities (Withdraw)	No data found.

Figure: The Eastern Railway Cyber-attack: Case Precis

4.10 The Anthem Attack

Conflict Background:

The cyber-attack in which hackers stole the names, birth dates, Social Security numbers, home addresses and other personal information of 78.8 million current and former members. The kind of information stolen falls under HIPAA, also known as the Health Insurance Portability and Accountability Act, which is the federal law governing the security of medical data. The California Department of Insurance released today the examination findings and settlement agreement concerning the cyber security breach of health insurance giant Anthem Inc., which compromised 78.8 million consumers' records. Anthem agreed to make a number of enhancements to its information security systems, and also agreed to provide credit protection to all consumers whose information was compromised. Anthem is paying more than $260 million dollars for security improvements and remedial actions in response to this breach. California Insurance Commissioner Dave Jones was one of seven insurance commissioners leading the national investigation of the Anthem cyber breach.

Cyber Case Detail	
Case Code	The Anthem attack
Status Quo States	US
Non Status Quo States	State Sponsored Adversaries from Asia.
Region	North America
Conflict Type	Interstate
Motive	Sabotage
Phase1	April 2014
Phase2	Dec 10 2014
Phase3	Jan 27 2015
Phase4	No Data Found.
Phase5	Feb 4 2015

Table: The Anthem Attack: Case Detail

Phase	Activity
Dispute	Phase1 April 2014: "This was one of the largest cyber hacks of an insurance company's customer data," said Insurance Commissioner Dave Jones. "Insurers have an obligation to make sure consumers' health and financial information is protected. Insurance commissioners required Anthem to take a series of steps to improve its cybersecurity and provide credit protection for consumers affected by the breach. In this case, our examination team concluded with a significant degree of confidence that the cyber attacker was acting on behalf of a foreign government. Insurers and regulators alone cannot stop foreign government assisted cyber-attacks. The United States government needs to take steps to prevent and hold foreign governments and other foreign actors accountable for cyber-attacks on insurers, much as the President did in response to Russian government sponsored cyber hacking in our recent presidential election. " [PR1]
Conflict 2A (Reconnaissance)	Phase 2A Dec 10 2014: An investigation by the insurance commissioners' examination team and a separate internal investigation by Mandiant, an information security firm hired by Anthem, revealed the data breach began on February 18,

	2014, when a user within one of Anthem's subsidiaries opened a phishing email containing malicious content.[PR1]
Conflict 2B (Replicate)	Phase 2B Dec 10 2014: Opening the email permitted the download of malicious files to the user's computer and allowed hackers to gain remote access to that computer and at least 90 other systems within the Anthem enterprise, including Anthem's data warehouse. [PR1]
Hostilities (Assault)	Phase 3 January 27 2015 : The cyber breach was first discovered by Anthem on January 27, 2015. In early February 2015, Anthem and its affiliates announced the company had suffered a major breach, which compromised 78.8 million consumer records, including records of at least 12 million minors.
Post Hostilities (Obfuscation)	No Data Found.
Post Hostilities (Withdraw)	Phase 5 February 2015: The team found Anthem's improvements to its cybersecurity protocols and planned improvements were reasonable.

4.11 Operation Aurora

Conflict Background:

Operation Aurora was a series of cyber-attacks conducted by advanced persistent threats such as the Elderwood Group based in Beijing, China, with ties to the People's Liberation Army. First publicly disclosed by Google on January 12, 2010, in a blog post, the attacks began in mid-2009 and continued through December 2009. [W1]

We will closely examine the investigation from Google that was made public in a blog. [B3]

Cyber Case Detail	
Case Code	Operation Aurora
Status Quo States	US
Non Status Quo States	Adversary based in Beijing, China [W1]
Region	Western Hemisphere
Conflict Type	Interstate
Motive	Sabotage
Phase1	Prior to 2009
Phase2	Prior to 2009
Phase3	Mid 2009 - December 2009
Phase4	2010

Phase5	2010

Table: Operation Aurora: Case Detail

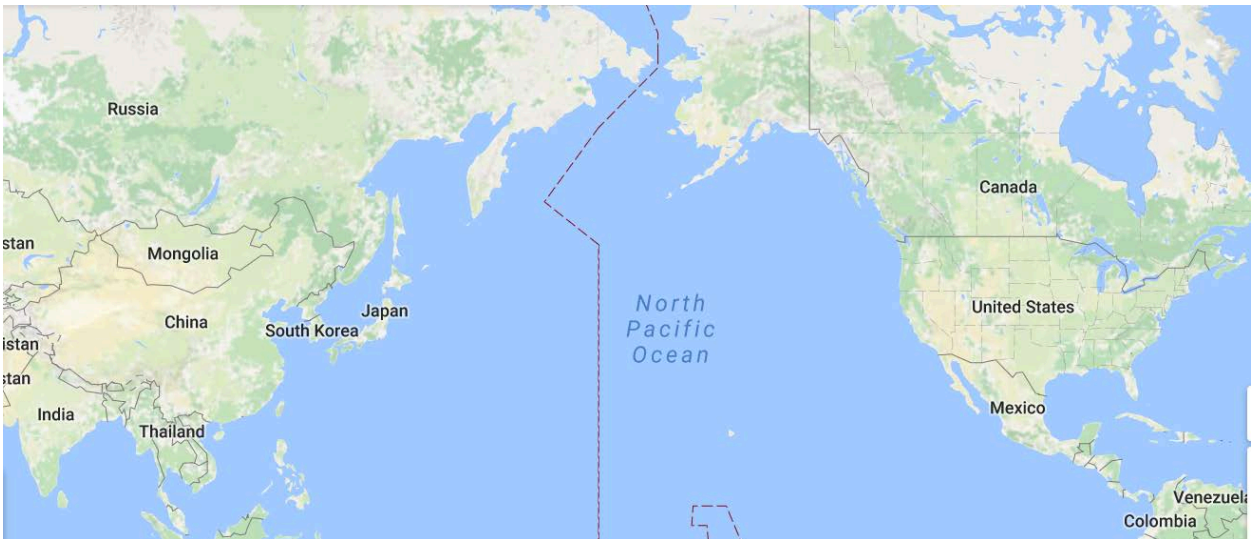

Figure16: Operation Aurora: Map of conflict region

Phase	Activity
Dispute	Phase1 Prior to 2009 : In its blog posting, Google stated that some of its intellectual property had been stolen. It suggested that the attackers were interested in accessing Gmail accounts of Chinese dissidents. According to the Financial Times, two accounts used by an employee had been attacked, their contents read and copied; his bank accounts were investigated by state security agents who claimed he was under investigation for "unspecified suspected crimes". However, the attackers were only able to view details on two accounts and those details were limited to things such as the subject line and the accounts' creation date.[B3]
Conflict 2A (Reconnaissance)	Phase2a Prior to 2009: McAfee reported that the attackers had exploited purported zero-day vulnerabilities (unfixed and previously unknown to the target system developers) in Internet Explorer.
Conflict 2B (Replicate)	Phase 2b Prior to 2009: Once a victim's system was compromised, a backdoor connection that masqueraded as an SSL connection made connections to command and control servers running in Illinois, Texas, and Taiwan, including machines that were running under stolen Rackspace customer accounts. The victim's machine then began exploring the protected corporate intranet that it was a part of, searching for other vulnerable systems as well as sources of intellectual property, specifically the contents of source code repositories.

Hostilities (Assault)	Phase 3 Mid 2009 - December 2009: Zero day vulnerability used targeted intellectual property, email accounts of specific individuals hence invading privacy.
Post Hostilities (Obfuscation)	Phase 4 2010: This was a zero day vulnerability which is the hardest to detect.
Post Hostilities (Withdraw)	Phase 5 2010: To prevent future cyber-attacks such as Operation Aurora, Amitai Etzioni of the Institute for Communitarian Policy Studies has suggested that China and the United States agree to a policy of mutually assured restraint with respect to cyberspace. This would involve allowing both states to take the measures they deem necessary for their self-defense while simultaneously agreeing to refrain from taking offensive steps; it would also entail vetting these commitments. [B3] The German, Australian, and French governments publicly issued warnings to users of Internet Explorer after the attack, advising them to use alternative browsers at least until a fix for the security hole was made. The German, Australian, and French governments considered all versions of Internet Explorer vulnerable or potentially vulnerable. In an advisory on January 14, 2010, Microsoft said that attackers targeting Google and other U.S. companies used software that exploits a hole in Internet Explorer. The vulnerability affects Internet Explorer versions 6, 7, and 8 on Windows 7, Vista, Windows XP, Server 2003, Server 2008 R2, as well as IE 6 Service Pack 1 on Windows 2000 Service Pack 4. [B3]

Table: Operation Aurora: Case Precis

4.12 Operation Orchard

Conflict Background:

In 2007, a small flight of IAF fighter aircraft entered Syrian airspace undetected, dropped 17-tons of munitions on a military facility that reportedly housed fissile nuclear materials, and escaped unscathed. The IAF strike, titled Operation Orchard, quickly led to rumors that the IAF was able to execute this strike despite the existence of Syria's formidable air defense network – the same defenses that worried US policymakers in 2011 – by using a U.S.-developed cyber capability.

The Syrians were said to have been building the reactor with help from North Korea. The Israeli military's intelligence unit, known as 8200, was reportedly tipped off to this by the U.S. National Security Agency, which intercepted conversations between Syrian officials at the reactor and North Koreans.

Cyber Case Detail	
Case Code	Operation Orchard
Status Quo States	Syria
Non Status Quo States	Israel
Region	Middle East
Conflict Type	Interstate
Motive	Sabotage
Phase1	Sep 2006
Phase2	Late 2006
Phase3	Sep 6th 2007
Phase4	September 2007
Phase5	September 2007

Table: Operation Orchard: Case Detail

Figure17: Map of Conflict Region

Figure18: Operation Orchard: Suspected nuclear reactor site in Syria before it was bombed.

Phase	Activity
Dispute	Phase1 September 2006 through September 2007: Israel's concern about the facility really kicked into gear when it discovered that Iranian President Mahmoud Ahmadinejad traveled to Syria in 2006, according to Der Spiegel. The magazine alleges that Ahmadinejad promised the Syrians more than $1 billion to hasten their progress on the project.
Conflict 2A (Reconnaissance)	Phase2a: Agents of Israel's intelligence service hacked into the computer of a senior Syrian government official a year before Israel bombed a facility in Syria in 2007, according to Der Spiegel. [W17] The intelligence agents planted a Trojan horse on the official's computer in late 2006 while he was staying at a hotel in the Kensington district of London, the German news magazine reported Monday in an extensive account of the bombing attack. [W17]
Conflict 2B (Replicate)	Phase 2b: The weapon siphoned files from the laptop. The files contained construction plans for the Al Kabir complex in eastern Syria — said to be an illicit nuclear facility — as well as letters and hundreds of detailed photos showing the complex at various stages of construction
Hostilities (Assault)	Phase 3 September 5 2007: Late in the evening of September 5, when 10 Israeli fighter jets departed from a base in Northern Israel around 11 p.m. and headed west over the Mediterranean. Seven of them turned east to Syria, flying low, and took out a radar station with their missiles. About 20 minutes later they released their bombs on Al Kabir, located in the desert near the Euphrates river about 80 miles from the Iraq border.

