CYBERWAR: ROLE OF NON-STATE ACTORS

A Dissertation submitted to the Panjab University, Chandigarh for the award of Masters of Philosophy in Social Science, in partial fulfilment of the requirement for the Advanced Professional Programme in Public Administration

By

GS Sabherwal
(Roll No 4531)

Under the Guidance of
Dr Surabhi Pandey

45th ADVANCED PROFESSIONAL PROGRAMME IN PUBLIC ADMINISTRATION
(2019-20)

INDIAN INSTITUTE OF PUBLIC ADMINISTRATION
NEW DELHI

CERTIFICATE

I have the pleasure to certify that Shri GS Sabherwal, has perceived his research work and prepared the present dissertation titled ‘**Cyberwar: Role of Non-state Actors’,** under my guidance and supervision. The dissertation is a result of his own work and to the best of my knowledge, no part of it has earlier comprised any other monograph, dissertation or book. This is being submitted to Panjab University, Chandigarh, for the degree of Masters of Philosophy in Social Sciences in partial fulfilment of the requirement for the Advanced Professional Programme in Public Administration of Indian Institute of Public Administration, New Delhi.

I recommend that the dissertation of Shri GS Sabherwal is worthy of consideration for the award of M. Phil. degree of Panjab University.

(**Dr. Surabhi Pandey)**
Supervisor
Indian Institute of Public Administration
IP Estate, Ring Road
New Delhi

ACKNOWLEDGEMENT

I am extremely grateful to my guide Dr. Surabhi Pandey for her invaluable guidance and constant encouragement during the course of the study. The dissertation in its present form has been possible only due to her painstaking efforts in going through the draft and making valuable suggestions/corrections. All through the study she guided me patiently, tirelessly and cheerfully. She has been extremely generous in giving preference to my dissertation work despite her extremely busy schedule.

I extend my sincere thanks to Prof. G Bhattacharjee, Programme Director and Prof. Neetu Jain, Programmme Co-director, who are a constant source of encouragement during the course of the program.

I am also thankful to the staff of APPPA office, specially Shri Manish Rawat who provided logistic support during the writing of this dissertation.

Last but not the least, I am grateful to my wife Shabnam and my children Naina and Angad for their help, support and patience during the process of writing this dissertation and pursuing the program.

(GS Sabherwal)
(Roll No. 4531)
45th APPPA

Table of Contents

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

1.	APT	Advanced Persistent Threats
2.	CAN	Computer Network Attack
3.	CERT	Computer Emergency Response Team
4.	CNE	Computer Network Exploitation
5.	COTS	Commercial-Off-The-Shelf
6.	CPU	Central Processing Unit
7.	DDoS	Distributed Denial of Service
8.	DOD	Department of Defense
9.	DoS	Denial of Service
10.	FBI	Federal Bureau of Investigation
11.	FSB	Federal Security Service
12.	ICT	Information and Communication Technology
13.	IP	Internet Protocol
14.	IT	Information Technology
15.	MITM	Man-in-the-Middle
16.	OPSEC	Operation Security
17.	OS	Operating System
18.	PC	Personal Computer
19.	PDA	Personal Digital Assistant
20.	PLC	Programmable Logic Controllers
21.	PPI	Pay-Per-Install
22.	PRC	People’s Republic of China
23.	RAT	Remote Administration Tool
24.	RBN	Russian Business Network
25.	SCADA	Supervisory Control and Data Acquisition
26.	Tech	Technology
27.	VPN	Virtual Private Network

CYBERWAR: ROLE OF NON-STATE ACTORS

EXECUTIVE SUMMARY

1. Computer and Internet are one of the greatest human's inventions. Since their arrival, they have transformed our society and improved our lives. The rising significance of cyberspace to modern civilization and its increasing use in global dominance is becoming a tool for national power globally. The primary difference between a cyber-attack to commit a crime or attack is found in the **intent of the attacker**. Innovative and sophisticated cybercrime tools allows nation state or criminals to remain undetected while they initiate cyber-attacks against other nations. A small hacker, either working independently or being hired by the state, could take on a Nation State by his mere geekiness and an encounter like David vs Goliath could be a reality.

2. Cyber warfare is emerging as a smarter and effectual method to wage war as it seeks to achieve political goals without extensive use of armed forces. Cyberspace has become the fifth domain of warfare after land, maritime, air and space.

3. In the advent of large-scale cybercrime and cyber operations, it is vital to have cybersecurity means in place. Cybersecurity refers to the practices, protocols and techniques designed to protect devices, software, data and network from attack, damage, manipulation or unauthorized access.

4. The tools used for Cyber-incidents and Cyber-attacks are common to cybercrime and so are the individuals, groups, underground organisations who are employed by terror outfits and nation-states to meet their motivations and ends. The difference between the state and non-state actors has been eclipsed and lack of competent cyber workforce may compel states to hire non-state actors. The inherit characteristics of cyberspace like its asymmetric nature, obscurity, non-attributability, easy access, the legal ambiguity and its role as an efficient medium for protest, crime,

espionage and aggression, makes it a favourable territory for nation-states as well as non-state actors in cyber conflict. Hence there is a requirement

(a) To study the trends in role of non-state actors in cyber-incidents,

(b) To assess the reasons for Nations to hire non-state actors,

(c) Identify future means of Cybersecurity.

5. The research was Exploratory primarily based on “Case Study” method. A total of 19 Cyber incidents and Cyberattacks were studied since 1999 whose data was available in open source.

6. The main purpose has been to study the various non-state actors who coexist in cyberspace and their employment by nation-states in cyberspace operations. Based on the analysis of cyberattacks and cyber-events, the conflicts can be categorized in the following categories: -

(a) Nation states vs Nation states,

(b) Non-state actors vs Nation states and

(c) Non-state vs Non-state actors

7. The first category, i.e. Nation states vs Nation states conflict is a legitimate act wherein it has some legality and an intrinsic justifiable cause. These conflicts are closely related to the definition of Cyberwar. Our main concern is on the other two categories of conflict namely; **Non-state actors vs Nation states** and **Non-state vs Non-state actors** and the role played by the Non-state actors in them.

8. The requirement to initiate a political agenda with a strategic edge, nation-states are tempted to employ cyber non-state actors. It nevertheless assures significant asymmetric advantages to a weaker nation-state with anonymity and provides an efficient shield against subsequent blame and political ramifications. While some nation-states might favour ratifying a novel legal framework defining acts of hostility

in cyberspace, it seems likely that many others would find it far more beneficial to maintain the present obscurity that surrounds cyberspace and perhaps even actively deter such initiatives. Even though if an international group is successful in framing cyberwar rules and aligns it with international law, it probably would still be ineffective as the employment of non-state actors in cyberspace operations is still in effect legally a gray-area.

9. The case studies have highlighted this new category of Non-state Vs Non-state actors which could have far-fetched consequences in the near future. Anonymous has openly challenged ISIS and their online resources and operations. It has provided a glimpse of what information warfare might look like in the future. Perhaps such a test might turn out to be a gift in disguise for the security organisations. It could also highlight gaps and seams between multiple disciplines, like cyber security, critical infrastructure protection, civil rights and civil liberties, information operations, countering violent extremism, counterterrorism and law enforcement.

10. Due to obscurity nature of cyberspace, it has been rather difficult to determine the exact type of actors being involved, however the types of attacks have been closely studied. It may be seen that Spear-phishing, DDoS, Thumb-drive infected malware and SCADA attacks have been predominant with percentages as high as 42.11%, 21.05% and 15.8% respectively.

11. It is vital for individuals to understand that cybersecurity and cyber defense are of vital importance. Actors are constantly attempting to exploit any vulnerability in systems and networks to manipulate or deny access. The inference from the attacks clearly highlight that humans are the most vulnerable component of any cyber system and human error allows attackers achieving these goals even though individuals and organizations subscribe to best practices. It is thus important to subscribe to the best

computer-practices and mitigate the risk of cyber-attacks. Also, it is clearly revealed that majority of the time cybercrime tools were utilised and exploited. Hence, same cybersecurity practices that protect users against everyday cyber-incidents and cyber criminals will provide adequate protection against nation-backed cyber-attackers.

12. Some contemporary and futuristic ideas on cybersecurity are suggested as, employing latest technology in creation of a newer and securer Internet infrastructure and protocols, splintering of the Internet into subnets, utilize a version of Block Chain technology to make the net safer, deploy artificial intelligence to identify new attacks and instead of fearing the hackers, lure them into a trap and use the information to train the computer to recognise and stop future attacks. Also, IoT is gradually maturing and surely needs security protocols to be built-in its protocol else we will see a much unsafe cyberspace with increasing dependencies on IoT.

CHAPTER - 1

CYBERWAR : INTRODUCTION AND AN OVERVIEW

1.1 Introduction

"A Crime will happen where and only when the opportunity avails itself."

Computer and Internet are one of the greatest human's inventions. Since their arrival, they have transformed our society and improved our lives. Information and Communication Technology (ICT) is the field involving technology and covers wide range of areas that include computer hardware, software, information systems, programming languages etc. It has become a valuable source for development, commerce, communication, entertainment, companionship and is bound to affect profoundly almost all human activities including education, industry, commerce, governance, personal lives and social life around us. On 30 Jun 2011, Pope Benidict XVI joined Twitter. This incident reinforces the fact that none of us can avoid embracing the internet wave of connectivity and socializing. With about half the world's population, i.e approx. 3.2 billion, connected to the internet, India stands second with approx. 460 million.

Cybercrime, once the territory of discontented genius teenagers as depicted in the movies "War Games" and "Hackers", has developed into a mature and complicated threat to the open nature of the net. Cyber-criminals, akin to their non-virtual traditional criminal counterparts, look for gaps in law enforcement. The news reports are filled with inputs of devastating denial of service attacks, vandalised web pages and new computer viruses worming their way through the cyber. However, there are innumerable other cyber incidents that are kept undercover due to private industry's hesitancy to announce its vulnerability and the government's anxiety on security.

Experts believe and give an argument that there is no agreed-upon definition for "cybercrime" because "cyberspace" is just a new specific instrument used to help commit crimes that are not new at all. It refers largely to any criminal activity that pertains to or is committed through the use of the Internet. A wide variety of conduct fits within this extensive definition. The term ''cybercrime'' is sometimes used synonymously with Internet crime, technological crime, digital crime, economic crime or electronic crime, to describe crime committed with computers or other ICT devices.

1.2 Statement of Research Problem

A cyber-attack is deliberate exploitation of computers, technology-dependent systems and networks. Cyber-attacks use malicious code to modify computer code, data or logic, leading to disruptive results that can compromise data and lead to cybercrimes, such as identity theft and information manipulation. Irrespective of Cyber Strategy and Cyber tactics used, Cyberattack is an act of war if compared with *Principles of War by Clausewitz*. Cyber Warfare aptly represents Sun Tzu's definitive order of attack when engaging an enemy - *First attack the enemy's strategy, then his alliance, next his army, and last his cities*. Cyberspace has become the fifth domain of warfare after land and maritime have been supplemented by two additional domains, air and space.

The rising significance of cyberspace to modern civilization and its increasing use in global dominance is becoming a tool for national power globally. The inherit characteristics of cyberspace like its asymmetric nature, obscurity, non-attributability, easy access, the legal ambiguity and its role as an efficient medium for protest, crime, espionage and aggression, makes it a favourable territory for nation-states as well as non-state actors in cyber conflic **(Johan Sigholm, 2016)** t. A small hacker, either working independently or being hired by the state, could take on a Nation State by his mere geek-ness and an encounter like David vs Goliath could be a reality.

The most significant shift, in the Cyberwar, is in the demographics of war is the influx of civilians into battle. The difference between the state and non-state actors has been eclipsed. Also, cyber operations can take place anywhere and everywhere and has led to complete loss of physical battlefield. Members of Al-Qaeda or ISIS, be particularly likely to turn to cyber-weapons to compensate for the lack of kinetic forces. Also, Nations may use such means to meet their political and geo-strategic dominance. Lack of such cyber workforce may compel states to hire non-state actors to avoid attributability and complications at a later stage.

Increasingly, in the last decade, war is also moving towards the cyber realm, state armies, but also violent non-state actors, are thither extending their scope of action. Recent cyber events linked to military operations, such as the Georgian cyber-attacks or “Operation Israel” conducted by the hacker group Anonymous, highlight the central role played by non-state actors in such context, clearly demonstrating their ability and boldness to participate in cyberwarfare whether with state actors or against them.

In the advent of large-scale cybercrime and cyber operations, it is vital to have cybersecurity means in place. Cybersecurity refers to the technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security is vital because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. As the incidents and sophistication of cyber-attacks grow, governments and corporates, especially those that are tasked with safeguarding information relating to national security, infrastructure, health or financial data, need to take steps to protect their sensitive information and corporate secrets. Nations have to have their own cyber security strategies and policies in place. Also, Nation states have to come together to work out on common policies to prevent any cybercrimes or operations being originated from their state against any other state, its infrastructure or any other organisation.

1.3 **Purpose or Objectives**

The objectives of the research are as follows: -

(a) To study the trends in role of non-state actors in cyber operations/ cyber war.

(b) To assess the reasons for Nations to hire non-state actors for cyber operations.

(c) Identify future means of Cybersecurity against cyber-attacks.

1.4 **Rationale or Justification**

A cyber related incident of national significance may take any form; an organized cyber-attack, an uncontrolled exploit such as computer virus or worms or any malicious software code. A national disaster with significant cyber consequences is capable of causing extensive damage to the info, infra or key assets. Large-scale cyber-attacks may jeopardise the government, public and private sector resources and services by disrupting functioning of critical information system. Complications from disruptions of such a magnitude may threaten lives, economy and national security.

Computer networking technology has also blurred the boundaries between Cybercrime, Cyber-terrorism, Cyber-espionage and Cyberwar. Officials in government and industry now say that cybercrime and cyber-attack services available for hire from criminal organisations are a growing threat to national security. Innovative and sophisticated cybercrime tools allows nation state or criminals to remain undetected while they initiate cyber-attacks against other nations. Many experts point out that past incidents of conventional terrorism have already been linked with cybercrime and that computer vulnerabilities may make government and civilian critical infrastructure systems seem attractive as targets for cyber-attack.

As per Jeffrey Carr, Principal Investigator of the open source intelligence effort Project Grey Goose, ample evidence is available that many of the non-state hackers who participated in the Georgian and Gaza cyber wars were also involved in other petty cybercrimes **(Carr, 2011)**. It was, in effect, their "day job." The main difference is in the intent, wherein

(a) Cybercrimes are performed for personal gains

(b) Whereas, Cyberwar has no personal gains but affect interest of nation-states.

(c) Another reasoning goes that one is a military problem, whereas the other is a law enforcement problem.

(d) If a terrorist group were to launch a cyber-attack to cause harm, such an act also fits within the definition of a cybercrime.

The primary difference between a cyber-attack to commit a crime or to commit terror is found in the **intent of the attacker**, and it is possible for actions under both labels to overlap. International acts of cyber conflict (commonly but inaccurately referred to as cyberwar) are intricately enmeshed with cybercrime, cyber security, cyber terrorism, and cyber espionage. The web of interconnections, sense of anonymity, lacking geographical limits, advanced technology and sense of obscurity, complicates the issues and makes the core issue and intent even murkier.

> ***At this time, it is unknown if the attacks originated from the North Korean Army, a lonely South Korean Student, or the Japanese-Korean Mafia. Indeed, all of these entities could have been involved in the attacks at the same time. This is because the differentiation between Cyber Crime, Cyber***

> ***Warfare and Cyber Terror can be a misleading one—in reality, Cyber Terror is often Cyber Warfare utilizing Cyber Crime.***
>
> ***—Alexander Klimburg, Cyber-Attacken als Warnung (DiePresse.com, 15 July 09)***

Organised crime syndicates from Russia, Japan, Hong Kong, and the U.S. are consolidating their influence in the underground world of cybercrime because the risk-reward ratio is so good. As per Gartner, an IT analyst firm, worldwide expenditure on cybersecurity products and services has been $114 bn in 2018 and is expected to exceed $124 bn in 2019.

Cyber warfare is emerging as more smart and effectual method to wage war as it seeks to achieve political goals without extensive use of armed forces. Further, cyber domain has already become a domain where strategic advantage can be achieved. Apropos, Cyberwar is a potent tool in this warfare and hence spearheading the Strategy of Global Dominance. Kinetic cyberattacks can cause direct or indirect physical damage, injury or death solely through exploitation of cyber vulnerabilities. With advent of technology and embed Supervisory Control and Data Acquisition (SCADA) Systems implies significant Kinetic Cyber Threats in future. IOT is another area of concern which would have far reaching infrastructure threat with no security standard or protocols in place.

The tools used for Cyberwar and Cyber-terrorism are common to cybercrime and so are the individuals, groups, underground organisations who are employed by terror outfits and nation-states to meet their motivations and ends. Many cyber criminals are also engaged as non-state hackers during times of cyber conflict. Hence there is a requirement to understand the role being played by the non-state actors, why are they being hired by nation states and identify future means in Cybersecurity to prevent ant cyber-attacks or incidents.

1.5 Research Design

The research design will be Exploratory primarily based on “Case Study” method.

1.6 Research Questions

The research questions are as under: -

(a) What are the trends in role of non-state actors in cyber operations/ cyber war?

(b) What are the reasons for Nations to employ non-state actors for cyber operations?

(c) What are the future means of Cybersecurity against cyber incidents?

1.7 Scope of the Study

The scope of the study is limited to data available in open source related to Cyber incidents and Cyber-attacks adopted by various Nation-States and Non-State actors.

1.8 Methods to be Applied and Data Sources

Most of the information for the research will be procured from secondary sources that would include case studies, books, journal articles, research documents, internet and other relevant materials published from time to time. A period of past 1999 will be considered for the research.

1.9 Chapter Scheme

The dissertation will progressively deal with the issue and has been divided into following parts: -

(a) **Chapter 1**. Introduction.

(b) **Chapter 2.** Literature Review.

(c) **Chapter 3.** Cyberwar – Attacks, Attackers, Techniques and Tool.

(d) **Chapter 4**. Cyberwar - Case Studies.

(e) **Chapter 5.** Data Analysis and Findings.

(f) **Chapter 6.** Conclusion and Future Implications.

CHAPTER - 2

LITERATURE REVIEW

Gazula, Mohan B. Gazula, 2017 states that the case studies of cyberattacks in recent past reveal the far-reaching effects of cyberwar. The case studies especially the Stuxnet- targeting of Iranian nuclear programme and DDoS on Estonian cyberspace, US Elections of 2016 and WannaCry ransomware attack in 2017 are apt example demonstrating a shift of Nation-States into cybercrimes. It elaborates cybercrimes at organisational levels and still have a lot of criminal secrets to unfold.

(a) **Objective.** Following case studies were studied:-

(i) Ukrainian Power Grid.

(ii) Kosovo War.

(iii) Russia-Georgia War.

(iv) Operation Cast Lead.

