A Military Planning Methodology for Conducting Cyber Attacks on Power Grid

Mehmet Saglam

Thesis submitted to the faculty of
the Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Computer Science and Applications

Bruce M. Lawlor, Co-chair
Ing-Ray Chen, Co-chair
Wenjing Lou

May 5th, 2014
Falls Church, Virginia

Key words: Cyber Warfare, Power Grid, Cyber Attack, Kinetic Attack

A Military Planning Methodology for Conducting Cyber Attacks on Power Grid

Mehmet Saglam

(ABSTRACT)

Power grids are regarded as significant military targets and have been targeted with kinetic attacks in previous military operations. These attacks resulted in significant levels of physical destruction, which, in the long-term, both undermined the success of the operations and caused severe adverse effects on the human terrain. Since power grids have grown as a result of introducing advanced technologies, they have also become more dependent upon cyberspace and are thus exposed to cyber attacks. Since cyber attacks have demonstrated the ability to creating physical/nonphysical effects with surgical precision, they have emerged as a credible option for disrupting power operations for a reasonable duration. However, these types of attacks sometimes require complex coordination with entities from distinct fields for efficient planning; a lack of awareness of the global picture about how to conduct these attacks could result in miscalculations and cause a repeat of the same past failures.

Motivated by this fact, this thesis holistically analyzes the steps involved in conducting cyber attacks on power grids for the purpose of gaining military superiority and provides a comparison for the capabilities, challenges, and opportunities of kinetic and cyber attacks. For the purpose of creating a comprehensive framework for this thesis, the following considerations have been incorporated: the analyses of goals, targets, solutions, and effects of previous military operations; the physical and cyber infrastructures of power grids; and the features, challenges, and opportunities of cyber attacks. To present the findings, this document has adopted a novel military methodology for both the cyber attack analysis and the comparison of the means.

Acknowledgements

I would like to take this opportunity to acknowledge the many people who played important roles for this thesis.

First and foremost, I would like to thank my thesis committee: Major General (Ret.) Bruce Lawlor, Dr. Ing-Ray Chen, and Dr. Wenjing Lou. MG Lawlor, your insight and knowledge in military science have enormously contributed my development, your advice and ideas have significantly shaped this document, hence my two years with your guidance have truly been memorable. Dr. Chen, your tolerance and faith in me enabled this research to be conducted. Dr. Lou, your instructions have helped me to find my course from the first semester of my study. I would like to express my gratitude for it has been great pleasure working with all of you.

I am also indebted to many of my colleagues and friends whose support I will not soon forget. Having this chance, I would like to appreciate the efforts of David Bisaillon for helping me to better express my research. I am also grateful to Dr. Tacettin Koprulu, Dr. Charles Clancy, and Celil Unuver for their invaluable comments, feedbacks, and advice. I would also like to thank TRN CDR Mahmut Arduc for his valued support which provided great opportunities for my research.

But, without a doubt, the greatest appreciation I have goes to my wife, Esra Sahin Saglam, who supported my academic endeavors, encouraged me during exhausting hours of studies, and kept me sane with her unconditional love.

The opinions and conclusions expressed herein are those of the graduate student author and do not necessarily represent the views of the Turkish Naval Forces Command. (References to this study should include the foregoing statement.)

.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AC	Alternating Current
AGC	Automatic Generation Control
AMI	Advance Metering Infrastructure
AMR	Automatic Meter Reading
AP	Access point
ARP	Address Resolution Protocol
AVR	Automatic Voltage Regulator
BDA	Battle Damage Assessment
C&C	Command and Control
C3	Command, Control, and Communications
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CERT	Computer Emergency Response Team
COTS	Commercial Off-The-Shelf
DAS	Data Acquisition Server
DER	Distributed Energy Resources
DMS	Distribution Management System
DNS	Domain Name Server
EMP	Electromagnetic Pulse
EMS	Energy Management System
FACTS	Flexible AC Transmission System Devices
GBU	Guided Bomb Unit
GC	Governor Control
HAN	Home Area Network
HMI	Human Machine Interface
HVDC	High Voltage Direct Current
IDS	Intrusion Detection System

IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
MAC	Media Access Control
NATO	North Atlantic Treaty Organization
NERC	North American Electric Reliability Corporation
NSA	National Security Agency
OAF	Operation Allied Force
ODF	Operation Desert Storm
OPORD	Operation orders
OSI	Open Systems Interconnection
PEV	Plug-in Electric Vehicle
PGC	Power Grid-Cyberspace Domain
PLC	Programmable Logic Controller
PMUs	Phasor Measurement Units
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SE	State Estimation
SQL	Structured Query Language
TLAM	Tomahawk Land Attack Missile
UN	United Nations
UNPROFOR	United Nations Protection Force
VARC	Volt-Ampere Reactive Compensation
VPN	Virtual Private Network
WAM	Wide Area Monitoring
WAN	Wide Area Network

Chapter 1

Introduction

1.1 Motivation

Power grids are regarded as significant targets in military operations. Operation Desert Storm (Iraq – 1991) and Operation Allied Force (Yugoslavia – 1999) provide modern examples of national power grids being specifically and significantly attacked [76, 79]. These operations also demonstrated that destroying the power grid can cause long-term, adverse, unintended consequences on the civilian population. In addition and not only from a humanitarian perspective, but destruction of a power grid can also create negative effects on the success of the operation by causing blowback effects on human terrain [81, 89]. Recently, national critical infrastructures have become more interdependent, with the electric power grid taking center stage [22]. As technologies have matured, power grids have continued to evolve, improving reliability, increasing the quality of power, and reducing costs. As a result, the efficiency of the power operations has improved, yet at the same time, the grid become more complex and fragile. For these reasons, the criticality of a power grid as a target has increased from military perspective, but unfortunately the harmful effects of creating long term disturbances on civilians have also increased.

The evolution of the power grid has also introduced advanced control and communication technologies to the electrical infrastructures. Hence, power grids have become more dependent upon cyberspace and, therefore, more exposed to cyber attacks. Meanwhile, it has been demonstrated that cyber attacks are capable of creating both physical and non-physical effects on their target systems with surgical precision. Therefore, to improve efficiency of military operations and reduce collateral damage on civilians, cyber attacks have emerged as a viable option for disrupting power operations. Unfortunately, this is still a growth industry to military planners and systematic steps for conducting these types of attacks to achieve military superiority, as well as the distinct capabilities, challenges and opportunities offered by cyber-warfare have not been well documented. This paper discusses how to conduct these types of attacks on power grids in the context of a novel military methodology, and analyzes the features of these attacks with a comparison with kinetic attacks.

1.2 Background

The area of this research spreads around three fields: military science, power engineering, and computer science. In addition, it addresses an audience of political/military decision makers, technical persons that conduct cyber attacks, and scholars. This diverse target audience creates its own challenges in devising a sound approach to the study of this matter. Therefore, the research itself provides the required fundamental knowledge. This section will present some brief and additional background information related to historical relevance of power grids in previous military operations, cyber attacks in military operations, and the cyber attacks against cyber-physical systems.

1.2.1 A Target of Military Operations: Power Grid

1.2.1.1 Operation Desert Storm (Iraq - 1991)

Operation Desert Storm was waged by U.S.-led coalition forces against Iraq in response to the Iraqi invasion and annexation of Kuwait. The war was conducted between January 17th and February 28th in 1991. The coalition forces specifically and significantly targeted the Iraqi national power grid. One of the clearly identified target sets attacked from the onset of hostilities in the opening days of the operation were "electric power generation, transmission, and control facilities" [79]. Several targets were hit multiple times [83] with a combination of unguided general purpose bombs, laser guided bombs, and/or Tomahawk missiles. Eventually, eleven of 20 major power plants were destroyed, an additional six were heavily damaged, and nine of 28 transmission substations were destroyed [83]. As combat operations unfolded, 92% of power grid's serving capacity was destroyed causing a massive blackout in Iraq [93].

1.2.1.2 Operation Deliberate Force (Bosnia - 1993)

Operation Deliberate Force was NATO's first extended air operation in coordination with the United Nations Protection Force (UNPROFOR). It was directed against Yugoslavia to undermine military capabilities of the Bosnian Serb Army, since they had threatened and attacked UN-designated safe areas in Bosnia and Herzegovina during the Bosnian War. The operation was conducted between August 30th and September 19th in 1993. Military decision makers (i.e. Allied Air Forces Southern Europe - AIRSOUTH) [17] planned to target the power grid, yet neither the North Atlantic Council nor the UN Security Council could come to an agreement on the strategic cost-benefit analysis [90].

1.2.1.3 Operation Allied Force (Yugoslavia - 1999)

Operation Allied Force was NATO's first military operation without approval of the UN Security Council [32] and was directed against Yugoslavia in response to their military campaign of ethnic cleansing of Kosovar Albanians [33]. The operation was conducted between March 24th and June 10th in 1999. Political leaders of NATO could not unanimously consent to destroying the Yugoslavian power grid because of their concerns of the possible long-term effects on the civilian population. Instead, as a result, the option to use "Soft Bombs" [75] was approved. "Soft Bombs" were designed to cause short-circuits on power equipment and create temporary effects on the power grid. Eventually, and even though they took down 70% of the grid's capacity [80], these attacks were seen as inefficient because Yugoslavian restoration efforts were able to restore power within hours. Later, NATO political leaders approved a conventional weapons attack on the grid due to its criticality [76]. Several power plants and transmission substations were hit and destruction impacted over 80% of the power grid's serving capacity [80].

1.2.1.4 Operation Iraqi Freedom (Iraq - 2003)

Operation Iraqi Freedom was waged by a U.S.-led coalition forces against Iraq in order to depose the Ba'athist government of Saddam Hussein. Combat operations began March 19th and concluded on May 1st, 2003, when Baghdad, the capital city of Iraq was captured by coalition forces. Since the operation aimed to unseat the government and would require a full-scale invasion to do so, every attempt was made to minimize damage to the civilian infrastructure. On March 21st, despite these intentions, the Basra high voltage power line was destroyed. Moreover, on April 3rd, the Al-Doura power plant was damaged and Baghdad was plunged into blackout conditions while coalition forces were capturing Saddam International Airport. The Iraqi government blamed coalition forces for sabotaging the power plant and urged people to use their private generators to light up the city; despite these claims, U.S. military officials insisted that coalition forces did not knowingly bomb any significant part of Iraq's power grid [91].

1.2.1.5 Operation Odyssey Dawn (Libya - 2011)

Operation Odyssey Dawn was initially a U.S.-led operation with command later transferred to NATO authorities. It was directed against military forces in Libya loyal to Colonel Qaddafi to enforce UN Security Council Resolution 1973 [44] which demanded "an immediate ceasefire" and authorized forces "to take all necessary measures to protect civilians." The operation began on March 19th, 2011, was conveyed under NATO command as Operation Unified Protector on March 31st, and finally ended on October 31st, 2011. The power grid was not

specifically targeted in the first place; however, allied military leaders suggested NATO "to be freed restraints that have precluded attacking infrastructure targets" such as power grid [45] on May 15th. Although this was not approved, nevertheless, several areas in the country were blacked out by both local Qaddafi and anti-Qaddafi factions in order to gain military superiority [92].

1.2.2 Cyber Attacks in Military Operations

This section presents some applications of cyber attacks from previous military operations which may or may not have been conducted by personal under military commands.

In *Operation Allied Force*, the U.S. forces utilized cyber attacks to distort the images of air traffic controller displays in order to deceive the Yugoslavian air defense systems. This attack was "essential to the high performance of the air campaign" [87].

In *Operation Iraqi Freedom*, cyber attacks were planned against Iraqi financial systems [57] to effectively shut off Saddam Hussein's cash flow and were responsible for freezing billions of dollars during the initial phases of the war [87]. However, these actions had not been approved by the U.S. administration, due to interconnectivity of global financial system which could create collateral damage if attacked.

In *the South Ossetia War* (Georgia - 2008), the Georgia administration was exposed to cyber attacks mainly aimed to create chaos. Attacks were directed to the internet infrastructure in addition to websites of government and news agencies in an effort to prevent dissemination of information [3]. As a result, several web-based public services were halted due to the excessive levels of traffic. For instance, the National Bank of Georgia ordered all banks to stop conducting electronic services between August 9th and 18th [9].

In days leading up to *Operation Odyssey Dawn*, the U.S. government debated launching a cyber attack on Libya's air defense system. Eventually, that course of action was rejected since demonstration of such an attack could unveil the capabilities of them and might encourage other nations to acquire these capabilities [47].

1.2.3 Cyber Attacks on Cyber-Physical Systems

Cyber attacks can create harmful effects on physical infrastructures by targeting cyber-physical systems which are integrations of computation, networking, and physical processes. This section presents the capabilities of cyber attacks on cyber-physical systems by referring: sample

attacks and demonstrations, intelligence gathering efforts, and the intentions and allegations related to cyber attacks on power grids.

1.2.3.1 Sample attacks and demonstrations

Studying previous military campaigns, research demonstrations, and security exercises can help expose the effects of cyber attacks on cyber-physical systems. Some relevant examples are listed below:

In June 1997, an information operations exercise, named "Eligible Receiver," was conducted to see what coordinated cyber attacks could do to U.S. military functions in the Pacific Theater. The exercise was conducted in cooperation with the U.S. Department of Defense, National Security Agency, and Federal Bureau of Investigation. The exercise targets of the red teams included unclassified military computer systems, 911 emergency systems, and the U.S. national power grid. Red teams used common hacker tools that were available online. The results were classified, yet one year later Deputy Secretary of Defense John Hamre, stated that "We didn't really let them take down the power system in the country, but we made them prove that they knew how to do it." [43].

Within a two month period, commencing in February 2000, a former employee of Hunter Watertech, a SCADA equipment vendor in Australia, conducted cyber attacks on at least 46 occasions targeting the Maroochy Shire Sewage Treatment Facility in Queensland. He had installed radio equipment and a computer in his car and drove around the facility while issuing malicious radio commands to the sewage equipment. As a result, 800,000 liters of raw sewage spilled out into local parks and rivers [12].

In January 2003, the Slammer worm penetrated Ohio's Davis-Besse nuclear power plant [13]. The worm used a circuitous route to enter the plant network, first penetrating an unsecured network of a Davis-Besse contractor, then passing to the corporate network of the plant through a firewall by using a "trusted" connection. Once inside the corporate network, the worm found an unpatched Windows server for the MS-SQL vulnerability. The patch had been released by Microsoft six months prior, but had yet to be installed by plant personnel. By using the server, Slammer spread to the plant network and created congestion in both the corporate and plant networks. As a result was a crash of the Safety Parameter Display System, which monitors the most critical safety parameters at a nuclear power plant such as coolant systems, core temperature sensors, and radiation sensors. One hour later, the Plant Process Computer also crashed. It took four hours and six hours to restore these systems, respectively. Fortunately, the incident did not

pose a safety hazard, since the plant had been offline for eleven months due to an unrelated repair.

In March 2007, researchers conducted an experiment, dubbed "Aurora," to demonstrate the effects of exploiting a specific vulnerability in a power plant control system [117] at the U.S. Department of Energy's Idaho National Laboratory. They launched cyber attacks to exploit the vulnerability in order to take control of the power generator. Then, malicious code was injected by researchers which caused the generator to misbehave, shake, smoke, and stop, which was all captured on a video monitor recording the event. The demonstration had implications that the self-destruction of a generator could likely be implemented the huge power generators as a framework and that coordinated attacks could cause widespread damage on a power grid.

In June 2010, the Stuxnet worm was discovered by security experts. The goal of the worm was to create destructive effects on specific industrial systems by manipulating the operations of programmable logic controllers (PLC) in the target system. Stuxnet used several methods to penetrate the target network [16]. Stolen real security clearances were used, instead of forged ones which are common for attacks, to circumvent security mechanisms. USB flash drives were utilized to infiltrate isolated networks. A total of four unpatched vulnerabilities were exploited in order to get the required privileges in the target system. The worm then stayed dormant until reaching its specific target which was a particular model of PLC made by Siemens. When Stuxnet reached the target, it altered the PLC's operational code. At the same time, it monitored the accesses to the PLC in order to conceal its injections. The altered code caused the PLCs to misbehave in a way that damaged the centrifuges in the uranium enrichment lab at the Natanz nuclear facility in Iran [123]. Furthermore, the worm also hid the created effects from the operators. Several reports alleged about the damage that Stuxnet was believed to have created. The most detailed report came from the Institute for Science and International Security, a private group in Washington, D.C., that indicated nearly one-fifth of Iran's nuclear centrifuges were damaged. The damage from Stuxnet was not admitted to by Iranian officials in the first place, yet in November 2010, the Iranian president, Mahmoud Ahmadinejad made a statement about the impact of Stuxnet on the Iraqi enrichment program as "They succeeded in creating problems for a limited number of our centrifuges with the software they had installed in electronic parts." [49].

1.2.3.2 Intelligence gathering efforts

Cyber attacks are utilized to gather information about targeted organizations. The targets could vary including embassies, research institutions, private companies, and energy, oil and gas industries. These attacks can use several methods which are becoming more and more advanced

to penetrate their "classified" targets, acquire information, and wipe clean their traces. To show the capabilities of intelligence campaigns, the main features of recent malwares are presented below:

Duqu, discovered in October 2011, is an intelligence gathering malware that target entities such as industrial infrastructures and system manufacturers in order to conduct future attacks that may create physical effects on its targets [40]. The structure of it is nearly identical to the Stuxnet worm. Duqu uses specifically targeted emails with an attached Microsoft Word document that contains an exploit to install itself. It also uses a valid stolen digital certificate to evade from defensive mechanisms. After the infection, instead of self-replication, Duqu receives orders for consecutive targets from its command and control (C&C) server [41]. The designers of the malware are specifically looking for information that can be used to launch future destructive attacks such as design documents, operational specifications, etc. However, the tools to gather this type of information are modular and hence different malicious packages are used for different requirements (e.g. an info-stealer that can record keystrokes, etc.). Duqu automatically removes itself from the target system after 30 days by default, but it also configured to remove itself if no communication can be established with the C&C server to prevent possible discovery [40].

Flame, discovered in May 2012, is a complete attack toolkit that is more complex than Duqu and designed for general intelligence gathering purposes [55]. The features of it are similar to the Stuxnet and Duqu worms. Unlike Stuxnet and Duqu, Flame's process for intruding the target network has not been determined. It spreads slowly via USB flash drives and over local area networks, using known exploits to infect its targets. Furthermore, it also uses bluetooth to collect information and propagate by turning on the infected machines bluetooth as a beacon [56]. The information that the malware looks for is not specified, but included emails, documents, messages, etc. To collect these types of information, Flame captures screenshots, records conversations via internal microphone, sniffs the network traffic, and intercepts keystrokes. The key to Flame's complexity is its completeness, in other words, its ability to steal data in numerous ways [56]. Although the malware do not have a suicide timer, its handlers are able to send a removal module which completely wipes itself and every single trace of it from the target system [55].

The Mask, discovered in February 2014, is an intelligence gathering malware which is more sophisticated than Duqu with a purpose of gathering sensitive data from the infected systems [96]. Its target set includes government institutions, embassies, energy, oil and gas industries, research institutions and so on. Infection of the malware relies on targeted emails with

links to malicious websites which contains a number of exploits for infecting the victim [58]. Upon infection, the victim is redirected to a benign website which could be a YouTube movie or a news portal without noticing the attack [96]. Furthermore, the malware uses a legitimate certificate from an unknown or fake company to minimize the chance of detection. The creators of the Mask, specifically aim to collect encryption keys, virtual private network (VPN) configurations, and several other types of encryption keys. For this sake, the Mask utilizes its extremely modular design rather than using one big program [58] to intercept network traffic, Skype conversations, and keystrokes; to analyze Wi-Fi traffic; and to capture screenshots, etc.

1.2.3.3 Intentions and allegations related to cyber attacks on power grids

Attribution of cyber attacks is a difficult problem to solve due to anonymity and obscurity features of cyberspace. Even though the attacks may be attributed correctly, though highly unlikely, they provide deniability to the attacker for the same reasons. Furthermore, as seen in the examples above, the advanced cyber attacks use sophisticated techniques to conceal their effects and traces. Hence, determining the cause of a power blackout, whether it is a device fault or a cyber attack, may not be possible. Therefore, credibility of real world cyber attack examples on power grids and the intentions of nation states tend to remain as allegations only; though some nations will declare their intentions publicly.

The 2003 North East blackout in U.S. and Canada that affected nearly 50 million people and 9300-square-miles was officially attributed to various factors. Prominently, "overgrown trees" were denoted as the trigger factor for the cascading effects that caused more than 100 power plants to shut down. During the blackout, the communications of the utility companies responsible to manage the power grid was disrupted by a computer virus, further exacerbating the problem [1]. None of the reported factors attributed to the power failure included foreign intervention; however, experts in cyber security and intelligence areas claimed, with confidence, that China's People Liberation Army had gained access to a power grid control network serving the northeastern U.S. which played a role in the power outage [111].

In January 2005 and September 2007, two power blackouts occurred in Rio de Janeiro and Espirito Santo-Brazil, respectively. The first affected three cities and tens of thousands of people; the second blacked out three million people for a two-day period in dozens of cities. After these incidents, official reports attributed the causes to several non-cyber factors, yet the allegations to the contrary still surfaced [113]. Eventually, in May 2009, U.S. President Barack Obama stated, "We know that cyber intruders have probed our electrical grid, and that in other countries, cyber attacks have plunged entire cities into darkness." He did not indicate any specific

country at the time; however, intelligence sources reconcile this statement with these Brazilian blackouts [110]. Interestingly, two days after President Obama's statement, Brazil experienced the worst blackout in over a decade, leaving more than 60 million people in darkness. The Brazilian government quickly denied the cyber attack allegations, and blamed the weather conditions for causing the outages. But, Brazil's National Space Research Institute quickly responded to this by stating "the weather during the outage was not capable of producing this kind of disruption" [113].

In June 2013, the Obama administration revealed the existence of a classified U.S. Cybersecurity Framework (Presidential Policy Directive 20 [104]) which was issued in October 2012, and included the principles and processes related to defensive and offensive cyber attacks. The document stated that targets of these attacks could include "physical or virtual infrastructure controlled by computers or information systems," hence power grids would be considered a typical target. The document also discussed the effects of cyber attacks, and indicated them as "ranging from subtle to severely damaging." Additionally, the directive signified the importance of gathering intelligence about those targeted networks by mentioning the required accesses and tools for executing an attack and directly stated, "the U.S. Government shall make all reasonable efforts…to identify the adversary and the ownership and geographic locations of the targets and related infrastructure where defensive and offensive cyber effects operations will be conducted" [104].

In the final analysis, power grids are still regarded as significant targets in military operations; cyber attacks have been utilized in previous military operations to fulfill operational needs; and the effects of cyber attacks on cyber-physical systems including power grids, recent intelligence campaigns, and public and alleged intentions of nation states demonstrate that as a part of military operation cyber attacks could be conducted on power grids to gain military superiority.

1.3 Research Objective

Cyber attacks can be conducted on power grids to gain military superiority as explained above. However, these types of attacks require interdisciplinary efforts from military science, power engineering, and computer science fields. For the sake of efficiency and operability, the entities from these distinct fields must have fundamental knowledge about the other fields; otherwise, the planned operations might cause harmful unintended consequences. For instance,

during Operation Desert Storm (Iraq – 1991), the President of the U.S. left most of the fighting decisions to the military leaders [79]. One of the consequences of these decisions was that the destruction inflicted on civilian infrastructure reached unforeseen levels and further contributed to the destabilization of Iraq. Therefore, the effects of the operation beyond the military domain caused blowback effects on human terrain [89]. There was another example of the lack of coordination between the operation planners and executors [79] in the same military operation. In order to better manage the restoration time of the power grid, the weaponeers and military planners intended to target the transformer facilities adjacent to the power plants; however, the pilots were unaware of that particular consideration and when their bombing runs destroyed the generator facilities instead, it caused unnecessary harm on civilian infrastructures by making the restoration time longer. This point highlights that the entities involved in either the planning or execution phases of a military operation must have fundamental knowledge about the other fields. In addition, researchers would also need awareness of the global picture when conducting these types of operations to be able to study efficiently in their specific fields.

Additionally, political and military decision makers would need policy guidelines which include knowledge about the capabilities, challenges, and opportunities of cyber attacks regarding their specific targets (e.g. power grids), and a comparison of kinetic and cyber means to be able to choose the right attack options for military operations under consideration.

This research aims to fulfill these requirements; hence, the objectives of this research are to analyze how cyber attacks can be conducted on power grids in the context of a military methodology; and to compare the capabilities, challenges and opportunities of cyber and kinetic means for attacking power grids.