Post Hostilities (Obfuscation)	Phase 4: The attack, dubbed "Operation Orchard," seemed to come out of nowhere and was marked by a resounding silence from both Israel and the United States afterward. The attack was a silent operation.
Post Hostilities (Withdraw)	Phase 5: Both the status quo and non-status states decided to keep deal with the matter in silence post attack.

Table: Case Precis: Operation Orchard

4.13 The Shamoon Attack I & II

Conflict Background:

Shamoon, also known as Disttrack, is a modular computer virus discovered by Seculert in 2012, targeting recent NT kernel-based versions of Microsoft Windows. The virus has been used for cyber espionage in the energy sector. Symantec, Kaspersky Lab, and Seculert announced its discovery on 16 August 2012. Similarities have been highlighted by Kaspersky Lab and Seculert between Shamoon and other malware [W1].

The Shamoon attack although inflicted on a Saudi Corporation, it is being discussed here as a cyber-warfare case due to its signature of a state sponsored attack. Saudi Aramco is state owned and the attack erased data on three-quarters of its corporate PCs – documents, spreadsheets, e-mails, files – replacing all of it with an image of a burning American flag. Although the US Intelligence pointed to Iran as the perpetrator, there is no specific evidence to support that. [W13]

TechRadar summarize the virus as a "dropper, wiper and reporter". [W12]

Cyber Case Detail	
Case Code	Shamoon I & II
Status Quo States	Saudi Arabia
Non Status Quo States	Adversary (Iran)
Region	Middle East
Conflict Type	Interstate
Motive	Sabotage
Phase1	Before Aug 2012 (Shamoon I) Before November 2016 (Shamoon II)
Phase2	Mid 2012 – Aug 2012 (I) Early November 2016

Phase3	15 Aug 2012 ; November 2016
Phase4	Aug 2012 through November 2016
Phase5	November 2016

Table: The Shamoon Attack I & II : Case Detail

Figure19: Shamoon I & II : Map of Conflict Region

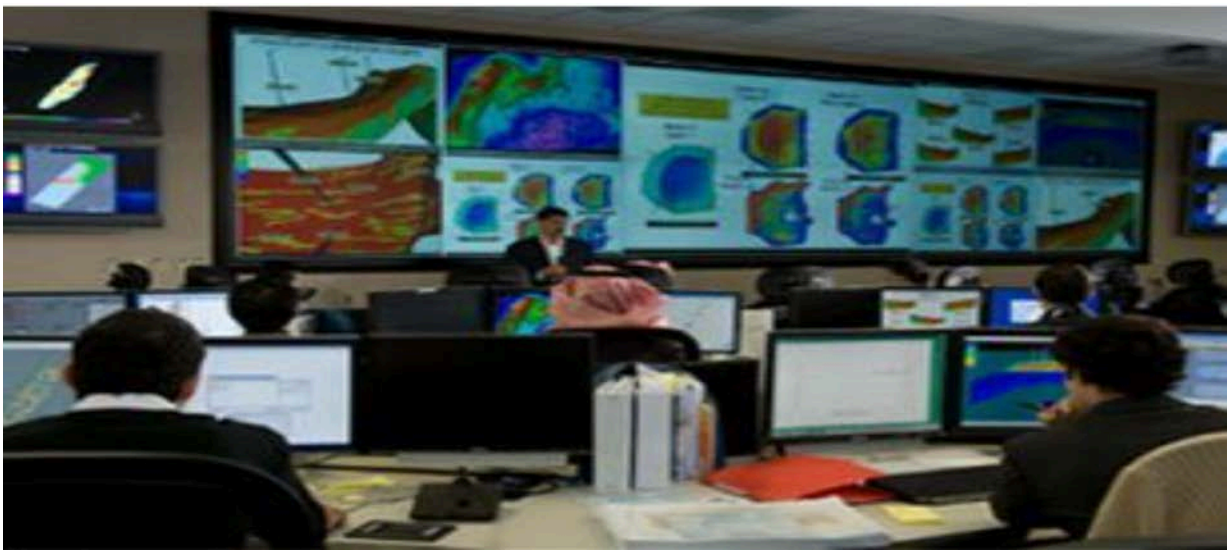

Figure20: Shamoon I: Saudi Aramco 30,000 workstations affected (Image source Saudi Aramco)

Phase	Activity
Dispute	Phase1 2012 (I) 2016 (II): The first known attack appears to be with the Saudi Arabian national oil company (Saudi Aramco). Although the company did not officially announced this right away, they were forced to isolate their computer network on August 15. Saudi Aramco's ability to supply 10% of the world's oil was suddenly at risk.
Conflict 2A (Reconnaissance)	Phase2a Mid 2012 (I) Late 2016 (II): It started sometime in mid-2012, a former security advisor to Saudi Aramco after the hack recalled. One of the computer technicians on Saudi Aramco's information technology team opened a scam email and clicked on a bad link. The hackers were in.[W14]
Conflict 2B (Replicate)	Phase 2b Mid 2012 through Aug 15 2012: The malicious code is transmitted through the Internet and then proceeds to move through networked computers, targeting computers which are not Internet connected. As data is removed it is sent back to the hacker's central computer. The 'dropper' component of the virus copies itself to a system task on the Windows OS.
Hostilities (Assault)	Phase 3 Aug 15 2012 (I), November 2016 (II): On Aug 15 2012 a person with privileged access to the Saudi state-owned Oil company's computers, unleashed a computer virus to initiate what is regarded as among the most destructive acts of computer sabotage on a company to date. Attack on 35,000 Aramco computers which render infected computers unusable, causing the company to spend a week restoring their services. The company goes offline after the attack. Shamoon II (November) The attack targeted at least one organization in Saudi Arabia, which aligns with the targeting of the initial Shamoon attacks. It appears the purpose of the new Disttrack samples were solely focused on destruction, as the samples were configured with a non-operational C2 server to report to and were set to begin wiping data exactly on 2016/11/17 20:45. [W15]
Post Hostilities (Obfuscation)	Phase 4 Aug 2012 ; November 2016: When the work of the virus was complete the attacker executed the module, which wiped all the evidence of its work and the virus itself.
Post Hostilities (Withdraw)	Phase 5 Early 2013; Early 2017: Five months later, with a newly secured computer network and an expanded cyber security team, Saudi Aramco brought its system back online. An attack of that size would have easily bankrupted a smaller corporation. [W14]

Table: Shamoon I & II: Case Precis

4.14 Russian hackers tracking Ukrainian artillery

Conflict Background:

The background between these two states is discussed in the Ukrainian power grid case. Per reports the motive for the intelligence would have likely been used to strike against the artillery in support of Russia-backed separatists in eastern Ukraine [W11].

A hacking group linked to the Russian government is being blamed for using a malware implant on Android devices to track and target Ukrainian artillery units from late 2014 through 2016, according to a report [B2].

Cyber Case Detail	
Case Code	Ukrainian Artillery Tracking
Status Quo States	Ukraine
Non Status Quo States	Russia
Region	Europe
Conflict Type	Interstate
Motive	Espionage
Phase1	20 Feb 2013
Phase2	Early 2014 through 2016
Phase3	Early 2014 through 2016
Phase4	Late 2014
Phase5	December 2014 Through 2016

Table: Case Detail: Ukrainian Artillery attack

Phase	Activity
Dispute	Phase1: Before 20 Feb 2013: The malware was able to retrieve communications and some locational data from infected devices, intelligence that would have likely been used to strike against the artillery in support of pro-Russian separatists fighting in eastern Ukraine, the report from cyber security firm CrowdStrike found. From late 2014 and through 2016, FANCY BEAR X-Agent implant was covertly distributed on Ukrainian military forums within a legitimate Android application developed by an Ukrainian artillery officer [B2].

Conflict 2A (Reconnaissance)	Phase2a May 2013 through 2016 : A developer App internally developed in the Ukrainian military is installed which had some 9000 users, reduced the time to fire the D-30 from minutes to seconds. Use of trojanized application was later found in the military application. [B2] Successful deployment of the FANCY BEAR malware within this application may have facilitated reconnaissance against Ukrainian troops. The ability of this malware to retrieve communications and gross locational data from an infected device made it an attractive way to identify the general location of Ukrainian artillery forces and engage them. The hacking group, known commonly as Fancy Bear or APT 28, is believed by U.S. intelligence officials to work primarily on behalf of the GRU, Russia's military intelligence agency [B2].
Conflict 2B (Replicate)	Phase 2b Early 2014 through 2016: 9000 users had the application running with the malware in the distribution forums.[B2][W11]
Hostilities (Assault)	Phase 3 Early 2014 through 2016 : April 2014 pro-Russian forces begin seizing government resources in Eastern Ukraine. July/Aug 2014 Malaysia Air Flight MH8 destroyed by pro-Russian separatists.[B2][W11]
Post Hostilities (Obfuscation)	Phase 4 Late 2014: The weapon (malware) was hidden in an Android application used by the Military for quick deployment of a war weapon. DDoS and targeted intrusions in media, financial and political entities in Ukraine.
Post Hostilities (Withdraw)	Phase 5 December 2014 through 2016: Minski Ceasefire signed but malicious app observed in distribution on forums.

Table: Ukrainian Artillery Attack: Case Precis

4.15 Yellowstone 1

Conflict Background:

In early 2014 hacktivists believed to be operating from Iran launched a cyber-attack on the Las Vegas Sands Corp. that shut down large sections of the casino company's computer networks in response to the Casino owners comments on Iranian foreign policy[w8]. Israel and Iran have interacted since Israel's birth in 1948[w1]. Although ideology has played a role, their respective regional strategic interests have largely shaped their relationship. Relations between the two countries were relatively close until the 1979 revolution. Arms transfers

from Israel to Iran continued for a short time, but there have been no publicly acknowledged deals since 1982. The 1982 Israeli invasion of Lebanon mobilized the Shiites. Iranian troops deployed in Lebanon and sired Hezbollah to fight Israel. Through a proxy, Iran now faces Israel across a common border. Iran also armed and funded Islamic Jihad, which carried out terrorist attacks within Israel in the 1990s and from Gaza since the 1980s. Iran's controversial nuclear program has raised the stakes for both sides in their regional rivalry. Some Israelis believe that their security justifies military action to ensure Iran does not acquire a bomb.