(v) The Tulip Revolution.

(vi) The Jasmine Revolution.

(vii) DUQU (1.0 &2.0)

(viii) The Eastern Railway Website Defacement.

(ix) The Anthem Attack.

(x) Operation Aurora.

(xi) Operation Orchard.

(xii) The Shamoon Attack I &II.

(xiii) Russian Hackers Tracking Ukrainian Artillery.

(xiv) Yellowstone 1.

(xv) SONY Corp's Hollywood Studio.

(xvi) Attack on Estonian Government.

(xvii) Operation Dust Storm.

(xviii) Operation Anarchist.

(xix) The Deception Program.

(xx) Operation Desert Storm.

(xxi) Operation Buckshot Yankee.

(xxii) US Elections 2016

(xxiii) Wannacry.

(b) **Research Method.** Case Study based research

(c) **Gaps/Limitations.** Covers the cyber incidents without any suggestions for cybersecurity measures and role of Non-state actors.

Bussolati, Nicolò. Bussolati (2015), in his paper 'The Rise of Non-State Actors in Cyberwarfare' states the increase in role of non-state actors in the cyber-attacks in the recent past **(Bussolati, 2015)**.

(a) **Objective**. The first part considers how digital technologies stimulated an increasing role for non-state actors in the international system and accelerated the demise of the state as primary actor of international law. Moreover, it conducts a taxonomical analysis of non-state actors operating in cyberspace, highlighting their present and future role in cyber warfare. Finally, it examines how they relate to the states, and how the peculiarities of cyberspace affect their structures and modus operandi. The second part evaluates, in light of these morphological and operative features, the challenges to international law posed by the non-state actors' involvement in this new paradigm of warfare. In the first place, it considers how their participation in cyber war may be covered by the traditional corpus of norms regulating armed conflicts. Moreover, it analyzes issues related to the attribution of the act, and the ability of the state to respond to cyber threats deriving from non-state actors under the law of self- defense.

(b) **Research Method**. Descriptive.

(c) **Gaps/Limitations.** It lacks giving future means for cybersecurity taken by nations.

Carey III, Colonel Casimir C. Carey III, (2013), states in his thesis, 'NATO's Options for Defensive Cyber Against Non-State Actors', (US Army War College Fellowship). United States Army War College, Civilian Research Project, US Army, that Overt state-to-state cyber conflicts are unlikely for the foreseeable future.

(a) **Objective.** States prefer to retain plausible deniability through surreptitious sponsorship of non-state cyber militias. International legal norms, NATO's Article 5 requirements, and UN Security Council procedural issues seem to limit NATO's options in responding to cyber events by non-state actors. However, there are three circumstances under which NATO may legally take cyber countermeasures against non-state actors:

(i) When a nation-state fails to enforce the law against non-state actors within its borders;

(ii) When a cyber-disruption is tantamount to an economic blockade; and

(iii) If there is intelligence that indicates a pending cyber-attack by force, thereby necessitating anticipatory self-defence.

(b) **Research Method**. Descriptive.

(c) **Gaps/Limitations.** It limits use of cyberwar options for NATO only and misses out suggestions for other global & international organisation and states.

Sigholm, Johan. Sigholm, (2016) states the circumstances for non-state actors to be indulged in cyber-attacks.

(a) **Objective.** This paper studies the various non-state actors who coexist in cyberspace, examines their motives and incitements, and analyses how and when their objectives coincide with those of nation-states. Literature suggests that many nations are currently pursuing cyberwarfare capabilities, often times by leveraging criminal organizations and irregular forces. Employment of such non-state actors as hacktivists, patriot hackers, and cyber-militia in state-on-state cyberspace operations has also proved to be a usable model for conducting cyberattacks. The paper concludes that cyberspace is emerging as a new tool for state power that will likely reshape future warfare.

(b) **Research Method**. Descriptive.

(c) **Gaps/Limitations.** However, due to the lack of concrete cyberwarfare experience, and the limited encounters of legitimate cyberattacks, it is hard to precisely assess future effects, risks and potentials.

Cyberwar: Law and Ethics for Virtual Conflicts. Ohlin, Jens D., Govern, K. & Finkelstein C. (Eds.), have compiled a book with essays on Cyberwar. The part-I attempts to expose foundational and conceptual issues in Cyberwar. The second chapter covers civil-military divide in cybersecurity and cyberwar. Subsequently, it covers the ethics of hacking and espionage and finally the attribution of legal and moral responsibility for cyber activities. It covers the comprehensive examination of cyber operation challenges for meeting military objectives.

Tallinn Manual. In 2009, the NATO Cooperative Cyber Defence Centre of Excellence a research and training institution based in Tallinn, Estonia, invited an independent group of experts to produce a manual on the international law governing cyber warfare. In doing so, it followed in the footsteps of earlier efforts, such as those resulting in the 1880 Oxford Manual, the International Institute of Humanitarian Law's 1994 San Remo Manual on International Law Applicable to Armed Conflicts at Sea, and the Harvard Program on Humanitarian Policy and Conflict Research's 2009 Manual on International Law Applicable to Air and Missile Warfare. The project brought together distinguished inter-national law practitioners and scholars, the so-called 'International Group of Experts' or 'Experts', in an effort to examine how extant legal norms apply to this new form of warfare. In 2013, the effort resulted in the publication of the Tallinn Manual on the International Law Applicable to Cyber Warfare. That product has served as an invaluable resource for government legal advisors and scholars since its publication. The Tallinn Manual's focus was on cyber operations involving the use of force and those that occur in the context of armed conflict.

However, Tallinn Manual is not an official document, but rather the product of two separate endeavours undertaken by groups of independent experts acting solely in their personal capacity. The Manual does not represent the views of the NATO CCD COE, its sponsoring nations, or NATO. This implies there is ample space for Non-State actors to pursue their aims in absence of proper legal framework worldwide.

CHAPTER - 3

CYBERWAR – ATTACKS, ATTACKERS, TECHNIQUES AND TOOLS

3.1 Introduction

My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

-The Mentor, "The Conscience of a Hacker"

Computers were first man made machines which could follow instructions and process them. Initially they were simple but with advancement in technology, they became faster, cheaper and personalised. Earlier, they were stand-alone, but later they were networked and subsequently got connected to the World Wide Web. Today, we are totally hooked onto the computers, smartphones and Internet, because, a large number of facilities like governance, healthcare, banking, civic infrastructure and social networking are accessible due to them. This led to term of ‘cyberspace’ and also prefixing ‘cyber’ to various activities pertaining to them.

3.2 Cybercrime

Some experts believe that computer crime is nothing more than ordinary crime committed by high-tech computers and that current criminal laws on the books should be applied to the various laws broken, such as trespass, larceny, and conspiracy. Others view cybercrime as a new category of crime requiring a comprehensive new legal framework to address the unique nature of the emerging technologies and the unique set of challenges that traditional crimes do not deal with; such as jurisdiction, international cooperation, intent, and the difficulty of identifying the perpetrator.

Experts believe and give an argument that there is no agreed-upon definition for “cybercrime” because “cyberspace” is just a new specific instrument used to help commit crimes that are not new at all. It refers largely to any criminal activity that pertains to or is committed through the use of the Internet. A wide variety of conduct fits within this extensive definition. The term ‘‘cybercrime’’ is sometimes used synonymously with Internet crime, technological crime, digital crime, economic crime or electronic crime, to describe crime committed with computers or other ICT devices.

This is especially true given that so many types of cybercrime and abuse of information systems, including **(McQuade, 2009)**:

(a) Negligent use of information systems while violating security policies or engaging in unsound information security practices and thereby exposing systems and data to cyber-attacks.

(b) Conventional crimes involving use of computers or other types of electronic IT devices for communications and/or record keeping in support of their illegal activities.

(c) Online fraud such as phishing, spoofing, spamming, or otherwise deceiving people online for financial gain as in cases of credit card fraud and identity theft.

(d) Hacking, computer trespassing, and password cracking in order to break into computer account passwords and/or unlawfully enter information systems to commit online and/or offline crimes.

(e) Malicious writing and distribution of computer code that involves creating, copying, and/or releasing malware (i.e., disruptive or destructive viruses, Trojans, worms, or adware/spyware programs).

(f) Digital piracy of music, movie, and/or software especially via peer-to-peer networks.

(g) Cyber harassments, threat, intentional embarrassment, or coercion, including cyber bullying.

(h) Online stalking and other cyber-sex offending, including sending unwanted pictures or text of a sexual nature, promoting sex tourism, or using the Internet to facilitate human trafficking for sexual or other purposes.

(i) Academic cheating and scientific misconduct by students, teachers, or professors to plagiarise (i.e., take written credit for the writing or ideas of others), cheat on assignments or exams, or fake research methods or findings.

(j) Organised crime that involves use of the Internet by ethnic-based gangs to facilitate combinations of illegal and legal activities such as smuggling and selling of people, weapons, and drugs.

(k) Government and free-lance spying including corporate espionage that involves illicit use of spyware and key logger software to discover data that can be stolen or used to commit additional crimes; and

(l) Cyber terrorism by people trying to advance ‘‘social, religious or political goals by instilling widespread fear or by damaging or disrupting critical information infrastructure.’’

The growing importance of cyberspace to modern society and its increasing use as an arena for dispute, is becoming a national security concern for governments and armed forces globally. The special characteristics of cyberspace, such as its asymmetric nature, the lack of attribution, the low cost of entry, the legal ambiguity, and its role as an efficient medium for protest, crime, espionage and military aggression, makes it an attractive domain for nation-states as well as non-state actors in cyber conflict **(Sigholm, 2016)**. A small hacker, either working independently or being hired by the state, could take on a Nation State by his mere geek-ness and an encounter like David vs Goliath could be a reality.

3.3 Cyber-attack, Cyber-terrorism and Cyber-warfare

Before we proceed any further, it is imperative to look at some important terms and their meaning with specific reference to crimes. A cyber-attack is deliberate manipulation of computer systems, technology-dependent enterprises and networks. Cyber-attacks use malicious code to modify computer code, logic and data resulting in disruptive effects that lead to cybercrimes, such as information and identity theft. Cyber-attack is also known as computer network attack (CNA).

Computer networking technology has also blurred the boundaries between Cybercrime, Cyber-terrorism, Cyber-espionage and Cyber warfare. Officials in government and industry now say that cybercrime and cyber-attack services available for hire from criminal organisations are a growing threat to national security. New and sophisticated cybercrime tools could operate to allow a nation state or terrorist group to remain unidentified while they direct cyber-attacks through the Internet. Many experts point out that past incidents of conventional terrorism are dubbed as cybercrime.

Additionally, cybercrime is the laboratory where the malicious payloads and exploits used in cyber warfare are developed, tested, and refined. The reason why it is such an effective lab environment is because cracking a secure system is valuable training, and it’s happening every day inside the cyber underground.

Organised crime syndicates from Russia, Japan, Hong Kong, and the U.S. are consolidating their influence in the underground world of cybercrime because the risk-reward ratio is so good. Although law enforcement agencies are making sustained progress in cybercrime detection and enforcement, cyberspace is still a crime syndicate’s dream environment for making a lot of money with little to no risk. To sum up, it is evident that cybercrime happens to be a subset to Cyber terrorism and Cyber warfare, i.e. it manifests itself at the root of Cyber-war and Cyber-terrorism.

As with the term cyberspace, there is no universally accepted definition of cyberwarfare. Accordingly, general definition are:-

(a) “Cyberwarfare refers to a massively coordinated digital assault on a government by another, or by large groups of citizens. It is the action by a nation-state to penetrate another nation’s computers and networks for the purposes of causing damage or disruption.” But it adds that “the term cyberwarfare may also be used to describe attacks between corporations, from terrorist organizations, or simply attacks by individuals called hackers, who are perceived as being warlike in their intent.” **(Cyber Warfare Law and Legal Definition)**

(b) The US Department of Defense defines cyber operations as “the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace.” A computer network attack is defined as “actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and network themselves.” **(Dictionary of Military and Associated Terms (JP 3-0), 2010 (As Amended Through 15 Oct 2011)** .

(c) A further definition of cyberwar is “a conflict that uses hostile, illegal transactions or attacks on computers and networks in an effort to disrupt communications and other pieces of infrastructure as a mechanism to inflict economic harm or upset defenses.” **(Coleman, 2008)**

(d) And finally, according to a recent UN Security Council Resolution, “Cyber warfare is the use of computers or digital means by a government or with explicit knowledge of or approval of that government against another state, or private property within another state including: intentional access, interception of data or damage to digital and digitally controlled infrastructure. And production and distribution of devices which can be used to subvert domestic activity." **(Dunnigan, 2002, p. 11)**

3.4 Types of Attacks

In this age of automation and connectivity, almost all technology-dependent systems are vulnerable to cybercrimes. Here are the most common targets for cybercrimes:

(a) **Military and Intelligence Attacks.** Espionage hackers may target military and government computers. National security increasingly depends on computers, ranging from the positioning of Air Force satellites to plans for troop deployment throughout the world.

(b) **Business Attacks**. Businesses fall target to their competitors. The economic competition is becoming more and more fiercer. Industrial espionages are on the rise because of the competition among national economies. Even friendly-nations of the past have become economic-enemies and indulged in stealing of patents.

(c) **Financial Attacks.** Professional criminals target Banks and other financial parties for financial gain. We are dependent more on computer to pay our bills and deposit our checks electronically. Theft and fraud cases are increasingly done electronically.

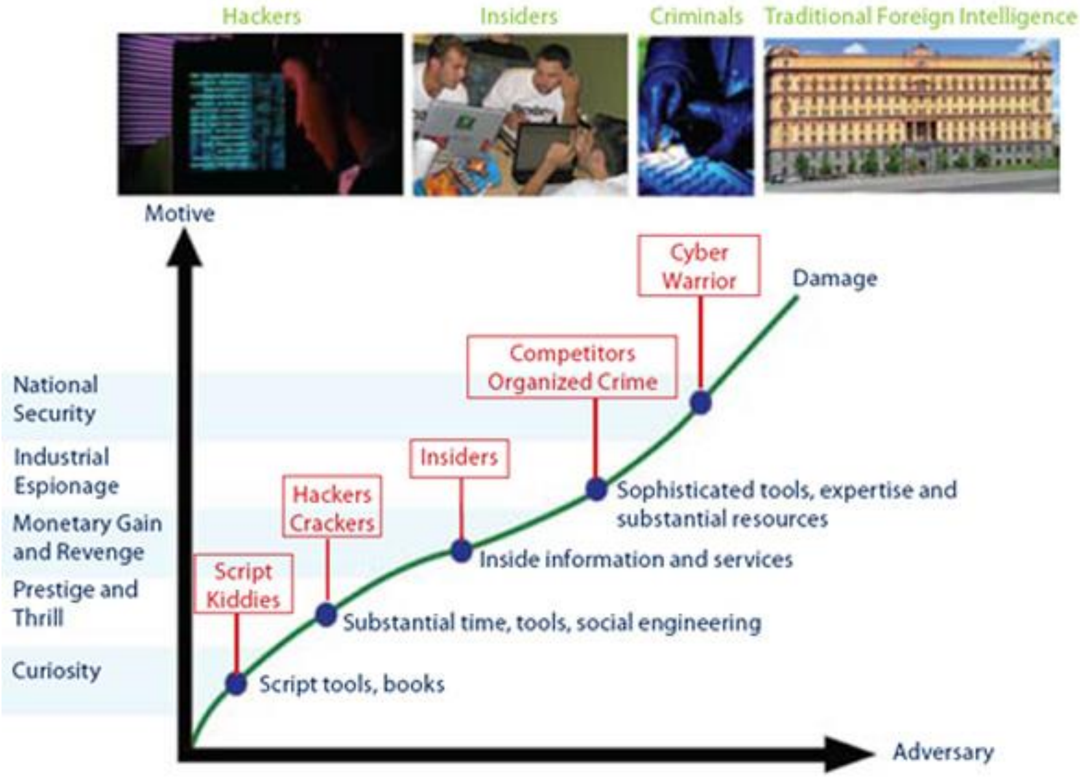
(d) **Terrorist Attacks**. Terrorists may target any organisation but especially government and enterprise computers. Their purposes could be to paralyse the government or cause disastrous accidents.

(e) **Grudge Attacks**. Any company can be the target of its own employees or ex-employees. Similarly, universities may be the target of their students and former students. Their goals are for revenge.

(f) **<u>'Fun' Attacks</u>.** Any organization can be the target of crackers, sometimes they're seeking for the intellectual challenge, and sometimes they are professionals who may do it to be hired.

3.5 <u>Types of Cybercrime Actors</u>

The cybercrime perpetrators could be amateurs, students or members of an organised group. Some of the offenders are as mentioned in Figure 1.


Hackers
Insiders
Criminals
Traditional Foreign Intelligence
Motive
Cyber Warrior
Damage
Competitors Organized Crime
National Security
Industrial Espionage
Insiders
Sophisticated tools, expertise and substantial resources
Hackers Crackers
Monetary Gain and Revenge
Inside information and services
Script Kiddies
Prestige and Thrill
Substantial time, tools, social engineering
Curiosity
Script tools, books
Adversary

<u>Figure 1. Types of Cybercrime Actors (Rai, 2011)</u>

The cyber criminals are bright, eager and highly motivated to accept technological challenges. The cyber threats are from:-

(a) **<u>Ordinary Citizens.</u>** These are the most common users of Internet, however unknowingly, they could be part of passive 'zombies' victims of Botnet.

(b) **Script Kiddies.** These are users who are looking for quick rewards and are not fully aware of hacking. They are like vandals or graffiti artists of the net. They typically look for existing, easy to use malware, pre-made scripts or easy to use auditing & penetrating tools to identify and exploit remote computers or resources on the net. They may seem harmless but due to indiscriminate usage and carelessness cause serious harm and damage.

(c) **Insiders.** The insiders are the main source of cybercrimes for many companies.

(d) **Hackers.** They crack into networks simply for the challenge of it. They are namely of the following types:-

> (i) Black-hat hackers. These are malevolent types and hack for their own personal cause and benefits. Steal credit card numbers or use the stolen numbers for purchase of online merchandise. They were originally called as ‘crackers’.
>
> (ii) White-hat hackers. These are the ethical hackers who have high moral standards and specialize in penetration and validation support.
>
> (iii) Gray-hat hackers. These are usually akin to white-hat hackers but may occasionally violate law and wear a black-hat instead.

(e) **Hacktivists.** Simply put, a **hacktivist** is someone who uses hacking to bring about political and social change. The term “**hacktivist**” traces back to 1994, originating from the hacker group “Cult of the Dead Cow.” Hacktivism started as a way for people to protest online to affect change.

(f) **Patriot hacker.** These hackers’ main motives are to aid and support own nation-states in an ongoing real-world conflict or war. This is usually done by disruptive actions against an adversary or enemy-state.

(g) **Malware Authors.** They are specialized form of black-hat hackers who develop code for criminal purposes. They are highly skilled and can evade anti-virus, anti-spyware and anti-malware applications.