1.4 Contributions

Cyber attacks are emerging options for disrupting power grids [22, 45, 104], but they have not been fully implemented in military operations yet. Features, capabilities, and the options of cyber attacks [2, 4, 5, 21, 28], and effects of previous military operations [76, 79, 17] have been specifically studied before; however, they have not addressed the needs of military operations nor have they included power grid oriented assessments, respectively. Furthermore, previous researches quantitatively analyzed attacker behaviors [124, 125], domain-based security models [129], and specific types of attacks on different set of control systems such as integrity attacks on Automatic Generation Control [52, 126], State Estimation [127], and Energy

Management Systems [114, 115]. However, comprehensive qualitative approaches that could determine conducting cyber attacks on power grids from a wider perspective have not been followed by researchers. In addition, utilizing cyber attacks will introduce new challenges and opportunities that are unique from those related to kinetic attacks. Military planners and researchers need a global picture of conducting kinetic or cyber attacks on power grids for efficient plans and studies. Therefore, meticulous, holistic, and area-specific researches are required to help analyze cyber attacks on power grids from a military perspective.

This research comprehensively and qualitatively clarifies the steps for conducting cyber attacks on a power grid; discusses the factors to improve the efficiency of the operation; and compares capabilities, challenges, and opportunities of kinetic and cyber means. For this sake, it first introduces a novel 7-step military planning methodology, and then provides analyses of cyber attacks for each step of the methodology to include: goals, systems analysis, targets, intelligence, options, execution, and lessons learned. Lastly, this research uses the same methodology to compare the conduct of kinetic and cyber attacks on power grids.

1.5 Outline

The remainder of the research is organized as follows. Chapter 2 introduces a novel 7-step military methodology for analyzing attack type-target pairs. It also describes how to conduct cyber attacks on a power grid in a step-by-step fashion as part of military operation. In addition, it briefly discusses the factors that affect the efficiency of the operation in each step. Chapter 3 analyzes the capabilities, challenges, and opportunities of both kinetic and cyber attacks, by providing a comparison of these means in the context of the proposed methodology. Finally, Chapter 4 provides concluding remarks and presents several topics as extensions for future work.

Chapter 2

The Methodology: Cyber Attacks on Power Grid

A seven-step military planning methodology was created to analyze the feasibility of cyber attacks against a power grid. The seven steps, as depicted in figure 1, consist of goals, system analysis, targets, intelligence, options, execution, and lessons learned. This methodology incorporates the analyses of previous relevant military combat operations; power grids; and the tools, techniques, and procedures of cyber attacks.

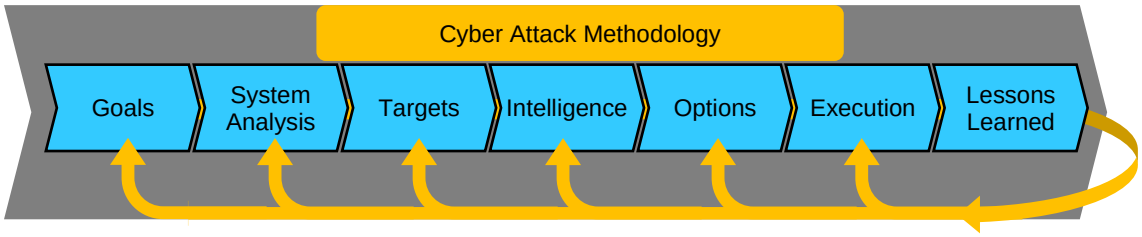

Figure 1: The Steps of Cyber Attack Methodology on Power Grids

A concise overview of the contents of each step is described as follows. The *Goals* step analyzes the goals and results of previous relevant military operations regarding the disruption-destruction tradeoff. It also assesses the potential benefits of conducting attacks on power grid as part of a military operation. The *System Analysis* step analyzes power grids by first looking at legacy systems. Then, it examines the evolution of the grid, the Smart Grid concept, and cyber security and dependency issues. The *Targets* step briefly discusses the target set of Operation Desert Storm (ODS) and Operation Allied Force (OAF). Then it compiles and prioritizes potential target sets of power grids and discusses the critical factors for effective targeting. The *Intelligence* step evaluates the required types of information, the sources of them, and the tools and methods to gather them for producing usable intelligence. In addition, it discusses the methods for finding system vulnerabilities and the factors that affect efficiency of information gathering efforts. The *Options* step analyzes cyber attack options on the grid and their consequences, and discusses sample attack patterns of these options. The *Execution* step identifies the access points of a target network and analyzes the methods for overcoming defensive mechanisms in order to clarify conducting operation in cyberspace. It then discusses the operational factors that affect the success rate of a cyber attack. Finally, the *Lessons Learned* step

evaluates the methodology from a wider perspective to provide feedback to each respective step. Additional details pertaining to each step is provided in the following pages.

2.1 Goals

Power grids are regarded as legitimate targets in military operations, as long as the disruption mainly affects military facilities, according to the International Committee of the Red Cross [75]. However, as power distribution grids continue to evolve in most countries, they are increasingly becoming heavily integrated systems. As a result, it may not be possible to shut down the power of military facilities without creating significant adverse consequences for large parts of the civilian population. Therefore, the Yugoslavian power grid was in the target set during *Operation Deliberate Force* in 1993 [17], yet was not attacked since neither North Atlantic Council nor the UN Security Council could come to an agreement on the strategic cost-benefit analysis [90]. Additionally, the national power grid of Iraq was not targeted during *Operation Iraqi Freedom* (2003) and evidence shows that the grid operated almost properly until the siege of the capital city, Baghdad [91]. Most recently, coalition forces elected not to target the Libyan power grid during *Operation Odyssey Dawn* (Libya – 2011); the power grid was, however, attacked by both local Qaddafi and anti-Qaddafi factions to gain military superiority in some cases [92].

It is practically impossible to specifically shut down only the military-related aspects of a nation's power distribution system; nonetheless, *Operation Desert Storm* (Iraq – 1991) [79] and *Operation Allied Force* (Yugoslavia – 1999) [76] provide modern examples of national power grids being specifically and significantly targeted by military operations. This section will more closely analyze the goals of these two military operations to better understand potential goals and objectives that could be achieved by attacking power grids.

The goals of the Operation Desert Storm were; to incapacitate, discredit, and isolate the Saddam Hussein regime; to eliminate Iraqi offensive/defensive capability and make military reconstitution long-term and difficult to achieve; to create conditions leading to Iraqi withdrawal from Kuwait; to sever supplies and command; and to destroy the Iraqi army in Kuwait [77]. A National Security Directive [78] was signed on January 15th, 1991, and the aerial bombardment started two days later. A White House spokesman indicated that the necessary precautions would be taken to reduce collateral damage and to minimize civilian casualties [78]. However, as combat operations unfolded, 92% of power grid's serving capacity was destroyed causing a

massive blackout in Iraq [93]. This was mainly the result of Col. John A. Warden's Five Rings Strategy [86] which aimed to attack the enemy's five centers of gravity of leadership, key production, infrastructure, population, and fielded military forces in order to physically paralyze it. By extension, according to post-war analyses [76, 79], the reasons of targeting the national power grid in this operation could be listed as; to incite rebellion against the Hussein regime especially in the majority Shi'ite south; to impose long-term problems on the Iraqi leadership by forcing them to cooperate with the West in order to restore its electricity; to amplify the economic and psychological impact of international sanctions; to create psychological effects on Iraqi citizens; and to reinforce other strategic goals such as weakening air defenses and military communications. However, even though attacks on power grid related targets were largely executed successfully and the lights of Baghdad did go off, as well as most of the central and southern Iraq, were extinguished, the coalition attacks did not succeed in weakening citizens' support for the regime [79].

The goals of Operation Allied Force were defined as; immediate termination of violence and repressive activities by the Milosevic government; withdrawal of Yugoslavian forces from Kosovo; stationing UN peacekeeping forces in Kosovo; safe return for all refugees; and the establishment of a political framework agreement for Kosovo [76]. The operation started in March 24th, 1999 and lasted for 78 days. From the outset, the military targets such as Yugoslavian air defense and command and control systems were attacked up to the 44th parallel. After April 23rd, NATO escalated the attacks, pushing north of the 44th parallel and forcing Milosevic forces to withdraw from Kosovo. These expanded attacks targeted major infrastructures, including the power grid [76]. In the hopes of preventing serious long-term consequences, the power grid was first attacked on May 3rd utilizing BLU-114/B "Soft Bombs" (a special-purpose munition for attacking electrical power infrastructure, detailed information in section 2.5). The announced intent was to disrupt military communications and confuse the air defense units of Yugoslavian 3rd Army in Kosovo [80]. These initial attacks took down 70% of the grid's capacity, but only for a short period of time [80]. During the final two weeks of Operation Allied Force, power plants and transmission substations were subsequently targeted and hit by conventional bombs. Despite the Pentagon's declaration that indicated only 35% of the power generation capacity had been destroyed [94], when the cumulative effects of the attacked transmission substations were combined the actual level of destruction impacted over 80% of the power grid's serving capacity [80]. According to the post-war analysis [76], the reasons behind these attacks on the power grid were: to adversely impact the Yugoslavian communication and military supply capability; to tighten the operation's squeeze on the political leadership of the Milosevic government and break

its will to fight; to prevent the distribution of petroleum, oil and other lubricants; and to stress power supplies for critical assets such as communication systems, air defenses, transportation, TV and radio broadcast.

As we more closely analyze these two operations, it becomes obvious that the aim was indeed to achieve legitimate military and political goals, but the decisions and the actions taken had resulted in long term civilian infrastructure destruction as collateral damage and created severe effects on human terrain [88] which has to be determined with air, sea, land and cyberspace. These effects on the human terrain can quickly bring into question the validity of the success of the military operation. Therefore, the **tradeoff** between the long term effects of ***destruction*** of the power grid and the short term effects of its ***disruption*** become an ever-growing concern.

Operation Desert Storm symbolized the ***destruction*** side of the tradeoff. Most of the attacks on the Iraqi power grid mounted in the opening days of the operation. Overall, 215 sorties were carried out using a combination of unguided bombs, laser guided bombs, or Tomahawk missiles [79]. Eleven of 20 major power plants were destroyed, with 6 more heavily damaged and at least 9 of 28 transmission substations damaged which required foreign assistance to repair [83]. Between the 6^{th} and 7^{th} day after the outset of the operation, the Iraqis shut down the entire power grid to prevent additional damage. These actions significantly weakened air defenses and interrupted military communications, since the emergency backup generators of the Iraqi military were neither powerful nor reliable enough to compensate the power loss [79]. It also had the effect of plunging the civilian population into darkness to creating psychological effects on the population.

In contrast to the strategists' goals, the shutdown of the power grid did not incite rebellion against the government by the Iraqi citizens [79], but it did trigger many long term problems for them. According to research [81] conducted two months after the conclusion of combat operations, Iraq had regained only 23% of its prewar electricity output and this had come at the expense of cannibalizing other power plants or substations. The impact was widespread. Due to lack of electricity [81-83], most of the water treatment facilities could not operate to providing potable water. Sewage treatment operations were also interrupted and resulted in raw sewage being discharged into the Tigris River for weeks. The sewage treatment capacity of Baghdad had only been restored to 50% when the assessment [81] was conducted. The drinking water of southern Iraq became severely contaminated and water-borne diseases such as cholera, gastro-enteritis, and typhoid reached to epidemic levels as a result. Healthcare services were

restricted due to lack of electricity, required logistics, refrigeration, and hygienic conditions, leading to a further increase in the spread of several infectious diseases. Food preserving and distribution operations halted. Child mortality rates increased nearly fourfold compared to prewar levels. The broad scale in the level of power loss was significant and had a harsh impact on businesses and industries. These facts further contributed to the destabilization of Iraq for the long-term which in turn amplified the negative effects of them. In addition to humanitarian and economic concerns, these facts, henceforth, fortified anti-western stream in the country [89], where inciting rebellion against the government was an intended objective [78] in the first place.

In this military operation, the President of the U.S. left most of the fighting decisions to the military leaders [79]. As a consequence of some of their decisions, and due to the interconnectedness of military and civilian infrastructures, the impact of war upon civilians reached unforeseen levels. However, as previously indicated, the White House had fully intended the military to take necessary precautions for reducing collateral damage and minimizing civilian causalities [78]. When viewed in that specific light, the operation may not be viewed as successful, primarily due to miscalculation of the effects that are beyond the military domain. This highlights the growing need for political decision makers to be involved in defining goals and target sets. In summary, since military operations may have significant long term political, economic, humanitarian, and military effects as witnessed in Operation Desert Storm, military leaders should not be solely responsible for defining goals and target sets, without political leaders' oversight and approval.

Conversely, leaving approval of target sets to political leaders also must be balanced since it also hosts some drawbacks. In *Operation Allied Force*, NATO's civilian leaders had sole responsibility to determine the targets and they did not approve destruction of the Yugoslavian power grid until the final two weeks of the operation. The constraints on military decision makers [75] led to the use of Soft Bombs for targeting the power grid; which, though it avoided creating severe humanitarian conditions at first, caused only short-term blackouts in the country and had little military benefit. Additionally, the slow target generation and approval process of civilian leaders also hindered the military's ability to fight effectively [76]. Yugoslavian forces were able to respond to the allied actions with rapid regeneration and reconstitution efforts. As a result, by the end of the first month, nearly 80% of the strikes conducted were revisiting targets which had been attacked at least once previously. Additionally, some militarily vital targets (e.g. command bunkers) could not be attacked until obtaining the civilian decision makers' approval [76], a process which typically took longer than a month. As a result, since the effects from attacking a

power grid extends beyond military-related areas, the responsibility to conduct such attacks should not rest solely with the military decision makers. With this in mind, it is also important that the decision-making mechanism must be created wisely to prevent delays which would reduce the efficiency of the operation.

On ***disruption*** side of the tradeoff, two particular cases stand as examples, *Operation Allied Force* and *the 2003 Northeast Blackout*. In these two cases, power grid operations were disrupted temporarily which created short term power outages in broad areas.

In *Operation Allied Force*, NATO's civilian leaders, particularly French President Jacques Chirac, were against destroying the Yugoslavian power grid [76]. Soft Bombs were used to cause widespread power outage while not destroying the physical infrastructure. Soft Bombs had been tested previously in Iraq (1991). They short-circuited transformers and switching equipment on the ground without physically destroying them. On May 3rd, 1999, the first soft bomb attack blacked out 70% of the country; however, the effects of it were cleaned up within 15 hours by Yugoslavian efforts [75]. In this period, NATO planners believed they achieved their goal without any destruction, but it was short-lived. When the target was attacked for a second time using the same soft bomb technology, it took only four hours to restore energy since the personnel had experience to draw upon and the response time decreased [75]. The enemy's ability to make adjustments and quickly repair the power grid rendered the Soft Bombs an ineffective weapon to create wide area blackouts for a reasonable time frame.

The *2003 Northeast Blackout* (detailed information in section 2.2.4.2) caused a significant power outage for large parts of the area including the northeast U.S. and eastern Canada. The blackout lasted two days in some areas and impacted over 50 million people. This created a significant impact on national critical infrastructures, resembling effects that could be expected by a military attack in a war or prewar scenario.

The event affected transportation, communications, energy, financial services, and emergency services in some ways [1]. From a military operation planning perspective, it may hinder C4ISR, logistics, and mobilization efforts. In addition, it could create psychological effects on civilians by paralyzing the country, right before or during a war. However, since this power outage took two days to fully restore, the benefits of it would likely be limited from attacker's perspective. The Northeast Blackout case demonstrates that this time frame may be insufficient to widely hamper the operations of the public telephone network which form the backbone of several types of communications. This relatively brief duration of power outage may not be

enough to significantly hinder military operations, but at least the impact to the civilian population would be short-lived as well.

As shown above, there exists a tradeoff between destruction and disruption of power grid. Destruction may provide significant military benefits in the short term, but its long term effects for civilians create suffering conditions which makes the political success of the operation questionable. Conversely, while disruption causes less damage on civilian infrastructures, the short term power outage may not yield a sufficient advantage to support military operations. At this point, cyber attacks could play a balancing role for this tradeoff by causing required period of power outage and reducing the collateral damage on power grid.

Analyses of the previous military operations' goals and consequences by considering the destruction-disruption tradeoff would present **the need for a new and novel strategy** for attacking the power grid in military operations. This need could be fulfilled by utilizing **cyber attacks** against these targets. These types of attacks could help by achieving a broader variety of goals than their conventional counterparts.

Disrupting the power grid for a reasonable period of time, or destroying key nodes within the grid would also likely interrupt the lines of supply, paralyze communications, disturb mobilization efforts, and degrade C4ISR efforts. It also increases the importance of night combat superiority which could be utilized if the attacker does not have the same capabilities. Since confusion and uncertainty would increase in a war time blackout scenario, it would certainly make defending more complex, especially for air defenses. Additionally, the enemy's offensive military capability would be hampered without proper defenses and with a lack of information. Putting the enemy into darkness could also create a significant impact on its psychology. Depending upon the severity of the blackout, it could also break the adversary's will to fight and encourage defection of the enemy forces. By combining the aforementioned objectives, widespread power outages would tighten the operation's squeeze on both the enemy's military and political leadership.

Furthermore, inherent features of cyber attacks could be utilized to be able to achieve additional goals. Since physical distances are irrelevant in cyberspace, cyber attacks can be conducted to an enemy anywhere in the world without risk of losing assets. Cyber attacks also can be conducted as a precursor to coordinated combat operations to create the conditions that plunges the enemy government into chaos. The first critical point in this case is the attribution problem of cyber attacks. The second is the penetration possibility of cyber attacks through defenses. Lastly, military operations create psychological effects on civilians which could result

with dissolving or uniting them against the attacker. If the critical line between these two behaviors can be determined, then well-planned cyber attacks could maximize the efficiency of the operation, due to their both destruction and disruption capabilities.

In the final analysis, power grids are legitimate targets for military operations. The goals related to power grid could vary. Yet the created effects depend on the tradeoff between the destruction and disruption of the power grid. Destruction of the grid may provide benefits for short term but creates severe consequences for long term. Contrarily, disruption may not cause severe effects for civilians but it also may not support military operations sufficiently due to its short term effects. Cyber attacks could balance this tradeoff. Conducting cyber attacks on a power grid may allow specific targeting of key nodes in the grid. This could prevent the unnecessary destruction of other non-critical grid assets and better manage the temporal impact caused by power outages. Furthermore, cyber attacks can also fulfill additional objectives comparing to conventional means due to their inherent features.

2.2 System Analysis

A power grid is an interconnected network for delivering electricity from suppliers to consumers. The network topology and its elements have been changing based on needs and technological developments [28] since its birth over a century ago. Currently, the power industry aims to adapt its infrastructures to reflect the concept of "Smart Grid" which uses advancements in several areas; such as telecommunications, automation, monitoring, artificial intelligence, and distributed power generation to improve efficiency and increase reliability of the electricity supply. Using sophisticated information technology in the power grid has introduced the vulnerabilities of these technologies into the grid and exposed it to cyber attacks. The grid's vulnerability has also increased drastically because of the highly interdependent nature of a nation's critical infrastructures. Not only theoretical research but also latest power blackout experiences demonstrate that the power grid is one of the most important critical infrastructures for a nation. This section analyzes legacy power systems, evolution of the smart grid concept, security related issues, and dependency on the power grid.

2.2.1 Legacy Power Systems

Legacy power systems mainly consist of three parts: generation, transmission, and distribution of electricity.

2.2.1.1 Power generation

Power plants house generating units to produce electric power by converting primary energy from a variety of sources; such as, fossil fuel, solar, nuclear, hydro and wind power.

Power generation units are also divided into three sub categories: base load, intermediate, and peaking units [10]. Base load units meet steady demand by operating throughout the year except during hours of repair and maintenance, hence they have to be economical and reliable (e.g. nuclear, coal, and hydroelectric plants). Intermediate units (e.g. combined-cycle gas turbine plants and older thermal generating units) operate for long hours to meet changing demand by altering their output easily. Peaking units (e.g. gas turbines and hydroelectric plants with reservoirs) must be able to start and stop instantly since they operate when the demand reaches its peak.

2.2.1.2 Power transmission

Transmission systems carry electricity for long distances by linking generation and distribution units. The transmission network consists of substations and power lines which are often attached to high towers. Other times they are buried underground, for example, in densely populated areas.

Substations house transformers, measurement instrumentation, switchgear, and communication equipment. Transformers alter voltages from higher to lower levels before they are put into the distribution network. The voltages altered by the substations could vary from region to region or country to country ranging from 50kV up to 1.000kV [10]. Measurement instrumentation records data related to voltage, current and other power characteristics for monitoring and control reasons. Switchgear consists of circuit breakers and other types of switches to connect/disconnect the system to the entire network in case of maintenance or emergency. Communication equipment transmits the states of switchgear and the data recorded by the measurement instrumentation to a control center, and receives commands from the control center to manage the substation.

Transmission lines carry the power to a lower voltage level transmission substation or, at the end, to a distribution substation. However, the power that can be carried on a line is limited by either voltage stability, thermal or transient stability constraints. The form of carried power is normally three-phase alternating current (AC) but it can also be high voltage direct current (HVDC).

2.2.1.3 Power distribution

Distribution networks consist of distribution substations, transformers, and transmission lines. They carry power from transmission networks to customers. Generally, parts of the power grid that carry up to 35kV are considered a part of distribution network.

Distribution substations connect transmission and distribution networks. The transformers housed in the substations step voltage down to primary distribution levels. The management of the process could be monitored and controlled by monitoring equipment and circuit breakers. Yet the level of automation is lower than transmission substations [10].

Distribution networks have a radial topology, or "Star network," that supports a single connection between the substation and the customer. To increase reliability, ring or loop topology could be used which uses an alternative route to the customer in case of accident or maintenance [28]. In highly populated areas, mesh distribution networks offer alternative routes from substations to customers which increase their reliability but also makes them more complex.

The power that comes through distribution substations and goes to the customer must be stepped down to secondary distribution level [10] by transformers that generally are mounted on a pole or buried next to the customers' locations.

The three parts of Legacy Power System behave as one complex body that is synchronized inter and intra sections as a whole. To manage and control this ever built largest machine [1] necessitates extensive measurement, communication and control systems [48]. The necessary control systems in power plants are inherently built into the system itself. Monitoring and control systems in transmission networks have also been updated for over the last few decades. However, most distribution networks have not been upgraded with high-tech modernizations efforts since they are typically considered as user end-points of service.

2.2.2 Evolution of the Grid

The current challenges and benefits of the power industry have led to the evolution of power grid. Although the reasons and motives behind the evolution may vary from country to country, they can be grouped in three classes as: security and quality of supply, internal market, and environment. To meet the requirements of these constraints, authorities took respective steps in several areas. First, transmission networks started to use new equipment and technologies to improve efficiency, reliability, and security. Second, distribution networks, which have typically utilized advance technologies the least, have met with intelligent two-way communication systems. Third, distributed energy generation technologies have been developed to balance the

negative effects of bulk power generation systems. In addition to the steps taken in the three main parts of the system, the advancements are aimed at integrating service providers, energy market data, and customers into the system to make the power grid more harmonized, efficient, and smart.

2.2.2.1 The reasons behind the evolution

Several reasons have evolved to make implementing new technologies to the power grid inevitable. Though they may depend on a nation state's or an international entity's priorities, they can be grouped under three classes, those of: security and quality of supply, internal market, and environment as depicted in figure 2.

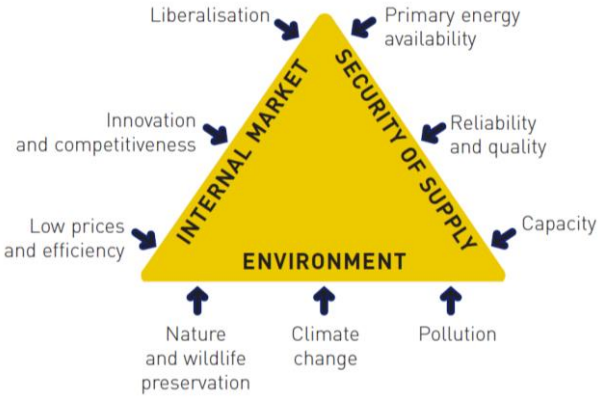

Figure 2: The Reasons of the Evolution, European Smart Grid Technology Platform, "Vision and strategy for Europe's electricity networks of the future," European Commission Community Research Report [Online], EUR 22040, 2006. Available: ftp://ftp.cordis.europa.eu/pub/fp7/energy/docs/smartgrids_en.pdf, Used under fair use, 2014.