Cyber Case Detail	
Case Code	Sands Corp Attack
Status Quo States	US
Non Status Quo States	Iran
Region	Western Hemisphere
Conflict Type	Interstate
Motive	Sabotage
Phase1	October 2013
Phase2	Oct 2013 to Jan 2014
Phase3	Jan. 8, Jan 21, Jan 22 2014
Phase4	Oct 2013 – Feb 10 2014
Phase5	March 2014

Table: Yellowstone I: Case Detail

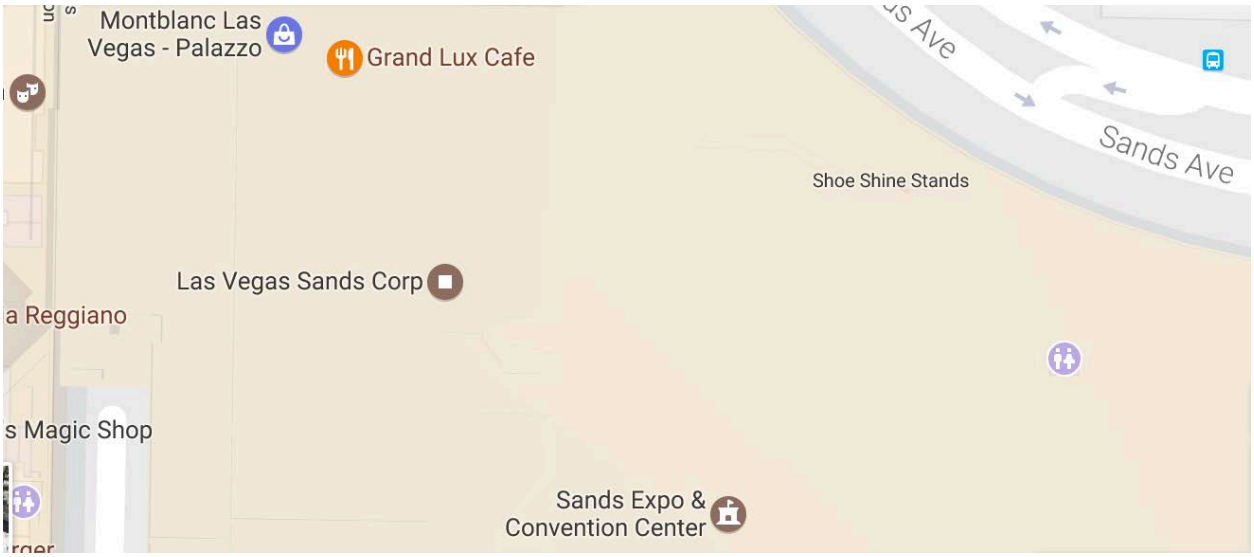

Figure21: Yellowstone1: Location of attack

Figure22: Yellowstone1: Casino's website showing burning US locations post attack

Phase	Activity
Dispute	Phase1: Jan 8 2014: Adelson, the rich Casino owner was speaking at a panel discussion on "Will Jews Exist?" at Yeshiva University in New York. He said he would put an end to any nuclear ambitions by Iran by detonating an atomic bomb in an unpopulated desert area of that country. He added: "And then you say, 'See? The next one is in the middle of Tehran."
Conflict 2A (Reconnaissance)	Phase2: Oct 2013 – Early Jan 2014: The earliest attempts to break into the Sands' networks involved brute-force attacks on the Sands Bethlehem in Pennsylvania, which uses computer systems, separate from the company's flagship casino in Las Vegas.
Conflict 2B (Replicate)	Phase 2b: Before February: Those efforts continued through the rest of January and into early February, when the hackers located the login information for a Las Vegas-based Sands senior computer systems engineer who had briefly spent time at the Pennsylvania site. That data enabled the hackers to launch the Feb. 10 "malware bomb" aimed directly at the computer systems in Las Vegas.
Hostilities (Assault)	Phase 3 Oct 2013 – Feb 10 2014: The attack, apparently precipitated by Sands CEO Sheldon Adelson's comments that the U.S. should use nuclear weapons to threaten Iran, could cost the company at least $40 million in repair and recovery efforts. The assault replaced the casino's content with their own, including a photo of Adelson with Israeli Prime Minister Benjamin Netanyahu, a U.S. map showing flames over the locations of Sands casinos and a list of Social Security numbers and e-mail addresses belonging to employees at the

	Pennsylvania location. A malware bomb wiped out about three-quarters of the company's Las Vegas computer servers. Computers were flat-lining, e-mail was down, most phones didn't work, and several of the technology systems that help run the $14 billion operation had sputtered to a halt
Post Hostilities (Obfuscation)	Phase 4 Oct 2013 – Feb 10 2014: The attack was done undercover by hackers although later reports suggest that Iran was involved.
Post Hostilities (Withdraw)	Phase 5 March 2014: This was a one-time attack in response to comments made by the Casino owner's public speech. The website and servers were restored back online and operational.

Table: Yellowstone1: Case Precis

4.16 Sony Corp's Hollywood studio

Conflict Background:

Although hostility between the two countries remains largely a product of Cold War politics, there were earlier conflicts and animosity between the U.S. and Korea. In the mid-19th century Korea closed its border to Western trade. In the General Sherman incident, Korean forces attacked a U.S. gunboat sent to negotiate a trade treaty and killed its crew, after fire from both sides because it defied instructions from Korean officials. A U.S. retribution attack, the Shinmiyangyo, followed.

Korea and the U.S. ultimately established trade relations in 1882. Relations soured again in 1905 when the U.S. negotiated peace at the end of the Russo-Japanese War. Japan persuaded the U.S. to accept Korea as part of Japan's sphere of influence, and the United States did not protest when Japan annexed Korea five years later. Korean nationalists unsuccessfully petitioned the United States to support their cause at the Versailles Treaty conference under Woodrow Wilson's principle of national self-determination.

Sony Pictures Entertainment was the victim of devastating cyber-attack in late November and early December 2014 that involved the release of stolen data including multiple yet-to-be-released films and personal employee information like social security numbers and salaries. Its been confirmed by US officials that North Korea orchestrated the hack, because the North Korean's did not like an upcoming film called 'The Interview' by Sony Pictures.

Cyber Case Detail	
Case Code	Sony Pictures Attack
Status Quo States	US

Non Status Quo States	Iran
Region	Western Hemisphere
Conflict Type	Interstate
Motive	Sabotage
Phase1	Months before November 2014
Phase2	November 2014
Phase3	Late November 2014
Phase4	December 16 2014
Phase5	February 2015

Sony Pictures Attack: Case Detail

Figure23: Sony Pictures Attack: Sony websites threatening to release data hacked by the group

Figure24: Sony Pictures Attack: map of headquarters

Phase	Activity
Dispute	Phase1 July 2014: When the BBC reached out to North Korean officials asking if they were behind the attack on Sony, they were given a curious response of "Wait and see." North Korea had also complained to the United Nations about the movie earlier this year in July, while not naming it specifically. This shows that the dispute had already started when the Movie in question had been publicized.
Conflict 2A (Reconnaissance)	Phase2a prior to November 2014: The malware used in the Sony attack took full advantage of the unprotected files and servers. For example a hacker could easily spot files named "password".
Conflict 2B (Replicate)	Phase 2b November 2014: Sony breach spread across servers as passwords were freely available to the hackers.
Hostilities (Assault)	Phase 3 July 2014 - November 2014: US Based Sony pictures make a movie with a plot to assassinate North Korean leader. North Korea complains to UN of the "movie". Just before the release of the movie attacks are launched over the Sony computer network and web servers. A lot of personal data is compromised. Web sites display hostile messages with demands leading to not release the movie.

Post Hostilities (Obfuscation)	Phase 4 November 2014 to : No clear trail on the source of the attack. Initial reports claimed that there was some Korean language signature in the analysis of the malware. Post attack there was another breach which reportedly pointed to involvement of Russian hackers. This shows the obfuscation.
Post Hostilities (Withdraw)	Phase 5 Feb 2015: Accusations had been made against North Korea and others, but ultimately the person(s) responsible for the breach were never brought to justice

Table: Sony Pictures Attack: Case Precis

4.17 Attack on Estonian Government

Conflict Background:

Estonia is a small country in Northern Europe. It borders the Baltic Sea, Latvia, and Russia. That last one is big in every sense of the word. A former Soviet satellite, Estonia was on the wrong end of a half-century occupation that turned the country into a hyper-militarized border zone from which the Soviet Army poised its war-fighting power toward the West.

In the middle of the 20th century, the country was traded back and forth between the Soviets and Nazis in bloodshed that resulted not just in tens of thousands of Estonian deaths but also a brutal authoritarian disruption to their society that ultimately lasted for decades. Before that, Estonia was ruled for centuries by powers like Sweden and Denmark.

In 2007, the Estonian government was getting ready to move a Bronze Soldier which was installed by the previous USSR. In response, ethnic Russians in the country rioted in the worst unrest Estonia had seen since the brief but bloody war of independence that commenced when the Soviets occupied the country in 1944.

Cyber Case Detail	
Case Code	Attack on Estonian Government
Status Quo States	US
Non Status Quo States	International Intelligence agencies
Region	Europe
Conflict Type	Interstate
Motive	Espionage and Sabotage

Phase1	27th April 2007
Phase2	6th April 2007
Phase3	September 2007
Phase4	2008
Phase5	2008

Case Detail: Attack on Estonian Government

Figure25: Attack on Estonian Government: Map of Conflict region

Phase	Activity
Dispute	Phase1 Early 2007: Estonia is Europe's most connected country. They've pioneered e-government and Internet voting. They're a world leader in Internet freedom. To say the country is "wired" would be a misnomer—it's Wi-Fi that saturates the air these days, so they're thoroughly wireless. In 2007, Estonian Govt was getting ready to move a bronze statue of a soldier that was installed previously during the USSR regime. This did not go well with the Russian population. The Estonian network was under attack, a tsunami of traffic was a botnet which are a horde of computers numbering in the hundreds of thousands, enslaved by hackers to act as a weapon for a botnet master. In enough quantity, bandwidth is a hard, blunt object that threatens to knock networks down.
Conflict 2A (Reconnaissance)	Phase2a April 2007: No data found.