(h) **Cyber criminals.** There are three major types of criminal behavior: espionage, fraud and abuse. The common motivation of a criminal is financial gain.

(i) **Organized Cybercriminals**. These groups have a loose organisation and may utilise many agents, including many from the actors mentioned above. The borderless and anonymous nature of cyber space allows otherwise disconnected individuals to connect and form criminal network. Some will have expertise in developing hacking tools and vulnerabilities, others who will carry out the attack and yet others who will launder the cash. At the centre of the web is a cybercrime boss with the ideas, the targets and the contacts. These are the groups with the capability attacks on banks, law firms and other big businesses. Organised cybercrime groups are also increasingly performing long-term, targeted attacks instead of indiscriminate scatter-gun campaigns. They are generally motivated with money and power

(j) **Cyber espionage agents**. It involves gaining classified or sensitive information without the knowledge of the owner. They usually intercept info that passes through the network, but also employ infiltration and surveillance tools to gather targeted data and info.

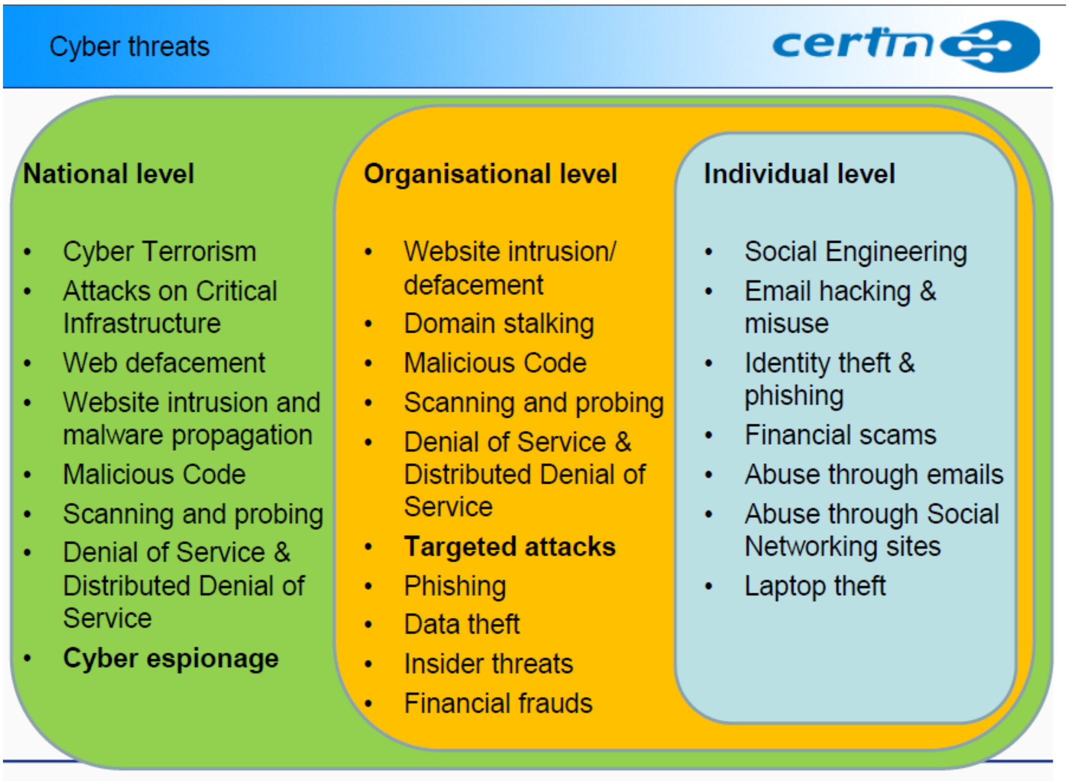
(k) **Vandals.** Vandals can be roughly divided into two groups: users and strangers. Users are those who are authorised to use the system they abuse, but they have extended their privileges. Strangers are those who are not authorised to use the system in any way. A main motivation of vandal is to damage the system or data files.

(l) **Cyber terrorists.** Terrorist groups using cyber networks to formulate plans, raise funds, spread propaganda, conduct terrorist-like activities etc.

The roles played by these actors may vary with the situation and sometimes may overlap too. Depending on their current aim and goal, the actors may conveniently move between these categories and also enjoy obscurity as provided by the cyberspace. However, these categorizations are still relevant, as they clearly specify a role being played by an actor at a particular time.

3.6 Types of Threats and Trends

As per Dr Gulshan Rai, Director General, Indian Computer Emergency Response Team (CERT-In), levels of threats from cyber-attacks could be classified as shown in Figure 2.



Cyber threats

National level

- Cyber Terrorism
- Attacks on Critical Infrastructure
- Web defacement
- Website intrusion and malware propagation
- Malicious Code
- Scanning and probing
- Denial of Service & Distributed Denial of Service
- **Cyber espionage**

Organisational level

- Website intrusion/ defacement
- Domain stalking
- Malicious Code
- Scanning and probing
- Denial of Service & Distributed Denial of Service
- **Targeted attacks**
- Phishing
- Data theft
- Insider threats
- Financial frauds

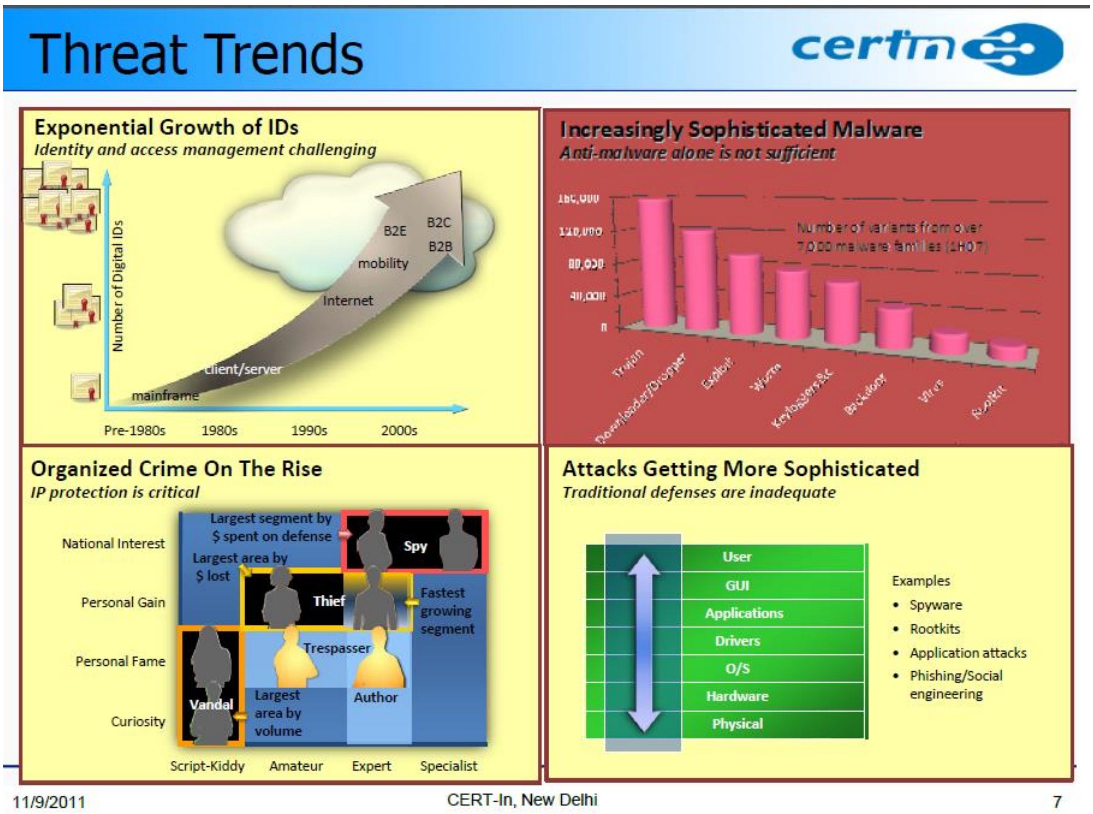
Individual level

- Social Engineering
- Email hacking & misuse
- Identity theft & phishing
- Financial scams
- Abuse through emails
- Abuse through Social Networking sites
- Laptop theft

CERT-In, New Delhi

Figure 2. Cyber Threats (Rai, 2011)

If observed carefully, it evidently indicates that these are cybercrimes which are manifested by cybercriminals. He also exposed the recent trends with respect to organised crimes being on the rise, increase in sophistication of Malware and the attacks becoming more and more sophisticated. The same are as seen in Figure 3



Threat Trends

Exponential Growth of IDs

Identity and access management challenging

Increasingly Sophisticated Malware

Anti-malware alone is not sufficient

Organized Crime On The Rise

IP protection is critical

Attacks Getting More Sophisticated

Traditional defenses are inadequate

Examples
- Spyware
- Rootkits
- Application attacks
- Phishing/Social engineering

11/9/2011 CERT-In, New Delhi 7

Figure 3. Threat Trends (Rai, 2011)

3.7 Cybercrime Tools

Cybercriminals have developed a wide array of potential tools that have had varying degrees of success over the years. The following are a short list of some of these techniques.

(a) **Virus.** A program or piece of code that spreads from computer to computer without the users' consent. They usually cause an unexpected and negative event when run by a computer. Viruses contaminate legitimate computer programs and are often introduced through e-mail attachments, often with clever titles to attract the curious reader.

(b) **Worms and Trojans.** A Trojan is a malicious program unwittingly downloaded and installed by computer users. Some Trojans pretend to be a benign application. Many hide in a computer's memory as a file with a nondescript name. Trojans contain commands that a computer automatically executes without the user's knowledge. Sometimes it can act as a zombie and send spam or participate in a distributed denial of service attack. It may be a keylogger or other monitoring program that collects data and sends it covertly to the attacker. Worms are wholly contained viruses that travel through networks, automatically duplicate themselves and send themselves to other computers whose addresses are in the host computer. In the past, cybercriminals occasionally use worms and Trojans to hijack a victim's Web browsers. They replace the victims' home and search pages with links to Web spam, as well as drop links to the spam in the victims' bookmarks and on their desktops. To make money, they infect computers with malicious code that generates fraudulent ad views.

(c) **Phishing.** This a technique of extracting confidential information such as credit card numbers and username password combos by masquerading as a legitimate enterprise. Phishing is typically carried out by email spoofing.

(d) **SQL Injections.** An SQL injection is a technique that allows hackers to play upon the security vulnerabilities of the software that runs a web site. It can be used to attack any type of unprotected or improperly protected SQL database. This process involves entering portions of SQL code into a web form entry field – most commonly usernames and passwords – to give the hacker further access to the site backend, or to a particular user's account. When you enter logon information into sign-in fields, this information is typically converted to an SQL command. This command checks the data you've entered against the relevant table in the database. If your input data matches the data in the table, you're granted access, if not, you get the kind of error you would have seen when you put in a wrong password. An SQL injection is usually an additional command that when inserted into the web form, tries to change the content of the database to reflect a successful login. It can also be used to retrieve information such as credit card numbers or passwords from unprotected sites.

(e) **Theft of FTP Passwords.** This is another very common way to tamper with web sites. FTP password hacking takes advantage of the fact that many webmasters store their website login information on their poorly protected PCs. The thief searches the victim's system for FTP login details, and then relays them to his own remote computer. He then logs into the web site via the remote computer and modifies the web pages as he or she pleases.

(f) **Cross-site scripting.** Also known as XSS (formerly CSS, but renamed due to confusion with cascading style sheets), is a very easy way of circumventing a security system. Cross-site scripting is a hard-to-find loophole in a web site, making it vulnerable to attack. In a typical XSS attack, the hacker infects a web page with a malicious client-side script or program. When you visit this web page, the script is automatically downloaded to your browser and executed. Typically, attackers inject HTML, JavaScript, VBScript, ActiveX or Flash into a vulnerable application to deceive you and gather confidential information.

(g) **Bots.** A bot (short for robot) is a computer on which a worm or virus has installed programs that run automatically and allow cybercriminals access and control. Cybercriminals use viruses or other bots to search for vulnerable computers where they can load their own data. A botnet is a collection of these infected machines that can be centrally controlled and used to launch simultaneous attacks. Spammers, hackers, and other cybercriminals are acquiring or renting botnets, making it harder for authorities to track down the real culprits.

(h) **Keylogging.** Keyloggers are programs that covertly recover the keys typed by a computer user and either stores the data for later access or secretly sends the information to the author. The advantage of a keylogger program is that the cybercriminal does not need to trick a user into supplying sensitive information.

(i) **Bundling.** Covertly attaching a virus or spyware to a benign or legitimate download, such as a screensaver or a game. When the computer user downloads and installs the legitimate file, they are unwittingly also giving permission to install the criminal program.

(j) **Denial of Service**. An attack specifically designed to prevent the normal functioning of a computer network or system and to prevent access by authorised users. A distributed denial of service attack uses thousands of computers captured by a worm or Trojan to send a landslide of data in a very short time. Attackers can cause denial of service attacks by destroying or modifying data or by using zombie computers to bombard the system with data until its servers are overloaded and cannot serve normal requests.

(k) **APT.** An advanced persistent threat (APT) is a prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an period of time. The intention of an APT attack is usually to monitor network activity and steal data rather than to cause damage to the network or organization.

(l) **Zero-day exploits.** A zero-day exploit is a cyber-attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator.

(m) **Man in the Middle attack.** In cryptography and computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

(n) **Packet Sniffers.** Software programs that monitor network traffic. Attackers use packet sniffers to capture and analyse data transmitted via a network. Specialized sniffers capture passwords as they cross a network.

(o) **Rootkit.** A set of tools used by an intruder after hacking a computer. The tools allow the cybercriminal to maintain access, prevent detection, build in hidden backdoors, and collect information from the compromised computer.

(p) **Spyware.** Software that gathers information without the users' knowledge. Spyware is typically bundled covertly with another program. The user does not know that installing one also installs the other. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else.

(q) **Social Engineering.** Social engineering is not limited to cybercrime, but it is an important element for cyber-fraud. Social engineering tricks & deceives the recipient into taking an action or revealing information. The reasons given seem legitimate but the intent is criminal. Phishing is an obvious example; a certain percentage of users will respond unthinkingly to a request that appears to be from a legitimate institution.

(r) **Logic Bomb.** A logic bomb, also known as "slag code", is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It's not a virus, although it usually behaves in a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met. Malicious software such as viruses and worms often contain logic bombs which are triggered at a specific payload or at a predefined time.

(s) **Pharming.** Pharming is an attack intended to redirect your website traffic to another, probably bogus website. Sad news: pharming is not easily detectable on your computer. Pharming is usually done by infecting DNS servers which is beyond control and remains undetectable for a large part.

(t) **Internet message boards.** Internet message boards dedicated to stocks are fertile ground for impersonators. A habit of many posters to these boards is to cut-and-paste press releases and news stories from other electronic sources into their posts to alert other posters and visitors to that information. Frequently, posters will paste in a hyperlink to direct a reader to a source directly, as Hoke did in the Pair Gain hoax. In addition to the rising threat, as national level attacks become more plausible, the vulnerabilities have also increased.

Cyberwar Gray area – Non-state Actors. Cyberwarfare involves a plethora of actions, ranging from attacks to critical infrastructure, inflicting physical damage and casualties, monitoring and penetrating networks, espionage and disruptive actions. The stand-off nature of cyberattacks allows for striking tactical as well as strategic targets from large distances, using comparatively inexpensive technology. The involvement of civilians in recent cyber-conflicts have created a sizeable gray area between hacktivists, political hackers and legitimate combatants backed by nation-states. The debate has been fierce concerning if these people are individual and independent actors, motivated by political or nationalistic goals, or participants in covert government-orchestrated campaigns with the purpose to further the strategic political or military objective of the instigating state **(Applegate, 2011)** . Most cases of politically motivated cyber-actions that have occurred during recent years have been attributed to unidentified radical hackers or hacktivists. Such actions have ranged from mere annoyances, e.g. the defacement of websites in Japan in reaction to new anti-piracy legislation, to full-scale digital blockades of the target country. In cases such as the attacks on Estonian cyberspace resources in 2007, an intense debate continues as to whether the attacks were instigated by a nation-state, if they were the work of independent patriot hackers defending their country's honour or if an organized cyber-militia was responsible **(Ottis, 2011)** **(Applegate, 2011)**.

As cyberattacks can be launched by proxy, using trojanized unsuspecting end-users' computers, proving whether nation-states are engaging in cyberwarfare is naturally difficult. Cyber-militias have been suspected of performing several recent high-profile cyberactions that were, at least in part, sanctioned by nation-states. The list of nations engaging in political hacking includes Iran, Turkey, Israel, and North and South Korea **(Applegate, 2011)**. Two examples of nations involved in these types of attacks are the People's Republic of China and the Russian Federation. Both of these countries are rapidly building cyberwarfare capabilities, and have developed large bodies of doctrine and technology in support of this new concept **(Carr, 2011)**.

As cyberspace, unlike other arenas associated with warfare, provides a high level of anonymity, attackers can carry out actions in this domain with little or no risk of attribution. Nation-states thus have little or no incentive to support a legally binding definition of cyberwar, which would limit their freedom of action, or to formally take responsibility for executed cyberattacks. Furthermore, cyberattacks can be carried out inexpensively, and can, at least in theory, cause extensive damage or at least trigger severe disruptions to ICT-based services. In addition, if a nation-state can covertly initiate, fund, or control such attacks, relying on non-state actors to carry out the attacks in their stead, they can reduce the already low risk of political implications, and potentially achieve their objectives without the burden of adhering to the Law of Armed Conflict. This gives an attacker a tremendous asymmetric advantage, especially for smaller nations that cannot prevail on a kinetic battlefield. As a result, employment of non-state actors in cyberspace operations is likely a very attractive option for nation-states or an equivalent body, especially when pursuing limited strategic goals **(Sigholm, 2016)**.

CHAPTER - 4

CYBERWAR – CASE STUDIES

4.1 Introduction

Gazula, (2017) has made research of past cyber warfare incidents and has mapped relevant data as per the well known CASCON method utilised for kinectic warfare. He has suitably modified the decision-support system to suit the Cyber attack incidents. In order to make an in-depth study leading to the circumstances for a cyberattack/ incident and find answers to the Research questions, it is vital to study and analyse various cyberattacks and incidents over a period starting 1999.

Gazula, (2017) states that “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”. He describes Cyberwarfare Case Study phases in the following categories and as illustrated in Figure 4:-

(a) **Planning Phase.** 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 (akin to an attacker), dispute, mission

(b) **Reconnaissance phase.** 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

(c) **Replicate phase.** 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

(d) **Assault phase.** 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

(e) **Obfuscation phase.** 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

(f) **Withdraw phase.** 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 **(Gazula, 2017)**.