The security and quality of supply is critical since more than two-thirds of bulk power generation is dependent upon the fossil fuel industry which brings several of its own constraints regarding production, transportation, security, etc. Therefore, reducing the criticality of primary energy availability makes implementing distributed energy generation technologies more important. Moreover, the more highly developed countries need a more reliable and high quality power supply to securely operate their highly energy dependent infrastructures and use technological tools which are more fragile to voltage oscillations. Additionally, the existing capacity and new infrastructure investments for power grid may not be able to meet the increasing demand thus making it more important to improve the existing capacity of the grid [5]. Since security and quality of supply are growing in importance, implementation of smart

technologies to reduce primary energy dependency, improve reliability and quality of power, and increase the capacity is inevitable.

Internal market is another area that fuels the evolution of grid. The growing deregulation of state or privately owned monopole structure of power grids in many countries [73] gives the control of power generation, transmission, and distribution to different entities by dividing into several regions for each part. Since, the power grid behaves as a synchronized complex body, it is becoming harder to manage it without implementing new technologies [28]. Furthermore, innovation and competitiveness in the market after deregulation continues to incorporate new technologies [34] to shave the peak demand, to address electric vehicle charging issue, to integrate smart appliances to the network, etc. In addition, market prices are being driven down as a result of increased competition between power suppliers, forcing suppliers to improve their efficiency [69] by offering alternative power use of plans to customers [34], increasing electricity trade between regions, etc. The effects of internal market that drives the evolution also necessitates new communication technologies that can help power grid management involving hundreds of entities in some countries, to be able to serve to new technologies, and trends.

Environmental concerns are also an important aspect that drives the evolution. Governments and non-governmental organizations have adopted initiatives to preserve nature and wildlife by increasing the use of renewable resources [34]. These entities are also encouraging and/or forcing power suppliers to use less carbon emissive resources [68] in order to reduce environmental pollution and minimize the impact on climate change. Utilizing more renewable or carbon-free resources to address environmental concerns necessitates implementing new technologies that can provide monitoring and control infrastructure and also provide reliable and sustainable energy supply.

The reasons for the power grid's evolution originate from the basic tenets of securing and improving quality of supply, internal market and environmental concerns and are driving power grids to a more efficient, reliable, clean and hence to a more smart state. Nearly every country has taken some of the necessary steps to make their power grids smarter according to their priorities.

2.2.2.2 The steps of the evolution

The major efforts to make power grids more efficient and more reliable have been focused on transmission system. To this end, power system stabilizers, phase shifting transformers, flexible AC transmission system (FACTS) devices, and phasor measurement units

(PMUs) installed on transmission networks [70]. In addition, the advent of real time controls and control room visualizations significantly improved the power grid's efficiency.

However, since recent efforts for improving efficiency focused on the transmission network, distribution systems have fallen behind them [70]. As a result, the rate of power outages and disturbances related to the distribution network has reached 90% [69]. Automatic meter reading (AMR) systems were attractive when first introduced. But the industry soon realized that they could not solve the demand side management problem [34], since the AMRs use one-way communication to inform power suppliers and do not let utilities take corrective actions [69]. This led to the introduction of the advanced metering infrastructure (AMI) which enabled two-way communications between customers and suppliers.

Meanwhile, deregulations and internationalizations of the power market started and increased the number of entities in generation, transmission, and distribution areas [60]. As a result, the need for communication between field devices and various controllers required the addition of common protocols and software [22] instead of older proprietary ones. Open communication protocols further decreased the cost of communication and integration. These communication protocols utilized power lines and leased telephone lines at first, but eventually began using wireless, satellite, internet protocol (IP), and wireless mesh networks due to bandwidth requirements and other benefits [19].

The power generation side has also affected by the evolutionary progress. Deregulations in the power market and advancements in using renewable resources have enabled suppliers to use transmission networks to utilize several alternative sources from long distances away [7]. In other words, customers could use electricity from whichever power plant operates at the cheapest price. In short, with reduced costs and an increased number of possible sources, efficiency is improved.

Even though the first steps for evolution were taken at the transmission networks, they have since spread to distribution and generation domains and in doing so, have increased the efficiency and reliability by making the grid smarter.

2.2.2.3 The overall situation

Every country aims at keeping up with the trends to improve efficiency and reliability in their power grid, but the steps taken in this direction have risen dramatically since 2006 [72].

The evolution has spread all over the world yet 80% of the investments will have been focused on only 10 countries until 2030 [71]. The U.S. will dominate the market over the next

two years and is already projected to spend nearly $60 billion on an intelligent smart grid infrastructure until 2030. By 2016, China is projected to take the lead with a planned investment of $99 billion by 2030. Emerging markets also aim to improve power grid efficiency. India and Brazil currently claim the third and sixth spots in smart grid investments respectively. France, Germany, Spain, and the United Kingdom play leading roles in European Union and will share the biggest part of research and development efforts to make the EU's power grid smarter. Japan and South Korea also round out the top 10 list due to their great ambition in improving their power grid.

In short, more or less every country aims to improve their power grid's efficiency and reliability by making them smarter. But even though the U.S. and Chinese markets seem to have a strong financial foundation, they still have a long way to reach the conceptual Smart Grid framework.

2.2.3 The Concept "Smart Grid"

The will and the means of countries to improve the efficiency and reliability of their nations' power grids have put them in a place where most of them have incorporated some type of intelligent control equipment in their grids [10]. However, in order to achieve the full advantages the conceptual smart grid will require more work even for the countries which already have modernized grids.

2.2.3.1 The ultimate picture of Smart Grid

The Smart Grid is defined by the North American Electric Reliability Corporation (NERC) as "the integration of real-time monitoring, advanced sensing, and communications, utilizing analytics and control, enabling the dynamic flow of both energy and information to accommodate existing and new forms of supply, delivery, and use in a secure and reliable electric power system, from generation source to end-user." [2]. In other words, Smart Grid requires real-time control and process, two-way communication infrastructures, and intelligent tools to harmonize bulk power generation, transmission, distribution, operations, market, customers, and service providers [53]. To help visualize it, a conceptual reference diagram for smart grid information networks is provided in figure 3 and a short explanation of its sub-domains is provided below. In addition, more detailed information related to the logical reference model of conceptual framework can be found in [23].

In *Bulk Generation* power is generated by using fossil, nuclear, and/or renewable resources. This domain also stores electricity to be able to manage the diversity of renewable

resources [53]. Bulk generation domain is linked to the transmission domain to transfer electricity. It also linked to market and operations domains over wide area networks. It includes electrical equipment, including remote terminal units (RTUs), programmable logic controllers (PLCs), fault detectors, and equipment monitors.

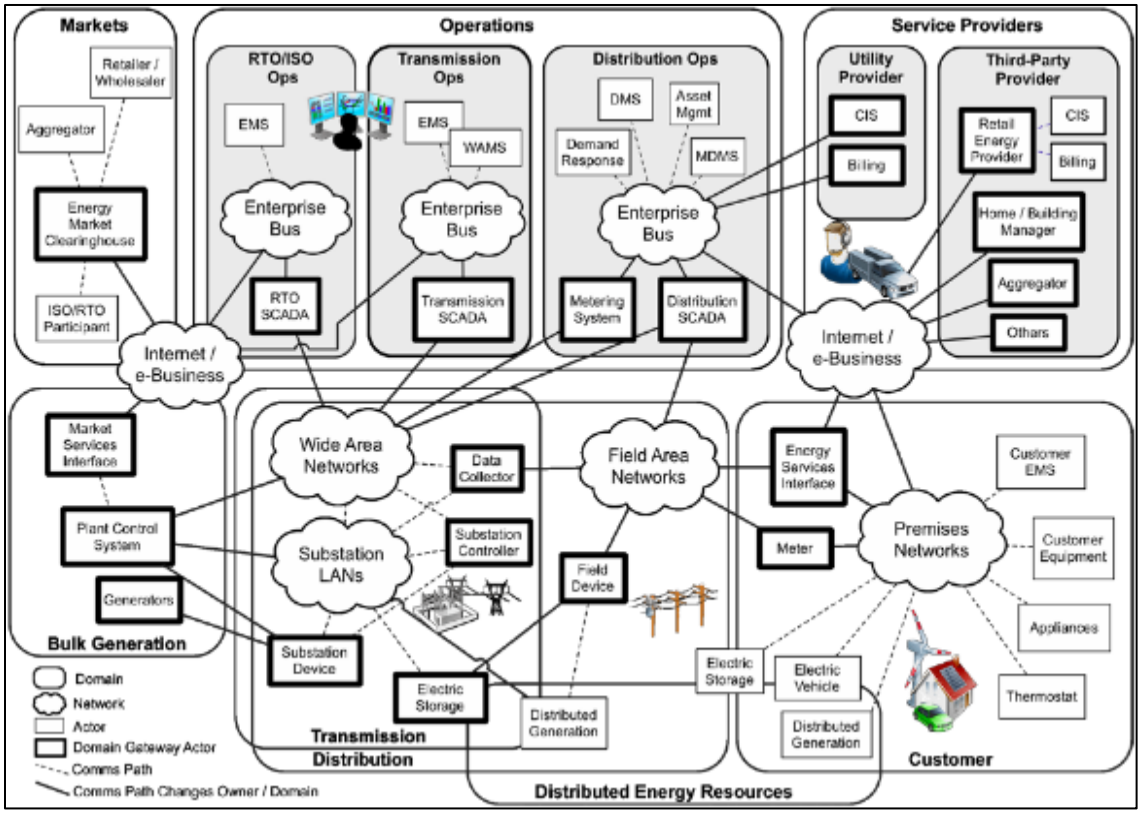

Figure 3: Conceptual Reference Diagram for Smart Grid Information Networks, Office of the National Coordinator for Smart Grid Interoperability Engineering Laboratory Staff, "NIST framework and roadmap for smart grid interoperability standards," NIST Special Publication [Online], 1108R2, Release 2.0, Feb. 2012. Available: http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_20_corr.pdf, Used under fair use, 2014.

Transmission domain transfers electricity from its generation source and distributes it over multiple substations and transmission lines. Transmission is generally managed by regional transmission organizations or independent system operators. Their responsibility is to manage transmission by balancing the demand and supply. This domain also supports small scale power generation and storage. Additionally, much of the information captured from the transmission network is sent to the control center and used to help achieve self-healing functions and increase

wide area situational awareness and control. Generally, sensors and actuators provide remote control in substations [34].

Distribution domain connects the transmission domain and customers by delivering electricity. Its electrical and communication infrastructure includes and supports feeders, transformers, distributed energy resources (DERs), AMI, plug-in electric vehicles (PEVs), and sensors with two-way communication capability. The distribution domain is also connected to operations and customer domains over field area networks. Sensors and actuators provide remote control in substations [34].

Operations domain organizes the distribution, transmission and generation domains in an efficient and optimal manner by using Energy Management System (EMS) for transmission domain; Distribution Management System (DMS) for distribution domain; and Automatic Generation Control (AGC) for generation domain. It also uses field area networks, wide area networks (WAN), and the Internet to obtain and relay control information. These information domains are obtained by using supervisory control and data acquisition (SCADA) systems. They manage activities such as monitoring, control, fault management, maintenance, analysis and metering [53]. The operations domain may be further divided into sub-domains which could be controlled by different organizations.

Market domain maintains the balance between supply and demand of electricity. It consists of retailers who supply power to customers, traders who buy electricity from suppliers and sell it to retailers, suppliers of bulk electricity, and aggregators who combine smaller DER resources for sale. This domain communicates with the operations and generation domains over the Internet or an intranet.

Customers expand, store, or generate (by DERs) electricity. This domain consists of home, commercial or industrial buildings. It communicates with the distribution, operations, service provider and market domains. A two-way communications interface between the customer's premise and the distribution domain is required to enable active participation in grid operations by the customer. A communication network within the customer's premise is required to enable the exchange of data and control commands between the supplier of the electricity and the intelligent customer appliances. This network, referred as a home area network (HAN), is expected to support applications such as remote load control, DER monitoring and control, reading of non-energy meters, and the integration with building management systems [53].

Service providers bring electricity to both customers and utilities. This domain manages services such as billing and customer account management for utility companies by communicating with the operations domain to get metering information as well as for situational awareness and system control. This domain must also communicate with HANs to provide smart services such as management of energy use and home energy generation.

2.2.3.2 Network architecture and control systems of Smart Grid

Smart grids use several networks to communicate with intelligent subsystems and domains to support expected functionalities. Since the communication infrastructure connects a great number of devices, it is constructed in a hierarchical architecture and each network takes responsibility of different geographical regions. In general, network architecture can be grouped under three classes: wide area, field area, and home area networks. These networks have distinct features and requirements for their integrity, availability, and confidentiality [53].

Wide area networks (WAN) [53] are the communication backbone of smart grid which connects highly distributed smaller area networks exist at different locations. The main role of the WAN is to provide communication between substations and control centers. In substations, real-time measurements are taken by RTUs/PLCs and sent to control centers, and in turn, the respective control commands are sent to the substations through the WAN.

Field area networks [53] are utilized by power system applications operating within the distribution domain to share and exchange information. These applications include, but are not restricted to, electrical sensors on distribution feeders and transformers, DERs in the distribution systems, RTU and PLC devices capable of carrying out control signals from DMS, PEV charging stations, and smart meters at the customer site.

Home area networks [53] provide infrastructure in the customer domain to implement monitoring and control of smart devices in customer premises. Home area networks have a role in providing new functionalities such as demand response and advanced metering infrastructure. Home area networks use an energy services interface, a secure two-way communication interface between the utility and the customer and enables smart appliances to be managed in an energy efficient manner by responding to pricing signals from the utility company.

The control systems in smart grid can be grouped under one of three classes: generation, transmission, or distribution [42].

Control systems in the generation domain [42] involve controlling the generator power output and the terminal voltage in the system.

Automatic Voltage Regulator (AVR) is used to improve power system stability by controlling the amount of reactive power absorbed or injected into the system. Digital control equipment enables the testing of algorithms for system stability improvement. This system generally uses Modbus communication protocols and operates on local area network of the plant control center.

Governor Control (GC) is the mechanism to control the primary frequency. This mechanism uses sensors to detect changes in speed that accompany disturbances. By doing this, it alters settings for changing power output from the generator. This system generally uses Modbus communication protocols and operates on local area network of the plant control center.

Automatic Generation Control (AGC) is the control mechanism that provides inter-area frequency equity. AGC correlates frequency deviation and net tie-line flow measurements to determine the error, which is sent to generating station to adjust operations. This mechanism uses a WAN for its operation.

Control systems in the transmission domain [42] uses switching and support devices to ensure that the power flowing through the lines is within safe operating margins and the correct voltage is maintained.

State Estimation (SE) uses field devices to estimate system variables such as phase angle and voltage magnitude to presume faulty measurements. This mechanism assists in making operational decisions by performing computations on the data which come through the WAN from thousands of sensors.

Volt-Ampere Reactive Compensation (VARC) controls reactive power in the transmission domain to improve its efficiency. This mechanism is designed to minimize voltage fluctuations and has the potential to help avoid blackout situations. In general, FACTS control devices are used for this mechanism which communicate each other and function autonomously [27].

Wide area monitoring (WAM) systems assist in decision making at the control center by using PMU based systems that measure phase angles of voltage phasor [10]. This mechanism uses global positioning system to accurately timestamp the measurements and uses WAN for its real-time operations.

Control systems in the distribution domain [42] enable direct control of the load at the end user level by the utility company.

Load Shedding provides active, proactive, and manual control for the distribution network to operate at safe levels. This mechanism uses remote controlled relays and load shedding schemes to shed a load when the need cannot be supported by the utility company and can prevent possible cascading blackouts of the grid.

AMI and Demand Side Management aims to incorporate renewable energy, increase reliability, and provide granular consumption monitoring to customers. The efficiency of AMI depends on the employment of smart meters and appliances into the customer premise. This mechanism enables utilities to implement load control switching to disable the consumer's smart devices when demand spikes.

2.2.3.3 Power grid EMS and SCADA systems

In most cases, the control systems for the power generation and transmission phases are managed via hierarchically structured control centers within the operations domain. These control centers are responsible for conducting power delivery and take into consideration the system's efficiency, reliability and security. Energy management systems encompass the SCADA systems for monitoring and controlling vast and widely dispersed operations and form the foundation of the control centers as illustrated in figure 4.

Control center communications can be categorized as one of three classes: the communication inside the center, communications within the SCADA operations, or communication with other outside links. The communication inside the control center uses a local area network to provide connectivity of various subsystems such as the SCADA system, AGC, load forecasting, etc. SCADA operations, on the other hand, utilize a WAN, leased telephone lines, and satellite communication, etc. to provide communication between the SCADA server and various field devices. Control centers also have outside links between other control centers, software or hardware vendors, and corporate networks which typically use WAN and leased telephone lines.

Energy Management Systems (EMS) analyzes real-time measurements gathered by the SCADA system to provide reliable operation within the generation and transmission domains. The roles of EMS include alerting operators to any vulnerability resulting in possible contingencies and calculating possible operational changes to improve the operational conditions [22]. Typically, EMSs have communication connections used to exchange data describing the

real-time conditions of neighboring grids. To provide secure and reliable operation, EMS requires strong data integrity and availability [20].

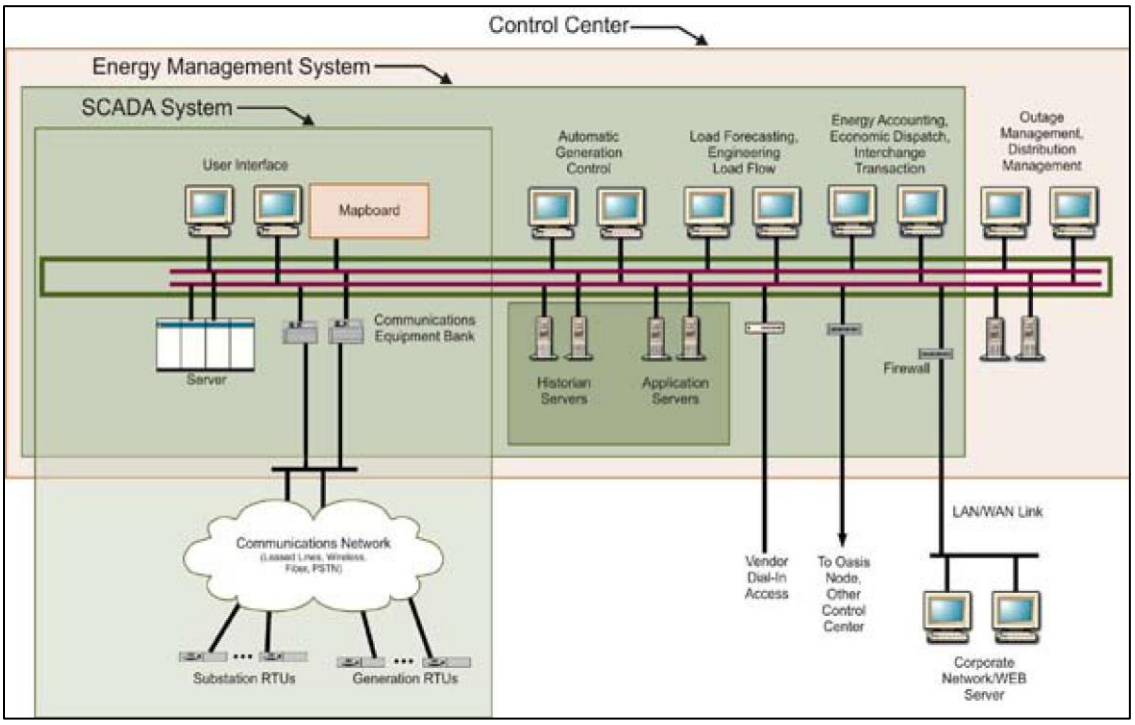

Figure 4: Typical Control Center Configuration for Power Grid, Control System Roadmap Steering Group, "Roadmap to secure control systems in the energy sector," Energetics Inc. Report [Online], Columbia, MD, Jan. 2006. Available: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/roadmap.pdf, Used under fair use, 2014.

Supervisory Control and Data Acquisition (SCADA) systems works with EMS to provide three critical functions: supervisory control, data acquisition, and alarm display [19]. The SCADA system consists of computers and display units connected via various communication systems to remote terminal units that are placed at substations to collect data and perform control of intelligent devices. SCADA systems poll RTUs to gather real-time measurements from all substations periodically and send out control signals to the substations to execute specific orders [7]. These orders may include, but are not limited to, opening and closing of circuit breakers, adjusting control set points for transformer taps, generation of power plant outputs and voltage levels, and direct current transmission line flows [22].

Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) are special purpose microprocessor-based devices that are resident in remote areas to monitor and/or control electrical equipment [7]. They are capable of converting analog signals to digital or vice versa,

and can provide communication between control system and field devices [22] such as sensors, actuators, controllers, pulse generators, etc.

The efficiency and reliability of power grid operations depend mainly on the effective management of control centers utilizing EMS for advanced calculations and control. SCADA systems play the role of data collection for EMS calculations and sends control signals to the field devices. In the field, RTUs and PLCs execute the orders that come through various networks.

2.2.4 Cyber Security and Dependency

As legacy power systems all over the world continue to evolve they are, in effect, becoming smarter. However, even though smarter systems make the power grids more efficient and reliable in terms of operations, they also become more vulnerable from a cybersecurity perspective. National critical infrastructures are increasingly becoming more interdependent, especially in relation to power grid, financial services, information technology, and telecommunications [7]. Therefore, the ever-growing importance of cybersecurity and its impact on power grid issues is not something that should be overlooked.

2.2.4.1 Cyber security of the "Smart Grid"

Smarter power grids offer more efficient and reliable operations but they also introduce more cyber vulnerabilities [2] into the system and hence make the power grid more open to cyber attacks.

Many power grid control systems in use today were designed primarily with an eye towards operability and reliability. Security issues were not as great a concern when many of the legacy systems were designed because they typically operated in isolated environments and generally relied on proprietary software, hardware and communication protocols [60] which made them hard to know and hard to reach. Moreover, industrial control systems are designed to have a 20-year lifecycle, whereas the lifecycle for business information technology is only 3 to 5 years and shrinking. It is not a stretch to say that the legacy systems in use today were built for a specific purpose and generally has neither extra capacity nor enough performance to be able to deal with today's security mechanisms.

System integration is another issue that makes smarter grids more vulnerable. Initially, there were three discrete domains: substation, control center, and corporate networks [59]. Substation networks managed control equipment in the field. Control center networks issued commands for their execution in substations. Corporate networks used the data manually, or with disks related to other two domains. For the sake of efficiency, these domains have evolved to

become more connected and integrated. This enabled corporate networks to access control data on the field even through firewalls between domains. On the other hand, it also opened the way to field control systems through corporate networks making them more vulnerable [60].

In addition to the way proprietary corporate networks access their control systems, the geographically dispersed nature of substations and field devices make using IP networks or the Internet an efficient mean to manage communications. Research [8] shows that more than 75% of SCADA related devices are "connected to internet" and 47% of them have "unresolved security issues." The need for utility maintenance personnel to remotely connect, troubleshoot, or repair field devices likely creates an alternative access [38] for intruders.

The complexity of power grids and integrated networks make securing them harder than ever and by extension more vulnerable. Deregulations and the internationalization of power grids have created a huge network and dramatically increased the number of devices, entities, and possible connections. This has also affected the hardware domain, making management of this vast and complex network even more challenging, especially in case of emergency. These factors are why more people and broader areas have become victims of power blackouts recently [66] and why the power utilities' cyber security specialists may not be able secure the system comprehensively.

Smarter power grid applications promise improved efficiency and reliability by monitoring and controlling more nodes in real-time. This necessitates the need for more intelligent devices (RTUs, PLCs) and, in turn, a greater integration of communications, both which could make the grid more vulnerable. Increasing the number of intelligent devices in the system and then integrating all different types of them together have two negative effects. First, it increases the number of possible access points from an intruder's point of view, thus more points to defend. Second, the integration of different types of devices requires the commercial off-the-shelf (COTS) software or open communication protocols [34] instead of proprietary ones which have previously contributed system security. Hence, using COTS software and open protocols make power grid more vulnerable.

Another way that using COTS software and open protocols make power grid more vulnerable is due to the information availability of smarter grids. Older power grids used proprietary software and protocols which often provided "security through obscurity" for the system [19]. Yet, since smarter grids increasingly utilize COTS software and open protocols, and utility companies often host their products' information on their websites; it is becoming easier to collect enough data to conduct an effective cyber attack on power grid [60]. Additionally, since

numerous professional hackers are already familiar with those software programs and protocols, a large number of tools to attack power grid control systems are already available online.

As evidenced, smarter power grids introduce new vulnerabilities to the system. Since all power grids are becoming smarter, the level of vulnerability may depend on the level of smart applications implemented and the security provided. In summary, old control devices, system integration, unsecure internet connections, the complexity of the power grid, COTS software and open protocols, and information availability related to the system are but a few of reasons for increased vulnerability. These reasons further undermine the cyber security of power grids and therefore make them susceptible to cyber attacks.