Conflict 2B (Replicate)	Phase 2b April 2007: Over the course of several days, the botnets hit banks, broadcasters, police, and the national government. The parliament and ministries networks were overwhelmed, government communication networks were knocked down. The national emergency number buckled. The country's Internet infrastructure was being hit hard with unrelenting traffic that was orders of magnitudes larger than what Estonian networks were capable of handling.
Hostilities (Assault)	Phase 3 September 2007 : Estonia plans to remove the bronze statue of a solder. Riots start in the Russian regions of Estonia. Estonia's internet infrastructure goes down.
Post Hostilities (Obfuscation)	Phase 4 April 2008: Pinpointing and crediting a state-level cyber-attack is a difficult task that can easily rise to near impossible. Although there was no proof of origin of the attack found immediately due to the obscure nature of the attack, a year later a Russian individual living in Estonia was charged of this attack.
Post Hostilities (Withdraw)	Phase 5 2008: After four days under attack, it took face-to-face meetings between Lindqvist and Estonia's top cybersecurity authorities to begin to persuade the world's Internet service providers to single out and blacklist the attackers. Russia implemented limited sanctions against Estonia during this period, suspending some trains carrying passengers and raw materials to Tallinn. This attack was first of its kind and called the 'Web War'. Web War I changed all this with Estonia, too, and it had broader effects that continue to ripple through NATO to Russia and to the rest of the world today.

Table: Attack on Estonian Government: Case Precis

4.18 Operation Dust Storm

Conflict Background:

Threat actors behind the Operation Dust Storm have been active since at least 2010, the hackers targeted several organizations in Japan, South Korea, the US, Europe, and other Asian countries. Experts believe that the group is well organized and well funded, a circumstance that lead the researchers to speculate the involvement of a nation-state actor. Dubbed "Operation Dust Storm," the APT is the work of a sophisticated hacking group or army backed by a nation-state—most likely China based on ample circumstantial evidence to the United Nations about the movie earlier this year in July, while not naming it specifically.

Cyber Case Detail	
Case Code	Operation Dust Storm
Status Quo States	Japan
Non Status Quo States	International Intelligence agencies
Region	East Asia
Conflict Type	Interstate
Motive	Sabotage
Phase1	2010 - 2016
Phase2	2011 - 2015
Phase3	2015
Phase4	2015
Phase5	2016

Table: Operation Dust Storm: Case Detail

Figure26: Operation Dust Storm: Map of conflict regions

Phase	Activity
Dispute	Phase1 2010 - 2016: International Cyber espionage and state sponsored sabotage is

	commonplace in the 21st Century. This is a case example where international spy agencies with state sponsored traits launch an attack on Infrastructure on Asian countries like Japan. The attack timeline extends from 2010 which leveraged an unpatched browser vulnerabilities to continually forwarding victims in Japan and south Korea's SMS messages and call information back to their C2 servers
Conflict 2A (Reconnaissance)	Phase2a 2015: The attack was staged over several years where hackers used domain names and gather information using browser vulnerabilities and zero day watering hole attack. The spy group had been observed leveraging a malware application that called "ZLIB backdoor," with hard-coded proxy addresses and credentials, to silently gain access to private networks and collect information for reconnaissance purposes. Cyber espionage targets have included Japanese companies involved in power generation, oil and natural gas, construction, finance and transportation.
Conflict 2B (Replicate)	Phase 2b 2015: The pattern of the attack seems to be that the hackers would slowly spread the weapon using zero day and other vulnerabilities.
Hostilities (Assault)	Phase 3 2015: In July and October 2015, the same perpetrators launched attacks against a Japanese subsidiary of a South Korean electric utility as well as a major Japanese oil and gas company. Cylance also reported that the attackers began seriously ramping up its mobile operations in May 2015, adopting and customizing Android backdoors to collect SMS messages as well as enumerate and exfiltrate files from affected devices in Japan and South Korea. More than 200 domains hosting the Android malware have been discovered to date.
Post Hostilities (Obfuscation)	Phase 4: Largely undetectable through standard antivirus programs, the backdoor gives attackers the ability to upload and download files, impersonate log-on sessions, manipulate Windows services, mimic keystrokes and mouse clicks, execute shell commands and more.
Post Hostilities (Withdraw)	Phase 5: No data found.

Table: Operation Dust Storm: Case precis

4.19 Operation Anarchist

Conflict Background:

It should not be surprising to anyone that super power nations are often involved in espionage activities especially in sensitive or historically problematic regions where problems escalate quickly. Such espionage activities could take place with allies or with adversaries' states. UK and US were involved in one such espionage activity called the Operation Anarchist. Operation Anarchist was a joint operation between the American National Security Agency and British Government Communications Headquarters to monitor advanced weapons systems in the Middle East, with a particular focus on Israel. Begun in 1998, it was publicly exposed in January 2016 as a result of documents released by Edward Snowden. It has been called the worst intelligence breach in Israel's history.

Cyber Case Detail	
Case Code	Operation Anarchist
Status Quo States	Israel, Iran
Non Status Quo States	USA, Britain
Region	Middle East
Conflict Type	Interstate
Motive	Espionage
Phase1	1998
Phase2	1998
Phase3	1998
Phase4	1998
Phase5	2016

Table: Operation Anarchist: Case Detail

Figure27: Operation Anarchist: Map of conflict region.

Phase	Activity
Dispute	Phase1 1998 Operation Anarchist was a joint operation between the American National Security Agency and British Government Communications Headquarters to monitor advanced weapons systems in the Middle East, with a particular focus on Israel. In addition to Israel, advanced weapons systems used by Egypt, Turkey, Iran, Syria, and Hezbollah were also hacked into. In particular, the operation managed to obtain footage of Iranian-made drones operated by the Syrian government.
Conflict 2A (Reconnaissance)	Phase2a 1998: The Israeli Air Force's UAV fleet was its primary target. Encrypted video transmissions between drones and their bases were intercepted from Troodos and analyzed using powerful computing systems, as well as the open-source software tools ImageMagick and AntiSky, which allow users to patiently sort through the pixels to decrypt them. This was the preferred method over using the massive computing power it would have taken to unscramble the encrypted signals in near real time.
Conflict 2B (Replicate)	Phase 2b 1998 - 2016: In addition to footage from drone cameras, the operation also tracked the movements of Israeli drones, using the special parts of transmissions when the drone would update the base on its location. In addition to Israel, advanced weapons systems used by Egypt, Turkey, Iran, Syria, and Hezbollah were also hacked into.

Hostilities (Assault)	Phase 3 1998-2016: The surveillance allowed the NSA and GCHQ to see the payloads the drones were carrying. While drones were the primary target, on January 3, 2008, technicians from Menwith Hill managed to capture 14 seconds of cockpit footage from an Israeli F-16 fighter jet on a bombing mission over Gaza, showing a target on the ground being tracked. A sub-operation of Operation Anarchist, code-named Operation Runway, tracked the Israeli Black Sparrow air-launched missiles, which were used as targeting missiles during tests of the Arrow missile.
Post Hostilities (Obfuscation)	Phase 4 1998-2016: The operation was run out of GCHQ headquarters in Cheltenham, with most of the surveillance taken from RAF Troodos, a Royal Air Force communications installation in the Troodos Mountains of Cyprus, with RAF Menwith Hill, a joint US-British satellite surveillance base in Britain, also participating.
Post Hostilities (Withdraw)	Phase 5 2998-2016: Begun in 1998, it was publicly exposed in January 2016 as a result of documents released by Edward Snowden. It has been called the worst intelligence breach in Israel's history.

Table: Operation Anarchist: Case Precis

4.20 The Deception Program

Conflict Background:

When considering past cases of cyber terrorist attacks arguably the most notorious attacks was during the cold war in 1982, the CIA allegedly found a way to disrupt the operation of a Siberian gas pipeline to the Soviet without using traditional explosive devices such as missiles or bombs. Instead, they caused the Siberian gas pipeline to explode using a portion of a code in the computer system that controls its operation in what they tagged as "logic bomb." When many people think of Siberia, they imagine freezing temperatures and enormous wasteland; however, Siberia contains a huge supply for natural gas. Conversely, getting this natural gas from the far reaches of the Russian northwest into Moscow posed problematic. The Soviet Union had the skills and knowledge to engineer a solution, although a manual operation would stand too strenuous. Furthermore the Soviet Union did not have the computing expertise to automate more of the processes. Consequently, the KGB (Committee for State Security) sent an operative to a Canadian company to steal the software in order to create the pipeline.[34]

The Euro-Siberian gas pipeline under construction, officially called "Rossiya No. 6" by the Soviet Union, was part of a large-capacity, long- distance network originating from the natural gas fields of the Taz Peninsula, in the Western Siberian region of Yamal, north of the Arctic Circle. Rossia No. 6 was to ultimately consist of a double 56-inch wide, 4451 kilometer

long pipeline joining Urengoi field to the border town of Uzhgorod, where it is to be connected with the MEGAL pipeline over Czechoslovakia to the West European gas network.

Cyber Case Detail	
Case Code	Siberian Pipeline
Status Quo States	Soviet Union
Non Status Quo States	United States
Region	Europe
Conflict Type	Interstate
Motive	Sabotage
Phase1	1982
Phase2	1982
Phase3	1982
Phase4	1982
Phase5	2016

Table: Siberia Pipeline: Case Detail

Figure28: Siberia Pipeline: Map of gas pipeline

Phase	Activity
Dispute	Phase1 1940 through 1990 The Soviet pipeline dispute arose when the US imposed controls on pipeline-related technology in response to Soviet activity in Poland.28 The embargo, generally viewed as short-sighted by West European countries, caused a major crisis in Euro-American relations.

	This marked the era of the cold war between primarily the USSR and the USA. The Cold War was to dominate international affairs for decades and many major crises occurred including the Cuban Missile Crisis, Vietnam, Hungary and Berlin Wall.
Conflict 2A (Reconnaissance)	Phase2a 1982: The CIA project leader and his associates studied the Farewell material, examined export license applications and other intelligence, and contrived to introduce altered products into KGB collection. American industry helped in the preparation of items to be "marketed" to Line X. Contrived computer chips found their way into Soviet military equipment, flawed turbines were installed on a gas pipeline, and defective plans disrupted the output of chemical plants and a tractor factory.[W20] One of the first software "Trojans" in an Early SCADA/ICS proprietary technology was introduced as weapon. The Trojan Horse was loaded into the technology used in Siberian Gas Pipeline from a Canadian Industrial hardware firm.
Conflict 2B (Replicate)	Phase 2b 1982: "In order to disrupt the Soviet gas supply, its hard currency earnings from the West, and the internal Russian economy, the pipeline software that was to run the pumps, turbines and valves was programmed to go haywire after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds," Mr Reed writes.
Hostilities (Assault)	Phase 3 1982: While there were no physical casualties from the pipeline explosion, there was significant damage to the Soviet economy. Its ultimate bankruptcy, not a bloody battle or nuclear exchange, is what brought the Cold War to an end.
Post Hostilities (Obfuscation)	Phase 4 1982: The project proved to be a model of interagency cooperation, with the FBI handling domestic requirements and CIA responsible for overseas operations. The program had great success, and it was never detected.[W20]
Post Hostilities (Withdraw)	Phase 5 1982: Although some military intelligence officers avoided compromise, the heart of Soviet technology collection crumbled and would not recover. [W20]

Table: Siberian Pipeline: Case Precis

4.21 Operation Dessert Storm

Conflict Background:

Post-World War II international dynamics gradually drew the United States into a deeper political relationship with Iraq. The onset of cold war raised fears in Washington about Soviet expansion into Middle East and generated a determination among American leaders to prevent the spread of communism in Iraq. When Saddam Hussein seized power in Baghdad in1979, mounting tension between the two gulf powers erupted into war in September 1980 when US got involved in the Iran-Iraq war and shifted toward a position of supporting Iraq. In the aftermath of Iran-Iraq war, Iraq sought territorial and economic gains at the expense of Kuwait and in 1989 and 1990 Iraq decided to use force against the tiny emirate.