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

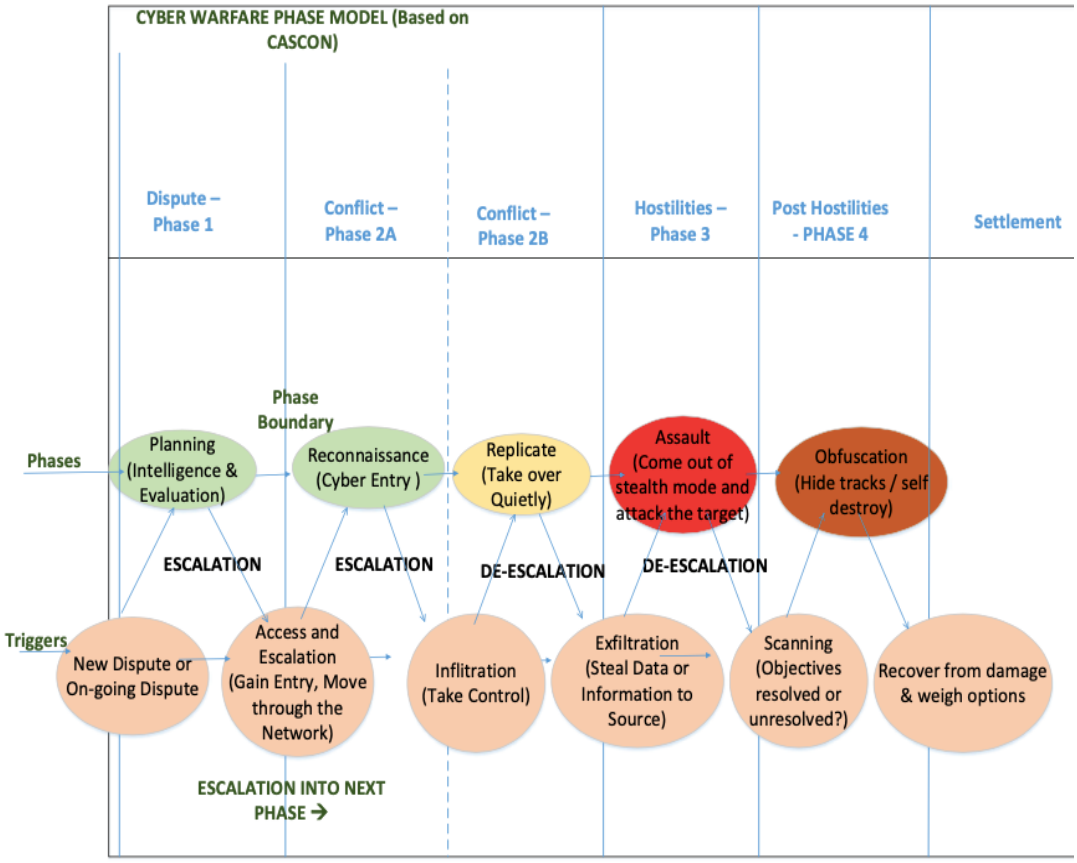
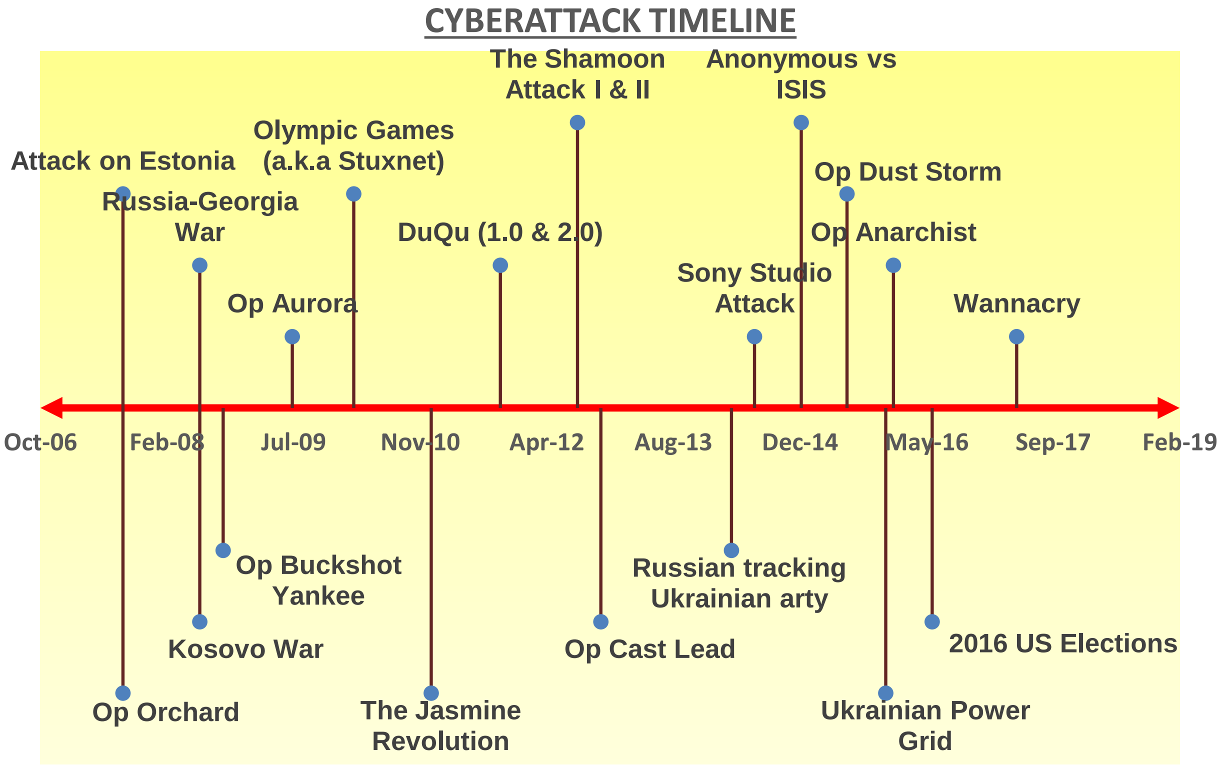

CYBER WARFARE PHASE MODEL (Based on CASCON)
Dispute – Phase 1
Conflict – Phase 2A
Conflict – Phase 2B
Hostilities – Phase 3
Post Hostilities - PHASE 4
Settlement
Phase Boundary
Phases
Planning (Intelligence & Evaluation)
Reconnaissance (Cyber Entry)
Replicate (Take over Quietly)
Assault (Come out of stealth mode and attack the target)
Obfuscation (Hide tracks / self destroy)
ESCALATION
ESCALATION
DE-ESCALATION
DE-ESCALATION
Triggers
New Dispute or On-going Dispute
Access and Escalation (Gain Entry, Move through the Network)
Infiltration (Take Control)
Exfiltration (Steal Data or Information to Source)
Scanning (Objectives resolved or unresolved?)
Recover from damage & weigh options
ESCALATION INTO NEXT PHASE →

Figure 4. Cyberwarfare Phase Model

4.2 Case Studies

A number of prominent and publicized Cyberwar incidents from 1999 onwards were researched for this thesis. Each case has been researched, analysed and formulated. Tables of important cases as researched by **Mohan B. Gazula, (2017),** and written using the model of the CASCON framework, have been referred and included in this thesis. Each of the case studies begins with a short background of the conflict to understand the parties involved. The 'status-quo state' were the victims and the 'non-status quo state' were the one who initiated the attack. Finally, each case has been analysed for its most probable - **Attribution, Actors** and **Cyberwar Tools**.



4.3 Olympic Games (a.k.a Stuxnet)

Cyber Conflict Background. Iran and the US lack formal diplomatic relationship. In 2010, the Stuxnet virus was used to significantly damage the Iranian nuclear program and was probably developed by Israel or the United States explicitly for this reason **(Jacob, 2017)**.

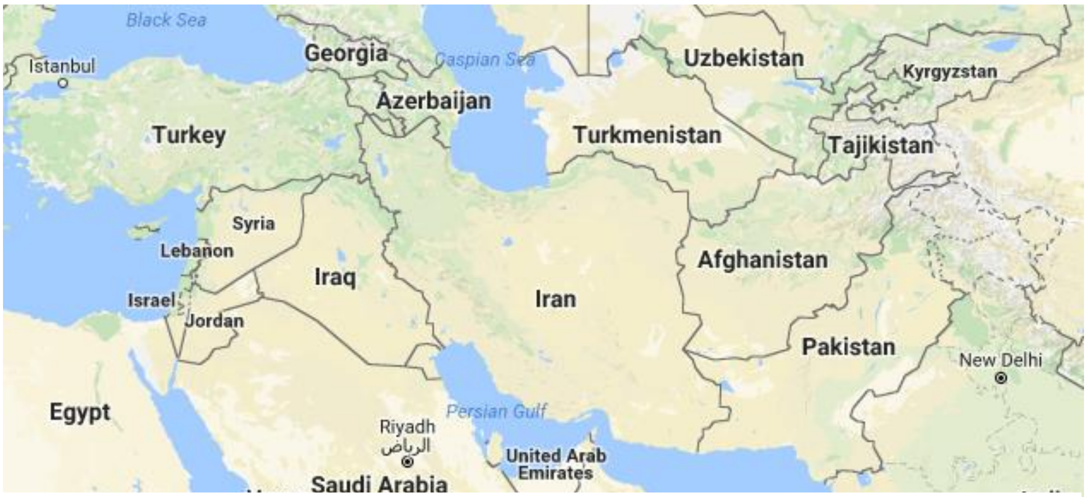


Figure 5. Olmpic Games: Region of Conflict

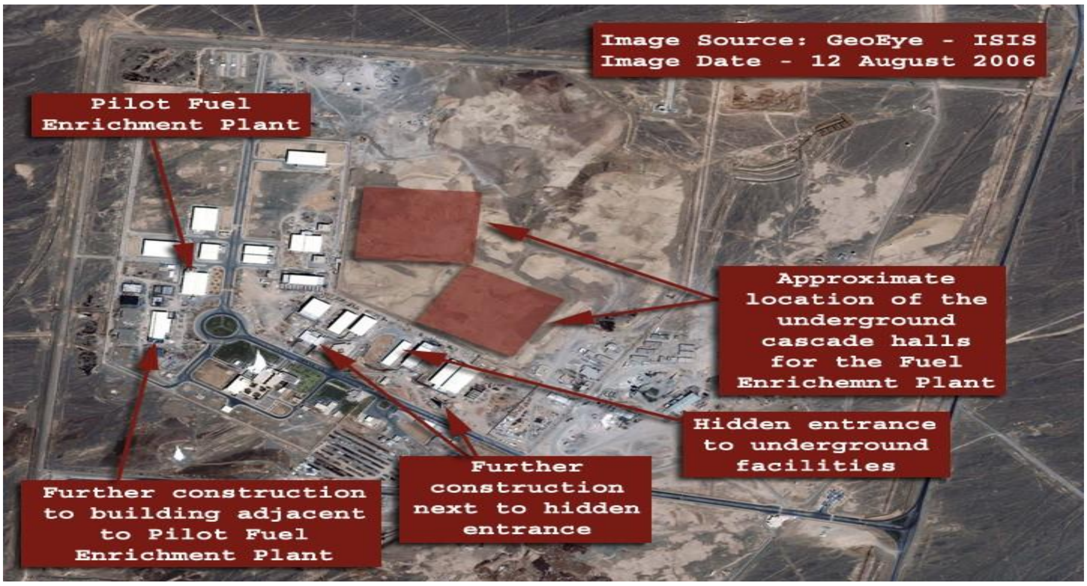


Image Source: GeoEye - ISIS
Image Date - 12 August 2006
Pilot Fuel Enrichment Plant
Approximate location of the underground cascade halls for the Fuel Enrichemnt Plant
Hidden entrance to underground facilities
Further construction next to hidden entrance
Further construction to building adjacent to Pilot Fuel Enrichment Plant

Figure 6. Map showing Natanz where the secret nuclear program was hosted (courtesy: Institute for science and security)

Table 1. Case Precis for Olympic games (Gazula, 2017)

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)	Phase 2a 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.

Stuxnet Analysis. Those who studied the Stuxnet worm described it as the first “cyber super weapon” that could be used in more destructive cases. It is still debated whether the use of this virus was an act of war, as it was not violent and no humans suffered physical harm from it. However, it destroyed or at least sabotaged the Iranian atomic program and therefore must be seen as a violent act of someone to destroy the progress of the Iranian government **(Jacob, 2017)**.

(a) **Likely Cyber Tools used.** Stuxnet worm, the arrival of which was a watershed in the security world. Some consider it to be the most sophisticated malware ever publicly disclosed. Stuxnet contains malware aimed at the programmable logic controllers (PLCs), designed to destroy SCADA networks: those that run factories, the electric power grid, refineries, pipelines, utilities, and nuclear power plants.258 Most industrial systems are run on computers which use Microsoft’s Windows 7 operating system. Hackers constantly probe software for what are known as zero day vulnerabilities: weak points in the code never foreseen by the original programmers. On a sophisticated and ubiquitous piece of software such as Windows XP.

(b) The makers of Stuxnet found four weaknesses and utilized them. No one in cyber security had ever seen anything like it. It targeted a specific component: the frequency converters made by the German equipment manufacturer, Siemens, that regulate the speed of the many thousands of spinning centrifuges used in the Iranian uranium enrichment process. The worm then took control of the speed at which the centrifuges spun, making them turn so fast in a quick burst that they would be damaged but not totally destroyed. At the same time, the worm masked that change in speed from being discovered at the control panel with a rootkit piece of code that intercepts security queries and sends back false 'safe' messages, indicating that the worm is innocuous.

(c) **Likely Actors.** Such an act is hostile, but one cannot claim it to be an act of war because we do not know exactly how far governments were involved in its creation, use, and target selection or even which governments ordered its use (Jacob, 2017). Although the makers of Stuxnet reportedly programmed it to expire in June 2012 and Siemens issued fixes for its PLC software, the legacy of Stuxnet lives on in other malware attacks based on the original code. These "sons of Stuxnet" include: -

(i) **DuQu (2011).** Based on Stuxnet code, DuQu was designed to log keystrokes and mine data from industrial facilities, presumably to launch a later attack.

(ii) **Flame (2012).** Flame, like Stuxnet, travelled via USB stick. Flame was sophisticated spyware that recorded Skype conversations, logged keystrokes, and gathered screenshots, among other activities. It targeted government and educational organizations and some private individuals mostly in Iran and other Middle Eastern countries.

(iii) **Havex (2013).** The intention of Havex was to gather information from energy, aviation, defense, and pharmaceutical companies, among others. Havex malware targeted mainly U.S., European, and Canadian organizations.

(iv) **Industroyer (2016).** This targeted power facilities. It’s credited with causing a power outage in the Ukraine in December 2016.

(v) **Triton (2017).** This targeted the safety systems of a petrochemical plant in the Middle East, raising concerns about the malware maker’s intent to cause physical injury to workers.

(vi) **Most recent (2018).** An unnamed virus with characteristics of Stuxnet reportedly struck unspecified network infrastructure in Iran in Oct 2018.

4.4 Ukrainian Power Grid

Conflict Background: Russia and Ukraine, were both part of the Union of Soviet Socialist Republic that formed in 1922. The two neighbouring 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 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.

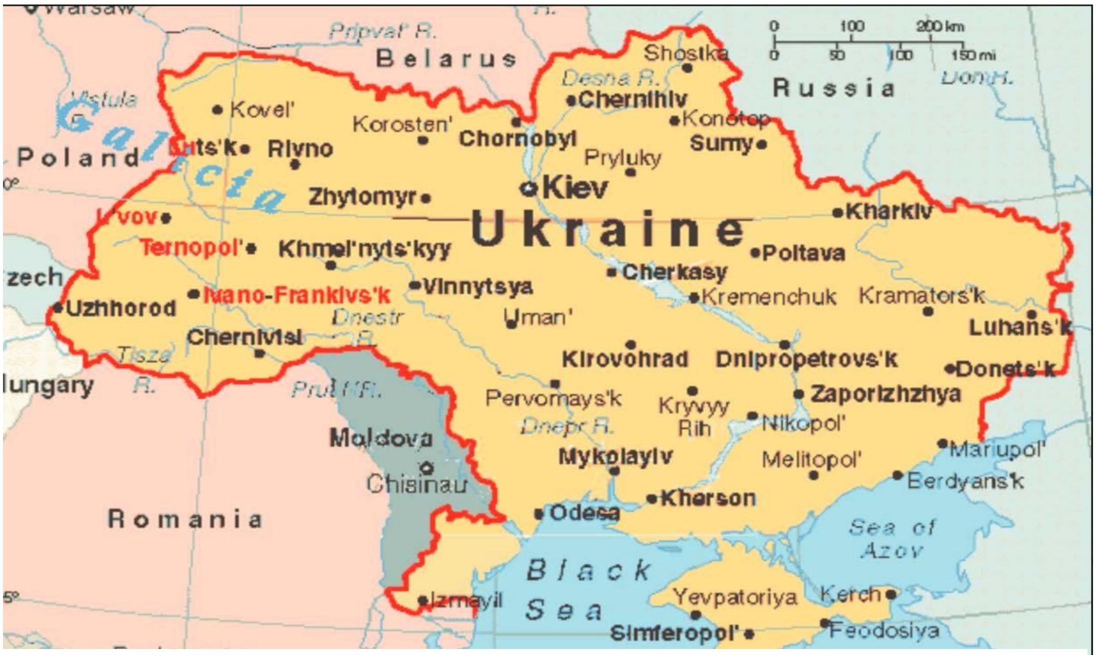


Figure 7. Russia and Ukraine: Region of Conflict

Table 2. Case Precis for Ukrainian Power Grid (Gazula, 2017)

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.
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 2b 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 3: December 23 2015: Armed with the malicious firmware, the attackers were ready for their assault. Sometime around 3:30 p.m. on Dec 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

Ukrainian Power Grid Attack Analysis. Shortly after the attack, Ukrainian government officials claimed the outages were caused by a cyber-attack, and that Russian security services were responsible for the incidents. Following these claims, investigators in Ukraine, as well as private companies and the U.S. government, performed analysis and offered assistance to determine the root cause of the outage **(Lee, Robert M., Assante, Michael J., Conway, Tim, 2016).**

(a) **Likely Cyber Tools used.** In summary, the malware attack consisted of the following attack elements:

(i) Spear phishing to gain access to the business networks of the oblenergos

(ii) Identification of BlackEnergy 3 at each of the impacted oblenergos

(iii) Theft of credentials from the business networks

(iv) The use of virtual private networks (VPNs) to enter the ICS network

(v) The use of existing remote access tools within the environment or issuing commands directly from a remote station similar to an operator HMI

(vi) Serial-to-ethernet communications devices impacted at a firmware level[15]

(vii) The use of a modified KillDisk to erase the master boot record of impacted organization systems as well as the targeted deletion of some logs[16]

(viii) Utilizing UPS systems to impact connected load with a scheduled service outage

(ix) Telephone denial-of-service attack on the call center.