2.2.4.2 Power grid dependency of critical infrastructures

Critical infrastructures are defined comparably by various countries worldwide. In brief, they include those systems, whether physical or virtual, whose destruction or disruption would create a significant risk to a country's national security, economic safety, or public health. The U.S. government identified 16 total sectors as critical infrastructures in Presidential Policy Directive 21, with financial services, information technology sector, telecommunications, and power grid cited as the four most critical assets [7]. Interdependency analyses [22] further indicate that electric power takes center stage in identifying interdependencies. Traffic lights, airport operations, manufacturing, medical services, logistic services, and banks are some additional examples of sectors and services dependent upon the power grid. Real world incidents also prove the criticality of power grid, as witnessed in the 2003 Northeast Blackout in the U.S. and Canada [1].

The blackout started shortly after 2pm EDT on August 14, 2003 due a transmission line that went out of service in Columbus, Ohio as a result of a brush fire. This was followed by the failure of another transmission line after one hour. Later, a third line failed in the same area. These failures caused cascading effects on the grid until, by 4:10pm, the blackout covered an area including some parts of New York, Michigan, Ohio, Pennsylvania, New Jersey, Connecticut, Vermont, and Massachusetts in the U.S. and most of the province of Ontario in Canada. The blackout eventually impacted over 50 million people.

Power restoration efforts took almost two full days in many areas and had a devastating impact on several areas. Trying to calculate the sector-by-sector economic losses was extremely difficult to determine due to interconnected network of the modern economy and infrastructures, but the tangible effects of blackout could be listed. Airport operations were halted and forced to

close in Toronto, Newark, New York, Detroit, Cleveland, Montreal, Ottawa, Islip, Syracuse, Buffalo, Rochester, Erie, and Hamilton. Failure of emergency generators in hospitals affected the health care of patients dependent upon electrically-powered equipment, and resulted in the loss of critical materials due to lack of refrigeration. The legacy public telephone network generally remained functional, but the cellular phone system was rendered ineffective in some affected areas. Water supply systems failed for both lack of pressure and increased rate of bacteria. The rate of fires increased, raw sewage spread around cities, subways and rail networks were affected, the operation of eight oil refineries was paused, and banking operations were halted in some areas, to list but a few.

As evidenced by the details provided above, the dependency of critical infrastructures to the power grid clearly emerges in blackout cases and can have disastrous effects in many sectors. Again, this highlights the dependency of critical infrastructures upon the power grid, and the increasing cyber vulnerability the grid faces. These factors make this an important issue for both national security and military operations.

2.3 Targets

Targeting defined by the U.S. Air Force Targeting Doctrine as "the process for selecting and prioritizing targets and matching appropriate actions to those targets to create specific desired effects that achieve objectives, taking account of operational requirements and capabilities." [24]. It forms a critical link that binds the goals and tactical applications of a military operation. Hence, it is essential to properly identify the target set regarding to the commander's intent. Additionally, analyses of target systems crucially improve the efficiency of targeting process.

Historically, the meaning and the priorities of this process have changed over time [99]. Eventually, creating the intended effects became the critical objective and the process was relabeled as effects-based targeting. In effects-based targeting, destruction is considered as a means but not the end state itself. In other words, the aim of effects-based targeting is to compel enemy decision makers to respond in ways favorable to the attacker's overall campaign objectives, with the first- or second-order operational or strategic level effects created by any means. These effects could be listed as deceive, disrupt, degrade, deny, and destroy which all have several alternative means to get achieved.

In the case of a power grid as a target, there are several alternative methods or approaches for creating each effect mentioned above. Yet, civilian infrastructure dependency and fragility

makes targeting a power grid special. For instance, most of the power grid's nodes could be targeted, which targeted before [79], to destroy and hence create long term effects. This may fulfill numerous goals, but unfortunately it also causes prolonged suffering to the civilian population (detailed information in section 2.1). On the other hand, there are other methods to achieve the same goals. Disrupting or destroying well-analyzed, critical nodes in the network is likely to destabilize the network with effects propagating along the grid [28]. Thus, recovering electrical services would take a reasonable time period that would both fulfill the goals to support military operation as well as create tolerable effects on the civilian infrastructure. The carefully analyzed target set of this method not only reduces collateral damage, but also supports the legitimacy of the operation. Therefore, for the sake of efficiency, target prioritization and selection factors will be analyzed in this section. Yet, since the lessons learned from previous military operations could be significant, the targets and resultant effects of *Operation Desert Storm* and *Allied Force* will be analyzed first.

The target set of *Operation Desert Storm* was divided into 12 groups: leadership; command, control and communications (C3); air defense; airfields; nuclear, biological and chemical weapons; railroads and bridges; Scud missiles; conventional military production and storage facilities; oil; naval ports; Republican Guard Forces; and electricity [79]. Before the electricity target set was attacked, the Iraqi Power Grid included a mixture of thermal, hydro-electric, and gas turbine generating stations of which 20 main stations provided over 99% of total power for the nation. Almost 46% of the electrical generating capacity was as surplus for peak periods and other considerations. These power plants connected with a 132kV transmission network to transfer and reduce power for the distribution system. Overlaying this network, "the 400kV Supergrid" was connected north and south throughout the country via four transmission substations [83]. The Operation Orders (OPORD) of Operation Desert Storm reflected the planners' focus on an effects-based plan, but did not specify the precise level of physical damage to be inflicted on the grid or the other target sets. The target type pertaining to the grid was clearly identified as the "electric power generating, transmission, and control facilities" [79]. On Jan 17th, 1991, the first day of the war, at least 10 of the 20 main power plants were heavily bombed. Furthermore, 14 of 20 were hit multiple times, including many after they had ceased to be operational (e.g. Hartha Thermal Power Plant was hit 13 times, the last attack came 15 minutes before the cease fire) [83]. Eventually, 11 of the 20 main power plants were destroyed, with 6 additional power plants sustaining heavy damage. On the transmission network side, at least 9 of 28 substations (2 out of 9 were on the Supergrid) were successfully targeted [83]. Control facilities were also a desired target type as prescribed by the OPORD; unfortunately, which

control facility sites were targeted and their associated levels of destruction could not be determined by this research. In summary, three sets of targets were identified in the Operation Desert Storm OPORD regarding the Iraqi power grid. These targets were attacked and destroyed to varying degrees with conventional weapons which created long term effects.

In *Operation Allied Force*, fixed targets were divided into 11 groups: ground force facilities; command and control facilities; lines of communication; petroleum, oil, and lubricant related facilities; industry; airfields; border posts; electrical power facilities; counter-regime targets; air radars; and missile launch equipment [76]. The electrical power facilities of Yugoslavia were targeted in response to two different military objectives. The first objective was to create short-term effects on power grid. This was to be accomplished by using Soft Bombs to attack five transmission substations of the network located at Obrenovac, Nis, Bajina Basta, Drmno, and Novi Sad on May 3rd, 1999, the 41st day of the war. Targeting these facilities created temporary effects but in a wide area that covers 70% of the country [76]. Unfortunately, due to the insufficient effects of the first attack, the same targets needed to be re-attacked with the Soft Bombs once again. However, the effects of the second attack were remediated in a much shorter period of time by Yugoslavian forces. In light of the failure to achieve the first objective, the second objective of crippling Yugoslavian power generating capability and hence destroying the power plants was adopted. Starting on May 24th, NATO forces targeted the critical power plants in Belgrade, Novi Sad, Nis, and Kostalac with conventional weapons for three consecutive days causing significant damage [76]. The effects were more severe than the first attacks and blacked out 80% of the country which also created permanent consequences. In short, the Yugoslavian power grid had been targeted with two different objectives that both caused wide area blackouts. The first attacks created short-term effects, while the second attack resulted in serious long-term consequences.

As can be observed from these two particular military operations, there are several lessons learned to be considered. First, planning the effect, not the level of damage, was the priority. Second, the targeted nodes were in the generation, transmission, and operations domains. Third, destroying a large number of nodes in the network is likely to create long term suffering conditions for civilians and might not be necessary to achieve stated military objectives. Fourth, using conventional bombs to physically destroy targets is not the sole targeting solution (i.e. other means could be utilized as Soft bombs). Fifth, attacking transmission-only set of targets could cause wide area blackouts. Sixth, but not the last, the duration of the blackout must be sufficient to allow achievement of operational goals. Henceforth, the targeting process should consider

creating effects which should last a reasonable time period and also not induce civilians to suffer intolerably. Additionally, there is no need to attack a large number of nodes, since power utilities make contingency plans for single failure cases (N-1 rule) in which a major generating unit or transmission facility fails. Thus, they mostly plan their system to operate somewhere between N-1 and N-2 [22]. As such, an attack on a small, well-planned, targeted set of nodes, depending to the size of the network, could create a wide area blackout. This objective has typically been achieved by conventional means until now; however; cyber warfare tools present alternative methods. These methods could enable military planners to target cyberspace related assets in addition to conventional targets that were attacked before.

2.3.1 Target Set Prioritization

Individual or combined set of nodes in different domains could be targeted to create a wide area blackout with conventional or cyber weapons. Distribution, generation, and transmission domains remain potential targets.

The distribution domain has a greater number of components than other domains since they have lower capacities and service a smaller area. In some cases they have additional alternative substations and routes, especially in mesh networks [1]. Also, due to the requirement to be prepared to respond to daily incidents and emergency events (e.g. storms), utilities are better postured to rapidly fix distribution system components and typically have a greater supply of spare parts. For these reasons, targeting distribution networks is inefficient from a targeting perspective since the intended results would not meet time and space requirements of the intended blackout [22].

In the *generation* domain, power plants do not necessarily operate throughout the year. Some of plants are built to provide energy only for peak periods or to compensate for ones that are failed or under maintenance. Hence, if a country is not already suffering from a power shortage, there is typically plenty of surplus generating capacity within the power grids. The Iraqi power grid, for example, had an electrical surplus of almost 46% before the *Operation Desert Storm* [83]. Therefore, attacking a small set of power plants may not be an effective strategy, except if a country heavily relies on them.

Transmission substations continue to stand as effective targets in transmission domain for several reasons. First, they are scarce in number when compared other nodes in the grid. Second, they have become more highly stressed than before due to the power grid's evolution [22]. Third, most utilities do not own spares, and their replacement may require 20 months or longer to put in

place (including 6-12 months for delivery) because, among other factors, they are very large, difficult to move, and often custom-built [1]. Furthermore, the transmission substations are, in most cases, highly automated and do not host onsite personnel which increases the possibility of the cyber attacks' success, since monitoring and control functions could be easily misguided in highly automated systems.

In the final analysis, a set of targets chosen from the transmission domain would be the most effective. Secondly, a small set of power plants could stand as effective targets if a country heavily relied upon them. However, targeting the nodes of a distribution network would not be an effective strategy since they could not meet neither space nor time requirement of the intended blackout.

2.3.1.1 Control mechanisms as targets

Individual nodes of the power generation and transmission (i.e. power plants, transmission substations) can be identified as targets and attacked in offensive cyber operations similar to their conventional counterparts. Moreover, individual control mechanisms of power grids that monitor, supervise, and manage the overall systems could also be targeted uniquely in cyber operations. In the transmission domain, the criticality of the control systems depends on their involvement level in the grid, and they can be categorized as *State Estimation*, *Volt-Ampere Reactive Compensation*, and *Wide Area Monitoring* systems (detailed information in section 2.2.3.2). On the other hand, the power generation domain hosts an *Automatic Generation Control* mechanism that has authority on several plants and could be a viable target as well. Other control mechanisms in the power generation domain (e.g. *Automatic Voltage Regulator*, *Governor Control*) are also potential targets, but they only control individual plants so the attacks would just affect those individual targets instead of a set of nodes.

2.3.2 Critical Factors for Targeting

Deliberate targeting is essential for creating a wide area blackout for a desired duration. Since the power grid is a huge and complex network, there are several factors that must be considered for conducting efficient cyber attacks. These critical factors are presented in table 1.

The *Number of nodes* is the first factor that must be considered. Since the power grids have evolved for decades to become more reliable and efficient, numerous nodes must now be attacked to significantly disrupt its operation. From a defender's perspective, attacking several nodes may also prevent determining the origin of the attacks clearly, and hence delay taking

timely defensive actions [43]. However, the number of targeted nodes must be balanced to reduce long term effects on civilian infrastructures.

Number of nodes	Reaction of network
Connectivity of nodes	Restoration plans
Load level of nodes	Possibility of repair
Seasonal load variance	Generation node criticality

Table 1: Critical Factors for Targeting

Connectivity of nodes is critical when selecting specific nodes as targets; however, despite all available research [28], it is not always possible to determine the eventual effects of the attack by considering only the initial nodes connectivity. By increasing the number of subsequent neighborhoods to be analyzed, one can achieve more accurate results. In other words, it is better to analyze the highest *n*-th degree neighborhood relationship of the initial node, which then must be balanced with computational efficiency. Furthermore, the other sub-factors of connectivity must also be considered in that analysis [97, 98].

Load level of nodes must also be considered since they represent the tension on the network. The effects of attacking the highest-load-level-node or the lowest-load-level-node vary depending on the load distribution of the entire network [29]. Interestingly, in some cases, targeting the lowest-load-level creates the more severe consequences. Incorporating load levels of the entire network to targeting calculations would improve the efficiency of the process.

The *seasonal load variance* affects the network's load distribution by changing the power generating sources [11]. Some examples of this would be the increase of power generation from hydroelectric plants in fall and winter or the rising ratio of fossil fuels for generating power in the summer months. These changes affect the location of power generated, and hence the route that energy transfers through. Seasonal load variance impacts the stress over transmission network, and thus it stands as an important factor for the targeting process.

The *reaction of network* consists of the actions scripted in the contingency plans of the network. These plans may include various predetermined scenarios from which to recover in various emergency cases. For instance, a common initial reaction of the network is to disconnect the sub-regions of the grid which are self-sufficient, and redistributing the load in an effort to stop prevailing cascading effects [28]. Since it is important to foresee the opponent's moves after an attack, incorporating reaction of network to targeting process is a crucial consideration.

Restoration plans consider the actions taken after an attack has been conducted and power blacked out. Since achieving the desired blackout duration period is essential to achieving operational objectives, it is important to also consider the power grid's restoration plans. After a wide area blackout, nearly all the power plants would be shut down to protect themselves from electrical surges, thus black-start diesel-powered generators, which are capable of starting-up independent of the bulk power system, play a critical role in the restoration plans [22]. Hydroelectric plants, combustion turbine generators, and other power plants which uneconomically host black-start diesel generators could be used in this case. Therefore, targeting the connections of black-start diesel-powered generators must be considered in an effort to disrupt restoration plans and hinder rapid power grid recovery.

Another critical factor for identifying targets is the *possibility of repair*, since it affects the restoration efforts to recover the grid. Restoration success, and conversely the attack's success, depends on this factor. In fact, several sub-factors can also be identified such as the adversary's speed of supplying spare parts, the capability of repair, the target's physical proximity to the conventional battlefield, etc. Therefore, improving the success rate of the targeting process requires careful consideration of the node's possibility of repair.

Generation node criticality indicates the power grid's dependency to individual power plants. This factor must be particularly considered when the grid is dependent upon a few number of plants, in most cases, nuclear or hydroelectric ones [11]. In a case in which the benefit of targeting a power plant exceeds the threshold level that is the minimum value for achieving the objectives, then the plant or transmission substation that connects it to the grid could also be included in the target set.

The consideration factors for deliberately targeting the power grid in order to create wide area blackout for a desired time period are not strictly limited to the aforementioned factors, but for the respective reasons presented, these factors must be considered and incorporated into system network simulations to effectively select and prioritize the nodes upon which to conduct cyber attacks.

2.4 Intelligence

Intelligence discipline requires exploiting various information sources and thoroughly analyzing the results in order to support the commander's decisions and actions. The results of this process may be crucial to operation's success or failure. When conducting cyber attacks on a

power grid, research shows that the more information on the specific target system would make the attack more robust [28], more efficient [28], and harder to detect [46]. Hence nation states have started programs to produce intelligence on power grid either undercover [111] or publicly [104].

In general, intelligence efforts include data collection; information processing and exploitation; and analysis and production of intelligence, in chronological order [103]. Since the final step of this process has too much variation depending on the features of the specific target system and the commander's intent, for the purpose of discussion in this section, the first two steps will be analyzed by identifying the required types of information, the sources, and the ways to gather them for producing intelligence in order to conduct cyber attacks on power grid.

2.4.1 Required Types of Information and their Sources

The required information for an efficient attack shall be sought in the Power Grid - Cyberspace (PGC) Domain (figure 5) consisting of (1) Physical, (2) Logic, (3) Cyber Persona, and (4) Physical Persona Layers. Each layer generally hosts specific types of structures and information on it, but it is also possible to reach corresponding information as a result of the links between the layers. Hence, layer-specific and multi-layer information gathering efforts must be done in order to produce the most detailed and efficient intelligence.

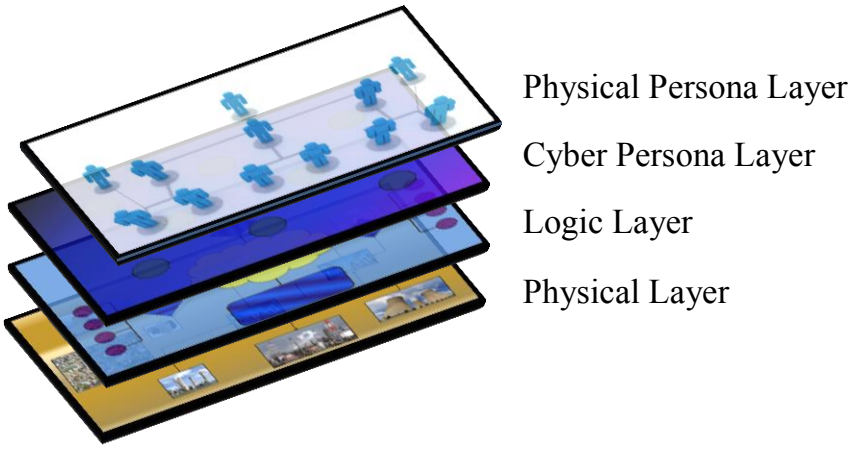

Figure 5: Four-Layered Power Grid-Cyberspace Domain

The *Physical Layer*, as the base of the domain covers the geographic location; power network structure; load distribution and variance; reaction plans; restoration plans and capabilities; and the hardware related information.

Geographic locations of the assets are relevant, even for attacks conducted in cyberspace. Since physical effects are intended for the end-state, modeling the power network is a necessity which requires the location information. This type of information would primarily support modelling the grid with exact node locations and an approximation of transmission line length. Location information is also required when intruding the cyber network via wireless connection points. In this case, it would be necessary to be within physical range of the coverage area. Additionally, the location information also would support data gathering efforts in the Physical Persona Layer. The set of physical assets for this group of information includes power plants, transmission substations, control centers, critical measurement and control equipment in the grid.

Information related to the power network structure is also important [28], since it enables visualization of the grid to approximate effectiveness of potential attacks. The structure must include the physical assets mentioned above. Additionally, incorporating load distribution and variance information would be necessary to analyze admittance/resistance levels and estimate the power on the grid. The load variance is impacted by several factors (e.g. seasonal effects, planned maintenances, etc.), and hence must be analyzed to calculate the situation at the time of an attack.

The information related to the reaction of the power network and the restoration plans and capabilities also must be analyzed to further understand the situation after an attack. Knowledge of this information could help identify the defender's consecutive actions and capabilities and would enable an attacker to conduct more persistent and sophisticated attacks. For instance, islandization is one of the pre-planned defensive actions in a failure situation, and if it could be accurately predicted as a result of to this analysis, target nodes could be chosen to defeat the target system. In addition, usage of certain types of tools could be planned to hamper post-attack restoration efforts [110]. Load redistribution plans, restoration actions, capability of restoration due to the level of technical and logistical issues could also be included in this group of information.

Hardware related information is also grouped under Physical Layer. This includes the data of ownership, type, specifications, and communication means. This set of data would be utilized for gathering information on other layers. Moreover, physical security of the hardware could also be added in this group, if the attack options include intruding the cyber network via on-site equipment either using wireless or physical connections. The scope of gathering data should cover critical equipment in the target node (e.g. transmission substation, power plant, control center, etc.).

The *Logic Layer* stands on the top of the Physical Layer and includes software; cyber network; and communication and security protocols.

Information related to software must encompass operating systems and the operational and other irrelevant applications that the target system hosts. The ownership, version, configuration, and features of the associated software are the source of critical information and provide deep understanding of how system works, and enabling the attacker to detect vulnerabilities [35].

Cyber networks consist of both control and corporate networks that are in cooperation with the target system. The information required prior to conducting an attack in this realm must cover the possible communication paths into and out of the network that provide connection to control network, corporate network, or internet. Knowledge of the network map would provide significant information for an attacker to more precisely conduct the operation [61] since it would help to elude the defensive mechanisms such as firewalls, intrusion detection systems, etc. Furthermore, information pertaining to domain names, subnet masks, opened ports, address ranges, network addresses, active machines, virtual hosts, outdated systems, and virtualized platforms [63,100] would also help to decipher the network's layout for identifying attack tools, vectors, and vulnerabilities.

Communication and security protocols obviously regulate the communication and its security in the system. Since successful intrusion of the target system is one of the initial steps of an attack, it is crucial to understand the rules of communication and security precautions. Because of the general structure of the cyber networks (figure 6), it is essential to gather information about both corporate and control networks of the target system. Significant types of information to help one understand the protocols would include, but not be limited to, authentication; remote access procedures; password complexity requirements and change frequencies; firewall and intrusion detection system configurations; and certificate revocation policies [63, 100].

The *Cyber Persona Layer* consists of cyber personas [25] that are the cyber identities in the target network. Cyber personas differ from physical personas and often exist in one-to-many or many-to-one relationships with them. For instance, a person may have several accounts on the network, or an account may be managed by several people, as is a common case in industrial control systems. The significant information in this layer which would facilitate the execution of a cyber attack includes: usernames, email addresses, passwords, access credentials, and digital certificates [105].

The *Physical Persona Layer* consists of real persons who have authority to access the corporate or control network of the target. The main relevance of gathering information on Physical Persona Layer is because the human still remains the weakest link in the security chain [106] and presents multiple options to the potential attacker. Several objectives could likely be achieved (at least intruding Cyber Persona Layer) by using the gathered data, some of which could be utilized for social engineering, bribing, or even blackmailing. At stake would include, company structures; employee, vendor, and customer lists; personal and organizational websites; home addresses; telephone numbers; respective cyber persona entities; frequent hangout locations; computer knowledge; social network accounts (e.g. Facebook, Twitter, etc.); and dark secrets of targeted physical personas; all of which could stand as potential sources of information [63, 107].

2.4.2 Exploring the Power Grid - Cyberspace Domain

The Four-Layered PGC Domain has an interlinked structure that attaches each layer to all the other layers bilaterally (i.e. the connections are not only between the layers 1-2, 2-3, 3-4; but also 1-3, 1-4, and 2-4). Hence, it is possible to access any one layer from any other. The layers also host a massive amount of information under the types mentioned above. Therefore, the efficiency of exploring the Domain to produce usable intelligence becomes critical. Since the intended end-state is to create effects on the physical infrastructure directly or indirectly, the exploration should start from the Physical Layer in a goal-oriented manner, although the order of subsequent steps could change. These steps include intra- and interlayer information gathering efforts to reach the goal.

As an example, information gathering steps to produce usable intelligence to support the execution of an attack on a critical transmission substation could be described simply as:(1) identify the critical node in Physical Layer (layer 1); (2) determine the network in Logic Layer regarding to the critical node in Physical Layer (layer 2); (3) identify the target critical node in Logic Layer (layer 1→2); (4) determine the authorized real entities for the target node in Physical Persona Layer (layer 1→4, and 4); (5) gather information about authorized persons for reaching their respective entities in Cyber Persona Layer (layer 4, 4→3); and (6) identify the authorized entities in Cyber Persona Layer related to the target in Logic Layer (layer 3→2). These steps describe but one possible track to follow. Numerous alternatives exist, yet they should all start from Physical Layer for the sake of goal-oriented exploration. After these steps, an attack could be conducted to take the control of the entity in Cyber Persona Layer, to manage the node in

Logic Layer, to be able to attack the critical node in Physical Layer (layer 4→3→2→1). This will be further analyzed in the forthcoming sections.

2.4.2.1 The methods and tools for exploration

A partial list of the types of information available in *Physical Layer* include: physical location; network structure; load distribution and variance; reaction plans; restoration plans and capabilities; and the hardware. The methods and tools for exploration may support either single or multiple layers of the Domain.