On January 16 1991, Operation Dessert Storm began. The conflict, as known as the Gulf War, was waged by a U.N. authorized coalition force from 34 nations led by the United States in response to Iraq's invasion of Kuwait. A network borne Virus was first detected in computer systems at Ames Research Center also known as the Morris Worm incident [45]. Two years after the Morris Worm incident, the same security loopholes still existed, with very few updates to defense mechanisms, and cyber attackers again exploited precisely the same vulnerabilities. These loopholes were compounded by the increased connectivity of TCP/IP and allowed a group of hackers based out of the Netherlands to gain control of server hosts in the ARPAnet, and then to use those hosts as a springboard into the MILnet. Security expert, Andrew Landsman describes the attacks very well, excerpt below.

The first indications of the widespread break-ins into MILnet hosts were from log entries in Department of Energy (DoE) machines. The attackers broke into DoE machines using what now seems like very rudimentary attack methods, including password guessing (or sometimes even using null passwords), exploiting a VMS vulnerability in the SYSMAN utility, exploiting trust relationships between hosts, and a few others. Once they gained access to a host, they often already had super-user privileges, but if they did not, they exploited other vulnerabilities to take complete control of the victim systems. They then installed back doors. By breaking into hosts at DoE sites such as Los Alamos National Laboratory, Lawrence Livermore National Lab, Fermi National Lab, Sandia National Lab, and Brookhaven National Lab, the attackers had more than enough springboards from which they could launch attacks against MILnet hosts at military centers such as US Navy Headquarters, the Pacific Fleet Command, Rome Air Force Base, Kelly Air Force Base, the Pentagon, and many more, which they did successfully day after day for well over a year.

Cyber Case Detail	
Case Code	Operation Desert Storm
Status Quo States	US
Non Status Quo States	International Hackers
Region	Middle East

Conflict Type	Interstate
Motive	Espionage
Phase1	1990
Phase2	January 16 1991
Phase3	1991
Phase4	1991
Phase5	1991

Table 1: Operation Dust Storm: Case Detail

Figure29: Operation Dessert Storm: Map of conflict region

Phase	Activity
Dispute	Phase1 July 1990: Iraq's invasion of Kuwait in July 1990. Iraq accused the United States and Israel of deliberately weakening Iraq by encouraging Kuwait to reduce oil prices. When Iraq began to threaten Kuwait early in July 1990, the United States staged maneuvers in the Gulf to warn Iraq against taking military action against the United Arab Emirates and Kuwait.
Conflict 2A (Reconnaissance)	Phase2a 1990: The first indications of the widespread break-ins into MILnet hosts were from log entries in Department of Energy (DoE) machines. The attackers broke into DoE machines using what now seems like very rudimentary attack methods, including password guessing (or sometimes even using null passwords), exploiting a VMS vulnerability in the SYSMAN utility, exploiting trust relationships between hosts, and a few others.

Conflict 2B (Replicate)	Phase 2b Jan 16 1991: Once the attackers broke into DoD hosts, they used commands such as grep in Unix systems to discover files that contained the information they desired: information about military equipment, weapons systems, troop and warship movements (especially in connection with Operations Desert Storm and Desert Shield) and much more—they often even searched for "nuclear." The attackers stole so much information that they quickly filled the hard drives of their own machines. They then resorted to downloading huge amounts of information onto systems at the University of Chicago and Bowling Green University. The worst part of the fiasco was that the DoE's Computer Incident Advisory.
Hostilities (Assault)	Phase 3 1991: The attackers stole so much information that they quickly filled the hard drives of their own machines. They then resorted to downloading huge amounts of information onto systems at the University of Chicago and Bowling Green University. The worst part of the fiasco was that the DoE's Computer Incident Advisory _Capability (CAIC) noticed and reported the attacks to the DoD.
Post Hostilities (Obfuscation)	Phase 4 1991: The weapon operated undetected after sending 'beacons' to a remote command and control server.
Post Hostilities (Withdraw)	Phase 5 1991: Fortunately, the criminals were not politically motivated. Instead the hackers tried to sell the information to Saddam Hussein for one million dollars. Hussein, for whatever reason, never took them up on the offer, possibly thinking it a hoax. Needless to say, had he done so, the Desert Storm conflict may have taken a drastically different course.

Table: Operation Dust Storm: Case Precis

4.22 Operation Buckshot Yankee

Conflict Background:

A worm named Agent.btz had spread widely among military computers around the world, especially in Iraq and Afghanistan, creating the potential for major losses of intelligence. Pentagon officials consider the incident, discovered in October 2008, to be the most serious breach of the U.S. military's classified computer systems. The response, over the past three years, transformed the government's approach to cybersecurity, galvanizing the creation of a new military command charged with bolstering the military's computer defenses and preparing for eventual offensive operations. The efforts to neutralize the malware, through an operation code-named Buckshot Yankee, also demonstrated the importance of computer espionage in devising effective responses to cyber threats. The first sign of trouble was a mysterious signal emanating from deep within the U.S. military's classified computer

network. Like a human spy, a piece of covert software in the supposedly secure system was "beaconing" — trying to send coded messages back to its creator. The presence of US troops overseas had given rise to espionage from International Intelligence agencies.

Cyber Case Detail	
Case Code	Operation Buckshot Yankee
Status Quo States	US
Non Status Quo States	International Intelligence agencies
Region	Middle East
Conflict Type	Interstate
Motive	Espionage and Sabotage
Phase1	June 2008
Phase2	October 2008
Phase3	October 2008
Phase4	October 2008
Phase5	October 2010

Table 2

Figure30: Region of attack

Phase	Activity
Dispute	Phase1 October 2008: The presence of US troops overseas had given rise to espionage from International Intelligence agencies.
Conflict 2A (Reconnaissance)	Phase2a 2006 – 2008: Weapon (malicious code) uploaded itself onto a network run by the US Central Command. This is a network administrator's worst fear, a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary.
Conflict 2B (Replicate)	Phase 2b 2008: The malicious code spread undetected on both classified and unclassified systems establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control.
Hostilities (Assault)	Phase 3 2008: The weapon had the ability to scan computers for data, open backdoors, and send through those backdoors to a remote command and control server. It took pentagon nearly 14 months of stop and go effort to clean out the worm. The Assault in this case was not very effective as the 'beacon' to which the code was talking to was never ever respond.
Post Hostilities (Obfuscation)	Phase 4 2008: The weapon operated undetected after sending 'beacons' to a remote command and control server.
Post Hostilities (Withdraw)	Phase 5 October 2010: US created Cyber Command Control. This attack was a large trigger to the creation of the Cyber Command Control. The NSA and the military investigated for months how the infection occurred. They retrieved thousands of thumb drives, many of which were infected. Much energy was spent trying to find "Patient Zero," and finally two years from the date of attack the patient zero (thumb drive) was traced to an infected flash drive that was inserted into a U.S. Military laptop at a base in the middle east.

Table: Operation Buckshot Yankee Case Precis

4.23 2016 US Elections

Conflict Background:

The U.S. intelligence community, in a joint January 6, 2017 declassified report, stated that Russian President Vladimir Putin "most likely wanted to discredit Secretary Hillary Clinton because he has publicly blamed her since 2011 for inciting mass protests against his regime in late 2011 and early 2012, and because he holds a grudge for comments he almost certainly saw as disparaging him." On March 20, 2017, FBI Director James Comey testified that Putin "hated Secretary Clinton so much that the flip side of that coin was he had a clear preference

for the person running against the person he hated so much."

Cyber-attacks by foreign governments are a constant threat to political campaigns. Since campaign operations are temporary, they often do not invest heavily in the kind of security those financial institutions, large companies and government agencies spend millions or billions of dollars on each year.

After the break-up of the Soviet Union in 1991 and the end of the Cold War, the U.S.-Russian relationship took on a new dimension, and contacts between citizens expanded rapidly in number and diversity. Russians and Americans work together on a daily basis, both bilaterally and multilaterally, in a wide range of areas, including combating the threats of terrorism, nuclear arms proliferation, HIV/AIDS and other infectious diseases, and other global challenges. Not surprisingly, there remain issues on which both governments do not agree. Even after 200 years, the relations continue to evolve in both expected and unexpected ways.

Cyber Case Detail	
Case Code	US Elections
Status Quo States	US
Non Status Quo States	Russia
Region	Western Hemisphere
Conflict Type	Interstate
Motive	Espionage
Phase1	2016
Phase2	2016
Phase3	November 2016
Phase4	2016
Phase5	2016

Case Detail: US Election Hack

Phase	Activity
Dispute	Phase 1 Early 2015: Russian hackers penetrate the computer systems of the Democratic National Committee in an espionage operation that enabled them to read emails, chats and a trove of opposition research.