(b) **Likely Actors.** It is quite uncertain that who might have created the malware, but Russia looms as the likely suspect. For three years, a sustained series of cyberattacks has bombarded Ukraine's government agencies and private industry alike. The timing of those attacks coincides with Russia’s invasion of Ukraine’s Crimean Peninsula and its eastern region, known as Donbass. Earlier this year, Ukrainian president Petro Poroshenko declared in a speech following the second blackout that the attacks were performed with the “direct or indirect involvement of secret services of Russia, which have unleashed a cyberwar against our country.” Other researchers at Honeywell and Kiev-based Information Systems Security Partners have already argued that the 2016 blackout was likely perpetrated by the same hackers as the 2015 attack, which has been widely linked to a hacker group known as Sandworm and believed to have originated in Russia **('Crash Override': The Malware That Took Down a Power Grid, 2017)**.

4.5 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.

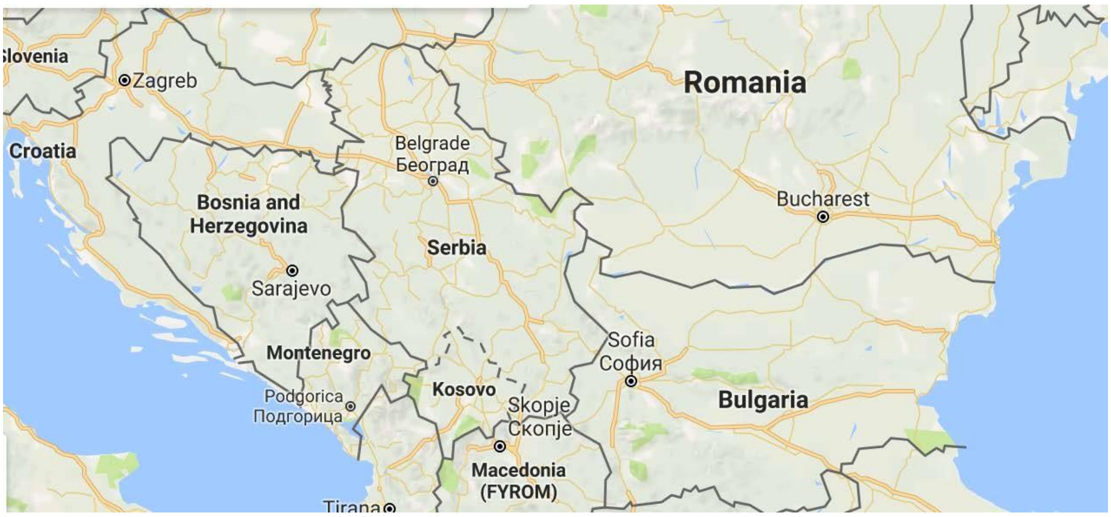


Figure 8. Kosovo War: Region of Conflict

Table 3: Case Precis for Kosovo War (Gazula, 2017)

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 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 non-functional because they were daily receiving more than 20,000 emails with malware in attachment. After these 78 intense days conflict ended. With it the 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 Kuma NoVo 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.

Kosovo War Analysis. Just as Vietnam was the world's first TV war, Kosovo in 1999 proved to become the first broad-scale Internet war. As NATO planes began to bomb Serbia, numerous pro Serbian or anti-Western hacker groups, such as the 'Black Hand,' began to attack NATO Internet infrastructure. It is unknown whether any of the hackers worked directly for the Yugoslav military. But their stated goal was to disrupt NATO military operations.305 US armed forces hacked into Serbia's air defence control to facilitate the bombing of Serbian targets. Later, in May 1999, NATO accidentally bombed the Chinese embassy in Belgrade, spawning a wave of cyberattacks from China against US government websites.

(a) **Likely Cyber Tools used.** NATO, U.S., and UK computers were all attacked during the war, via Denial-of-Service and virus-infected email (twenty-five different strains of viruses were detected). In the U.S., the White House website was defaced, and a Secret Service investigation ensued. While the U.S. claimed to have suffered "no impact" on the overall war effort, the UK admitted to having lost at least some database information.

(b) **Likely Actors.** Pro-Serbian hacker groups like "Black Hat" and Chinese cyber militia participated. NATO spokesman Jamie Shea blamed "line saturation" on "hackers in Belgrade."

4.6 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. 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

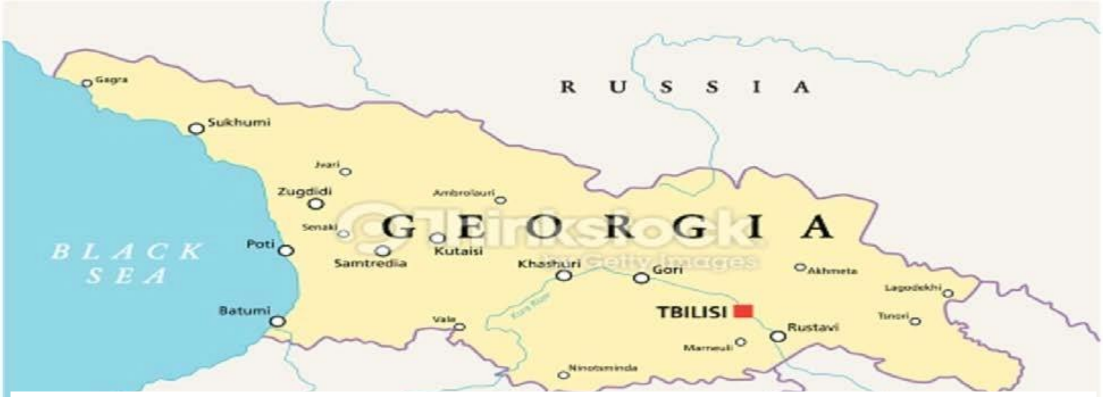


Figure 9. Russia-Georgia War: Map of Georgia

recently, its intentions to join NATO.

Table 4. Case Precis for Russia-Georgia War (Gazula, 2017)

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 DDoS, attacks - that overloaded and effectively shut down Georgian servers. As it turns out, the Jul 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.

Russia-Georgia War Analysis. Russian cyber forces acted decisively in support of the Russian invasion of Georgia. Massive DDoS attacks sought to isolate the Georgian population both from the Georgian government and from the rest of the world.

Not only did the attacks seek to disable Georgian government servers and media outlets, but they also sought to spread pro-Russian propaganda **(Stiennon, 2010, pp. 95-104)**. Targeted attacks went after the Georgian banking system, and when Georgian banks cut their Internet connections in the hope of protecting their clients' information, Russian botnets began sending false messages simulating cyber-attacks from the Georgian banks, aimed at the European banking system. This, in turn, triggered a host of defense mechanisms that only served to further isolate the Georgian banking system as well as shut down any ability to process credit card payments in Georgia. Shortly afterward, the entire Georgian mobile phone network was taken offline by DDoS attacks, effectively cutting off the small nation from most of the outside world.

(a) **Likely Cyber Tools used.** The cyber methodology was relatively crude which involved a brute-force DDoS approach that required enormous Georbot (botnets) to continually evolve and continue their attacks.

(b) **Likely Actors.** State actors with botnets support. From the point of view of international law, the cyber-attacks on Georgia were part of a legitimate political disagreement between two sovereign nations over control of territory deemed important to both, conventionally taken to be a legitimate cause for the use of force when attempts at diplomatic solutions are unsuccessful **(Schreier, 2015, p. 113)**.

4.7 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 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. Operation Cast Lead was a 22-day military assault on the Gaza Strip by the Israel Defense Forces (IDF), December 27, 2008 to January 18, 2009, in response to continued missile attacks originating from groups and individuals in the area. In response to the damage and casualties inflicted, cyber-attacks were launched against Israeli Web sites and other related sites by members and supporters of the Arab and Muslim communities.

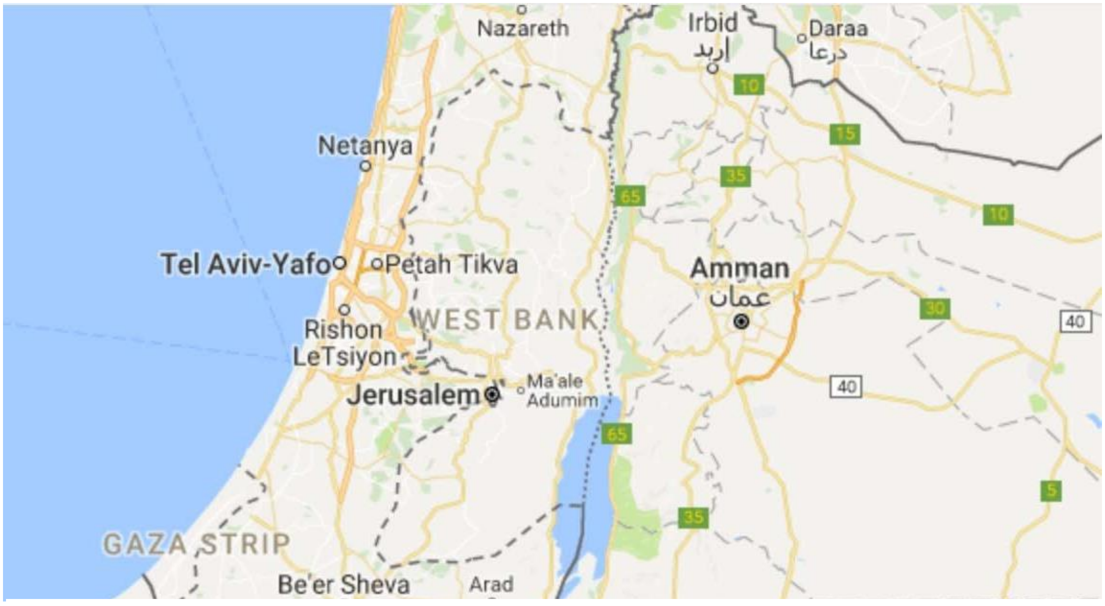


Figure 10. Region of Istrael and Palestine Conflict

Table 5. Case Precis for Operation Cast Lead (Gazula, 2017)

Phase	Activity
Dispute	Phase1December 2008: 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)	Phase 2A Early November 2012: 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.
Conflict 2B (Replicate)	Phase2A Early November 2012: 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.

Operation Cast Lead Analysis. Israel launches Operation Cast Lead against Palestinian militants in the Gaza Strip. A massive cyber war erupts between Israeli and Arabic hackers.

(a) **Likely Cyber Tools used.** Thousands of sites were attacked. Most of the attacks were Web site defacements containing images of victims and destruction in Gaza or appeals to Israel and the United States to stop the violence. Internet traffic was also redirected from legitimate sites to ones created by the hackers with similar images and messages and the apparent motivation of drawing the world’s attention to the plight of the Palestinians.

(b) **Likely Actors.** State and non-state hackers are involved on both sides. Most of the hackers were believed to be Moroccan, Algerian, Saudi Arabian, Turkish, and Palestinian, based on the information left on hacked Web sites. Israel and its supporters tried to respond with their own cyber-attacks, but they were less successful in winning international support for the incursion into Gaza. They used recruits to flood blogs with pro-Israel opinions and hacked a Hamas television station. Hackers supporting Israel also infiltrated pro-Palestinian Facebook groups and collected information about the group members. Israel also tried to pressure hosting companies to cut off service to hacker Web sites. A group of Israeli hackers also created the botnet Patriot to initiate distributed denial-of- service attacks against anti-Israel Web sites.

4.8 The Jasmine Revolution

Conflict Background: In 2011 thousands of Tunisians took 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.

Figure 11. The Jasmine Revolution: Map of the Conflict

Table 6. Case Precis for Jasmine Revolution (Gazula, 2017)

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

The Jasmine Revolution Analysis. Tunisian authorities allegedly carried out phishing operations to take control of user passwords and check online criticism. Both state and non-state websites had been hacked. Facebook remained accessible to roughly 20% of the population throughout the crisis whilst its passwords were hacked by a country-wide man-in-the-middle attack **(Madrigal, 2011)**.

(a) **Likely Cyber Tools used.** Phishing operations were carried out by the govt authorities. MIITM was used extensively.

(b) **Likely Actors.** State and non-state hackers are involved on both sides.

4.9 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.

This spy virus was discovered and linked to several countries, DuQu1.0 was first installed in 2011 and updated to DuQu 2.0 and it affected over 400 million computers. There were three computers in different hotels that hosted Iran Nuclear talks were targeted by the DuQu 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

Figure 12. DuQu 1.0/2.0 Map of Conflict

Table 7. Case Precis for DuQu 1.0/2.0 (Gazula, 2017)

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 DuQu 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.
Post Hostilities (Withdraw)	Phase5: Late 2011: No information found.

DuQu 1.0/2.0 Analysis. DuQu is a malware with zero-day exploits.

(a) **Likely Cyber Tools used.** Based on Stuxnet code, DuQu was designed to log keystrokes and mine data from industrial facilities, presumably to launch a later attack.

(b) **Likely Actors.** The source is same and hence the likely involvement of same actors as that of Stuxnet.

4.10 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 Dec 2009. Its name derives from a reference in its code that was identified by McAfee security company executive Dmitri Alperovitch. The Operation Aurora hack is unrelated to the similarly named Aurora Project, which was a U.S. action to simulate remote degradation of supervisory control and data acquisition equipment used in electrical generation.

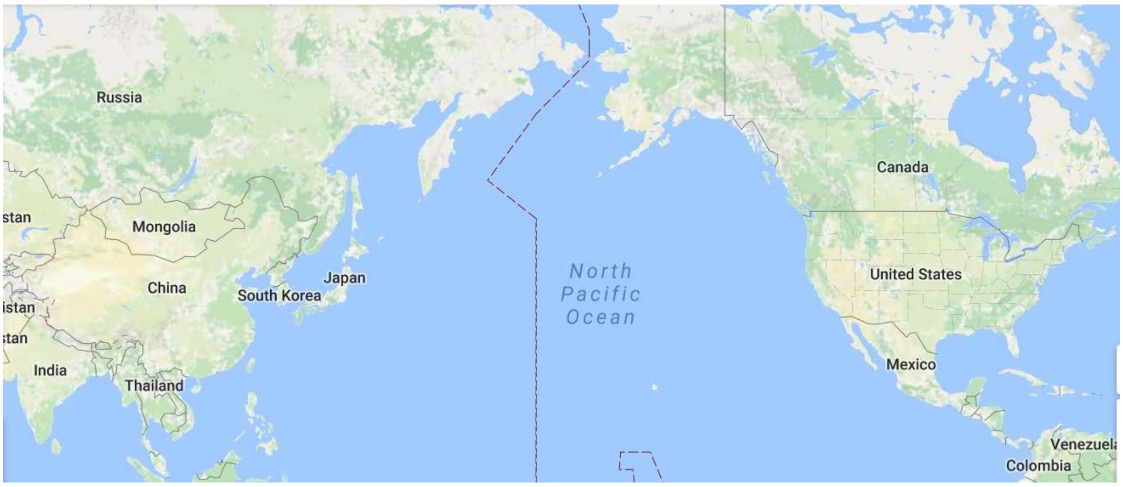


Figure 13. Operation Aurora

Table 8. Case Precis for Operation Aurora (Gazula, 2017)

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)	Phase 2a 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 Explore.
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. 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.

Operation Aurora Analysis. According to some media reports, a source within the Chinese government leaked that the campaign had been ordered by the Politburo. Like the intrusions upon Tibetan networks, the primary objective of Operation Aurora appears to have been an attempt to monitor dissidents. Specifically, the attackers attempted to use the Google source code to enable monitoring of Gmail users who have been linked to anti-government rebels, primarily located in the western provinces **(Wortzel, 2010, pp. 90-91)**. Some investigators, including the cyber security firm HBGary, have tracked the intrusions back to Shanghai Jiao Tong University and Lanxiang Vocational School, two schools directly tied to Baidu, a Chinese search engine that competes domestically with Google. As is their standard response in these matters, the Chinese government not only denied any involvement, but also immediately accused the United States of orchestrating the entire scenario.

(a) **Likely Cyber Tools used.** Operation Aurora relied on spear phishing against certain Google employees. Those who unsuspectingly followed a link in a received e-mail were directed to a Web site that contained malicious

JavaScript code. The specific exploit, known as Trojan.Hydraq, specifically targeted users navigating the Internet through the popular Microsoft Internet Explorer Web browser. Those victims using Internet Explorer became subject to an unidentified zero-day exploit that established a remote administration tool (RAT), allowing hackers to collect information about the user's activities and files. Having gained access to the accounts of victims, hackers proceeded to send e-mail messages to new potential victims, drawing on contacts lists to spread further.

(b) **Likely Actors.** It has been suggested that Aurora may have been linked to another hacking effort, Operation Shady RAT, which dates to 2006. As such, Aurora fits the description of an advanced persistent threat (APT). Evidence points to PRC culpability in the Aurora hack. Researchers from the security company VeriSign traced the hack to Internet Protocol (IP) addresses that had been compromised and used in an earlier distributed denial-of-service (DDoS) action against South Korea and the United States in the summer of 2009, and they noted patterns in the operations that further suggested that the entity responsible for the 2009 DDoS effort had also undertaken Operation Aurora.

Experts believe that the hacks emanated from some of PRC's premier universities in the computer science field. Students at Jiaotong University in Shanghai have defeated rivals from over 100 international institutions in such competitions as the 1997 Battle of the Brains competition sponsored by IBM. The potential involvement of another institution in eastern China, Lanxiang Vocational School, has also been debated. Officials at the school have denied any connection to the hack and have argued that personnel at Lanxiang lacked the sophistication to perpetrate it. However, the school is closely linked to the People's Liberation Army (PLA). Some analysts also believe that Unit 61398, the most notorious of the hacking entities in the PLA, may be connected to Operation Aurora. Unit 61398, like Jiaotong University, is in Shanghai. Evidence does suggest the unit's culpability in a number of other efforts geared toward gaining strategically and sometimes economically valuable information through espionage directed against foreign entities **(Sambaluk, 2017, pp. 215-216)**.