Information related to location and power network structure may found on the public websites of utility companies and academic institutes. As security awareness grows, one may find that these entities may have removed this type information from public access. Unfortunately, earlier versions of the information, which often has not changed a lot, is likely available via other sources [22]. This type of information, even the older versions, may include standardized geospatial datasets [28] which are highly valuable.

Logic Layer exploration requires analysis of the cyber network with its structural features; software that the nodes host; and the protocols on the layer.

From a structural point of view, power grid cyber networks have three common architectures [64], with minor adjustments made by individual businesses due to their own environmental variances. The most prevalent is the two-firewall architecture (figure 6). In this case, the corporate network is protected from public Internet by a firewall and the control system network is protected from the corporate network by a separate firewall that provides two-level security for the SCADA operations. The other types of common architectures [64] utilize firewall and Demilitarized Zone combinations to meet required security and operational needs.

Revealing the structure of the network down to the connection ports in the nodes has two types of methods as footprinting and scanning.

Footprinting is a passive type of reconnaissance. The attacker passively eavesdrops on network packets that host invaluable information. This method allows the attacker to analyze the traffic; identify active hosts; and determine the operating system and browser version. Additionally, since eavesdropping also reveals the information in unencrypted packets, it also reveals the software (e.g. MS Office, Adobe Flash, etc.) that the nodes host [61, 100]. Footprinting also provides critical information about the wireless networks generally used by control networks. Even in an encrypted network, the data packets provide Media Access Control (MAC) addresses of the devices [102] which are significant to infer the features of the devices in

the network. The popular tools for footprinting [63] include Aircrack-ng and Kismet for wireless networks and Wireshark, Ettercap and Tcpdump for other networks.

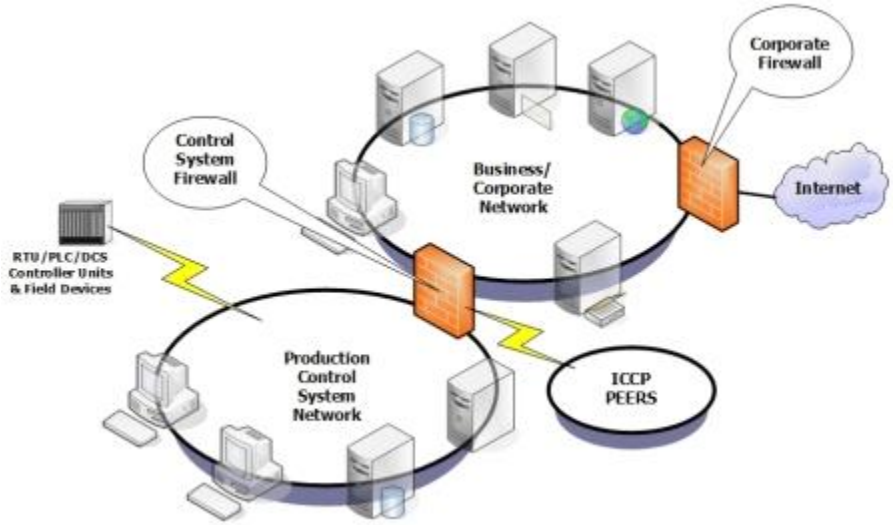

Figure 6: Two Firewall Network Architecture, U.S. Industrial Control Systems Cyber Emergency Response Team, "Overview of cyber vulnerabilities," ICS-CERT Documents [Online]. Available: http://ics-cert.us-cert.gov/ content/overview-cyber-vulnerabilities, Used under fair use, 2014.

Scanning, on the other hand, is an active reconnaissance effort. It is a more offensive method and incurs a greater risk of being detected. Scanning methods [63,102] consist of using pings to scan the ports of the nodes and network devices; creating artificial packets; and active IP packet fingerprinting (e.g. FIN probing, TCP ISN sampling, etc.). These efforts provide the attacker with information to determine open ports, available services, and the operating system in the nodes. It also reveals the routes in the network which is significant for mapping the network. Nmap, netcat, and traceroute are the widely used scanning tools [63,102] currently.

Active and passive methods can also be combined to analyze the traffic and the network. In one example and in an effort to improve the efficiency of an attack, alternative routes that network packets use could be disrupted or degraded in order to redirect the traffic to specific routers that are planned to be sniffed passively [102]. This method would decrease the number of routes that must be eavesdropped without actively attacking the target network and reduce the likelihood of the intrusion being detected.

Analyzing the websites on the target network would also help in exploring the Logic Layer. For instance, web addresses could be queried in Whois; a tool used to query the globally distributed set of databases that host domain names. This query would return information related

to domain registration date, which registrar it was registered with, contact information of the owners, and the Domain Name Server (DNS) information [102]. The contact information would then allow an attacker to cross Cyber or Physical Persona Layers for further exploration. Furthermore, since DNSs are responsible for fulfilling name resolution requests and host the respective IP addresses [102], the DNS information could be utilized to reach IP addresses [100] in the target network by querying several alternative websites (e.g. dnsquery.org). These IP addresses are quite significant in exploring the Logic Layer.

Revealing the type of SCADA software that the nodes in the target control network host is also significant, since it allows passing the next steps in attack planning. This information can typically be reached by public sources (e.g. the utility, regulatory organizations, system producers, etc.). Knowledge of the SCADA software configuration is critical to conducting a surgical cyber attack, but those configurations may differ due to the distinct features of the target environments. The specific configuration of the SCADA software can be ascertained either through Data Acquisition Server (DAS) databases or Human Machine Interface (HMI) display screens [95]. Since the unique identifiers for each sensor, breaker, etc. used in communication protocol are assigned by the DAS, this database provides critical information for identifying the physical nodes' logic representation. On the other hand, HMI screens present the easiest method to understand configuration of the target control system processes, therefore they often become a target of reconnaissance campaigns. For instance, analysis of Duqu malware reveal that it regularly saves screen shots in addition logging keystrokes and gathering other types of information [39].

Cyber Persona Layer exploration requires accessing databases, servers, and the computers on the specific target logic layer which holds usernames, email addresses, passwords, credentials, etc. There are a number of passive and active methods [27, 28] available to an attacker intent on mining this type of information to include eavesdropping, man-in-the-middle attacks, etc.

Physical Persona Layer exploration requires first analyzing the structure of the network, then the individual nodes in it. The structure information of the network includes organization breakdown structures; employee, vendor, and customer lists which could obtained by public web searches and basic social engineering tactics on the target corporate or its vendors; social networks (e.g. LinkedIn); specific searching tools (e.g. Maltego starts with analyzing email address, phone number, etc. before then searching and visualizing the entire created network); Freedom of Information Act (FOIA) requests, etc. These sources and methods would provide

invaluable information to help better understand the network in the Physical Persona Layer. On the other hand, the nodes on the network (i.e. humans), can be further analyzed by looking for personal and technical information within their resumes [102]; searching personal websites and social network accounts (e.g. Facebook, Twitter, etc.); observing them physically; accessing GPS tracker information from their mobile devices, vehicles, etc.; and conducting clandestine information gathering operations [107].

In addition to the mentioned layer-specific methods above, four additional methods could be utilized for revealing multiple layers. The first would be to use advanced searching techniques in standard search engines, or using an ever-increasing list of specialized search engines (e.g. shodanhq.com, pipl.com). This method could access information typically difficult to reach via standard queries by using the deep web which holds critical information related to the all layers (e.g. ShodanHq and Every Routable IP Project provide mapping internet accessed control devices [59, 95]). This method also may reveal significant documents that are shared unintendedly or without authorization [102]. The second method could be to use research papers in the areas such as design, operation, reliability, and security of power grids which might provide invaluable information for understanding the Physical, Logic, and Cyber Persona layers. Hence, it is significant to analyze and reverse engineer these researches, which may have already done the required analyses an attacker needs related to the target system. The third method could be to exploit disgruntled insiders that might be a significant source of information. This method would support the critical or vulnerable points [10] in addition to the general knowledge about the all the layers. The last method could be to conduct intelligence campaigns by using special malwares (i.e. malicious software). This method would enable reaching the information beyond public access and likely require the utilization of additional resources. These campaigns may target utility companies [40, 41], regulatory agencies [40, 41], government agencies [96, 101], academic research centers [96], system manufacturers, etc. If these campaigns are successful, any type of information that exists on the targeted networks, even prioritized target lists [101], would now be accessible. This method would support exploring all the layers in the PGC Domain.

2.4.2.2 Finding the vulnerabilities

Each layer within the PGC Domain has certain types of vulnerabilities inherent to the system and there are numerous methods which to detect them. For the *Physical Layer*, the vulnerable points in the power network can be determined by analyzing the target system which is generally studied in section 2.3. Vulnerabilities in the *Cyber Persona Layer* can be the result of weak protocols (e.g. password and authentication policies) or the vulnerable physical personas of

which either of them stands in a different layer. This is because the links in the Cyber Persona Layer would only connect it to the other layers and do not create a network in itself. On the other hand, the network in the *Physical Persona Layer* does hosts several vulnerabilities including, but not limited to, lack of education; dissatisfaction; dark secrets; fondness for money, power, etc. The techniques used to detect these types of vulnerabilities will not be analyzed in this thesis, but they would include web searches; social network analyses; social engineering methods; physical and technical traces.

The *Logic Layer* also hosts multiple points of vulnerability [20] whether in cyber network, software, or protocols. Examples of each could be network component configuration, unpatched software, or improper authentication respectively. Other sources of vulnerabilities in network and protocols can also be found in [18], [35], and [100]. Methods for finding the vulnerabilities in industrial control networks may have unique characteristics. For a long time, the proprietary software and protocols of the industrial control networks had provided "security through obscurity", but as these shifted from proprietary to commercial-off-the-shelf (COTS), and some companies becoming more prevalent in the market it has made it easier to determine the vulnerabilities [14]. For instance ABB, General Electric, Siemens, ALSTOM, Schneider-Electric, TELVENT, and NARI are the companies that are the most prevalent both in RTU/PLC production and SCADA software development markets [15]. Therefore, the number of different target software formats has decreased and accessing the code of them has become easier. Moreover, the number of revealed vulnerabilities in industrial control systems has also increased since the Stuxnet attack (detailed information in section 1.2.3.1). Many of these vulnerabilities are gathered mainly in SCADA software, HMIs, and PLCs with 49%, 28%, and 11% respectively [95]. The types of the vulnerabilities presented a diversity such as buffer overflow, input validation, resource exhaustion, authentication, and cross-site scripting with 26%, 8%, 5%, 5%, 5% and so on, respectively [109].

Several methods exist for finding these types of vulnerabilities in the Logic Layer. The first is to use the released vulnerabilities that have not been patched yet. Since control systems are expected to perform without interruption, software upgrades cannot be applied rigorously [18]. After a new version of software is created and before it can be applied, there is a waiting period until the vendor tests and validation can be completed, which in some cases may take several months [22]. Historically, 19% of the released vulnerabilities will not be fixed within 30 days from the time it is detection and, in certain cases, vendors would not fix them at all. Published reports [95] expose that 33% of ABB's, 20% of General Electric's, and 12% of Siemens's

vulnerabilities have been left unpatched and these are the leading companies in the market. The released vulnerabilities can be accessed from several databases such as those for national Computer Emergency Response Teams (CERTs), international security projects (e.g. VIKING Project), or Corporate CERTs. The most frequently used databases for this reason could be listed as ICS-CERT, NVD, CVE, BUGTRAQ, OSVDB, and so on [95].

The second method for finding vulnerabilities in the Logic Layer is by discovering new vulnerabilities on potential target systems. Vulnerability scanning tools (e.g. Nmap, Nessus, etc.) can be utilized for detecting vulnerabilities on operating systems, databases, protocols, services and as well as in SCADA software [102]. However, finding new vulnerabilities requires additional resources such as target system test bed laboratories and area-specific expertise for further analysis. Other tools or procedures, such as fuzzing methods (e.g. Fuzzball) that send invalid, unexpected, or random data to the software; and reverse engineering tools (e.g. IDA Pro) that use interactive disassemblers, can be used [35]. Additionally, older published papers, from a time when security was not a priority, by owners or designers of the target system, can be uncovered and used identify new vulnerabilities.

The third method for finding vulnerabilities in the Logic Layer is by purchasing the information on the vulnerabilities and exploitation from the black market or boutique providers [100]. The price of these services would depend on several factors and may vary between $40,000 and $250,000. Some providers could offer nearly a hundered vulnerabilities in one year, showing the importance of the market [108]. Nation states are one of common customers of the market. For instance, the United States' National Security Agency (NSA) planned to spend $25 million on exploit purchases in 2013 for approximately more than a hundred vulnerabilities [116]. The other significant nation state spenders would be Israel, Britain, Russia, India, and Brazil [108].

The last method nation states might employ for finding vulnerabilities in the Logic Layer is using the insiders of vendor companies. Even companies that zealously protect their software's source codes could be at risk of being compromised. In certain cases they likely provide this information to the governments via senior or junior level insiders, thereby increasing the likelihood of identifying vulnerabilities. Additionally, nation states could persuade these insiders or willing employees to insert vulnerabilities (e.g. backdoors) into their products by appealing to their patriotism or ideology; by bribing, blackmailing, or extorting them; or by applying political pressure [61].

2.4.3 Discussions for Information Gathering

The factors that affect information gathering efficiency consist of several issues. They include, but are not limited to, the ones listed below.

First, information gathering efforts must be applied cautiously, since the tools and techniques to gather information and those used to conduct attack on a target system can closely resemble each other [63] making it easy to blur the distinction between intelligence gathering and conducting attack. Therefore, upon detection of intelligence gathering activities, and without any insight into the perpetrator's intent, an adversary could suppose an attack is imminent or is currently being conducting on its power grid and could take respective actions which could unintendedly or prematurely escalate the situation.

Second, active reconnaissance efforts of a campaign should be extended over a reasonable time period. Since the target system is critical to the adversaries, they would expend significant resources to defend it, but they would likely do so with an effort not to draw attention of defensive precautions such as wisely configured firewalls, intrusion detection systems, honeypots, etc. Therefore, by lowering the intensity of active efforts, an adversary could increase the probability of success of the campaign. On the other hand, one should also keep in mind that the vulnerabilities or other types of information gathered tend to be time sensitive. In other words, compromised user account information and configuration of the security mechanisms could be changed, or the vulnerability that is planned to be exploited could be patched prior to execution of the attack so it is critical to keep the information up-to-date or conduct the attack in a reasonable time period.

Third, the radar cross section of the information gathering malware should be kept as small as possible. In other words, it is critical to take precautions to reduce the detection possibility of the tools that are utilized. One method could be to use target-oriented pervasion patterns to reach the target system. This method reduces detection possibility, yet it also limits the ways to reach the target system. Other methods should be devised to improve the success of the operation from this point of view.

Fourth, active information gathering tools should be designed in a way that, in case of detection, they can create confusion on the adversary's side. Anonymizing the control source of the tool is one method that could prevent attribution. Injecting misguided traces into the tool could also further deceive the adversary. Encrypted communications could further shroud the intentions in secrecy. Additional methods should be devised to keep actual operations covert, even if active information gathering tools are detected.

Lastly, information gathering tools should be created in a modular structure. Because the detection of information gathering efforts could reveal the intentions and cause unintended escalation, it is significant to devise the malware in separable modules. In this case, the first module should be able to settle in the attack node and open a backdoor for further steps. Subsequent modules could be configured and dispatched to the target depending on the campaign's needs. This method could harden counterintelligence activities for the operation. At the end, this backdoor also could be used as an attack vector which has already been utilized and analyzed before.

2.5 Options

Emerging weapon technologies present numerous alternatives to meet operational goals. Conventional munitions, Soft Bombs and EMP weapons can all degrade, disrupt, and/or destroy [26] power grid in physical world. The use of these types of weapons creates primary effects on the target. In cyberspace, various cyber weapons could also create resembling impact on the grid by creating secondary effects on the target. The options for conducting a cyber attack can be grouped as either those against integrity, availability, or confidentiality of the power system operations. Before analyzing these options, one should analyze the options used in previous military operations against that power grid.

In *Operation Desert Storm* (ODS), the power grid was attacked by using over 85 tons of non-precision, unguided munitions and almost 13 tons of guided munitions (e.g. TLAMs, laser guided weapons in GBU series). Soft Bombs were employed in combat for the very first time, but only in very few numbers [112]. These attacks destroyed 92% of power grid's serving capacity and required years to restore.

In *Operation Allied Force* (OAF), the power grids was initially attacked by Soft Bombs (CBU-94), but were subsequently retargeted by conventional guided and unguided munitions [76]. During the first wave of the attacks, Soft Bombs were used exclusively. The Soft Bomb, a cluster-munition, carried 200 BLU-114/B submunitions that were dispensed by SUU-66/B tactical munition dispenser over a large area. These submunitions carried chemically treated carbon graphite filaments, only a few hundreds of an inch thick, which would float in the air like a dense cloud. These conductor filaments cause a short circuit when they contacted power substation equipment and were able to create a blackout without creating collateral damage. Unfortunately for the war planners, the filaments were able to be cleared in a short time allowing

restoration of the power grid. In the second wave of the attacks, power grid nodes were attacked by traditional guided and unguided munitions which created long term destruction for 80% of the power grid's serving capacity [75].

The attack options in cyberspace have been grouped under numerous taxonomies [5, 20, 27, 28, 30, 37, 65]. In this analysis, conceptual classification method that divides the attacks as either one of those against integrity, availability, and confidentiality would be used. These types of attacks could be conducted against computer systems, networks, and/or the information resident in transiting these systems or networks.

In general, attacks against integrity include insertion, alteration, or deletion of the data. In the case of a power grid, this type of attack could trick the system into making wrong decisions or actions by creating effects on the source, destination, timestamp, or the body part of the data packets. The aim of attacks that are against the availability of the system would be to deny normal services to the legitimate users. Their objectives are to deplete or overwhelm the resources of the system in order to delay or impede the communications [30]. Attacks against availability would create more harmful effects on the power grid than upon other IT systems due to its real and non-real time operations' criticality [5]. For instance, the grid requires services available less than 4ms for protective relaying, 1s for transmission wide-area situational awareness monitoring, seconds for substation and feeder SCADA data, etc. [7].

Attacks against confidentiality would aim to undermine the secrecy of the data such as personal privacy and proprietary information (e.g. customer power usage data, corporate secrets, confidential portions of electric market information) for the power grid case [23]. Since attacks against confidentiality have no real potential benefits in a military operation, they will not be a primary concern for this research. Integrity and Availability attacks [4], on the other hand, could create significant primary or secondary physical effects on the power grid [25] with first or second order consequences, respectively. Calculation of potential damage that could be created by an attack is a challenging issue in cyberspace, yet [115] and [5] analyze the attacks against power grid integrity, and availability from this perspective, respectively.

Victims of the attacks against integrity and availability could be grouped under one of three classes: data in control network (e.g. sensor readings, control commands), control network devices (e.g. sensors, actuators, RTUs, etc.), and the databases (e.g. DAS) in the network as depicted in figure 7. Cyber attacks could target either one specific group or a set of them.

Furthermore, these types of attacks can be conducted via three different communication links [5]. The links are: (1) between field devices (e.g. sensors, actuators) and RTU/PLCs; (2) between RTU/PLCs and the SCADA control center; and (3) between the SCADA control centers that share information to be able to monitor the regions that are not under its control. The goal of these attacks may include taking down a specific generation/transmission substation unit or degrading control systems (e.g. AGC, SE, VARC, WAM) of the grid to mislead management of the entire network as indicated in section 2.3.1.

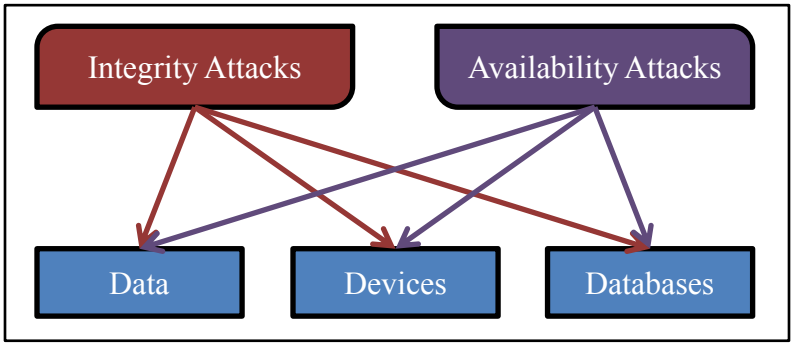

Figure 7: Cyber attack options

2.5.1 Attacks against Integrity

Integrity attacks can be mounted on the *data*, the *devices*, and/or the *databases*.

Numerous *data integrity attacks* (e.g. Smurf, ARP Spoofing, Baseline Response Replay, Transport Sequence Modification, etc.) exist [2, 4, 5, 7, 20, 27, 65, 114] regarding the communication protocols (e.g. Modbus, DNP3, IEC61850, ICCP, etc.) that various networks utilize. These types of attacks can affect the status of control equipment directly as well as indirectly by altering sensor readings in an effort to trick the operator into reconfiguring the system into a destabilized situation. These attacks would provide insertion, alteration, or deletion of the sensor reading or a control command in the network. For instance, it might be possible to insert messages to spoof field RTU into the network; modify the legitimate sensor readings that field devices send to the control center; or delete specific types of messages that alerts the operators for abnormal status. As a result of these actions, power operations could be jeopardized critically.

Device integrity attacks, on the other hand, target control system equipment including sensors and actuators. There are a number of ways and various means to compromise these devices [102] which is further analyzed in section 2.6. As a result of this type of attack, an attacker would be able to take the control of the device, and hence could create any desired sensor

reading, and use any control feature that a legitimate operator could control in physical limits of the device. For instance, in WAMs, a set of compromised PMUs could be used to relay misleading voltage phase angles. This could set the conditions for a cascading power failure. Moreover, a set of circuit breakers that are in critical locations could be utilized to trip respective transmission lines to create devastating effects on the power network. This integrity attack would also affect the availability of the system.

Database integrity attacks target the databases in the control and corporate networks, especially the DAS databases. It is possible to modify the database structure and manipulate their content through these attacks, if the system operators fail to properly sanitize the unexpected structured query language (SQL) statements [27]. Furthermore, if the database is configured improperly, it would enable an attacker to gain total control of the database or even execute commands on the system. Additionally, an attacker could also destroy the data [61] by permanently erasing it; thus, database integrity attacks could cause catastrophic damage on both cyber and power networks.

2.5.2 Attacks against Availability

Availability attacks can likewise be mounted on the *data*, the *devices*, and/or the *databases*.

Data availability attacks (Fragmented Message Interruption, Length Overflow, DFC Flag, Re-initialization, SYN Flood, etc.) can be conducted to various sets of targets [5, 7, 20, 27, 30, 65] and on different Open Systems Interconnection (OSI) layers (e.g. Physical, Network, Application, etc.). Their aim is to delay or hamper the communications by disrupting the channel of communication or the data passing through it.

Availability attacks on the communication channels can be conducted on different OSI layers. For instance, channel jamming attacks [5] against wireless networks (i.e. substation networks) create effects on physical layer. As a result, delivery of time-critical messages (e.g. alarms, protective messages, etc.) would be delayed or prevented. Another type of attack that could be conducted on the wireless networks is a spoofing attack [5] on MAC layer. In this case, an attacker could masquerade as other devices in the network and send forged address resolution protocol (ARP) packets. This could prevent communication of legitimate devices by deceiving the gateway node into believing that the attacker is a legitimate component within the network. Availability attacks on the network and transport layers also would delay or prevent delivery of the time-critical messages. The aim of these attacks is to decrease the performance of end-to-end

communication by flooding the communication channels. Distributed traffic flooding attacks and worm propagation attacks are some examples of availability attacks. Data availability attacks are most frequently conducted on the application layer and intended to exhaust the resources (e.g. CPU, I/O bandwidth) of a computerized device by flooding computationally intensive requests [5]. One example of this type of attacks is a SYN flood attack in which the attacker sends SYN requests faster than a machine can process [27], and hence prevents legitimate entities to connect to a server. The effective targets upon which this type of attack would be conducted effectively are SCADA servers which are the center of operational communications. Attacking the SCADA server would hamper both the field device communications and the coordination of region-level SCADA server coordination. This would inhibit the ability to create the global picture of the grid and thus hinder protection and restoration efforts.

Data availability attacks can also create effects on the data itself which can hinder operational communications [7, 20, 27]. For instance, fragmented message interruption attacks would send fake signs (i.e. FIR flag for first, FIN flag for final packet) to deceive the target device into believing that the fragmented message is already completed or a new one has started [7]. This would prevent the target device from properly receiving and combining fragments of the legitimate message.