Conflict 2A (Reconnaissance)	Phase 2a June 2016: Operatives from two Russian spy agencies had infiltrated computers of the Democratic National Committee, months before the US national election [B1]. One agency, nicknamed *Cozy Bear* by the cybersecurity company CrowdStrike, used a tool that was ingenious in its simplicity and power to insert malicious code into the DNC's computers, The other group, nicknamed *Fancy Bear*, remotely grabbed control of the DNC's computers.
Conflict 2B (Replicate)	Phase 2b June 2016: Post-analysis of the attack included small fragments of code called PowerShell commands. One of the PowerShell modules inside the DNC system connected to a remote server and downloaded more PowerShells, adding more nesting dolls to the DNC network.
Hostilities (Assault)	Phase 3 June 2016 to April 2017 [W1] : In June 2016, the Democratic National Committee (DNC) first stated that the Russian hacker groups Cozy Bear and Fancy Bear had penetrated their campaign servers and leaked information via the Guccifer 2.0 online personal.[W1] On July 22, 2016, WikiLeaks released approximately 20,000 emails sent from or received by DNC personnel. Debbie Wasserman Schultz resigned as DNC chairwoman following WikiLeaks releases suggesting collusion against Bernie Sanders' presidential campaign. On October 7, 2016, WikiLeaks started releasing series of emails and documents sent from or received by Hillary Clinton campaign manager John Podesta, which continued on a daily basis until Election Day. Podesta later blamed Russia for hacking into his email and claimed the leaks had "distorted" election results. In April 2017, CIA Director Mike Pompeo stated: "It is time to call out WikiLeaks for what it really is—a non-state hostile intelligence service often abetted by state actors like Russia." Pompeo said that the U.S. intelligence community had concluded that Russia's "primary propaganda outlet," RT, had "actively collaborated" with WikiLeaks.
Post -hostilities (Obfuscation)	Phase 4 2015 through June 2016 [B1]: The Cozy Bear intrusion relied primarily on the SeaDaddy implant developed in Python and compiled with py2exe and another PowerShell backdoor with persistence accomplished via the Windows Management Instrumentation (WMI) system, which allowed the adversary to launch malicious code automatically after a specified period of system uptime or on a specific schedule. The PowerShell backdoor is ingenious in its simplicity and power. It consists of a single, obfuscated command setup to run persistently.

Post-hostilities (Withdraw)	Phase 5 December 2016: The DNC attack was widely publicized, and documents/emails/other information leaked out to the public via WikiLeaks. Overall, the mission of the adversary was accomplished assuming the original intent was to prevent the DNC candidate from winning the 2016 election.

Table: Case Precis: US Elections

4.24 Wannacry

Conflict Background:

The WannaCry ransomware attack was a worldwide cyber-attack by the WannaCry ransomware cryptoworm, which targets computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.[W1]
Researchers have identified some similarities in the WannaCry code and tools used by State hackers in previous attacks. Although, they have cautioned that it is too early to definitively attribute the attack to a state actor.[W21]

Cyber Case Detail	
Case Code	Wannacry
Status Quo States	150 Countries
Non Status Quo States	
Region	World
Conflict Type	Interstate
Motive	Sabotage
Phase1	Prior to Jan 16 2017
Phase2	Jan 16 2017
Phase3	May 12 – May 13, 2017
Phase4	May 12 – May 13, 2017
Phase5	March 14 - May 14, 2017

Table: WannaCry : Case Detail

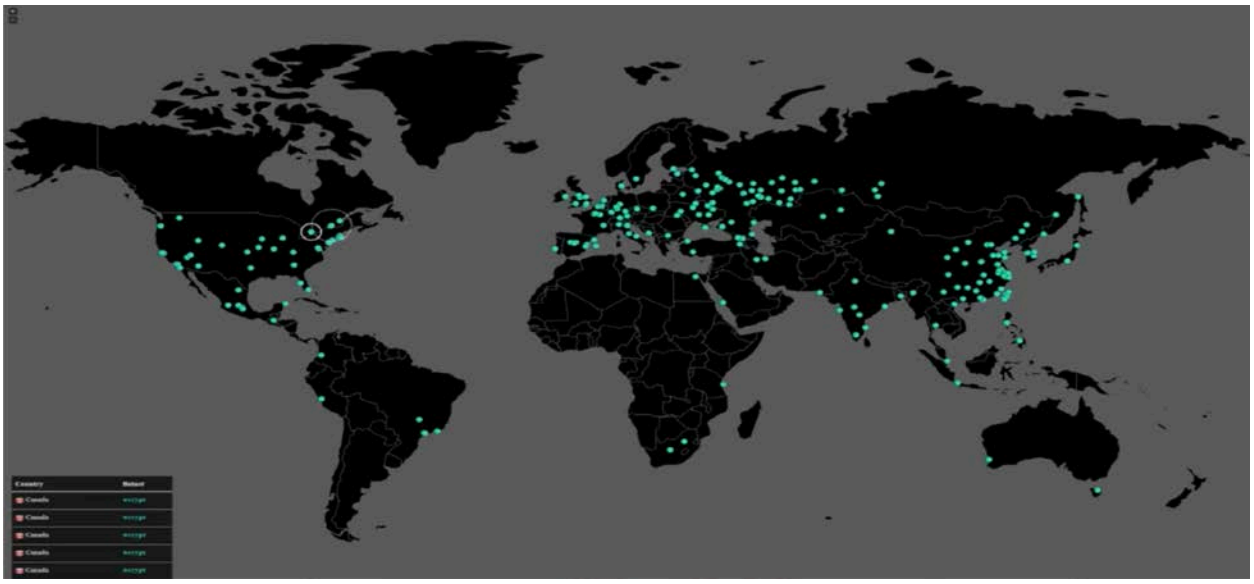

Figure31 : WannaCry: Regions simultaneously affected by the malware

Phase	Activity
Dispute	Phase1 Jan 16 2017: Cyber criminals are often state-sponsored and execute actions with tremendous resources leading to a larger impact of the attack. As discussed earlier, state-sponsored cyber-attacks can have deadly consequences.
Conflict 2A (Reconnaissance)	Phase2a Jan 16 2017: Before a ransomware can encrypt files, it needs to locate file shares on the network, which requires performing internal reconnaissance. WannaCry's behaviors were reconnaissance and lateral movement on the internal network, within the enterprise perimeter.
Conflict 2B (Replicate)	Phase 2b Jan 16 2017: WannaCry spread across local networks and the Internet to systems that have not been updated with recent security updates, to directly infect any exposed systems. To do so it used the EternalBlue exploit developed by the U.S. National Security Agency (NSA), which was released by "The Shadow Brokers" two months before.
Hostilities (Assault)	Phase 3 May 12 – May 13, 2017: The attack started on Friday, 12 May 2017, and has been described as unprecedented in scale, infecting more than 230,000 computers in over 150 countries. Parts of Britain's National Health Service (NHS), Spain's Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide.
Post Hostilities (Obfuscation)	Phase 4 May 12 – May 13, 2017: The WannaCry malware is indirectly loaded and is not directly exposed to the disk. Thus, obfuscating it from anti-virus software analysis.

Post Hostilities (Withdraw)	Phase 5 March 14 - May 14, 2017: Shortly after the attack began, a web security researcher who blogs as "MalwareTech" discovered an effective kill switch by registering a domain name he found in the code of the ransomware. This greatly slowed the spread of the infection, but new versions have since been detected that lack the kill switch. As per official news agencies reports, the cyber attack has slowed down drastically and has died down as of 19 May 2017.

5. Analysis of the Cases

5.1 Breakdown of Cyber-tools Used

Cyber-warfare is often portrayed in the same manner as nuclear weapons: fearfully elevated to the massive disruption of communication networks, power grids and nations' infrastructures. In reality, cyber-battles are more akin to the independent conflicts of the Cold War, occurring on even smaller, less physical scales. The following details the means through which cyber-warfare is engaged and, perhaps more crucially, describes how the versatile, small-scale goals of cyber-warfare differentiate it from the raw destruction associated with nuclear warfare.

5.1.1 Cyber-espionage

This is a common technique applied by state actors to gather information for illegal, exploitative methods. Most information retrieved does not contain state secrets or confidential information, but this mode can be utilized for blackmail purposes. In our case studies, it was seen during the Operation Anarchist where the US and British intelligence conducted a cyber-espionage activity to monitor advanced weapons systems in the Middle East, with a particular focus on Israel.

5.1.2 Web Vandalism

A cyber-warrior commits web vandalism by defacing a webpage and modifying aspects of its poorly secured framework. This is the digital equivalent of graffiti and serves as a means of agitation rather than harm. An infamous example in the case study was when the British government hacked an Al-Qaeda website and replaced a bomb-making recipe with HTML code for cupcake recipes.

5.1.3 Propaganda

This is a version of web vandalism where the spread of political propaganda, rather than mere agitation, is the focus of the attack. The cyber-warrior attacks a webpage by modifying its contents to advocate some sort of political message. This is considered a more severe

form of vandalism as the user is, in effect, censoring the target's message with their own. In the Sands Corp. case study, a non-status quo state had penetrated the company's websites, which were hosted by a third party, and defaced them, posting a photograph of Sheldon Adelson chumming around with Benjamin Netanyahu, as well as images of flames on a map of Sands' U.S. casinos in an effort to show Adelson's strong support for the Israelis. Al Qaeda uses their websites (ex: Ansar al-Mujahidin) for propaganda and to recruit candidates.

5.1.4 Confidential Data Acquisition

A more complex and severe form of cyber-espionage that involves gathering information on confidential subjects. Successful execution requires maneuvering through a target's complex security system with the intent of acquiring data about some confidential target, typically military information and trade secrets. The case study of Operation Desert Storm showed *attackers broke into DoD* hosts to discover files that contained the information about military equipment, weapons systems, troop and warship movements (especially in connection with Operations Desert Storm and Desert Shield) and much more; they often even searched for "nuclear." The attackers stole so much information that they quickly filled the hard drives of their own machines.

5.1.5 Distributed Denial-of-Service (DDoS)

This mode of attack occurs when a large quantity of computers send denial-of-service (DoS) attacks to another system in a different location. Thus attacks are accomplished with large groups of users accessing a website at the same time, overwhelming the server and forcing it to shut down. This attack prevents other users from accessing the website and can possibly damage the server hardware if proper protection is not installed, thus denying that website's service and information to other users. The attack also has higher prevalence due to its lower barrier of entry for novice hackers. In our case studies, we see quite a few instances of DDoS attacks, and it seems to be a common weapon used to disable networks on the non-status side. In the Ukraine Grid attack, for instance, the non-status quo side used DDos, TDoS type attacks on the status-quo side to launch a telephone denial-of-service attack against customer call centers to prevent customers from calling in to report the outage. TDoS attacks are similar to DDoS attacks that send a flood of data to web servers. In this case, the center's phone systems were flooded with thousands of bogus calls that appeared to come from a certain location.

5.1.6 Equipment Distribution

This typically is the interception of an electronic order for a product and/or service (such as a military armament supply) and the replacing and/or blocking of the order, so as to generate confusion and reduce the morale of the enemy's organization. This requires a moderately high degree of technical skill, as these orders are highly guarded against a cyber-attack because of their confidential nature. In our case studies, we did not see this type of

attack intentionally to intercept the electronic order system, but in some cases, such as the zero-day attacks and Morris worm type cyber-attacks, it is apparent the non-status quo side could have exercised this type of attack easily.