4.11 Operation Orchard

Conflict Background: In 2007, an Israeli Airforce (IAF) fighter aircraft entered Syrian airspace, conducted electronic warfare & cyber hacking and dropped 17 tons of precision 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. This was key to defeating Syria's highly advanced Russian-made integrated air defense system (IADS). Despite Israel's blatant use of military force, the operation did not make many headlines. It should also be noted that Operation Orchard was far more pre-emptive than Operation Opera, where the Iraqi reactor had been nearing completion **(Venable, 2017, p. 224).**

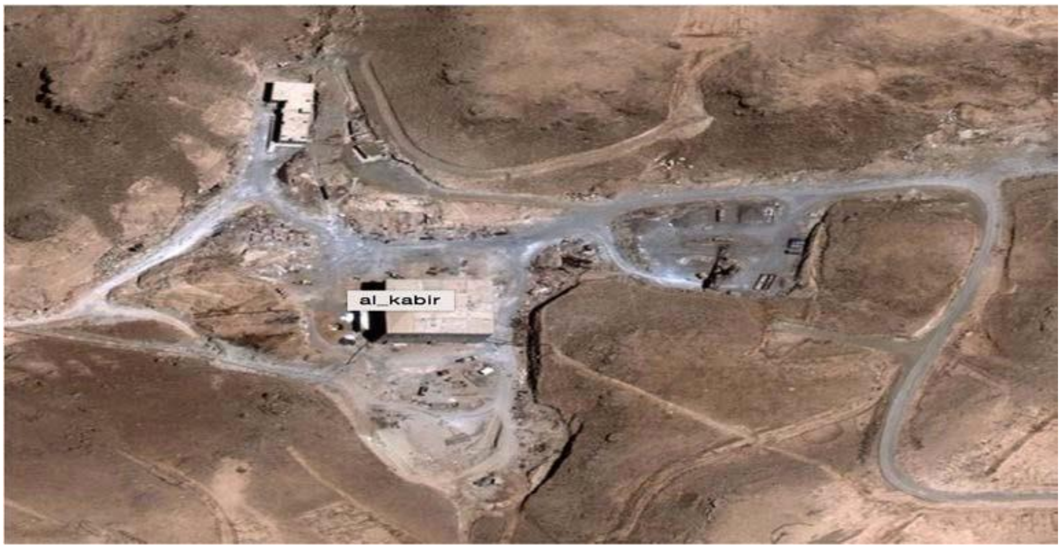


Figure 14. Operation Orchard: Suspected nuclear reactor site in Syria before bombed.

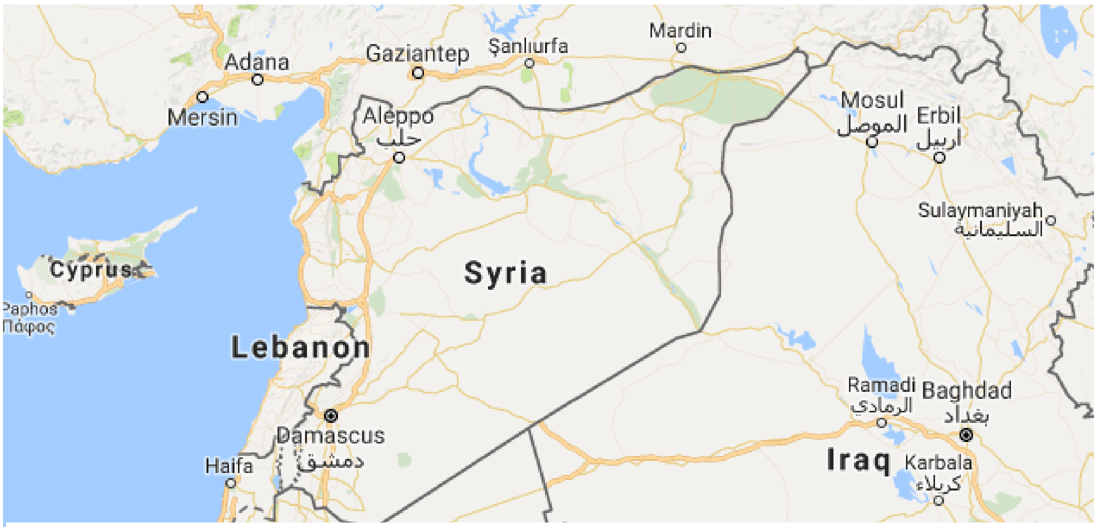


Figure 15. Operation Orchard's Map of Conflict.

Table 9. Case Precis for Operation Orchard (Gazula, 2017)

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. 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.
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.

Operation Orchard Analysis. Although the operational details are murky, and formal attribution has never been made or acknowledged, from the point of view of international law, the attack on an adversary’s illicit military installation was justified. A strike had been continuously threatened in the event that Syria pursued development of a nuclear weapons program. Both the cyber and conventional military actions were undertaken only after reasonable diplomatic efforts, including embargoes of illegal shipments of materials from North Korea, had failed to halt Syrian collaboration with North Korean agents. The pre-emptive cyber strikes were directed against military targets: radar and Russian-made air defense systems, much as a conventional attack might have been, enabling Israeli fighters to penetrate deeply into Syrian airspace with little resistance. Unlike the conventional attacks that followed, the cyber-attack attained the military objective of rendering defensive forces helpless, without widespread destruction of property or loss of life on either side **(Mahnaimi, 2007)**

(a) **Likely Cyber Tools Used.** There has been speculation that the attack incorporated a variation of a cyber tool developed by the United Kingdom's BAE Systems that facilitates penetration of communications links to IADS. Known as the Suter airborne network attack system, rather than jamming radar signals, it instead hacks into the IADS to control the functionality of time-critical operations by locating emitters precisely and then directing data streams into them that can include false targets and message algorithms **(Corfield, 2017, p. 43)**.

(b) **Likely Actors.** Formal attribution has never been made or acknowledged.

4.12 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.

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

Figure 16. Shamoon I & II : Map of Conflict Region

Table 10. Case Precis for Shamoon I & II (Gazula, 2017)

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 announce 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)	Phase 2a 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.
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.
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.

Shamoon I & II Analysis. The attack on Aramco was one of the most destructive virus attacks since Stuxnet, according to U.S. Secretary of Defense Leon E. Panetta. The Shamoon virus infected nearly 30,000 Aramco computers, which were rendered completely unusable after the attack. It took Saudi Aramco over a week to restore services after isolating their system. The Shamoon virus did not reach the drilling or refining operations control system computers, but much of the drilling and production data were lost because of data corruption by the virus. The Aramco cyber-attack demonstrates the dangers of neglecting network security and directly connecting critical systems to the Internet **(Quillman, 2017, pp. 12-13)**.

(a) **Likely Cyber Tools Used.** The Shamoon virus is a self-replicating modular computer virus that affects Microsoft Windows–based machines. The virus was primarily targeted for oil and energy companies. The virus is spread from one infected computer to other computers within the network. According to Symantec, the virus contains three components: a dropper, a wiper, and a reporter.

(i) The dropper is the primary component that initiates the copying and execution of itself as well as embedding the other components into the system.

(ii) The wiper is the destructive component that deletes files and overwrites files with corrupted JPEG images.

(iii) The reporter transmits the virus information back to the attacker.

(iv) The virus basically renders the computer systems unusable.

(b) **Likely Actors.** The Shamoon attack appears to have been a form of cyber sabotage. The attack was started by an insider, a disgruntled Saudi Aramco employee, who infected a computer system within Aramco's internal network. The employee was alleged to be working for the Iranian government. Sometime after the attack occurred, the Cutting Sword of Justice, a previously unknown hacker group, claimed responsibility for Shamoon. As proof of their involvement, the hacker group posted thousands of Aramco computer IP addresses **(Quillman, 2017, p. 13)**.

4.13 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.

Table 11. Case Precis for Russian Hackers Tracking Ukrainian Artillery (Gazula, 2017)

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.
Conflict 2A (Reconnaissance)	Phase 2a 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. 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.
Conflict 2B (Replicate)	Phase 2b Early 2014 through 2016: 9000 users had the application running with the malware in the distribution forums.
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.
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.

Analysis. 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.

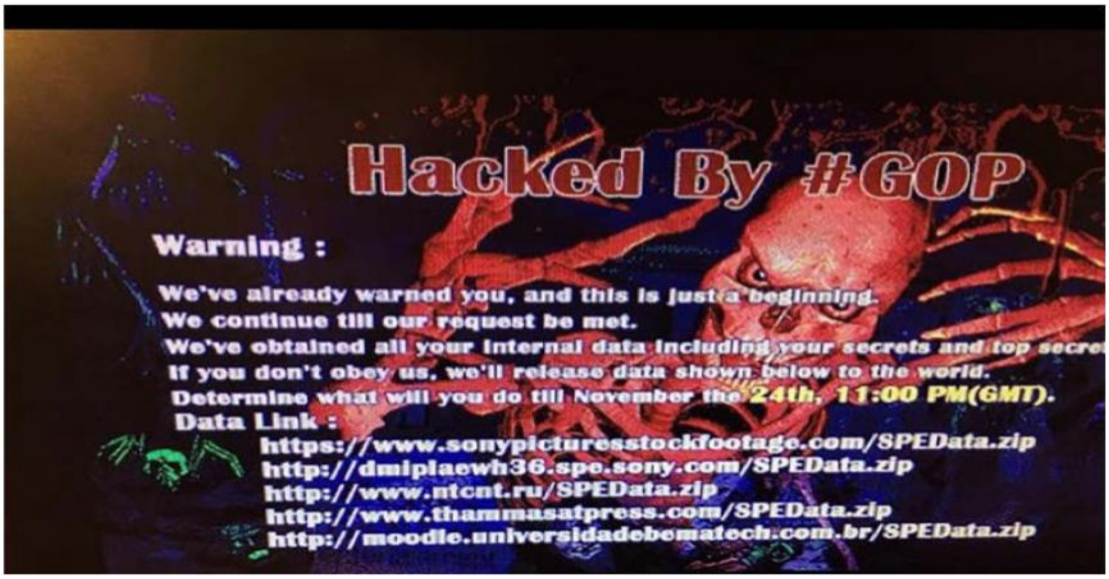
(a) **Likely Cyber Tools Used.** The weapon (malware) was trojanized in an Android application used by the Military for quick deployment of a war weapon. DDoS and targeted intrusions in media, financial and political entities in Ukraine were carried out.

(b) **Likely Actors.** Russian Hacker namely called Fancy Bear or APT 28.

4.14 Sony Corp's Hollywood Studio Attack

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. The Sony Hack was a November 2014 incident whereby hackers from the Democratic People’s Republic of Korea (North Korea) launched an attack against the servers of Sony Pictures Entertainment in Los Angeles, California.

The hackers sought to prevent the release of the comedy film *The Interview*, which depicted the assassination of North Korean leader Kim Jong-un.



Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secre
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Data Link :
https://www.sonypicturesstockfootage.com/SPEData.zip
http://dmiplaewh36.spe.sony.com/SPEData.zip
http://www.ntcnt.ru/SPEData.zip
http://www.thammasatpress.com/SPEData.zip
http://moodle.universidadebematech.com.br/SPEData.zip

Figure 17. Sony Corps Hacked Website

Table 12. Case Precis for Sony Corps Cyberattack (Gazula, 2017)

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.

Sony Corps attack Analysis. 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.

(a) **Likely Cyber Tools Used.** It is believed that the hackers first accessed Sony's network in September 2014. Over the next two months, the hackers eventually granted themselves administrator privileges that provided unlimited access to the company's network. Subsequently, the hackers then downloaded significant amounts of critical information from the servers without attracting notice because Sony encrypted almost none of its data. In addition, the hackers slowly copied the data from Sony servers to their own to hide the file transfers among Sony's legitimate data traffic. Soon after, the hacker's malware erased data on approximately half of Sony's computers and servers and also caused Sony's network to crash **(Wadle, 2017, pp. 273-274)**.

(b) **Likely Actors.** Initially, many speculated that a disgruntled employee had caused the Sony Hack. On 19 Dec 2014, the Federal Bureau of Investigation (FBI) publicly attributed the attack to North Korea.

4.15 Attack on Estonian Government

Conflict Background: Estonia is a small country in Northern Europe. It borders the Baltic Sea, Latvia, and Russia. At the forefront of the Estonian outcry were the escalating tensions with Russia that had peaked in the spring of 2007, ostensibly over a World War II monument. That February, the parliament in Tallinn had passed legislation prohibiting the display of structures on Estonian soil related to the 49-year (1940–1989) Soviet occupation of Estonia. Especially at issue was a statue known as the *Bronze Soldier* of Tallinn, a six-and-a-half-foot bronze sculpture of a Red Army regular standing in front of a section of stone wall vaguely resembling a mausoleum. The work was completed in 1947 in honor of the Soviet “liberators of Tallinn” from the Nazis.

Figure 18. Estonian Cyber attack

Table 13. Case Precis for Estonia Cyber Attack (Gazula, 2017)

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.

Estonian Cyber Attack Analysis. Both the US and NATO sent teams of computer security experts to help the Estonian authorities cope with the massive wave of DDoS attacks that paralyzed the country's government websites, banking industry, and media outlets. What struck many network security experts as unusual about the cyber-attacks was that they lasted weeks, and their intensity was extremely high. **(Schreier, 2015, p. 110)**.

(a) **Likely Cyber Tools Used.** Some botnets employed in the DDoS attacks on Estonian websites included up to 100,000 'zombie' PCs **(Schreier, 2015, p. 110)**.

(b) **Likely Actors.** Moscow denied any involvement in the DDoS attack, but they also refused to assist the Estonians in investigating the source of the attack. As Estonian authorities worked to restore servers and services, they also began to shift away from further antagonism of Russia and from urging a full-blown NATO condemnation of Russia. Russian public statements also began to change, admitting the possibility of the involvement of private Russian patriots acting on their own initiative **(Connelly, 2017, pp. 102-105)**.

4.16 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.

Figure 19. Operation Dust Storm: Map of Conflict

Table 14. Case Precis for Operation Dust Storm (Gazula, 2017)

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

Operation Dust Storm Analysis. Operation Dust Storm was first discovered by the Cylance SPEAR Team and confirmed with Cylance products. A five-year campaign focused on extracting sensitive information from Japanese oil, gas, and electric utilities through multiple backdoors. **(Brook, 2016)**.

(a) **Likely Cyber Tools Used.** Cylance Spear research indicates Operation Dust Storm has been operational since at least early 2010, and has employed a number of different operational techniques, including spear phishing, waterholes and zero-day exploits over time. Several antivirus companies initially detected early backdoor samples under the moniker Misdat, but the group has quietly evolved over the years to remain undetected and highly effective.

(b) **Likely Actors.** A large number of antivirus companies could also not detect what was done by Cylance Spear company. Seems a typical job of State-sponsored espionage.

4.17 Operation Anarchist

Conflict Background: It is acceptable 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.

Figure 20. Operation Anarchist

Table 15. Case Precis for Operation Anarchist (Gazula, 2017)

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.
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 1998-2016: 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.

Operation Anarchist Analysis. The documents highlight the conflicted relationship between the United States and Israel and U.S. concerns about Israel’s potentially destabilizing actions in the region. The two nations are close counterterrorism partners, and have a memorandum of understanding, dating back to 2009, that allows Israel access to raw communications data collected by the NSA. Yet they are nonetheless constantly engaged in a game of spy versus spy.

(a) **Likely Cyber Tools Used.** Encrypted video transmissions were hacked into.

(b) **Likely Actors.** US and UK Intelligence Service.

4.18 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 Oct 2008, to be the most serious breach of the U.S. military's classified computer systems. 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.

Figure 21. Operation Buckshot Yankee Area of Conflict

Table 16. Case Precis for Op Buckshot Yankee (Gazula, 2017)

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.

Operation Buckshot Yankee Analysis. The presence of US troops overseas had given rise to espionage from International Intelligence agencies. The Advanced Network Operations (ANO) team finally devised a way to counteract Agent.btz. The counter- program searched for the beacon signal of Agent.btz and mimicked its creator, effectively putting the malware to sleep. Then the painstaking process of removing the Agent.btz malware from U.S. government computers began **(Beckenbaugh, 2017, p. 218)**.

(a) **Likely Cyber Tools Used.** Malware program most probably propagated from an infected thumb drive.

(b) **Likely Actors.** Not identified.

4.19 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 20 Mar 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.

Table 17. Case Precis for 2016 US Elections (Gazula, 2017)

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. 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 : 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. 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: 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.

2016 US Elections Analysis. In the run up to the 2016 US presidential elections, Kremlin-backed hackers managed to break into the email of the Democratic National Committee and released them online to create embarrassment. According to the Washington Post, after revelations about Russian meddling in the run up to the 2016 US Presidential elections, President Obama authorised the planting of cyber weapons in Russia's infrastructure. "The implants were developed by the NSA and designed so that they could be triggered remotely as part of retaliatory cyber-strike in the face of Russian aggression, whether an attack on a power grid or interference in a future presidential race," the report said.

(a) **Likely Cyber Tools Used.** Spear phishing e-mail accounts and malware used for extracting DNC e-mails.

(b) **Likely Actors.** The high cost of such cyber incidents with no monetary gain to an individual, points finger at State-backed hackers namely two Russian cyber espionage intelligence groups the Fancy Bear and the Cosy Bear also known as APT 28 and APT 29 respectively.

4.20 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. 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.

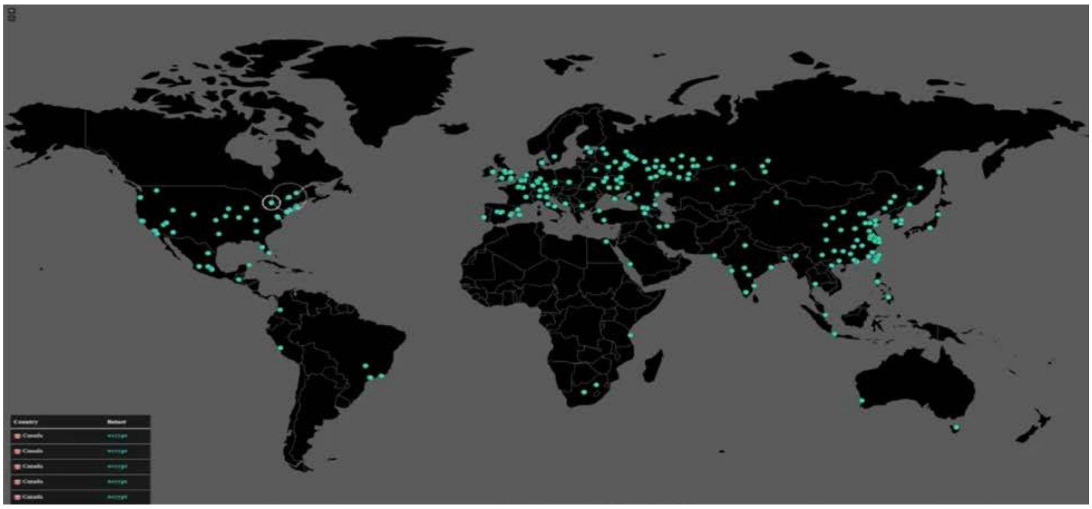


Figure 22. Wannacry Exploits Worldwide

Table 18. Case Precis for Wanncry (Gazula, 2017)

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.

Wannacry Analysis. The ransomware proved so virulent because it was supercharged with a zero-day vulnerability that had been stockpiled by the NSA, presumably to use in cyber espionage. But the tool was somehow acquired by the Shadow Brokers hacking group (quite how is extremely unclear) which then leaked it online. Once this happened other ransomware writers incorporated it into their software, making it vastly more powerful **(Nakashima, 2017)**.

(a) **Likely Cyber Tools Used.** Malware and Ransomware cryptoworm.

(b) **Likely Actors.** In Sep 2018, The US Department of Justice charges a North Korean programmer with involvement in some attacks including the WannaCry ransomware outbreak in 2017.