Availability attacks can also be conducted *on the devices and the databases*. This type of attack (e.g. Length Overflow, DFC Flag, etc.) could take a device/database offline or send fake messages to deceive other devices that the target is offline or busy [7]. Moreover, it might be possible to take the control of the targeted device after re-initialization since the configurations of device would be affected [65].

2.5.3 Sample Attack Patterns

This section will provide a brief analysis of the potential effects of integrity and availability attacks on target control systems and nodes.

AGC control systems have authority over regional GCs of the power plants in order to be able to provide frequency equity between these substations. The GCs try to keep the frequency to its nominal value in order to avoid large deviations (i.e. around 1.5Hz [52]) that could damage the generation unit. Due to the process's sensitivity and criticality, the AGC systems stand as one of the few control loops in the power grid that could work without human intervention. Meanwhile, researchers have analyzed the potential impact of cyber attacks on AGCs [52], and GCs [117]. One study, "Project Aurora," demonstrated that inserting or altering control commands could

result with power generation unit destruction. The experiment was conducted at the U.S. Department of Energy's Idaho National Laboratories in 2006 and demonstrated that the destruction can happen in less than a minute which increases the success probability of the attack [117]. Furthermore, a power generator accident at the Sayano-Shushenskaya Dam in Cheremushki, Russia in 2009 proved how the cyber attacks could cause catastrophic effects. In this case, the generator which had 10.650-megawatt generating capacity and weighed more than 1.000 tons, was mistakenly started by an operator over 500 miles away. As the generator began spinning, it rose in the air and exploded, killing 75 people and destroying eight of the remaining nine turbines at the dam [101].

VARC and WAM control systems resemble each other in that both require autonomous cooperation without human intervention and control a wide area. Hence, integrity and availability attacks on them could result in wide area voltage destabilization which may also cause physical destruction such as fires and explosions [27]. Several attack options exist for creating these types of effects. Denial of cooperative operation is one example that sends spurious packets to flood the communication network in order to jam and prevent critical information exchange [20]. Desynchronization attacks, on the other hand, targets the time that provide synchronization for a large amount of devices; thus, this type of attack could disrupt steady operation of the control devices. Lastly, data injection attacks that are directed against the integrity of the system could be used to manipulate sensor readings and control commands [27]. This type of attack may require compromising a set of devices to be able to evade defensive mechanisms.

SE control systems provide data for system operators to be able to execute load redistribution and dispatching actions. Hence, attacking its availability and integrity could potentially create catastrophic decisions by the operators [5]. However, falsifying this type of information requires coordination and power network topology knowledge. Since defensive, bad data detection systems use algorithms to identify falsified sensor data, an attacker must carefully orchestrate its actions to remain unobserved. Researches demonstrated that a relatively small number of sensors and only a modest degree of coordination are enough [114] to conduct this type of attacks [31]. However, the attacker would need to simultaneously alter the network (i.e. switch and breaker states) and the meter data to be able to stay consistent with normal situations for preventing detection [46].

Like the attacks against control systems mentioned above, individual control devices and sensors (e.g. circuit breakers, alarms, etc.) can also be effectively attacked. For instance, circuit breakers play a critical role as protective units in the network and can be attacked by both

integrity and availability attacks. Compromised circuit breakers or modified control commands could be used to trip certain branches of the network to alter the situation in a case in which power generation units connected to the grid cannot meet the demand, which may trigger blackouts [28]. Furthermore, since the breakers' role is to isolate the faulty equipment to protect the system, availability attacks on them would result with failure of their functionality. If this happens, additional breakers may be required to be opened which would further prolong the blackouts. Moreover, some circuit breakers could explode upon failure, resulting in damage to nearby equipment or causing fire [22], and further hampering the restoration efforts. On the other hand, alarm systems also could be attacked by deleting its messages or blocking the critical messages via integrity and availability attacks, respectively. These attacks would prevent system operators from being able to monitor contingencies and would thus affect reaction efforts negatively. In the 2003 North East Blackout case, protective actions were impeded because the alarm systems were affected by both a bug (XA/21) in the General Electric EMS and Blaster Worm. The bug took respective alarm equipment offline and the Blaster Worm delayed critical communication of the cyber network [110]. Therefore, cascading failures could not be prevented or responded to in required time period.

In the final analysis, integrity and availability attacks on the cyber network of a power grid could effectively meet the goals of military operations. They could both be utilized against power grid control systems and individual devices on the cyber network.

2.6 Execution

Cyber attack execution on a power grid, which is basically delivering the identified payloads to the targets, has as many challenges as their conventional counterparts. For instance, previous conventional attacks were constrained by geographical variables and enemy defenses. Despite these constraints, the right routes and methods were found; perimeter defenses were penetrated; and the operations were executed successfully [79]. Although the dynamic nature and unique characteristics of cyberspace diversify itself from physical world, successful cyber attacks and researches prove the viability of the routes and methods. In this section, execution of conventional attacks on the grid will be referred briefly; the access points of the targets in cyberspace and the methods to penetrate the defenses will be analyzed; and factors related to the success of the operation will be discussed in the end.

Conventional physical attacks were conducted on power grids in ODS and OAF. Geographical variables and adversary defenses challenged execution of the operations. For instance the distance of targets from the enemy borders, bordering domains (i.e. land or sea), meteorological conditions, the enemy's integrated air defense systems, electronic warfare capabilities, and other assets (e.g. navy ships, aircrafts, etc.) could be listed as some of the factors that constrained or steered the operation plans. However, the technologies and capabilities such as over-the-horizon weapon systems, air refueling assets, aircraft carriers, and Special Forces helped ease the problem. In ODS specifically, weapon payloads were delivered against Iraqi power grid targets via TLAMs (35%), F-16s and B-52s (15%), F-117s, F/A-18s, and A-6Es (12% each). Additionally, the Soft Bombs, which were still experimental, were all delivered by TLAM-D Kit2s. In OAF, the first wave of attacks was carried out by F-117s using the Soft Bombs only; yet TLAMs and various types of aircraft participated for the second wave. As a result of these operations the respective power grid targets were disrupted or destroyed.

2.6.1 Execution in Cyberspace

Cyber attack execution requires an understanding of the access points of the target network and the defenses on it in order to find efficient ways to intrude the system and devise methods to overcome defensive mechanisms as its kinetic counterparts. Since intelligence gathering may require target network intrusion, these ways and methods must also be utilized to conduct an intelligence gathering campaign.

As a result of technological, operational, and environmental variances between the power grids' cyber networks, the ways and methods to conduct the operation may change. Additionally, the required ways and methods to exploit a system would also depend on the identified targets and options, hence varying the required level of intrusion (e.g. device level, control center level). For instance, it is possible to compromise a set of devices in a specific area over the diagnostic access points. In this case, the defenses required to overcome might be limited to the maintenance equipment's (e.g. field personal's laptop) and control network's security mechanisms. In an alternative case, if a control center needs to be compromised, the control network might be accessed through the internet via a corporate network. In this case, the firewalls on the connection points of the networks, IDSs, IPSs, and other security protocols would pose a challenge to the operation. A number of other examples could be generated to illustrate this concept. Therefore, in this section, the access points of the target cyber network and the methods for exploiting the defensive mechanisms will be more closely analyzed.

2.6.1.1 Access points of target cyber network

Although they depend on the level of advanced technology involved, the access points (APs) of target cyber network can be listed as connection points between the networks, diagnostic accesses, dial-in modems and telephone connections, database links, wireless and bluetooth connections, and the insiders [15, 36, 50, 54, 64, 84].

Target networks consist of LANs which are connected through WANs. The LAN in a target network could be listed as corporate network, control network, or substation network. Generally, corporate LANs are connected to the internet, peer corporates (e.g. other utilities, vendors), and control networks; control LANs are connected to corporate network, peer control networks (e.g. backup control center, other control centers that are in coordination with), and substation LANs; and substation LANs are connected to control centers. The connection points of these networks stand as the primary APs of the target networks [64]. These APs are often secured with firewalls, which are challenging, yet possible to get through [84]. Firewalls generally advance to keep pace with state-of-the-art attack methods; however, insufficiently configured firewalls can be exploited. Specifically, the connections with the peer corporate and control networks are typically more trusted than the other connections, thus the security level of these APs could possibly be lower than others. As with any system, the security of the system depends on the security of the weakest member. As a result of exploiting these APs, the required level of intrusion could be reached step by step.

Diagnostic accesses enable vendors to provide service during system upgrades or when a system is malfunctioning. They can access the corporate network, control network, or field devices through dial-in modems or, more recently, by virtual private networks. They create additional APs for potential attackers without having to struggle with the target network's standard defensive mechanisms. Therefore, if a vendor company's internal resources or field laptops could be compromised, then the legitimate connection with the target network could also be exploited [15, 64].

Dial-in modems and telephone connections to the LANs in the target network would also provide unsecure APs because of their incompatibility with the advance security mechanisms [36]. In large and geographically-distributed corporations, it is very likely that the corporate LANs have unsecured telephone connections [84] which could be utilized as a first point of entry into the target network. Dial-in modems, on the other hand, though declining in number, still currently make up the vast majority of both corporate and control networks host. They have been

mostly used for primary or backup communications of field devices in addition to the corporate and control networks [64] and could be utilized as APs to various levels.

Database links between the control and the corporate networks provide mirroring system logs, and hence create additional APs to navigate between the control and corporate networks. This could allow specifically crafted SQL statements to query the databases. This would create vulnerability since almost all modern databases would allow this type of passage if not properly configured to block it [64].

Wireless networks enable mobility and modularity, and in return provide increased efficiency. For these reasons, wireless connections have become common for most devices and have been deployed in nearly every type of network. As a result, unsecured wireless gateways of the networks, and wireless enabled computers have created additional APs to both corporate and control networks [84] which can be exploited from a reasonable proximity. Moreover, the wireless communication of the field devices in substation networks is very common technology, thus both the devices and the gateways stand as APs [15] for the target network.

Bluetooth connections open additional APs to the target network, which has an increasing possibility by the use of more bluetooth-enabled devices (e.g. laptops, tablets, printers, etc.) on the corporate or control network. This mean of communication can also bridge the attack vector to the target network [84] by circumventing most of the security mechanisms.

Insiders, whether inadvertent or malicious, open the highest number of APs to the target network. Intentionally or not, they can insert infected media (e.g. flash drive, CD, etc.) to various levels of the network. Moreover, malicious insiders can even create APs to the backup systems [84] to allow an attacker to damage or wipe out critical data and software in the system. In some cases, they might be able to enable these APs from remote locations. Malicious insiders have been a very successful way to execute the operation; yet achieving this capability has its own nontechnical challenges.

2.6.1.2 The methods for circumventing the defensive mechanisms

Target cyber networks may host any number of in-depth defensive mechanisms such as firewalls, IDSs, IPSs, antivirus software, security protocols (e.g. authentication), etc. Attackers must be able to use methods and tools to circumvent these defenses in order to reach the target and infect it to activate the payload. If intended, it would also be possible to install a rootkit or Trojan horse in order to leave payload deployment and activation to a time in the future [6, 65].

To successfully execute the operation, an attacker should seek the weakest point in the system. Serial dial-in systems and wireless APs are typically seen as weaker points from the security perspective [84]. Due to the incompatibility with advanced technologies, dial-in modems might not host the proper security mechanisms required in order to cope with current cyber attacks. Some of these systems even may not require passwords or may still use default ones for some reasons [84]; while others, in most cases, might be vulnerable to brute force attacks. Promising wireless communication systems, on the other hand, have already been widely deployed and though their security measures are not as firm as other network APs, it does require a certain physical proximity which somewhat reduces the probability of an attack. However, this fact also makes wireless communications a weak point in the system by increasing the possibility of an attack [100]. Several attack types (e.g. modification, impersonation, etc.) exist [118] for overcoming defensive mechanisms in wireless systems. Therefore, wireless APs and dial-in systems could be chosen primarily to reach the target system due to lack of security measures.

Research and current attacks demonstrate that signature and behavior based state-of-the-art defensive mechanisms are also penetrable with various methods. These methods include but not limited to *web-based attacks*, *identity spoofing attacks*, *password attacks*, *social engineering methods*, *insiders*, and *compromised supply chains*.

Web-based attacks which can bypass defensive mechanisms by automatically downloading malicious code to the target computer from a website are called drive-by download attacks. The malicious code can be injected to either a legitimate website or a fake one which would be visited as a result of using DNS manipulation, DNS cache-poisoning attacks [100], social engineering methods [65, 14], etc. Additionally, some other techniques could be combined in order to direct users to infected websites without noticed. For instance, "The Mask" campaign uses spear-phishing emails that include links of a malicious website. The website accommodates a number of exploits devised to infect the directed visitor. After successful infection, which can happen in a moment, the malicious website redirects the victim without being noticed to the legitimate address that the user intended to reach which could be a YouTube movie or a news agency [96]. After downloading the malicious code, buffer overflow [27, 65], cross-site scripting [102], or other vulnerabilities could be exploited to cause execution of the code to infect the target. Moreover, emerging technologies present new opportunities to conduct these types of attacks. For instance, cloud services enable attackers to reach legitimate target websites over the cloud servers which possibly host numerous websites with varied security levels [100]. This fact further reduces the security level of the entire system by introducing weaker chains into the link.

Identity spoofing attacks enable the attacker to deceive defensive mechanisms by impersonating legitimate users. Common identity spoofing attacks include replay attacks, man-in-the-middle attacks, network spoofing attacks, and software exploitation attacks [51]. Additionally, using stolen credentials of legitimate users [64], hijacked VPN connections [50] or generated rogue certificates [41] could deceive defensive mechanisms where the attacker impersonates either users or the legitimate organizations.

Password attacks help bypass defenses by providing legitimate access right to an attacker. A password could be cracked by using brute force attacks which iteratively tries every possible password. This can be time consuming and easy to detect [102], yet depending on the strength of the password, they could also be very effective. Look up or "Rainbow" table is another type that stores every possible key combination which is encrypted with popular protocols. If the length of the password would grow then the attacker could use botnets to build up these tables [102]. Other methods of password attacks include man-in-the-middle attacks, social engineering, password sniffing, and guessing.

Social engineering methods provide circumventing defensive mechanisms by deceiving and manipulating legitimate users. They basically aim to influence someone's behavior via exploiting their emotions, or earning and betraying their trust in order to gain access to target systems [14, 102]. The most common social engineering attacks use emails. The information in the email would convince the user to download a file [100] or visit a compromised website. Compromised websites enables the web based attacks mentioned above. On the other hand, files (e.g. pdf, excel, word, etc.) that contain malicious code could slip through defensive mechanisms [65] and would be executed when the file opened. For instance, Duqu malware uses an MS Word document that contains a zero-day kernel exploit to propagate [39, 40]. This type of attack could be divided into three subcategories: phishing attacks target numerous people, spear-phishing attacks target a specific person, and whaling attacks target a specific senior member of the target organization [102]. Social engineering methods cover several other methods [14, 107] to circumvent defensive mechanisms.

Insiders also could be utilized to penetrate peripheral defenses of the target system. They could be either malicious or inadvertent, thus intentionally or unconsciously opening backdoors to target system by enabling the attack types mentioned above, plugging into malicious removable memory devices (e.g. flash drive, CD, etc.), or modifying defensive mechanisms configurations [100].

Compromising supply chains of the target organization is another method for evading defensive mechanisms. In this method, the attacker aims to preload the hardware with malicious code before the computer system delivered to the target organization. By doing so, the attacker can open backdoors to the system or execute certain malicious functions when specific conditions have been met, even with systems used in isolated networks [6, 50, 100].

2.6.2 Discussions for Attack Execution

Several factors exist that affect the efficiency of conducting cyber attacks on a power grid. They include but not limited the ones listed below.

First, being able to conduct consecutive waves of attacks is crucial. Previous military operations demonstrate that depending on the insufficiency of offensive attacks or the adversary's successful power restoration efforts, subsequent strikes might be required to accomplish operational goals [76, 79]. For this sake, either same or different types of kinetic weapons can be delivered with almost similar means in conventional operations. However, due to dynamic nature of cyberspace, the ways to penetrate target networks and the defensive mechanisms could change rapidly. For instance, the adversary could reduce level of automation by increasing human intervention, periodically change the cyber network's structure, or detect and patch the exploited vulnerabilities in the system. Hence, the attacker must devise methods to sustain in the target system. There are various methods an attacker could follow to reach that goal [22, 100, 102] such as infecting the system widely, which would enable further attacks even some failed equipment have reinstalled; implanting logic bombs that will wait until specific conditions are met; using remote access toolkits and Trojan horses; or gaining legitimate access rights by manipulating databases.

Second, it is significant to remove or manipulate attack traces to alleviate harmful effects of attack detection. Clear understanding of the attack by adversary would provide attribution, risk further use of the cyber weapon, and even result in counterattack with the same weapon after reverse-engineering and reconfiguration. Thus, to obfuscate the adversary, it is crucial to remove, or at least manipulate, the traces [63] that may provide understanding of how the cyber weapon reaches its target and how it exploits the system, etc. For instance, researches could not reveal the secret behind how Duqu malware infects the first computer in a network [39, 40]. Additionaly, it was found that Duqu malware removes itself at the 30th day of infection and even removes itself suddenly when there is no communication with the C&C servers [40]. For this sake, location obfuscation, log manipulation, and file manipulation techniques [102] could be utilized.

Moreover, the methods that are discussed in section 2.4.3 to deceive adversary about the source of the attack also should be performed.

Third, timing for target system penetration is critical for the success of the operation. Since system intrusion takes time, an attacker must start utilizing vulnerabilities to access the network and provide desired level of infection before a reasonable time period than the planned execution time. However, in this time period, the structure of cyber network and defensive mechanisms could change, vulnerabilities could be patched, or the attack could be detected. Therefore researchers [85] aim to determine optimal time window for exploiting vulnerabilities. Yet, the tradeoff problem for timing still stands as a critical factor for operational planning.

Fourth, the risk of creating unintended consequences is another factor that must be taken into consideration for attack planners. This factor could cause inexcusable results, yet could be common in wartime due to uncertainty and confusion. For instance, post-war analyses [79] claimed that the planners of ODS intended to destroy transformer facilities, yet the pilots, unaware of that, caused destruction of generator facilities which created additional long term unintended consequences. In the case of cyber attacks, there is also a risk of creating harmful results due to dynamic nature of both cyberspace and wartime scenarios. Hence, it is significant to inform the personal conducting the attacks about the specific goals, reasons, and targets. For similar reasons, the decision makers of the operation also need to understand technical details superficially to be able to take the risks into consideration.

2.7 Lessons Learned

Analysis of cyber attacks on power grids provides knowledge about previous military operations that targeted power grids and the steps of conducting those cyber attacks on the grid. This methodology helped identify both the critical factors for successfully conducting these types of operations and the previous mistakes that have made in their planning phases. Although the elements of each step can shed light on critical issues, it is more important to reevaluate these types of attacks from a broader perspective. This section will try to “zoom out” to get a broader perspective of the details of conducting the cyber attacks as well as providing a brief summary of the methodology.

2.7.1 Goals

Power grids stand as critical targets in military operations. Disabling the grid would likely interrupt the line of supply, hinder communications, disturb mobilization efforts, and

degrade C4ISR efforts. In addition, it could also create a significant impact on the adversary's psychology, possibly encouraging defection of the enemy forces. National power grids were specifically and significantly targeted during ODS and OAF for some of these very reasons.

Furthermore, cyber attacks could enable attackers to disable large parts of power grid even before the commencement of combat operations. Since national critical infrastructures depend heavily each other, loss of electricity over a wide area would also adversely impact the resources of the adversary as seen previously [1]. Therefore, these types of attacks would likely plunge the enemy into chaos and delay their preparations for war. Ideally, the attacks must be stealthy and the traces must be obfuscating in order to prevent clear attribution in case of detection. However, even if the attacks could be attributed correctly, which is very unlikely, the obscure nature of cyberspace would provide deniability to attacker. Besides, the uncertain nature of cyber attacks in Law of Armed Conflict [119] would potentially reduce the legitimacy of an adversary's counterattacks.

Both kinetic and cyber attacks can provide short or long term disruption/destruction as explained previously. Unfortunately, disabling the power grid would also possibly create harmful effects on the civilian population. The greater the physical destruction of the grid would require more time for restoration and recovery. Therefore, the intended operational goals for attacking a power grid should be identified wisely with special consideration for the disruption-destruction tradeoff. Otherwise, the attacks could create blowback effects by unifying civilians against the attacker or bring global attention to the negative effects on civilians from a humanitarian perspective.

Since the effects from attacking a power grid extends beyond military-related areas, the responsibility to conduct such attacks should not rest solely with the military decision makers. In other words, political leaders must take more initiatives for defining goals and target sets. With this in mind, it is also important that the decision-making mechanism must be created wisely to prevent delays which would reduce the efficiency of the operation.

2.7.2 System Analysis

Power grids take center stage in identifying interdependencies of critical infrastructures [22]. Telecommunications, transportation, manufacturing, IT sector, and financial services could be listed as the most dependent infrastructures [7] which also form the backbone of a nation's services.

Legacy power systems continue to evolve by introducing advanced technologies; hence, they are becoming smarter. This evolution incorporates a number of entities to manage the grid and is therefore becoming more standardized and open to web. As a result, they are also becoming more vulnerable to cyber attacks.

2.7.3 Targets

The target identification process should adopt an effects-based method to avoid creating unnecessary damage to the target network. For example, when the desired effect is to cause a wide-area blackout for a reasonable time period, choosing the transmission network which is the bottleneck of the system would be efficient for targeting. Critical transmission substations and control systems that orchestrate the nodes of the transmission network could also be included in target set. In addition, a set of power generation facilities might also be determined as efficient targets, if the network heavily depends on them. Without proper analysis, the attacker would likely need to target numerous power plants due to abundance of power generation, further complicating the operation and increasing the extent of the collateral damage. On the other hand, targeting distribution networks might not sufficiently create the desired effects since they provide power to a limited area and requires less time for system restoration. Therefore, they meet neither the space, nor the time requirements, of the intended blackout.

Several factors must be taken into consideration when trying to identify an efficient target set. In the first place, the number, connectivity, load level, and the load variance of the nodes are critical. An attacker should also be able to anticipate the adversary's consecutive moves to identify targets wisely; hence, reaction of the network, restoration plans, and possibility of repair must also be determined.

2.7.4 Intelligence

Nation states have already started to produce intelligence for conducting cyber attacks on critical infrastructures either in undercover [111] or public campaigns [104]. For this sake, an attacker should seek information in the four-layered PGC Domain (analyzed in section 2.4.1).

The information categories grouped in the domain consist of: physical location, power network structure, load distribution and variance, reaction plans, restoration plans and capabilities, and the hardware in Physical Layer; software, cyber network, and communication/security protocols in Logic Layer; cyber identities in Cyber Persona Layer; physical identities in Physical Persona Layer. The greater the fidelity of information collected about these categories, the more surgically precise the operations can be conducted.

Trying to identify vulnerabilities of the target is also part of the intelligence gathering efforts. Several methods exist for this sake. Utilizing known vulnerabilities that are released to public is a very efficient way, since power grid operators may not patch their systems in a short time for some reasons. Using scanning tools is another method to determine the vulnerabilities of target networks. Moreover, target system test bed laboratories and area-specific expertise could be incorporated to find vulnerabilities via fuzzing and reverse engineering tools. Information on specific system vulnerabilities is also available for purchase on the black market. Lastly, exploiting the insiders of vendor companies could enable reaching maintenance backdoors or the malicious insertion of access points to target networks.

Information gathering efforts in the PGC Domain must be conducted cautiously since their methods and techniques often resemble the same as conducting cyber attacks on the target. Hence, upon detection of information gathering activities, an adversary could presume an attack on its power grid is imminent or currently underway. This could unintendedly or prematurely escalate the situation.

2.7.5 Options

Cyber attacks against integrity and availability can create primary or secondary effects on a target power grid. VARC, WAM, and SE control systems of the transmission network; AGC and GC control systems of the generation facilities; and individual control devices in substations (e.g. circuit breakers, alarms, etc.) could specifically be targeted by these types of attacks. Integrity attacks can enable manipulation of sensor results or control commands which could actively destabilize or mislead the system operator to take erroneous actions. Availability attacks, on the other hand, would prevent sensor readings or control commands to reach the control center and sensors, respectively. Unfortunately, estimating the potential effects of these attacks is a challenging open research area which is a negative aspect of these options when they are compared to kinetic attacks.

2.7.6 Execution

Distances are irrelevant in cyberspace; hence, cyber attacks provide an invaluable advantage to an attacker when the depth of the target is a challenge. They also enable entry into the target area when by-passing conventional defenses is challenging. Even if an adversary employs state-of-the-art defensive mechanisms in cyberspace, the combination of numerous potential access points and entities in the network still creates vulnerabilities, since the system is only as secure as its weakest link.