5.1.7 Critical Infrastructure Attacks

This is the damaging of public utilities (power, water, fuel, communications, commercial or transportation systems) with a virus intended to disrupt their functionality. An understanding of complex software and the ability to circumvent cyber-security barriers is required for attacks of this degree. The effects of these viruses can be very detrimental and specific, as evidenced by the Stuxnet attack against the Iranian nuclear program.

5.1.8 Compromised Counterfeit Hardware

This involves the distribution of infected software from a manufacturer to its clients. The software, from as low as microprocessor code to normal desktop applications, hides the virus and remains dormant for extended periods of time before becoming active. The process requires several layers of connections to perform properly—specifically, communication with individuals within the production and manufacturing process. The infected software can accomplish an innumerable set of functions, from data dumping to destroying the computer's ability to work. This type of vulnerability is commonly referred to as a zero-day attack and was used in the Stuxnet case to destroy the non-status-quo side's nuclear power plant. The distribution occurred from the windows OS to the SCADA system controlling the nuclear reactor.

5.1.9 Theft or Destruction of Hardware

The more "brute-force" approach to cyber-warfare, the physical interaction with a computer, is considered to be the most effective way to gather information and disrupt an enemy. This is accomplished either by stealing or destroying the system's hardware. It is noted from the case studies that this is a popular weapon used in cyber-war cases, such as Stuxnet and Ukranian Power Grid.

5.1.10 Case Application – Performance Ratings

One of the applications of structuring information in the form of a CASCON table (detail, précis) is to be able to understand cyber-warfare in its different dimensions. One such dimension is that of performance rating. A cyber-attack requires tremendous planning in order to be under the radar of the target environment and achieve the strategic objective. From the cases discussed in this thesis, we can note that the footprint and signature is unique. I used a methodology pioneered by Spy-Ops [41] called Scenario-Based Intelligence Analysis (SBIA) and Transdisciplinary Intelligence Engineering (TIE) to rate individual cases. The results are shared in the table below; the approach on how it was arrived at is also described

here. The approach, featured in *Cyber Terrorism* magazine in 2006, drew the following response: "Scenario-Based Intelligence Analysis (SBIA) is a force- multiplier, value-added intelligence concept that can yield returns for the decision-maker. Not only can SBIA help reduce ambiguity that often plagues intelligence analysis, it also answers the 'So what?' of information collected. In the analytical world, this is where the rubber meets the road." [46]

Strategy	An attack that uses malicious code hidden inside a computer imported by a country. I gave a score of 1 if a hidden malicious code existed. This is the easiest way is to look for zero-day vulnerability in the case précis reconnaissance phase.
Objective	A non-status quo state was able to cause mass disruption of the status quo state's information infrastructure.
Weapon	The scale of weapon, such as a massive distributed denial of service attack. The case précis table's assault phase documents the weapon and its scale of attack.
Plan	Create the capability to launch a massive denial of service attack from within a targeted country. This could be accomplished by inserting malicious code into personal computers and laptops at the point of manufacture. The planning phase in the case précis implies whether the plan included such a capability. If so, a score of 1 was given.
Tactic	Covertly place malicious code in millions of computers at the point of manufacture. Hiding malicious code into the reported 50 million lines of code in VISTA or the reported 55 million lines of code in Linux would be the mechanism of delivery for the attack.
Imports	The United States imports a significant amount of advanced technology. One report showed that China exported nearly $74 billion of advanced technology products to the United States. The weapon used was from an imported product.
Detection	Uncovering this kind of attack with current testing techniques and practices is highly unlikely. It is like looking for a needle in a haystack—a few lines of code dispersed throughout the millions of legitimate lines of code. Limited tools are available to detect the hidden code, so the primary method of detection would be manual code inspection. Given that every computer would have to be checked for the hidden code, the likelihood of detecting this type of an attack would be very, very limited. In our cases, if the weapon was detected or diffused in time before any damage, a score of 1 was given to the case; if not, a 0 was given.
Result	At a designated time, all the computers infected with the malicious code would begin to flood the networks they are connected to with malicious transactions. This flood would inhibit the networks' ability to conduct legitimate transactions. As the volume of malicious transactions increases, the associated server(s) and network(s) would fail. The impact of the attack as is shown in the assault phase in the case précis table, points to such a problem.

Cases →	Stuxnet	Ukraine Power	Kosovo	Russia-Georgia	Cast Lead	Tulip	Jasmine	DuQu	Eastern	Anthem
Factors ↓										
Strategy	1	1	0	0	0	0	0	1	0	0
Objective	1	1	1	1	0	0	1	1	1	1

Weapon	1	1	1	1	1	1	0	1	1	1
Plan	0	1	1	1	1	1	1	0	0	0
Tactic	1	0	0	0	0	0	0	1	0	1
Imports	1	0	0	0	0	0	0	1	0	0
Detection	0	0	0	0	0	0	0	0	0	0
Result	0	0	0	0	0	0	1	0	0	0
Totals	**5**	**4**	**3**	**3**	**2**	**2**	**3**	**5**	**2**	**3**

Table: SBIA and TIE Rating for Cyber Cases (Part I) [41]

Cases →	Aurora	Orchard	Shamoon I & II	Ukrainian Artillery	Yellowstone I	Sony Corporation	Estonian Government
Factors ↓							
Strategy		1	1	0	1	1	0
Objective		1	1	1	1	1	1
Weapon		1	1	1	1	1	1
Plan		1	1	0	1	1	0
Tactic		0	0	0	0	0	0
Imports		1	1	1	1	1	0
Detection		0	0	0	0	0	0
Result		0	0	0	0	0	0
Totals		**5**	**5**	**3**	**5**	**5**	**2**

Table: SBIA and TIE Rating for Cyber Cases (Part II) [41]

Cases →	Dust Storm	Operation Anarchist	Deception	Desert Storm	Buckshot Yankee	Elections	WannaCry
Factors ↓							
Strategy	1	1	1	0	0	0	0
Objective	1	1	1	1	1	1	0
Weapon	1	0	1	1	1	0	1
Plan	1	1	1	1	1	0	1
Tactic	0	0	1	0	0	0	0
Imports	1	0	8	0	0	0	0
Detection	0	1	1	0	0	0	0
Result	0	0	1	0	0	1	0

Totals	4	4	7	3	3	2	2

Table: SBIA and TIE Rating for Cyber Cases (Part III) [41]

Using the above tables we deduce the following results:

1. A set of eight factors were compared against each case discussed in this thesis, a simple 1 or 0 score were awarded to each factor if it was relevant to the case. The sum of the score gave the total number.
2. A higher performance score (the 'Totals' row) indicates overall a better planning, execution and result for the cyber-attack.
3. As an example, let's look at the Deception case. This case was very well planned and executed and hence it has a higher score. The strategy to use a zero-day vulnerability, the scale of the attack which resulted in the pipeline explosion and the objective of crippling the infrastructure without causing any human loss or being detected gave it a high score of 8.
4. Another example of a low score could be the Eastern Railway defacement case where the score was low (2). This could mean that the plan was poorly made and executed. The objective was not achieved. A low score could also indicate that some of the data was not available to make a decision for that factor.

6. Conclusions

6.1 New Perspective on Cyber-warfare

The objective of this thesis was twofold. The first objective was to research historical cyber-warfare incidents from the past to the present and capture relevant data in a data acquisition phase. The first phase needed to analyze the timeline of events in this incident and develop the necessary insight to be able to analyze the parties involved in order to mark them as status quo side or non-status-quo side. This provided an indication of motive from the non-status-quo side and the progression of escalation. The second objective involved mapping the cyber-warfare incidents to MIT's CASCON framework. The CASCON mapping presented the data collected from the incidents in a structured form, which is important since its database of kinetic warfare was extensive.

The CASCON based analysis for cyber-incidents not only revealed insights into what actually happened during a cyber-incident, but helped answer key questions that could potentially cover some predictive behavior of involved states and conflicts in a region. There is undoubtedly a large amount of knowledge that is to be learned and considered, both from the historical point of view that CASCON provides and from current affairs. The results of this thesis are not meant to be conclusive, but a study of state-sponsored cyber- cases using MIT's CASCON to map and categorize information for future learning about conflicts involving states.

The following traits were apparent of cyber-warfare from the cases analyzed in this thesis:

- Reduced costs compared to conventional strikes.
- Higher efficiency in achieving the goal.
- The asymmetric nature of the cyber-attacks makes defense difficult.
- The anonymous nature of the offense allows the attacking government to circumvent approval by the world community compared with a military offensive.
- Possibility to conduct cyber-attacks in peacetime for immediate geopolitical ends, as well as to prepare for possible future kinetic attacks.

6.2 Using the CASCON (Extended) Method for Cyber-warfare

CASCON provided a framework to systematically gather, store, organize and analyze the information from various sources. Cyber-warfare incidents are inherently unproven due to the secretive nature of their operations. CASCON methodology helped in isolating status-quo from non-status-quo in the conflict situation and largely in giving history, form and context to an isolated cyber-attack. A brief introduction of how each step helped is given below:

Step 1. Case Detail. This step helped in identifying the parties, the locale, the underlying conflict region and the dates that mark the thresholds between phases. All of these items are shown on the case detail table at a glance.

Step 2. Case Precis. The case precis provided a short history, or precis, summarizing the major features of the case organized by phase. The phase model extended for cyber helped analyze the weapon and provides lenses through which typical cyber-attacks can be described using the case precis table.

Step 3. Factor coding. This thesis gave me an opportunity to think through code factors in cyber and document the most relevant ones. Two cases were analyzed with code factors for cyber; the corresponding table is provided in this thesis. The extended CASCON factors describe circumstances and events that have been influential in historical cases and determine whether each factor is present or not present in the new case. If present, the goal was to decide what influence the factor has in the case, whether toward or away from increased violence and to what degree.

7 Contributions

Following contributions were noted from this thesis:

- Cyber-warfare cases were researched and documented using the CASCON framework. Several books, articles, journals, reports and blogs were referenced (see list of references) to come up with a structure, intent, background and a possible pattern for the list of cases.

- The cases may or may not point to a pattern, but to the seasoned eye, they will likely reveal more than just structured information.

- Reading through the cases may give the reader a better understanding of the requirements of mapping cyber-warfare metadata in a new framework.

- One of the main contributions is that the research paves a path towards preparing a new case. It is often helpful to browse through the historical cases in CASCON's database to look at case detail, précis and factors windows.

- This thesis extended the steps of CASCON for cyber-warfare. A new phase model for cyber was created in an attempt to explain the details of the cyber-attack, type of weapon used, along with the planning and execution of the attack. The reconnaissance and obfuscation was noted for each cyber-case (refer to the case precis tables). A set of code factor categories and code factors were developed for cyber as an extension to the existing kinetic model to cover cyber-warfare (refer to the Olympic games and Ukrainian Power Grid cases). It was beyond the scope of this thesis to apply the code factors to all researched cases.