4.21 Anonymous vs ISIS

Anonymous, the self-styled vigilante group best known for malicious online exploits ranging from vandalism to data theft, opened a new tactic in its cyber-offensive against the Islamic State of Iraq and the Levant with a universal call to action against the terror group.

In 2015, an offshoot of Anonymous, which calls itself Ghost Security, also known as GhostSec, took credit for silencing tens of thousands of ISIS-related social media feeds and propaganda websites. GhostSec, first became known early 2015 when it called on its thousands of followers to help assemble then publicize a list of known Islamic State Twitter accounts. When Twitter removed many of those accounts (GhostSec claims 59,000 were removed in all), the hacking group then launched a flurry of distributed denial of service attacks against known ISIS websites, knocking them offline for various periods of time. Now the group claims it intercepted tweets among

ISIS members and forwarded them to international law enforcement. “Our mission is to eliminate the online presence of Islamic extremist groups such as Islamic State, al Qaeda, al-Nusra, Boko Haram and al-Shabab in an effort to stymie their recruitment and limit their ability to organize international terrorist efforts,” GhostSec’s website states.

GhostSec is made up of roughly 12 core members, but relies on hundreds of part-time volunteers to find out which accounts should be targeted. ISIS relies on a rotating cast of 50,000 to 70,000 accounts, the New York Times reported **(Gladstone, 2015)**, though a number of international terrorism experts have said it’s impossible to verify how much of an effect Anonymous is having.

It’s the latest battle between the Islamic State’s corps of cyber jihadis and Anonymous. They were so successful, ISIS began distributing a list of nearly 200 assassination targets, which included a number of prominent Anonymous Twitter accounts **(Stone, 2016)**.

Following the Nov 2015 Paris Attacks, Anonymous further announced a major, sustained operation against ISIS, declaring, "Anonymous from all over the world will hunt you down. You should know that we will find you and we will not let you go." ISIS responded on Telegram by calling them "idiots", and asking "What they gonna to [sic] hack?" By the next day, however, Anonymous claimed to have taken down 3,824 pro-ISIS Twitter accounts, and by the third day, more than 5,000. A week later, Anonymous increased their claim to 20,000 accounts and released a list of the accounts. A spokesman for Twitter stated that the company is not using the lists of accounts being reported by Anonymous, as they have been found to be “wildly inaccurate” and include accounts used by academics and journalists **(Cameron, 2015)**.

Anonymous vs ISIS Analysis. This could be a positive, though unconventional and certainly unsanctioned, supplement to ongoing efforts to counter violent extremism. If nothing else, the Anonymous offensive could provide authorities with new insight on how to exploit vulnerabilities in ISIL's online propaganda operation. If ISIL's online activity is disrupted by Anonymous, all the better. Such an effort could build momentum from other parts of the general population — beyond what law enforcement agencies and military forces can provide **(Brown, 2015)**.

(a) **Likely Cyber Tools Used.** Hacking Twitter accounts and DDoS.

(b) **Likely Actors.** Anonymous and ISIS.

CHAPTER - 5

DATA ANALYSIS AND FINDINGS

It is quite evident from the case studies and cyber-attack events analysed in previous chapters that cybercrimes mimic their real-world counterparts, i.e. to say, that nearly all cybercrimes would have elements of real-world crimes possible. They include theft, graffiti (defacing of sites), sale of drugs and contrabands, stalking, espionage, terrorism, stealing and manipulation of data, kinetic attacks etc. Similarly, all cyberattacks and cyberwarfare events have some shades of these crimes. It has also emerged that cyberspace conflicts are predominately a non-state activity and in most cases we observe that cyber-actions involve various non-state actors.

The distinctions between these actors may perhaps appear somewhat theoretical and artificial. For example, boundaries between script kiddies and hackers, between cyber-militias and patriot hackers or between cybercriminals and cyberespionage agents, may obviously be somewhat hazy. Individual actors can participate in multiple activities and roles concurrently. However, the distinctions between the actors are useful for analytical purposes.

5.1 Employment of Non-State Actors: Reasons

Cyberspace, unlike other arenas associated with warfare, provides a high level of anonymity and attackers can carry out actions in this domain with little or no risk of attribution. Furthermore, cyberattacks can be carried out inexpensively, and can, at least in theory, cause extensive damage or at least trigger severe disruptions to ICT-based services. In addition, if a nation-state can covertly initiate, fund, or control such attacks, relying on non-state actors to carry out the attacks in their stead, they can reduce the already low risk of political implications, and potentially achieve their objectives without the burden of adhering to the Law of Armed Conflict. This gives an attacker a tremendous asymmetric advantage, especially for smaller nations that cannot prevail on a kinetic battlefield. As a result, employment of non-state actors in cyberspace operations is likely a very attractive option for nation-states or an equivalent body, especially when pursuing limited strategic goals.

Advantages: The benefits are further explained below.

(a) Non-state actors can be employed to cater for the lack of cyber capabilities within the regular forces. The attacker has the upper-hand and gains the initiative. He can most often conduct cyberattacks covertly offering the advantage of surprise as well as the benefit of plausible deniability. The defender in a predictable manner is forced to respond.

(b) The cost of maintenance of a non-state actor is far lower than the regulars.

(c) The fast-changing pace of technology and cyber tools would have a high cost implication in training a standing army and hence hiring non-state actors ably equipped for a credible attack would be economical.

(d) By engaging non-state actors from previously identified Internet forums and social networks, rapid mobilization and suitably motivated technically-competent force can be accomplished at little or no cost.

(e) Non-state actors also retain the option in magnifying the scale of the attack and the effects of plausible deniability. Even if attribution is successful, i.e. the attacker is identified by the defender, the lack of applicable international laws covering cyberwarfare creates a useful shield of legal ambiguity.

(f) Employing non-state actors might raise suspicion in the international community, the lack of any hard evidence will protect the attacker political ramifications. Thus, the threat of a counterstrike is negligible.

(g) Due to gained initiative, the attacker can launch the cyberattack

(i) at the exact time

(ii) against the target of his own choosing and

(iii) using appropriate attack methods.

(h) The attacker could launch a cyberattack with a single computer, whereas the defender would require to employ all its cyber-resources, which can be prohibitively expensive.

(i) The attacker can decide the attack mode, scale and duration in order to cause desired effects.

Disadvantages. The disadvantages are further explained below: -

(a) Although the attacker may give clear directions as to which targets are to be attacked and by which weapons/methods however the actual actions by the non-state actors are uncontrollable and the cyberspace operations can be ineffective. Also, the depth of attack may be uncontainable and lead to far-fetched effects and consequences, which could be harmful for the attacker itself.

(b) The attacker risks creating unwanted collateral damage, by hitting unintended targets. Attacks could also grow beyond the intended size and scope. Overly zealous members of cyber-militias, not limited by the restrictions that govern military organizations, could opt to target civilian targets without thought of possible consequences.

(c) Attacks initiated by non-state actors could affect the attacker's network or resources negatively, by overloading common infrastructures, such as Internet backbone connections.

(d) Even though the laws of war are unclear concerning cyberspace, attacks that are linked back to the initiating nation-state could be politically devastating. Escalation may also lead to retaliation through conventional means **(Lewis, 2011)**.

(e) If cyberattacks are directed against civilian systems, as is most likely in one way or another, the initiating state could be accused of committing war crimes, or being branded as a sponsor of cyberterrorism, becoming pariah as far as international relations are concerned.

Employing non-state actors can potentially be risky in the long term, even though the immediate attacks are successful, as these might be unreliable. Criminals might try to blackmail a government in order not to disclose sensitive details, and contracted cyber espionage agents might defect to the opposing nation if offered political asylum.

5.2 Role of Non-State Actors

The main purpose of this paper has been to study the various non-state actors who coexist in cyberspace and their employment by nation-states in cyberspace operations. Based on the analysis of cyberattacks and cyberwar events, we find the conflicts to be categorized in the following categories: -

(a) Nation states vs Nation states,

(b) Non-state actors vs Nation states and

(c) Non-state vs Non-state actors

The first category, i.e Nation states vs Nation states conflict is an appropriate and legitimate act wherein it has some legality and justifiable cause included. These conflicts are closely related and included in the definition of Cyberwar. Our main concern is on the other two categories of conflict namely; **Non-state actors vs Nation states** and **Non-state vs Non-state actors** and the role played by the Non-state actors in them.

5.3 Non-state Actors vs Nation States

The requirement to initiate a political agenda with a strategic edge, nation-states are tempted to employ cyber non-state actors. It nevertheless assures significant asymmetric advantages to a weaker nation-state with anonymity and provides an efficient shield against subsequent blame and political ramifications **(Sigholm, 2016)**. If traced to the source, such attacks will legally be seen as criminal activity, possibly even in the unlikely scenario where comprehensive and irrefutable evidence can be provided, linking the nation-state and the attacker.

Nation-states have little incentive to openly take credit for cyberattacks. Doing so could lead to political or military recrimination, and might expose individuals to criminal prosecution if their responsibility for committed illicit actions was deemed to be against the laws and customs of war. While some nation-states might favor ratifying a novel legal framework defining acts of aggression in cyberspace, it seems likely that many others would find it far more beneficial to maintain the current ambiguity that surrounds cyberwarfare, and perhaps even actively undermine such efforts, as the asymmetric nature of cyberwarfare benefits those who lack the ability to dominate in conventional arenas. Even if the international community were successful in codifying cyberwarfare into alignment with international law, and thereby implement limitations of its use, it would probably still not be very effective as the employment of non-state actors in cyberspace operations is still in effect a gray-area.

5.4 Non-state Actors vs Non-state Actors

The case study has highlighted this new category which could have far-fetched consequences in the near future. Anonymous has openly challenged ISIS and their online resources and operations. It also could provide a glimpse of what information warfare might look like in the future, as public messaging campaigns are fought avatar-to-avatar. This visualises a campaign that is decentralized, flexible and asymmetric, yet still unified by drawing on the resources of a global cyber militia or non-hackers included It could also highlight gaps and seams between multiple disciplines, like cyber security, critical infrastructure protection, civil rights and civil liberties, information operations, countering violent extremism, counterterrorism and law enforcement. It could also be used to evaluate the mechanisms designed to foster collaboration between the complex network of community, industry, government and foreign partners **(Brown, 2015).**

While ISIS uses the Internet to recruit fighters and incite violence, the Anonymous counter initiative could lower the volume of the online echo chamber, and yield support for the war against ISIS and its extremist ilk. Perhaps such a test might turn out to be a gift in disguise for the security organisations.

5.5 Inference on Trends in Cyberattacks

The historical relations of the involved states, the technology existing at that time with the Dark-web and with cyber criminals were the cyber-tools commonly used in the cyberattacks. As the technology improved, the cyberattacks became more advanced and as expected the criminals were ahead of the cyber security and cyber-defense means. However the most common attacks have been: DDoS, malicious codes, viruses, worms and Trojans, SCADA kinetic attack – Stuxnet worm, spear-phishing, malware, stolen devices, phishing and social engineering, web-based attacks, ransomware etc. Due to obscurity nature of cyberspace, it has been rather difficult to determine the exact type of actors being involved, however the types of attacks have been closely studied in the 19 case studies and some statistics are as shown in Fiqure

23. It may be seen that Spear-phishing, DDoS, thumb-drive infected malware and SCADA attacks have been predominant with percentages as high as 42.11%, 21.05% and 15.8% respectively.

			Types of Attack												
Sl No	Date	Cyber Attack	Network Attack	DDos	Spear phising	Thumb drive Malware	SCADA	MITM	Trojan	Virus	Defacing	Traffic Routing	Malware	Ransomware	APT
1	Sep-07	Op Orchard	1												
2	Sep-07	Attack on Estonia		1											
3	Jul-08	Kosovo War		1	1										
4	Jul-08	Russia-Georgia War			1										
5	Oct-08	Op Buckshot Yankee				1									
6	Jul-09	Op Aurora			1										1
7	Mar-10	Stuxnet-SCADA				1	1								
8	Jan-11	Jasmine Revolution			1			1							
9	Oct-11	DuQu (1.0 & 2.0)					1								
10	Aug-12	Shamoon Attack I&II							1	1					
11	Nov-12	Op Cast Lead									1	1			
12	Apr-14	Ukrainian arty		1											
13	Jul-14	Sony Studio Attack			1										
14	Jan-15	Anonymous vs ISIS		1											
15	Jul-15	Op Dust Storm			1										
16	Dec-15	Ukrainian Power Grid			1		1								
17	Jan-16	Op Anarchist				1							1		
18	Jun-16	2016 US Elections			1								1		
19	May-17	Wannacry												1	
		Total	1	4	8	3	3	1	1	1	1	1	2	1	1
		Percentage	5.26	21.05	42.11	15.79	15.79	5.26	5.26	5.26	5.26	5.26	10.53	5.26	5.26

Figure 23. Inference on types of Cyber attacks

5.6 Common Reasons for Successful Cyberattack

Cyber-attacks are successful for several reasons. A few are mentioned in this section.

(a) Vulnerabilities in software - poor quality of software products and computer system configurations and these are the major point of entry for an attack.

(b) Poor information security procedures and practices, inadequate training in computer security and inadequate resources devoted to staffing the security function. Many organisations feel security as a "technical issue" and never perceived as a "managerial issue". Others have a feeling that security is a single day solution and not aware that it should be continuous process.

(c) "Zero-Day exploits", nothing but software vulnerability before a security patch created by the software vendor and distributed to protect users.

Some other reasons are that:-

(a) Amateur users have little or no awareness in effectively securing their computers,

(b) Vendors for COTS software often release the new products with errors. Approx. 80% of attacks are due to software errors or may be due to poor software product quality.

(c) Many users do not give much importance to patch management and they do "patches" several weeks after the patch is available even though many vendors periodically release fixes or upgrades.

(d) Many IT companies outsource software code development to a foreign country. By Offshore outsourcing there is a possibility of keeping a Logic Bomb or a Trojan horse or spyware or other malicious program into the product.

(e) A number of structural factors are also contributed for the growing vulnerabilities. A few are:

(i) increased use of COTS software and hardware;

(ii) use of robust and complex Operating system and softwares which makes impossible to test under all operating conditions;

(iii) Unbounded networks (Internet and PSN) having large numbers of access points;

(iv) pushing the software products by vendors into the market before they were fully evaluated and tested;

(v) failure to add security features as an integral part of the product design process, and

(vi) the current market practice of shipping products with bugs and follow up with patches, as users discover problems.

Three other important factors are also contributed to the growing threat to the critical information infrastructure.

(a) Sophistication and widespread availability and ease of use of hacking tools. Hacking tools and techniques are available/posted on web sites/ bulletin boards. Some organisations are offering the courses on hacking in the name of ‘Ethical Hacking’,

(b) Insertion of rootkits/ spywares/ trapdoors and other malicious programmes by foreign intelligence agencies or by competitors. An increasing amount of software and its components are written overseas and lends to a possibility of insertion of malicious programme codes in the embedded chips, components or systems manufactured abroad. Today more than twenty-five countries are gathering intelligence with electronic intrusion, and a large number of countries are developing information warfare.

Change in the motives and characteristics of the actors. Terrorist & Criminal organisations are increasingly recruiting hackers for financial fraud, theft of proprietary information and intellectual property.

5.7 **Means of Cybersecurity**

The case studies of cyberattacks and cyberwar, as reported in Chapter 3, clearly illustrate that majority of the time cybercrime tools were utilised and exploited. Hence, same cybersecurity practices that protect users against everyday hackers and cyber crooks will provide adequate protection against state-backed cyber-attackers. That means covering the basics:

(a) It includes purchasing, installing, and updating a competent antivirus program,

(b) Changing default passwords,

(c) Selecting and maintaining passwords that are difficult to break,

(d) Avoid using the same password for different systems,

(e) Using a firewall;

(f) Running periodic security scans

(g) Backing up and securing data,

(h) Ensuring all systems are patched and up-to-date (including the use of antivirus software),

(i) Ensuring that systems are only connected to the internet if necessary,

(j) Common sense actions, such as avoid opening suspicious communications and not clicking on unknown or embedded links,

(k) Managing connections on social media as well as controlling access to Wi-Fi routers

This may be enough to stop some attackers or at least give them enough extra work to do that they switch to an easier target. However, for particularly high-value targets this is unlikely to be enough: these attacks are called ‘advanced and persistent’. In this case it may be hard to stop them at the boundary and additional cybersecurity investments will be needed: strong encryption, multi-factor authentication, and advanced network monitoring. It may well be that you cannot stop them penetrating your network, but you may be able to stop them doing any damage.

At a higher level, nations and groups of states are developing their own cyber defence strategies. More broadly, to prevent cyberwar incidents, countries need to talk more: to understand where the boundaries lie and which kinds of behaviour are acceptable. Until that is done there is always the risk of misunderstanding and escalation.

5.8 **Prevention of Cyber-incident**

Cyber-incidents can be classified in many ways; one could divide them by who commit them and what their motivation might be or could divide these crimes by how they are committed. We can divide computer attacks by the types of computer security that ought to prevent them. There are four types of computer security:

(a) Physical security is protection of the physical building, computer, related equipment, and media (e.g., disks and tapes).

(b) Personnel security includes preventing computer crimes. That is to protect computer equipment and data from a variety of different types of people, including employees, vendors, contractors, professional criminals and others.

(c) Communications security is to protect software and data, especially when it passes from one computer to another computer across a network connection.

(d) Operations security is protection of the procedures used to prevent and detect security breaches, and the development of methods of prevention and detection.

The facets of each are shown in Table 19 below:-

Table 19. Types of Cybercrimes

Breaches of Physical Security	**Breaches of Personnel Security**	**Breaches of Communications and Data Security**	**Breaches of Operations Security**
Dumpster Diving	Masquerading	Data Attacks Unauthorised Copying of Data Traffic Analysis Covert Channels	Data Diddling
Wiretapping	Social Engineering	Software Attacks Trap Doors Session hijacking Tunnelling. Timing Attacks Trojan Horses Viruses and Worms. Salamis Logic Bombs	IP Spoofing
Eavesdropping on Emanations	Harassment.		Password Sniffing
Denial or Degradation of Service.	Software Piracy		Scanning

Some of the recommended preventions are as follows:-

(a) **Recommendation for the Physical Security.** Physical security can prevent disaster or at least to minimise the effects of them. Major concerns of basic physical security:

(i) Locks and keys. The first line of defense against intruders is to keep them out of your building or computer room.

(ii) Natural disasters, such as fire, flood, lightning, and earthquakes.

(iii) Environmental threats, such as electricity and heating and air conditioning systems.

(iv) If you want examine and validate a physical security program, you can use some types of tests, such as regular physical security inspections, random checks and penetration tests.

(b) **Recommendation for Personnel Security.** People are the biggest threat to computer. There are many types of people who imperil computers and information, ex. employees, vendors, contractors, professional criminals. It is necessary to develop a personnel security program according to different people/different threats. Important components of personnel security are background checks and careful monitoring on the job.