The methods used to penetrate enemy defenses in cyberspace include web-based attacks, identity spoofing attacks, password attacks, supply chain attacks, social engineering, and exploiting insiders. Acquiring the tools to use these methods may require fewer resources when compared to the means required in kinetic attacks.

There are several existing factors that affect the efficiency of conducting cyber attacks. First, persistence of accessibility in the system is important for consecutive waves of attack. Second, it is important to remove or manipulate attack traces to alleviate harmful effects of attack detection. Third, the timing for target system penetration is critical to the success of the operation. Fourth, the risk of creating unintended consequences is another factor that must be taken into consideration for attack planners.

Chapter 3

Comparing the Means:
Kinetic Attacks and Cyber Attacks

Kinetic and cyber attacks are both capable of creating the desired effects of a military operation. However, even though they have similarities in some aspects, they also have many different challenges and opportunities. The optimum solution could be chosen among the various options: pure kinetic attacks, cyber attacks, or a combination of them depending on the intentions, requirements, and capabilities of the attacker. In this section, kinetic and cyber attacks will be compared by applying the steps of the methodology to analyze their challenges and differences.

3.1 Goals

In most cases, similar goals can be achieved by using either kinetic or cyber attacks; however, the opportunities of these attacks may differ in some aspects.

The disruption–destruction tradeoff is one aspect in which the benefits of kinetic and cyber attacks differ. Previous military operations have demonstrated that kinetic attacks can create disruptions (i.e. short-term power blackouts), yet they were often insufficient and inefficient. However, if an adversary's reaction plans and restoration capabilities are well-analyzed, then kinetically attacking a small set of targets would produce an effective blackout until restoration efforts are complete. On the other hand, cyber attacks would offer greater flexibility to create disruptions as described in previous sections.

On the destruction side of the balance, cyber attacks can also provide indirect effects such as issuing misbehaving commands to generators or preventing the proper functioning of circuit breakers which are responsible to protect the elements of the grid. Kinetic attacks on the other hand, could provide flexibility by allowing the attacker to destroy any chosen element directly, providing a level of destruction which could be predicted with high fidelity. In addition, kinetic attacks can also be used to heavily destroy the elements of the power grid in order to tighten the operation's squeeze on the adversary's leadership.

Another differing aspect between kinetic and cyber attacks is their effect on the human domain. The adversary leadership, the civilian population, and the international community are three groups that must be analyzed separately. Since the aim of an operation is typically to compel enemy leadership to respond in ways favorable to the attacker's campaign objectives, it is significant to be able to predict the effects of the attacks on them. The effects of kinetic attacks can be predicted with some confidence, even if imprecise [62]. Yet, the complexity of the cyberspace domain may prevent the enemy leadership from determining the attacks and consequences in the middle of a crisis, and hence could introduce unnecessary urgency and panic into the enemy leadership's decision-making process [62]. Conversely, the obscurity of cyber attacks may also result in underestimation of the extent of the attacks.

Predicting the effects of both kinetic and cyber attacks on civilians or human terrain is even more difficult than predicting its impact upon the leadership. The attacks could unite or dissolve the population depending on several psychological and sociological factors (e.g. culture). For example, the intended effects of the kinetic attacks in Operation Desert Storm were aimed to incite rebellion against the government, yet it turned out to create an anti-western stream in Iraq [89]. In addition, the fire and explosions created by kinetic weapons create much higher levels of horror and anxiety within the human terrain than would cyber attacks. Yet, just knowing the fact that they are under cyber attack might cause many people to feel desperate since it would decrease their confidence on conventional defensive systems. Lastly, the effects of both types of attacks may resonate differently on the international community, and hence impact the legitimacy of the operation. Attackers often provide footage of kinetic smart weapon usage that demonstrate that only the required level of damage was inflicted, thus collateral damage was prevented. Therefore cyber attacks may enhance these arguments by further reducing the number of casualties and emphasize the military necessity of the targets.

Cyber attacks could provide additional flexibility to an attacker by enabling an attack before the onset of hostilities in a conventional war. This would provide several benefits (section 2.1) for the attacker. From the defender's perspective, the complexity of the attribution problem may prevent conventional counterattacks. However, even without a clear attribution the victim of cyber attacks may choose cyber counterattacks for retaliation. In some cases, it could also result in further escalation of the situation since the attacks could be viewed as a precursor to open hostilities and a declaration of war. However, even if attribution of the attacks is correctly ascertained, which is unlikely, the obscure nature of cyberspace would provide deniability to the attacker as was evidenced by the Stuxnet attack on Iran's nuclear enrichment facilities [123].

Besides, because of the uncertainty of cyber attacks in the Law of Armed Conflict [119], it would potentially reduce the legitimacy of adversary counterattacks.

Additionally, the nature of the cyber realm makes it very difficult to implement a preemptive strategy for the defender [62]. Because preemption depends on the early detection of moves and then preventing those attacks by moving first, the challenges with detection and attribution will hinder preemptive movement. If a preemptive strategy were carried out in cyberspace, it would likely cause misattribution of the actors and intentions, as well as overreactions and miscalculations.

3.2 System Analysis

System analyses of the target power grid are crucial for both kinetic and cyber attacks. Kinetic attacks typically require the analyses of the physical infrastructure in order to improve the efficiency of the operation and reduce collateral damage. Cyber attacks on the other hand would require additional analyses of the control systems and cyber network; hence, cyber attacks would require additional resources to conduct a system analysis.

3.3 Targets

Targeting processes of kinetic and cyber attacks on power grids resemble each other for the most part; however, the targets and the expected effects would differ in some cases depending on their capabilities.

Improving the efficiency of the operation necessitates simulations of the target system for determining the effects of both kinetic and cyber attacks, and hence identifying the critical nodes of the system. The target sets for both types of attacks resemble each other and consist of the transmission, generation, and operations domains. For instance, target sets pertaining to the power grid during Operation Desert Storm were focused on "electric generation, transmission, and control facilities" [79] and they were attacked via kinetic means. For cyber attacks, potential targets are in the same target sets as kinetic ones (detailed information in section 2.3.1). Targeting in the power generation and transmission domains share similarities, but the targets in the operations domain differ. Cyber attacks could specifically target control systems to surgically inflict the desired level of failure or damage. However, kinetic attacks even when employing "smart weapons," would not achieve the same level of precision and could destroy the control

centers resulting in an unexpected level of consequences and possibly creating long term effects to restore all the complex control systems. On the other hand, there are more limitations on target selection for cyber attacks. To provide a better opportunity for mission success, a critical node should be selected as a target if the node is connected to cyber network or at least host a computerized control system.

3.4 Intelligence

Intelligence requirements for conducting kinetic and cyber attacks may overlap in some aspects, but they do vary in most respects. Since the targeting process needs information for simulations or at least to identify the targets, both attack types require intelligence on physical layer (detailed information in section 2.4.1). This layer entails physical location; power network structure; load distribution and variance; reaction plans; restoration plans and capabilities; and the hardware. Hence the same methods for gathering information for cyber attacks (section 2.4.2.1) are also valid for kinetic attacks.

To conduct efficient cyber attacks, an attacker would need additional information in the Logic Layer, Cyber Persona Layer, and Physical Persona Layer (section 2.4.1). The methods and tools for gathering information in these layers (section 2.4.2.1), and the methods for finding vulnerabilities to circumvent defensive mechanisms (section 2.4.2.2) are detailed in the respective sections.

Kinetic attacks, on the other hand, would require different information due to the difference in the environment that the attack will be conducted. After utilizing the information on the Physical Layer, primarily for targeting processes, an attacker would need additional intelligence information to assist in choosing payload options as well as attack execution to include numerous factors such as defensive mechanisms in different domains, geographical, meteorological variables, etc.

From a broader perspective, the type of intelligence required to support kinetic attack execution is more general and resource-consuming than cyber attacks in terms of the defensive mechanisms and evasive technologies. Yet, intelligence on these areas could be utilized to support the conduct of attacks, not only the power grid, but also other types of targets.

3.5 Options

Kinetic and cyber attack options could both meet time and space requirements of an intended power blackout in military operations; however, they have different specifications and limitations.

Kinetic attack options include different types of munitions (e.g. cluster bombs, bunker busters, etc.) that create various effects in terms of the level of destruction and range. They can physically destroy their targets, and those attacks can be effectively carried out on power grid targets in transmission, generation, and operations (section 2.2.3.1). In addition to their intended targets, they may also inflict collateral damage which would possibly lengthen the restoration time, and hence extend the blackout duration. In the planning phase of the operation, the amount of kinetic weapons required to destroy a certain facility can be predicted with high confidence. For instance, if an attacker drops a 500-pound general purpose bomb on a power plant, he can calculate and predict the resulting structural damage, the number of casualties, and the collateral damage [62]. This enables the attacker to efficiently plan his attack.

Cyber attacks, on the other hand, consist of various types of integrity and availability attacks (sections 2.5.1 and 2.5.2). While integrity attacks provide insertion, alteration, or deletion of the data; availability attacks aim to use up or overwhelm the resources of the system in order to delay or impede the system operations. These attacks can be carried out on data, devices, or databases which would create primary or secondary physical effects on the target systems (section 2.5.3). Calculation of potential damage of these attacks is still an open research area, yet damage assessments related to integrity [115] and availability [5] attacks do exist.

3.6 Execution

Execution of the operation requires overcoming the defensive mechanisms to deliver the identified payloads to the target sets. Since kinetic and cyber attacks are conducted in unlike domains, their struggles to overcome the different defensive mechanisms use distinctly different methods and tools. For instance, kinetic attacks have to overcome defensive mechanisms such as anti-air missiles, radar systems, and reinforced bunkers and will use electronic warfare capabilities, guided missiles, stealth aircraft, etc. to do so. On the other hand, cyber attacks use web-based, identity spoofing, password attacks and so on (section 2.6.1.2) to cope with firewalls, IDSs, IPSs, antivirus software, or security protocols. Therefore, both kinetic and cyber attacks have distinct challenges and opportunities relating to several factors.

The required time to execute an operation is one factor in which both types of attacks have different types of challenges. Kinetic attacks require time to deploy the respective assets to the conflict area. This process can take days or months. For instance, the deployment of forces for Operation Desert Storm required nearly six months [79], though this duration also depends on the anticipated scope of the operation. Cyber attacks also require time to intrude the target system which could take days to months.

Security of the assets that execute the operation is another key factor. Securely conducting kinetic attacks with aircraft requires physically destroying or electronically suppressing the respective defensive mechanisms which might cause damage or put the assets at risk. An attacker, if it had the resources available, could also use different technologies (e.g. cruise missiles) in order to protect its own forces. Cyber attacks, in contrast, do not put at risk its own personal conducting the attacks, yet it may expose risk to a cyber-weapon that could be detected and reconfigured by the adversary.

The cost of the operation is a critical factor in which kinetic and cyber attacks differ widely each other. Kinetic attacks require significant financial and industrial resources to acquire the assets to conduct an operation. For instance, unit cost of single Tomahawk cruise missiles reaches to $1.4 million [120]. Even for an attacker that intends to acquire advance technologies by providing money and know-how; it would take years to procure systems such as stealth fighters, cruise missiles, etc. The unconventional nature of cyber attacks provides a significant advantage from this perspective. They can even inflict more harm to conventionally-defended targets with a lower cost. For instance, an attacker could procure an exploit of a vulnerable SCADA system at a cost in the range of $40,000-$250,000 [108]. Not only are the delivery payloads more cost-effective in cyber attacks, but the cost of intrusion methods is also lesser compared to its kinetic counterparts (e.g. bribing a critical insider or cost of compromising supply chain vs. price of stealth fighter jet program). In addition to lower costs, cyber attacks do not require a high-tech, industrial base to produce the required elements; hence, nation states who's military technology is lagging could still use cyber attack as a stepping stone.

Lastly, political, legal, or "environmental" limitations create different effects on kinetic and cyber attacks. For instance, kinetic attacks may require using airspace or military bases of several countries. Refusal by one of these countries to cooperate may create significant impact regarding its criticality as was a factor in Operation Iraqi Freedom (2003) [121]. Moreover, certain international conventions may limit the conventional force deployments in specific areas. The Montreux Convention is a prime example; it is focused on the Turkish Straits and enforces

limitations on the tonnage and durations of deployments in Black Sea [122]. Meteorological conditions, labeled as “environmental” factors in physical space, can also limit the operation. For instance, thick clouds, violent winds, heavy rain, and blowing sand restrained the efficiency of targeting sensors in Operation Desert Storm [79]. “Environmental” limitations of cyberspace such as “isolated” cyber networks affect and heavily limit the execution of the operations. On the other hand, since legal regulations in cyberspace have not yet matured [119], cyber attacks can be conducted with fewer legal restrictions.

3.7 Conclusion

An attacker can use kinetic attacks, cyber attacks, or a combination of them depending on its intentions, requirements and capabilities. Kinetic and cyber attacks can successfully create blackouts that meet the space and time requirements of a military operation. Yet, since they have distinct features and challenges, they have different limitations and opportunities. Kinetic attacks enable an attacker to calculate the effects of the attacks on the target and human terrain; they can also physically destroy any chosen target with a properly selected weapon. On the other hand, cyber attacks reduce costs; do not risk the security of the assets; could be conducted prewar times, yet still provide deniability; and are independent from geographical distances. Therefore, any of the three available attack options could be selected depending upon the limitations of the specific situation in order to improve effectiveness and the efficiency of the military operation.

Chapter 4

Conclusions

The steps of conducting cyber attacks on a critical target for military operations, in this case, a power grid, was analyzed and the findings presented in Chapter 2, including the required tools, several methods, and critical factors for improving the efficiency. In addition, the capabilities, challenges and opportunities of cyber attacks were compared to its kinetic counterparts in Chapter 3. In this section, two critical issues of this thesis are discussed as closing remarks and topics for future work are presented for consideration.

4.1 Discussions

4.1.1 Effects on Civilians and Mission Success

A power grid is regarded as a significant target in military operations; since nearly every aspect of modern life depends on it. Because of this dependency, power blackouts can create severe effects on the human terrain depending on its duration. The primary services affected during a blackout would include: communications, transportation, water, food, and health. On the other hand, it could also interrupt the lines of supply; paralyze military communications; disturb mobilization efforts; degrade C4ISR efforts; make defending more challenging, especially for air defenses; undermine the enemy's offensive capabilities; and create a significant impact on the adversary's psychology from a military perspective. However, short term blackouts cannot provide these same operational benefits, since militaries are prepared for wartime scenarios. In Operation Desert Storm, the Iraqi power grid was heavily damaged and took years to restore. These attacks severely impacted the quality of civilian life and therefore created blowback effects which eroded the overall success of the operation. In an effort not repeat history, Allied military forces dropped Soft Bombs on the power grid targets during Operation Allied Force. Unfortunately for the Allied units, Yugoslavian restoration efforts from the effects of the Soft Bombs were completed within hours and the short duration of the intended blackout did not meet the military operational requirements. This case proved the significance of the tradeoff between disruption and destruction of power grids.

Now, cyber attacks are seen as a growing option to find a feasible solution to fulfill the military needs without creating long-term, severe adverse effects on the civilian population. The capabilities, methods, and tools of cyber attacks were discussed in Chapters 1 and 2, and the conclusion is they could indeed be successfully implemented for these types of operations. However, the problem was not the means identified in the historical case studies, it was the overall goals and target sets of those military operations that created unforeseen damage on the infrastructures. Kinetic attacks could very well have created blackouts for a reasonable time period by matching the required blackout duration to the restoration time for the targets if destructed. Since the effects of military operations extend beyond the military domain when civilian infrastructures are targeted, the required responsibility to authorize such attacks also exceeds the level that military decision makers should take. In other words, political leaders must take a greater initiative in defining goals and target sets. In this way, the operational planners could consider their goals and objectives in a broader perspective, rather than purely militarily. This shift in mindset would help the overall success of the operation. In addition, this method could lift the unnecessary burden from military decision maker's shoulders. However, one drawback of this solution must be addressed. Previous military operations have demonstrated that the slow target generation and approval process of civilian leaders hinders the military's ability to fight effectively and can reduce the overall success of an operation. Thus, the decision-making mechanism must be devised wisely to prevent delays which would reduce the efficiency of the operation.

4.1.2 Prominent Benefits of Cyber Attacks

Kinetic and cyber attacks are both capable of creating blackouts for various durations. As stated above, identifying goals and target sets are critical issues regarding the effects on civilians and mission success. The means that are used, kinetic or cyber, on the other hand, is critical when the attacker's and defender's capabilities are compared, since both attack types have distinct challenges and opportunities. The prominent benefits of using cyber attacks are discussed below.

Cyber attacks are unconventional. They are easy to acquire for several reasons. First, they are less expensive than kinetic attacks. The vulnerabilities and exploitation opportunities of target power grids can be researched by a small dedicated team or, in some cases, be purchased either legally or on the black market for a reasonable price. Second, they have lesser technological requirements for the builders. Conversely, for kinetic weapons, potential attackers have to have access to advanced technology and a strong industrial base in various fields to create an advanced weapon system, since purchasing these weapons would have several constraints from other

entities. Third, cyber attacks can be constructed in a reasonable time period compared with the years required of a kinetic weapon procurement processes.

In addition, cyber attacks direct the conflict to a distinct domain, cyberspace which makes a defending nation's meticulously designed conventional defenses ineffective. Therefore, cyber attacks provide a greater advantage when penetrating the adversary's defenses and are more cost-effective from various perspectives.

Cyber attacks also provide critical superiority when the distance to the target is a significant challenge. Their speed of action, combined with the irrelevancy of physical distances in the cyberspace, provide tremendous benefits when compared the required time, resources, and risks to deploy forces in the physical world. Moreover, cyber attacks present an option to the attacker for conducting the operation without risking the physical security of its assets. However, if the adversary does detect the attacks, there could be some capability loss.

Cyber means also prevent the defender from being able to implement preemptive strategies which further reduces the risks from the attacker's perspective. Since preemption depends on detecting early moves and preventing the attacks by moving first, the inherent challenges of detection and attribution in the cyber realm hinder a preemptive first move by a defender. If a preemptive strategy were to be carried out in cyberspace, it could cause misattribution of actors and intentions, overreactions, and miscalculations; therefore, preemptive moves in the cyber realm are less likely when compared with kinetic counterparts.

Launching cyber attacks with surgical precision could also improve the legitimacy of the operation. Although, power grids are military-critical targets, military operational planners are concerned about both the potential collateral damage and the international community's reaction. Because of these concerns, they could be reluctant to target a power grid in some military operations. Cyber attacks could address these concerns at some level and improve the legitimacy of the operation.

Cyber attacks could also enable attackers to disable large parts of a power grid even before the commencement of hostilities. Since national critical infrastructures depend heavily on each other, the loss of electricity over a wide area would likely drain the resources of the adversary. Therefore, these types of attacks would likely plunge the enemy into chaos and further delay their preparations for war. Still, these cyber attacks must be stealthy and their traces must be obfuscating in order to prevent clear attribution in case of detection. However, even in the rare chance the attacks do get attributed correctly, the obscure nature of cyberspace would provide

deniability to attacker. Besides, the uncertainty of cyber attacks in Law of Armed Conflict would likely diminish the adversary counterattack's legitimacy.

4.2 Future Work

The military methodology introduced in this thesis is able to comprehensively analyze the various steps of cyber attacks on power grids. One important step excluded from the military methodology used for this study is Battle Damage Assessment (BDA). It is the estimate of damage resulting from the application of military force [102] in combat operations. BDA aims to compare post-execution results with the expected results generated during target generation and weaponeering; it is composed of physical, functional, and target system assessment [102]. These assessments provide invaluable information for operational planning; hence, the tools and methods for BDA should be embedded in this methodology to achieve greater fidelity.

In addition, as stated in Chapter 3, a combination of kinetic and cyber attacks could enable the attacker to utilize both types of attacks. However, since each of the attack strategies presents various alternatives for attackers, a combination of them would provide numerous choices and allow additional flexibility for military planners. Therefore, future studies may want to examine the best methods and alternatives for effectively combining kinetic and cyber attacks.

The scope of this thesis reflects the military's offensive concerns that aim to conduct cyber attacks on power grids. However, as a result of the trend that militaries have been adopting cyber means for their combat operations, the role of protecting critical infrastructures from cyber attacks is also a growing concern for militaries. Analyses of defensive methods and techniques on cyberspace have been specifically and quantitatively studied [2, 46, 50, 128] so far. Yet, even there exist defensive strategies proposed for utilities [4, 23, 34], addressing the concerns of military's defensive side with a holistic qualitative methodology is required to fulfill similar objectives of this thesis.

References

[1] Staff of Congressmen E.J. Markey, and H. A. Waxman, "Electric grid vulnerability: Industry responses reveal security gaps," U.S. House of Representatives Report [Online], Washington D.C., May 2013. Available: http://democrats.energycommerce.house.gov/sites/default/files/documents/Report-Electric-Grid-Vulnerability-2013-5-21.pdf

[2] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K.L Butler-Purry, "Towards modelling the impact of cyber attacks on a smart grid," in *IEEE International Conference on Smart Grid Communications* [Online], October 2010, pp. 244-249. Available: http://psalserver.tamu.edu/main/papers/FinalSubmission_KunFenMasLiuZouButIJSN11.pdf

[3] E. Tikk, K. Kaska, K. Runnimeri, M. Kert, A. Taliharm, and L. Vihul, "Cyber attacks against Georgia: Legal lessons identified," Cooperative Cyber Defense Center of Excellence [Online], Tallinn, Estonia, Nov. 2008. Available: http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

[4] Electric Power Research Institute, "Analysis of selected electric sector high risk failure scenarios," National Electric Sector Cybersecurity Organization Resource [Online], First Version, Sept. 2013. Available: http://www.smartgrid.epri.com/doc/nescor%20detailed%20failure%20 scenarios%2009-13%20final.pdf

[5] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," Computer Networks, Jan 2013, pp. 1344-1371.

[6] K. Saalbach, "Cyber war methods and practice," Universitat Osnabruck [Online], Aug. 2013. Available:http://www.dirk-koentopp.com/downloads/saalbach-cyberwar-methods-and-practice.pdf

[7] I. Ghansah, "Smart grid cyber security potential threats, vulnerabilities and risks," California Energy Commission, Sacramento, CA, CEC-500-2012-047, May 2012. Available:http://www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf

[8] S. Baker, S. Waterman, and G. Ivanov, "In the crossfire: Critical infrastructure in the age of cyber war," McAfee Labs Report [Online], 2009. Available: http://www.dsci.in/sites/default/files/NA_CIP_RPT_REG_2840.pdf

[9] J. Bumgarner and S. Borg, "Overview by the US-CCU of the cyber campaign against Georgia in august of 2008," US Cyber Consequences Special Report [Online], Washington D.C., Aug. 2009. Available:http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

[10] J. G. Kassakian, W.W. Hogan, R. Schmalensee, and H. D. Jacoby, "The future of the electric grid," Massachusetts Institute of Technology Report [Online], 2011. Available: http://web.mit.edu/mitei/research/studies/the-electric-grid-2011.shtml

[11] Wikileaks document [Online], “Brazil: Blackout-causes and implications”, Dec. 2009. Available: http://wikileaks.org/cable/2009/12/09BRASILIA1382.html

[12] J. Weiss, *Protectign Industrial Control Systems from Electronic Threats*. Cupertino, CA; Momentum Press, 2010.

[13] K. Poulsen, “Slammer worm crashed Ohio nuke plant network,” Security Focus [Online], Aug. 2003. Available: http://www.securityfocus.com/news/6767

[14] C. Hadnagy and P. Wilson, *Social Engineering: The Art of Human Hacking* [Online]. Indianapolis, IN: Wiley Publishing, 2010. Available: ftp://91.193.236.10/pub/docs/linux-support/security/The%20Art%20of%20Human%20Hacking.pdf

[15] T. Koprulu, “Akilli sebekeler icin siber guvenlik,” presented at Cyber Security Conference-Cyber Security Academy [Online], Ankara, Turkey, Nov. 2012. Available: http://siberguvenlik.org/siberguvenlik_sunumlari/akilli_sebekeler_icin_siber_guvenlik.pdf

[16] C. Albanesius and L. Seltzer, “Report: Stuxnet worm attacks Iran, who is behind it?,” PC Magazine – Security Watch [Online], Sept. 2010. Available:http://www.pcmag.com/article2/0,2817,2369745,00.asp

[17] R. C. Owen, “Deliberate force: A case study in effective air campaign,” Balkans Air Campaign Study [Online], Air University, Maxwell Air Force Base, AL, Jan. 2000. Available: http://www.au.af.mil/au/awc/awcgate/au/owen.pdf

[18] A. Hildick-Smith, “Security for critical infrastructure SCADA systems,” SANS Institute Report [Online], Feb. 2005. Available: https://www.sans.org/reading-room/whitepapers/warfare/security-critical-infrastructure-scada-systems-1644

[19] A. Dreher and E. Byres, “Get smart about electrical grid cyber security,” Belden Inc., WPPTD-Security-012011, 2010.