- The information from the cyber-warfare cases was applied towards a performance rating of the cases. This is a typical example of how metadata can be used to derive results. The score for each state-sponsored cyber case is discussed based on Scenario-based Intelligence Analysis (SBIA) and Transdisciplinary Intelligence Engineering (TIE), and a rating of individual cases was done. Each case was rated with a set of eight scenario-based factors and totaled to indicate the final performance rating for that case. Although the performance score is subjective to this thesis it may help the reader of the existence of such tools and a way to use them.

8 Future Work

This thesis started the work of mapping cyber-warfare cases and extending CASCON to include cyber. Future work could extend but not limited to the following:

8.1 Case Expansion

A limited set of about 24 cases based on investigative reports that they were state-sponsored were analyzed in this thesis. More cases could be researched.

8.2 CASCON Extension

This thesis extended the CASCON framework defined for kinetic warfare. The newly defined elements including cyber-phase model and code factors were used to categorize the limited set of cases in this thesis. These elements in this could be further extended.

8.3 Pattern Modeling

A system dynamics (SD) model for the nonlinear behavior of cyber-warfare could be developed keeping prediction and prevention in mind.

8.4 User Experience Using Software

A new software user interface and database similar to CASCON to add/modify new cyber-cases can be built.

9 References

1. Cyber Security Review. 26 Mar. 2017.
2. Bloomfield, Lincoln P., and Allen Moulton. *Managing International Conflict: From Theory to Policy: A Teaching Tool Using CASCON*. New York: St. Martin's, 1997. Print.
3. Carr, Jeffrey. *Inside Cyber Warfare*. 2012. Print.
4. Chapple, Mike, and David Seidl. *Cyber Warfare: Information Operations in a Connected World*. Burlington, MA: Jones & Bartlett Learning, 2015. Print.
5. Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge, MA: MIT, 2012. Print.
6. Choucri, Nazli. "Explorations in Cyber International Relations: A Research Collaboration of MIT and Harvard University." *SSRN Electronic Journal*. Print.
7. Choucri, Nazli, Christi Electris, Daniel Goldsmith, Dinsha Mistree, J. Bradley Morrison, Michael Siegel, and Margaret Sweitzer-Hamilton. "Understanding & Modeling State Stability: Exploiting System Dynamics." *SSRN Electronic Journal*. Print.
8. Clarke, Richard A., and Robert K. Knake. *Cyber War: The next Threat to National Security and What to Do about It*. New York: Ecco, 2012. Print.
9. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. Washington, DC: Executive Office of the President of the United States, 2009. Print.
10. Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016. Print.
11. Madnick, Stuart E., Xitong Li, and Nazli Choucri. "Experiences and Challenges with Using CERT Data to Analyze International Cyber Security." *SSRN Electronic Journal*. Print.

12. Madnick, Stuart, Nazli Choucri, and Jeremy Ferwerda. "Institutional Foundations for Cyber Security: Current Responses and New Challenges." *SSRN Electronic Journal*. Print.
13. Popp, Robert L., and John Yen. *Emergent Information Technologies and Enabling Policies for Counter-terrorism*. Hoboken, NJ: Wiley-Interscience, 2006. Print.
14. Reed, Thomas C. *At the Abyss: An Insider's History of the Cold War*. New York: Ballantine, 2005. Print.
15. Review, NATO. "The History of Cyber Attacks - a Timeline." *NATO Review*. Web. 26 Mar. 2017.
16. Russinovich, Mark E. *Rogue Code: A Novel*. New York: Thomas Dunne /St. Martin's, 2014. Print.
17. Russinovich, Mark E., and Kevin D. Mitnick. *Trojan Horse*. New York: St. Martin's Griffin, 2014. Print.
18. Russinovich, Mark E., and Howard Schmidt. *Zero Day*. New York: St. Martin's, 2012. Print.
19. Salim, Hamid M. "Cyber Safety : A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks." *DSpace@MIT*. Massachusetts Institute of Technology, 01 Jan. 1970. Web. 26 Mar. 2017.
20. Iheagwara, Charles M. "The Strategic Implications of the Current Internet Design for Cyber Security." *DSpace@MIT*. Massachusetts Institute of Technology, 01 Jan. 1970. Web. 26 Mar. 2017.
21. Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford UP, 2014. Print.
22. Stiennon, Richard. *There Will Be Cyberwar:b How the Move to Network-Centric Warfighting Set The Stage For Cyberwar*. Birmingham, MI: IT-Harvest, 2015. Print.
23. VanPutte, Michael A. *Walking Wounded: Inside the U.S. Cyberwar Machine*. Place of Publication Not Identified: Publisher Not Identified, 2017. Print.
24. Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown, 2014. Print.
25. Ziegler, Dustin P. *Foundations of a Defense Digital Platform: Business Systems Governance in the Department of Defense*. 2012. Print.
26. Nils Melzer. *Cyber Warfare and International Law.* 2011. White paper
27. Office Of Naval Research. *Dynamics of Undersea Cables: Emerging Opportunities and Pitfalls.* 2012. Report.
28. Michael Sechrist. *Cyberspace in Deep Water: Protecting Undersea Communications Cables By Creating an International Public-Private Partnership.* Harvard University: 2010. Report.
29. E-ISAC. *Analysis of the Cyber Attack on the Ukranian Power Grid.* 16 March, 2016. Defence Use Case.
30. Norway, Gjovik. *Cyber Warfare, An Unorthodox View From the Battlefield.* 18 September, 2015. Slides.
31. Stuart Madnick, Nazli Choucri, Steven Camiña, Wei Lee Woon. *Towards Better Understanding Cybersecurity: or Are 'Cyberspace' and 'Cyberspace' the Same?".* 15 December, 2012. Proceedings of the Workshop on Information Security & Privacy (WISP).
32. Nazli Choucri, Stuart Madnick, Priscilla Koepke. *Institutions for Cyber Security: International Responses and Data Sharing Initiatives'.* August 2016. Working Paper.

33. Director Of Central Intelligence. *Memorandum From CIA on MIT CASCON Project.* 5 February, 1974. Memorandum.
34. Mary Dobbing and Chris Cole. *Israel and the Drone Wars.* Paper.
35. Patriozio Mercial. *The Euro-Siberian Gas Pipeline Dispute - A Compelling Case for the Adoption of Jurisdictional Codes of Conduct.* Paper.
36. David Hollis. *Cyberwar Case Study: Georgia 2008.* 25 March, 2017. Small Wars Journal.
37. Georgetown University's Edmund A. Walsh School of Foreign Services. *Georgetown Security Studies Review.* 7 April, 2014. Article.

38. Robert J. Bunker. Fifth Dimensional Battle-space: Terrorism and Counter-Terrorism Implications; Claremont Graduate University; 2-10-2015.

39. Robert Bunker and Charles "Sid". Fifth Dimensional Operations: Space-Time-Cyber Dimensionality in Conflict and War—A Terrorism Research Center Book ; 2014.

40. Greylogic. Project Grey Goose Phase II Report - The evolving state of cyber warfare ; March 20, 2009.

41. Kevin Coleman. Cyber Warfare – White Paper.

42. CIIS Report. Cyber War Preparedness, Cyberspace Arms Control and the United States; No. 3 August 2014.

43. John Arquilla and David Ronfeldt. Cyberwar is coming, RAND Corporation.

44. Kevin Coleman. Critical Infrastructure Protection; May 24 2006.

45. D. Fisher, H. Finger, W. Kramer, J. Stanley. Report of Computer Virus Incident at Ames; November 2-5, 1988.

46. Technolytics Institute. World War III – A Cyber War has Begun; September 2007.

48. Xiaobing Li, Xiansheng Tian; Evolution of Power: China's Struggle, Survival, and Success; 2013.

Web References:
W1. Wikipedia (https://en.wikipedia.org).

W2. Internet Live Stats (www.internetlivestats.com).

W3 Security Affairs ;
Article; http://securityaffairs.co/wordpress/8153/malware/shamoon-malware-cyber-espionage-tool-cyber-weapon-or.html.

W4. Cyber War Preparedness, Cyberspace Arms Control and the United States; No. 3 August 2014.

W5. http://mil-embedded.com/guest-blogs/warfare-evolution-blog-moving-toward-next-generation-warfare/

W6. MIT Technology Review; Article; First Detailed Public Map of U.S. Internet Backbone Could Make It Stronger; by Tom Simonite; September 15, 2015.

W7. The Pentagon's Cyberstrategy ; Foreign Affairs; William Lynn September/October 2010 issue.

W8. *Bloomberg (*https://www.bloomberg.com).

W9. Before the Gunfire, Cyberattacks; John Markoff ; NY Times Aug 12 2008.

W10. U.S. code-cracking agency works as if compromised; Jim Wolf - Tehnology News Reuteurs ; Dec 16 2010.

W11. Radio Free Europe Radio Liberty https://www.rferl.org/ Report: Russian Hackers Tracked Ukrainian Artillery Units ; December 22 2016.

W12. Shamoon virus attacks Saudi oil company; Tim Sandle; Aug 18 2012; Digital Journal.

W13. New York Times ; Various articles including:

- In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back; Oct 23 2012.

W14. CNN Money; The inside story of the biggest hack in history; August 5, 2012.

W15. Shamoon 2: Return of the Disttrack Wiper; Robert Falcone; November 30, 2016; Unit 42;

W16. In Combat Debut, Navy Jammer Targets Libyan Tanks ; pencer Ackerman; 03.21.11.

W17. Mossad Hacked Syrian Official's Computer before Bombing Mysterious Facility; Kim Zetter; 11.03.09.

W18. Jasmine Revolution; Tunisian history; The Editors of Encyclopædia Britannica.

W19. Wired; Article: Kaspersky Finds new Nation-State Attack; Kim Zetter 06.10.15.

W20. CIA Library; A Deception Operation; The farewell Dossier; Duping the Soviets.

W21. Foreign Policy; Who Is Really to blame for the WannaCry ransonware? Report. May 15 2017.

W22. Goggle Maps; used for several the nation maps in this thesis.

Blogs:

B1. Bears in the Midst: Intrusion into the Democratic National Committee; June 15, 2016; Dmitri Alperovitch; From The Front Lines.

B2. Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units; December 22, 2016; Adam Meyers; Research & Threat Intel.

B3. A new approach to China". Google Inc. 2010-01-12. Retrieved 17 January 2010.

Press Releases:

PR1. Investigation of major Anthem cyber breach reveals foreign nation behind breach; California Department of Insurance; January 6 2017 Press release.