(c) **Recommendation for Communications and Data Security.** As more companies connect their networks to the Internet, communications security is particularly important. There are many different ways to protect communications:

(i) Access control, e.g., the use of good password. It is crucial to enforcing computer security in networked environments.

(ii) Cryptographic methods, e.g., encryption of transmitted data.

(iii) Physical protection and shielding of network cabling.

(iv) Firewall technology. It can protect internal systems and networks from other networks.

(d) **Recommendation for Operational Security.**

(i) Operations security includes two major aspects of computer security:

(ii) Ways you can increase awareness among potential victims of possible computer crimes.

(iii) Ways you can keep computer criminals from actually committing a computer crime.

It is vital for individuals to understand that cybersecurity is of vital importance. Actors are constantly attempting to exploit any vulnerability in systems and networks to manipulate or deny access. Humans are the most vulnerable component of any cyber system and human error allows attackers achieving these goals even though individuals and organizations subscribe to best practices. The best approach to defending against both semantic and syntactic attacks is the holistic one. It is especially important to subscribe to the best practices, use software known to be safe and stable, and cooperate within to mitigate the risk of cyber-attacks and maintain constant vigilance for effective cyber security and cyber defense.

CHAPTER - 6

CONCLUSION AND FUTURE IMPLICATIONS

Politically motivated cyber-incidents are likely to escalate in both frequency and scale and attribution for these acts is likely to remain infeasible because of the anonymity the cyberspace provides. As the number of global Internet users grows, problematic cyber-incidents related to such actors are also like likely to increase. Based on the analysis of cyberattacks and cyber-events, the conflicts can be categorized in the following categories: -

(a) Nation states vs Nation states,

(b) Non-state actors vs Nation states and

(c) Non-state vs Non-state actors

The first category, i.e. Nation states vs Nation states conflict is a legitimate act wherein it has some legality and an intrinsic justifiable cause. These conflicts are closely related to the definition of Cyberwar. Our main concern is on the other two categories of conflict namely; **Non-state actors vs Nation states** and **Non-state vs Non-state actors** and the role played by the Non-state actors in them.

The requirement to initiate a political agenda with a strategic edge, nation-states are tempted to employ cyber non-state actors. It nevertheless assures significant asymmetric advantages to a weaker nation-state with anonymity and provides an efficient shield against subsequent blame and political ramifications. While some nation-states might favour ratifying a novel legal framework defining acts of hostility in cyberspace, it seems likely that many others would find it far more beneficial to maintain the present obscurity that surrounds cyberspace and perhaps even actively deter such initiatives. Even though if an international group is successful in framing cyberwar rules and aligns it with international law, it probably would still be ineffective as the employment of non-state actors in cyberspace operations is still in effect legally a gray-area.

The case studies have highlighted this new category of Non-state Vs Non-state actors which could have far-fetched consequences in the near future. Anonymous has openly challenged ISIS and their online resources and operations. It has provided a glimpse of what information warfare might look like in the future. Perhaps such a test might turn out to be a gift in disguise for the security organisations. It could also highlight gaps and seams between multiple disciplines, like cyber security, critical infrastructure protection, civil rights and civil liberties, information operations, countering violent extremism, counterterrorism and law enforcement.

It is vital for individuals to understand that cybersecurity is of vital importance. Actors are constantly attempting to exploit any vulnerability in systems and networks to manipulate or deny access. Humans are the most vulnerable component of any cyber system and human error allows attackers achieving these goals even though individuals and organizations subscribe to best practices. It is thus important to subscribe to the best computer-practices and mitigate the risk of cyber-attacks. The case studies of cyberattacks and cyberwar clearly illustrate that majority of the time cybercrime tools were utilised and exploited. Hence, same cybersecurity practices that protect users against everyday cyber-incidents and cyber criminals will provide adequate protection against nation-backed cyber-attackers.

In addition to the cybersecurity measures enumerated in the previous chapter, some out-of-the-box and radical solutions for increased cybersecurity and cyber defense are as suggested: -

(a) We might also begin to see the erection of virtual walls, formation of controlled cyber borders and stricter logical or physical separations of cyberspace domains. One such proposed scenario is ‘cyber-balkanization’, referring to the splintering of the Internet into subnets for specific functions such as critical infrastructure management or internal government communications. However, advocates of net-neutrality oppose such a scenario.

(b) Creation of a new secure Internet infrastructure to reduce cyberattacks.

(c) Newer technology and advancements could be used to secure the internet better than what we see it today with security protocols.

(d) Employ a version of Block Chain technology to make the net safer.

(e) Instead of fearing the hackers, lure them into a trap **(Big Win for Cybersecurity: Scientists Are Using a 'New Tool' to Set Trap for Hackers, 2020)**. The method, called DEEP-Dig (DEcEPtion DIGging), ushers intruders into a decoy site so the computer can learn from hackers' tactics. The information is then used to train the computer to recognise and stop future attacks.

(f) As corporates struggle to fight off hackers and contain data breaches, some are looking to artificial intelligence for a solution. They’re using machine learning to sort through millions of malware files, searching for common characteristics that will help them identify new attacks. They’re analyzing people’s voices, fingerprints and typing styles to make sure that only authorized users get into their systems. And they’re hunting for clues to figure out who launched cyberattacks—and make sure they can’t do it again **(Janofsky, 2018)**.

(g) IoT is gradually maturing and surely needs security protocols to be built-in its protocol else we will see a much unsafe cyberspace with increasing dependencies on IoT.

The true nature of cyber-attacks, cyberwarfare and the actors engaging in these activities has unfortunately been heavily disguised by the rapid advancement and obscure nature of cyberspace. The employment of non-state actors in cyberspace operations, as volunteers in state-to-state conflicts, cyber-militias, cyber-mercenaries or organized cyber-criminals highlight many new problems. Although no concrete incidents have occurred where cyberattacks have resulted in physical injury or extended destruction of property. Also, the heavy cyber-dependency of modern western countries makes more damaging cyberattacks plausible in future times. Solutions to mitigate these types of dangerous events before they evolve into real threats to national security, there is an ever increasing role for academia, as well as practitioners, involved in the study of cyberwar to bring out some law and lasting solutions. It also seems unlikely that such conventions will be forthcoming in the immediate future thereby creating a window of opportunity for resource-limited actors who cannot prevail on a kinetic battlefield. Nation-states thus have little or no incentive to support a legally binding definition of cyberwar which would limit their freedom of action or to formally take responsibility for executed cyberattacks.

6.1 **Implications for India**

Cyberattacks are on an increasing trend in India with only the US and China placed higher in ranking. Bangalore, Mumbai and Delhi are among the states which receives the highest traffic with 48% of the total attack being recorded in Chennai during the first quarter of 2019. Earlier some DRDO computers were compromised and few govt sites were defaced by Pakistan. Subsequently, India was been severely hit by attacks from Shadow Network, an espionage group from China and uncontrolled aftermath of Stuxnet. Lately, Kundankulam Nuclear Power Plant (KNPP), came under a cyberattack in the last week of Oct 2019 and the damage was in the form of data theft wherein the same data can be employed to initiate future attacks on the power plant. Even ISRO encountered attacks prior to the Chandrayan-2 mission. Indian healthcare website was attacked in 2019 wherein medical records and information of 68 million patients and doctors were stolen.

Cyber-intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy. Digital India Mission and increasing cybersecurity concerns have transformed this area into a multi-billion-dollar industry, currently valued at $4.5 billion, expected to reach $35 billion by 2030. The three sectors which are heavily invested in cybersecurity efforts are the Government, Information and Technology Services and Banking.

India was among the top nations which came under ransomware attacks in 2019. Stop, Ryuk and Purga were the most prominent ones. Demands were marked to be as high as five million dollars but usually ranged between $1-5 million on an average. Records revealed that the money spent on resolving the issue and paying for the damages exceeded the ransom amount.

On 11 Dec 2019, Minister of Electronics and Information Technology, Mr Ravi Shankar Prasad, introduced the Personal Data Protection Bill in the Lok Sabha. The bill seeks to secure digital collection of data of individuals through the establishment of the Data Protection Authority which will supervise and authorise companies and institutions (domestic and global) from accessing personal information of the citizens of India. Furthermore, even an official cybersecurity policy would help shore up defences across the board. The most important requirement for internet security is increased effective coordination between ministries that are overseeing various aspects of cybersecurity, proper critical infrastructure protection and public-private partnership. Even a small country like Israel has allocated an annual budget of $20 Mn for cybersecurity. We should strictly follow the cybersecurity measures as listed in the chapter above.

Considering the size and scale of cyberspace in our nation, we need approximately Rs 25,000 crore budget. “Data is Oil”. While many countries have high oil resources as a big opportunity to gain revenues, India can use data mining as a revenue-generating avenue. PM Narendra Modi’s ‘Digital India’ initiative, is necessary for the country’s economic prosperity. However, India does not have security personnel, as Taiwan and many other countries, who are explicitly trained to counter cybersecurity threats. We lack infrastructure and lack qualified individuals. India can better equip themselves by providing vocational cybersecurity guidelines to its professionals. India can also participate in cybersecurity inter-govt exchanges and programs with other Asian countries and expose India to new opportunities, software and technology and an understanding of other country’s cybersecurity models and platforms.

It has been reported that the Indian army is subject to recurring cyberattacks to the tune of twice a month on an average. India also makes it to the list of top 15 least cyber-secure countries in the world. It has led to the creation of tri-service command which will administer and oversee cybersecurity and Space operations. The Ministry of Defence has appointed two-star officers from the Indian Army and the Indian Navy to lead the Armed Forces Special Operations Division (AFSOD) and the Defense Cyber Agency (DCA) respectively; two-star officers from the Indian Airforce were appointed to head the Defense Space Agency (DSA). The DCA, under Rear Admiral Mohit Gupta, has been assigned two important functions – to fight cyber-crimes and to define and set guidelines to tackle cyber warfare. This initiative may lead to sharing of intel among the three wings which may bolster better communication and friendly relations. Lt. Col. Rajesh Pant, National Cybersecurity Coordinator, announced that the Government of India plans on releasing new cybersecurity Policy by early 2020. This plan will take into consideration incoming technologies (like 5G) too, the last update was in 2013 **(Yolmo, 2019)**.

Next-generation of cyber-attackers and cyberterrorists are growing up with computers, smartphones and ready-to-use cyber tools. The dawn of cyberattacks of magnitudes greater than those previously witnessed would be a harsh reality. The latest threats with AI based cyber-attacks, Deep-fakes, disinformation on social-media, cyber threats with 5G tech, Quantum-computing and its effect on cryptology, etc are looming seriously on advancements in cyberattacks and cyber warfare. Technology, with some out-of-the-box thinking is vital to find a way out of this obscurity in cyberspace and improve means of cybersecurity. Concerned focus needs to shift towards the cyber arena with the UN, governments, global antivirus companies, cyber security & defense industry committing resources towards a safer and securer cyberspace. One could definitely hope for a balanced, sensible and responsible approach from all involved actors.

Bibliography

Applegate, S. D. (2011, Sep.-Oct.). Cybermilitias and Political Hackers: Use of Irregular Forces in cyberwarfare. *IEEE Security & Privacy*, *Volume 9, Issue 5.*

Beckenbaugh, T. L. (2017). Operation Buckshot Yankee. In P. J. Springer (Ed.), *Encyclopedia of Cyber Warfare.* Santa Barbara, CA: ABC-CLIO, LLC.

Big Win for Cybersecurity: Scientists Are Using a 'New Tool' to Set Trap for Hackers. (2020, Feb 28). Retrieved Mar 06, 2020, from News18: https://www.news18.com/news/buzz/big-win-for-cybersecurity-scientists-are-using-a-new-tool-to-set-trap-for-hackers-2519211.html

Brook, C. (2016, Feb 24). *Five-Year 'Dust Storm' APT Campaign Targets Japanese Critical Infrastructure*. Retrieved Mar 06, 2020, from Threat Post: https://threatpost.com/five-year-dust-storm-apt-campaign-targets-japanese-critical-infrastructure/116436/

Brown, M. A. (2015, Dec 14). Retrieved Feb 28, 2020, from The Rand Blog: https://www.rand.org/blog/2015/12/anonymous-vs-isis-wishing-the-vigilante-hackers-luck.html

Bussolati, N. (2015). The Rise of Non-State Actors in Cyberwarfare. In K. G. Jens David Ohlin (Ed.), *Cyberwar: Law and Ethics for Virtual Conflicts* (pp. 102-126). Oxford University Press.

Cameron, D. (2015, Nov 21). *"Twitter: Anonymous's lists of alleged ISIS accounts are 'wildly inaccurate'"*. Retrieved Feb 28, 2020, from The Daily Dot: https://www.dailydot.com/layer8/twitter-isnt-reading-anonymous-list-isis-accounts/

Carey III, C. C. (2013). NATO's Options for Defensive Cyber Against Non-State Actors . *(US Army War College Fellowship). United States Army War College*. US Army: Civilian Research Project.

Carr, J. (2011). *Inside Cyber Warfare, Second Edition.* New Delhi: O'Reilly.

Clarke, R. A. (2010). Cyber War: The Next Threat to National Security and What to Do About It. New York, USA: HarperCollins Publishers.

Coleman, K. (2008, Jan 28). *Coleman: The Cyber Arms Race Has Begun*. Retrieved Feb 20, 2020, from CSO Online: https://www.csoonline.com/article/2122353/coleman--the-cyber-arms-race-has-begun.html

Connelly, D. (2017). Estonian Cyber Attack (2007). In P. J. Springer (Ed.), *Encyclopedia of Cyber Warfare.* Santa Barbara, CA: ABC-CLIO, LLC.

Corfield, G. (2017). Cyber Attack. In P. J. Springer (Ed.), *Encyclopedia of Cyber Warfare. (Ed.).* Santa Barbara, CA: ABC-CLIO, LLC.

'Crash Override': The Malware That Took Down a Power Grid. (2017, Jun 12). Retrieved Feb 17, 2020, from Wired: https://www.wired.com/story/crash-override-malware/

Crowther, A. G. (2017). Cyber Defense. In P. J. Springer (Ed.), *Encyclopedia of Cyber Warfare.* (pp. 48-51). Santa Barbara, CA: ABC-CLIO, LLC.

Cyber Warfare Law and Legal Definition. (n.d.). Retrieved Feb 20, 2020, from US Legal: http://definitions.uslegal.com/c/cyber-warfare/

Dictionary of Military and Associated Terms (JP 3-0). (2010 (As Amended Through 15 Oct 2011, Nov 08). *Joint Chiefs of Staff*.

Dunnigan, J. F. (2002). *The Next War Zone: Confronting the Global Threat of Cyberterrorism.* New York: Citadel Press.

Gazula, M. B. (2017, Jun). *Cyber Warfare Conflict Analysis and Case Studies*. Boston University, Boston.

Gladstone, R. (2015, Mar 24). *Anonymous vs. ISIS: Wishing the Vigilante Hackers Luck Against the Murderous Jihadists*. Retrieved Feb 28, 2020, from The New York Times: https://www.nytimes.com/2015/03/25/world/middleeast/behind-a-veil-of-anonymity-online-vigilantes-battle-the-islamic-state.html?_r=0

Jacob, F. (2017). Cyberwar. In P. Springer (Ed.), *Encyclopedia of Cyber Warfare* (p. 71). Santa Barbara, CA: ABC-CLIO, LLC.

Janofsky, A. (2018, Sep 18). *How AI Can Help Stop Cyberattacks*. Retrieved from https://www.wsj.com/articles/how-ai-can-help-stop-cyberattacks-1537322940

Johan Sigholm, C. (2016). Non-State Actors in Cyberspace Operations. Swedish National Defence College.

Lee, Robert M., Assante, Michael J., Conway, Tim. (2016, Mar 18). E-ISAC and SANS ICS.

Lewis, J. A. (2011). Cyberwar Thresholds and Effects. *IEEE Security & Privacy*, *Volume 9, Issue 5.*

Madrigal, A. C. (2011, Jan 24). *The Inside Story of How Facebook Responded to Tunisian Hacks*. Retrieved Feb 17, 2020, from The Atlantic: https://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/

Mahnaimi, U. &. (2007, Sep 23). Israelis seized Nuclear Material in Syrian Raid. *The Sunday Times*.

McQuade, S. C. (Ed.). (2009). Connecticut, London: Greenwood Press.

Nakashima, E. (2017, Dec 18). *U.S. declares North Korea carried out massive WannaCry cyberattack.* Retrieved Feb 18, 2020, from The Washington Post: https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html

Ottis, R. (2011). Theoretical Offensive Cyber Militia Models. *Proc. 6th International Conference on Information Warfare and Security (ICIW).* Washington, D.C., USA,.

Quillman, S. A. (2017). Aramco Attack. In P. J. Springer (Ed.), *Encyclopedia of Cyber Warfare.* Santa Barbara, CA: ABC-CLIO, LLC.

Rai, D. G. (2011, Nov 09). Information Assurance. CDM, Secunderabad.

Relia, C. S. (2015). *Cyber Warfare: Its Implications on National Security. .* New Delhi: Vij Books India Pvt Ltd.

Sambaluk, N. M. (2017). Operation Aurora. *Encyclopedia of Cyber Warfare*. (P. J. Springer, Ed.) Santa Barbara, CA: ABC-CLIO, LLC.

Schreier, F. (2015). On Cyberwarfare. *DCAF White paper*, 113.

Sigholm, C. J. (2016). Non-State Actors in Cyberspace Operations. Swedish National Defence College.

Stiennon, R. (2010). *Surviving Cyber War.* Lanham, MD: Government Institutes.

Stone, J. (2016, Sep 01). *Ghost Security Hackers, Offshoot Of 'Anonymous,' Claim They Disrupted ISIS Attack By Intercepting Twitter Messages*. Retrieved Feb 28, 2020, from International Bussiness Times: https://www.ibtimes.com/ghost-security-hackers-offshoot-anonymous-claim-they-disrupted-isis-attack-2077993

Venable, H. P. (2017). Operation Orchard. In P. J. Springer (Ed.), *Encyclopedia of Cyber Warfare.* Santa Barbara, CA.: ABC-CLIO, LLC.

Venable, H. P. (2017). Operation Orchard. In P. J. Springer (Ed.), *Encyclopedia of Cyber Warfare.* Santa Barbara, CA: ABC-CLIO, LLC.

Wadle, R. (2017). Sony Hack. In P. J. Springer (Ed.), *Encyclopedia of Cyber Warfare.* Santa Barbara, CA: ABC-CLIO, LLC.

Wortzel, L. M. (2010). China’s Approach to Cyber Operations: Implications for the United States. In E. M. Marvel, *China’s Cyberwarfare Capability* (pp. 90-91). New York: Nova Science Publishers.

Yolmo, Y. R. (2019, Dec 19). Retrieved Mar 20, 2020, from Analytics India Magazine: https://analyticsindiamag.com/cybersecurity-in-india/