[20] M. Govindarasu, A. Hahn, and P. Sauer, “Cyber-physical systems security for smart grid,” Future Grid Initiative White Paper [Online], PSERC Publication 12-02, May 2012. Available: http://www.pserc.wisc.edu/documents/publications/papers/fgwhitepapers/Govindarasu_Future_Grid_White_Paper_CPS_Feb2012.pdf

[21] R. Lordan, “Coordinated cyber-physical attacks, high impact low-frequency events, and risk management in the electric sector,” Electric Power Research Institute, Palo Alto, CA, Dec. 2012.

[22] M. G. Morgan, M. Amin, E. Badolato, W. O. Ball, A. B. Nae, and C. Gellings, “Terrorism and the electric power delivery system,”, National Research Council of the National Academies [Online], Washington D.C., 2012. Available: http://www.nap.edu/catalog.php?record_id=12050

[23] The Smart Grid Interoperability Panel – Cyber Security Working Group Staff, "Guidelines for smart grid cyber security: Vol. 1, smart grid cyber security strategy, architecture, and high-level requirements," National Institute of Standards and Technology [Online], NISTIR 7628, Aug. 2010. Available: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

[24] U.S. Department of Air Force Staff, "Targeting," Air Force Doctrine Document [Online], AFDD 3-60, July 2011. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA454614

[25] R. Fanelli and G. Conti, "A methodology for cyber operations targeting and control of collateral damage in the context of lawful armed conflict," in *Fourth International Conference on Cyber Conflict* [Online], 2012, pp. 319-331. Available: http://www.ccdcoe.org/publications/2012proceedings/5_5_Fanelli&Conti_AMethodologyForCyberOperationsTargeting.pdf

[26] U.S. Department of Army Staff, "The targeting process," Department of Army Field Manual, No:3-60, Nov. 2010.

[27] I. Ali and M. Thomas, "Substation communication networks architecture," in *Power System Technology and IEEE Power India Conference*, Oct. 2008, pp. 1-8.

[28] J. Yan, "Modelling and analysis on smart grid against smart attacks," M.S. thesis [Online], University of Rhode Island, Kingston, RI, 2013. Available: http://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1018&context=theses

[29] J. Wang and L. Rong, "Cascade-based attack vulnerability on the U.S. power grid," *Safety Science* [Online], Volume:47, Issue:10, pp. 1332-1336, Dec. 2009. Available:http://www.cse.psu.edu/~smclaugh/cse598e-f11/papers/wang.pdf

[30] X. Li, I. Lille, X. Liang, X. Lin, and H. Zhu, "Securing smart grid: Cyber attacks, countermeasures, and challenges," IEEE Communications Magazine, Volume:50, Issue:8, pp. 38-45, Aug. 2012.

[31] A. Teixeira, G. Dan, H. Sandberg, and K. Johansson, "A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator," VIKING Project [Online], Nov. 2010. Available: http://arxiv.org/pdf/1011.1828.pdf

[32] RT News Network Report [Online], "15 years on: Looking back at NATO's 'humanitarian' bombing of Yugoslavia," Mar. 2014. Available: http://rt.com/news/yugoslavia-kosovo-nato-bombing-705/

[33] G. Ball, "Operation Allied Force," U.S. Air Force Historical Studies Office, Fact sheet [Online], Aug. 2012. Available: httrp://www.afhso.af.mil/topics/factsheets/factsheet.asp?id=18652

[34] A. Gerra, "Security strategy that should be adopted by utilities for smart grid implementation before standards hit the industry," M.S. thesis, University of Colorado, Boulder, CO, 2010.

[35] J. L. Hieb, "Security hardened remote terminal units for SCADA networks," Ph.D. dissertation [Online], University of Louisville, Louisville, KY, May 2008. Available: http://digital.library.louisville.edu/utils/getfile/collection/etd/id/436/filename/437.pdf

[36] S. Amin, "On cyber security for networked control systems," Ph.D. dissertation, University of California, Berkeley, CA, 2011.

[37] V. M. Igure, "A taxonomy of security vulnerabilities in SCADA protocols," Ph.D. dissertation, University of Virginia, Charlottesville, VA, Jan. 2007.

[38] A. Kalam and A. Zayegh, "Network security vulnerabilities in SCADA and EMS," presented at IEEE/PES Transmission and Distribution Conference & Exhibition: Asia and Pacific, Dalian, China, 2005.

[39] B. Bencsath, G. Pek, L. Buttyan, and M. Felegyhazi, "Duqu: Analysis, detection, and lessons learned," presented at European Workshop on System Security [Online], Bern, Switzerland, April 10th, 2012. Available: https://www.crysys.hu/publications/files/BencsathPBF12eurosec.pdf

[40] Symantec Corporation, "W.32 Duqu: The precursor to the next Stuxnet," Security Report [Online], Nov. 2011. Available: https://www.symantec.com/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

[41] J. Walter and D. Sommer, "McAfee labs consolidated threat report: Duqu," McAfee Labs Report [Online], M66234, M65791, M65790, M65789, and M66239, Dec. 2011. Available: http://download.nai.com/products/mcafee-avert/dil/Duqu_CTR_v2.2f.pdf

[42] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," in *Proceedings of IEEE*, Volume: 100, Issue: 1, Dec. 2011, pp. 210-224.

[43] SANS Institute Staff, "Can hackers turn your lights off? The vulnerability of the US power grid to electronic attack," GSEC Practical Assignment [Online], 2001. Available: http://www.sans.org/reading-room/whitepapers/hackers/hackers-turn-lights-off-vulnerability-power-grid-electronic-attack-606

[44] UN Security Council resolution 1973 [Online], "Security Council approves 'no-fly zone' over Libya, authorizing 'all necessary measures' to protect civilians, by vote of 10 in favour with 5 abstentions," Mar., 2011. Available: http://www.un.org/News/Press/docs/2011/sc10200.doc.htm

[45] J. F. Burns, "British commander says Libya fight must expand," The New York Times [Online], May 15th, 2011. Available: http://www.nytimes.com/2011/05/16/world/africa/16libya.html?_r=0

[46] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks on countermeasures," IEEE Journal on Selected Areas in Communications [Online], Volume: 31, No: 7, July 2013, pp. 1294-1305. Available: http://acsp.ece.cornell.edu/papers/KimTong13JSAC

[47] Daily Mail Reporter, "'Cyber weapons are like the Ferrari you keep in the garage' says US official after decision not to use hack attacks in Libya," Daily Mail News [Online], Oct. 18th, 2011. Available: http://www.dailymail.co.uk/sciencetech/article-2050521/U-S-considered-cyber-warfare-attack-plan-Libya.html

[48] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," in *IEEE Power and Energy Society General Meeting*, July 2010, pp. 1-5.

[49] R. Pomeroy, "Iran's cyber foes cause problems for centrifuges," Reuters [Online], Nov. 29th, 2010. Available: http://www.reuters.com/article/2010/11/29/idUSLDE6AS1L120101129

[50] Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," in Proceedings of the IEEE [Online], Jan. 2012, pp. 195-209. Available: https://sparrow.ece.cmu.edu/group/pub/Mo-Kim-etal-ProcIEEE-2011.pdf

[51] Y. Yang, T. Littler, S. Sezer, K. McLaughin, and H.F. Wang, "Impact of cyber-security issues on smart grid," in *Innovative Smart Grid Technologies (ISGT Europe)*, Dec. 2011, pp. 1-7.

[52] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: Impact identification," in *American Control Conference* [Online], 2010, pp. 962-967. Available: http://www.dcsc.tudelft.nl/~bdeschutter/private_20100705_acc_2010/data/papers/1469.pdf

[53] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," Computer Networks [Online], Volume: 55, Issue: 15, 2011, pp. 3604-3629. Available: http://www.ece.ncsu.edu/netwis/papers/11wxk-comnet.pdf

[54] G. N. Ericsson, "Cyber security and power system communication – essential parts of a smart grid infrastructure," IEEE Transactions on Power Delivery [Online], Volume: 25, No: 3, July 2010, pp. 1501-1507. Available: http://www.csit.qub.ac.uk/media/pdf/Filetoupload,286696,en.pdf

[55] J. Walter, "Flame attacks: Briefing and indicators of compromise," McAfee Labs Report [Online], May 2012. Available: http://www.mcafee.com/us/resources/white-papers/wp-mcafee-skywiper-brief-v-1-6.pdf

[56] Kaspersky Lab Staff, "The Flame: Questions and answers," SecureList [Online], Kaspersky Lab Blog, May 28th, 2012. Available: https://www.securelist.com/en/208193522/The_Flame_Questions_and_Answers

[57] C. Wilson, "Information operations, electronic warfare, and cyberwar: Capabilities and related policy issues," Congressional Research Service Report for Congress [Online], Mar. 2007. Available: http://www.history.navy.mil/library/online/infoops_cyberwar.htm

[58] McAfee Labs Staff, "Careto attack – The mask," McAfee Labs Report [Online], Feb. 12th, 2014. Available: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25037/en_US/McAfee_Labs_Threat_Advisory_Careto_Attack_The%20Mask_3.pdf

[59] McAfee Company Staff, "Smarter protection for the smart grid," McAfee Labs Report [Online], 2012. Available: http://www.mcafee.com/us/resources/reports/rp-smarter-protection-smart-grid.pdf

[60] Control System Roadmap Steering Group, "Roadmap to secure control systems in the energy sector," Energetics Inc. Report [Online], Columbia, MD, Jan. 2006. Available: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/roadmap.pdf

[61] H. S. Lin, "Offensive cyber operations and the use of force," Journal of National Security Law and Policy [Online], Volume: 4:63, Aug. 2010, pp. 63-86. Available: http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf

[62] B. T. Williams, "Ten propositions regarding cyberspace operations," Joint Force Quarterly, Issue: 61, 2011, pp. 10-17.

[63] H. P. Sanghvi and M. S. Dahiya, "Cyber reconnaissance: An alarm before cyber attack," International Journal of Computer Applications [Online], Volume: 63, No: 6, Feb 2013, p. 36. Available:http://research.ijcaonline.org/volume63/number6/pxc3885202.pdf

[64] U.S. Industrial Control Systems Cyber Emergency Response Team, "Overview of cyber vulnerabilities," ICS-CERT Documents [Online]. Available:http://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

[65] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing* [Online], 2011, pp. 380-388. Available: http://bnrg.cs.berkeley.edu/~adj/publications/paper-files/ZhuJosephSastry_SCADA_Attack_Taxonomy_FinalV.pdf

[66] James McLinn Rel-Tech Group, "Comparison of major grid failures in United States and around the world," IEEE Reliability Society Annual Technology Report [Online], 2009. Available: http://electrical-engineering-portal.com/comparison-of-major-grid-failures-in-united-states-and-around-the-world-part-1?goback=%2Egde_3452357_member_5825318518035329026#%2

[67] European Smart Grid Technology Platform, "Vision and strategy for Europe's electricity networks of the future," European Commission Community Research Report [Online], EUR 22040, 2006. Available: ftp://ftp.cordis.europa.eu/pub/fp7/energy/docs/smartgrids_en.pdf

[68] The Global Smart Grid Federation Report [Online], 2012. Available: https://www.smartgrid.gov/sites/default/files/doc/files/Global_Smart_Grid_Federation_Report.pdf

[69] H. Farhangi, "The path of the smart grid," IEEE Power and Energy Magazine, Jan. 2010, pp. 18-28.

[70] M G. Simoes, R. Roche, E. Kyriakides, A. Miraoui, B. Blunier, K. McBee, et al., "Smart-grid technologies and progress in Europe and the USA," in *IEEE Energy Conversion Congress and Exposition (ECCE)*, Sept. 2011, pp. 383-390.

[71] Intelligent Utility Staff, "Smart grid spend to be concentrated in 10 countries," Intelligent Utility Magazine, Volume: 4, Issue: 2, p. 8, 2012.

[72] V. Giordano, A. Meletiou, C. F. Covrig, A. Mengolini, M. Ardelean, G. Fulli, and et al., "Smart grid projects in Europe: Lessons learned and current developments," European Commission Joint Research Center Report [Online], JRC79218, 2013.Available: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/ld-na-25815-en-n_final_online_version_april_15_smart_grid_projects_in_europe_lessons_learned_and_current_developments_-2012_update.pdf

[73] Energy Weekly News Staff, "Power market liberalization will facilitate the penetration of smart grid systems," VerticalNews, Aug. 2012.

[74] Office of the National Coordinator for Smart Grid Interoperability Engineering Laboratory Staff, "NIST framework and roadmap for smart grid interoperability standards," NIST Special Publication [Online], 1108R2, Release 2.0, Feb. 2012. Available:http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_20_corr.pd f

[75] W. M. Arkin, "Smart bombs, dumb targeting?," Bulletin of the Atomic Scientists, Volume: 56(3), 2010, p. 46.

[76] B. S. Lambeth, *NATO's Air War for Kosova: A Strategic and Operational Assessment*. Santa Monica, CA: RAND Press, 2001.

[77] W. M. Arkin, "Fog of war – Instant thunder," The Washington Post [Online], 1998. Available: http://www.washingtonpost.com/wp-srv/inatl/longterm/fogofwar/ resources. htm

[78] U.S. National Security Directive 54 (NSD 54) [Online], Jan. 15th, 1991. Available: http://www.fas.org/irp/offdocs/nsd/nsd54.pdf

[79] K. Chan et al., "Operation Desert Storm: Evaluation of the air campaign," U.S. Government Accountability Office Report [Online], GAO/NSIAD-97-134, June 1997. Available: http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB443/docs/area51_23.PDF

[80] B. Gellman, "Allied air war struck broadly in Iraq; Officials acknowledge strategy went beyond purely military targets," The Washington Post [Online], June 23rd, 1991. Available: http://www.globalpolicy.org/component/content/article/169/36375.html

[81] The Harvard Study Team, "Special report: The effect of the gulf crisis on the children of Iraq," The New England Journal of Medicine [Online], Volume: 325, No: 13, Sep. 1991, pp. 977-980. Available:http://www.nejm.org/doi/full/10.1056/NEJM199109263251330

[82] C. Rowat, "UN agency reports on the humanitarian situation in Iraq," Campaign Against Sanctions on Iraq Society Report, University of Cambridge, Aug. 2000. Available: http://www.casi.org.uk/briefing/000707versailles.pdf

[83] International Study Team on the Gulf Crisis, "Health and welfare in Iraq after the gulf crisis," International Study Team Report [Online], Oct. 1991. Available: http://www.cesr.org/downloads/Health%20and%20Welfare%20in%20Iraq%20after%20the%20Gulf%20Crisis%201991.pdf

[84] W. T. Shaw, Cybersecurity for SCADA Systems. Tulsa, OK: PennWell Books, Section 2, Chapter 7, 2006.

[85] R. Axelrod and R. Iliev, "Timing of cyber conflict," Proceedings of the National Academy of Sciences of the USA, Dec. 2013.

[86] G. M. Jackson, "Warden's five-ring system theory: Legitimate wartime military targeting or an increased potential to violate the law and norms of expected behavior?," Graduation report [Online], Air University, Maxwell Air Force Base, AL, 2000. Available: http://handle.dtic.mil/100.2/ADA425331

[87] S. Elliot, "Cyber warfare and the conflict in Iraq," Infosec Island [Online], Aug. 20th, 2010. Available: http://www.infosecisland.com/blogview/6750-Cyber-Warfare-and-the-Conflict-in-Iraq.html

[88] D. G. Vincent, "Being human beings: The domains and a human realm," Graduation report [Online], U.S. Army War College, Carlisle, PA, 2013. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA590280

[89] D. H. Berchoff, "Critical analysis of US policy and options in dealing with Iraq," Seminar report [Online], National War College, U.S. National Defense University, Washington D.C., 2003. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a442518.pdf

[90] D. L. Dittmer and S. P. Dawkins, "Deliberate force: NATO's first extended air operation – The view from AFSOUTH," Center for Naval Analyses Research Center Report [Online], Alexandria, VA, June 1998. Available: http://cna.org/sites/default/files/research/4500003200.pdf

[91] Information Clearing House, "Destruction to infrastructure that is vital for public health," U.S. Charged with War Crimes – The Evidence File [Online]. Available: http://www.informationclearinghouse.info/article3464.htm

[92] I. Watson, J. Karadsheh, and J. Duran, "Libyans struggle to cope with blackouts, gas shortages," CNN International [Online], Aug. 8th, 2011. Available: http://www.cnn.com/2011/WORLD/africa/08/libya.war.shortages/index.html

[93] E. Rouleau, "America's unyielding policy toward Iraq," Foreign Affairs [Online], Jan., 1995. Available: http://www.foreignaffairs.com/articles/50577/eric-rouleau/americas-unyielding-policy-toward-iraq

[94] S. Schmemann, "From president, victory speech and a warning," The New York Times [Online], June 11th, 1999. Available: http://partners.nytimes.com/library/world/europe/061199kosovo-clinton.html

[95] G. Gritsai, A. Timorin, Y. Goltsev, R. Ilin, S. Gordeychik, and A. Karpin, "SCADA safety in numbers v1.1," Positive Technologies Security Report [Online], Boston, MA, 2012. Available: http://www.ptsecurity.com/download/SCADA_analytics_english.pdf

[96] Kaspersky Lab Security Report [Online], "Unveiling Careto – The masked APT," Feb. 2014. Available: https://www.securelist.com/en/downloads/vlpdfs/ unveilingthemask_ v1.0.pdf

[97] Y. Sun and T. J. Overbye, "Visualizations for power system contingency analysis data," Power Systems, IEEE Transactions [Online], Volume: 19, No: 4, pp. 1859–1866, 2004. Available:http://www.pserc.wisc.edu/documents/publications/papers/2004_general_publications/cavisualizationpapermarch02ieee.pdf

[98] A. Berstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman, "Power grid vulnerability to geographically correlated failures – analysis and control implications," arXiv preprint arXiv:1206.1099 [Online], 2012. Available: http://arxiv.org/pdf/ 1206.1099v1.pdf

[99] T. D. Hansbarger, "Effects-based targeting: Application in Operation Desert Storm and Operation Iraqi Freedom," M.S. thesis [Online], U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2004. Available: http://www.dtic.mil/cgi-bin/ GetTRDoc?AD=ADA428905

[100] A. K. Sood and R. J. Enbody, "Targeted cyberattacks: A superset of advanced persistent threats," IEEE Security and Privacy Magazine, Volume: 11, No: 1, 2013, pp. 54-61.

[101] B. Gertz, "Dam! Sensitive army database of U.S. dams compromised; Chinese hackers suspected," The Washington Times [Online], May 1st, 2013. Available: http://www.washingtontimes.com/news/2013/may/1/sensitive-army-database-us-dams-compromised-chines/?page=all

[102] J. Andress and S. Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.* Waltham, MA: Elsevier, 2011.

[103] U.S. Joint Chiefs of Staff Publication, "Joint intelligence," Joint Publication 2-0 [Online], Oct. 2013. Available: http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf

[104] U.S. Presidential Policy Directive 20 (PPD-20) [Online], "U.S. Cyber Operations Policy," Oct. 2012. Available: http://epic.org/privacy/cybersecurity/presidential-directives/presidential-policy-directive-20.pdf

[105] M. Clayton, "Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage," The Christian Science Monitor [Online], Feb. 2013. Available: http://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage

[106] E. Savitz, "Humans: The weakest link in information security," Forbes Magazine [Online], Dec. 2011. Available: http://www.forbes.com/sites/ciocentral/2011/11/03/ humans-the-weakest-link-in-informationsecurity/

[107] U.S. Department of Army Staff, "Human intelligence collector operations," Field Manual [Online], FM 34-52, Sept. 2006. Available: http://www.fas.org/irp/doddir/army/fm2-22-3.pdf

[108] S. Frei, "The known unknown: Empirical analysis of publicly unknown security vulnerabilities," NSS Lab Report [Online], Austin, TX, Dec. 2013. Available: https://www.nsslabs.com/system/files/public-report/files/The%20Known%20 Unknowns_1.pdf

[109] U.S. ICS-CERT Report [Online], *ICS Monitor*, Dec. 2012. Available: http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monthly_Monitor_Oct-Dec2012_2.pdf

[110] CBS News 60 Minutes Report [Online], "Cyber war: Sabotaging the system," Nov. 2009. Available: http://www.cbsnews.com/news/cyber-war-sabotaging-the-system-06-11-2009/

[111] S. Harris, "China's cyber militia," National Journal [Online], May 2008. Available: http://www.nationaljournal.com/magazine/china-s-cyber-militia-20080531

[112] J. Adams, *The Next World War: Computers are the Weapons and the Front Line is Everywhere*. New York, NY: Simon & Schuster, 2001.

[113] M. Mylrea, "Brazil's next battlefield: Cyberspace," Foreign Policy Journal [Online], Nov. 15, 2009. Available: http://www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace/

[114] A. Giani, E. Bitar, M. Garcia, McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," IEEE Transactions on Smart Grid [Online], Volume: 4, No: 3, Sept. 2013, pp. 1244-1253. Available: http://bitar.engineering.cornell.edu/SGC_attack.pdf

[115] A. Giani, R. Bentl, M. Hinrichs, M. McQueen, and K. Poolla, "Metrics for assessment of smart grid data integrity attack," *IEEE Power and Energy Society General Meeting: Energy Horizons – Opportunities and Challenges* [Online], July 2012. Available: http://www.inl.gov/technicalpublications/Documents/5517252.pdf

[116] B. Fung, "The NSA hacks other countries by buying millions of dollars' worth computer vulnerabilities," The Washington Post [Online], Aug. 31, 2013. Available: http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/

[117] J. Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," CNN News Report [Online], Washington D.C., Sept. 26th, 2007. Available: http://www.cnn.com/2007/US/09/26/power.at.risk/r

[118] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," International Journal of Computer Science and Information Security [Online], Volume: 4, No: 1&2, 2009. Available: http://arxiv.org/ftp/arxiv/papers/0909/0909.0576.pdf

[119] K. Kinley, "What constitutes an act of war in cyberspace?," M.S. thesis [Online], Air University, Wright-Patterson Air Force Base, OH, 2008. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD= ADA480404

[120] M. Weisgerber, “Syria strike wouldn’t be cheap,” Defense News Magazine [Online], Aug. 28th, 2013. Available: http://www.defensenews.com/article/20130828/DEFREG02/308280030/Syria-Strike-Wouldn-t-Cheap

[121] A. F. Krepinevich, “Operation Iraqi Freedom: A first-blush assessment,” Center for Strategic and Budgetary Assessment [Online], Washington D.C., 2003. Available: http://www.csbaonline.org/wp-content/uploads/2011/03/2003.09.16-Operation-Iraqi-Freedom-Assessment.pdf

[122] Convention Regarding the Regime of the Straits Signed at Montreux [Online], July 20th, 1936. Available: http://sam.baskent.edu.tr/belge/Montreux_ENG.pdf

[123] Symantec Corporation, “W.32 Stuxnet dossier,” Security Report [Online], Feb. 2011. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[124] R. Mitchell, and I.R. Chen, "Behavior rule based intrusion detection systems for safety critical smart grid applications," IEEE Transactions on Smart Grid, Volume: 4, No: 3, 2013, pp. 1254-1263.

[125] R. Mitchell, and I.R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," IEEE Transactions on Reliability, Volume: 62, No: 1, 2013, pp. 199-210.

[126] S. Sridhar, and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," IEEE Transactions on Smart Grid, Volume: 5, No: 2, 2014, pp. 580-591.

[127] K.C. Sou, H. Sandberg, and K.H. Johansson, "On the exact solution to a smart grid cyber-security analysis problem," IEEE Transactions on Smart Grid, Volume: 4, No: 2, 2013, pp. 856-865.

[128] J. Kirsch, S. Goose, Y. Amir, D. Wei, and P. Skare, "Survivable SCADA Via Intrusion-Tolerant Replication," IEEE Transactions on Smart Grid, vol. 5, no. 1, 2014, pp. 60-70.

[129] L. Pottonen, “A method for the probabilistic security analysis of transmission grids,” Ph.D. dissertation [Online], Helsinki University of Technology, Espoo, Finland, April, 2005. Available: http://lib.tkk.fi/Diss/2005/isbn9512275929/isbn9512275929.pdf