SABOTAGE IN THE DIGITAL ERA

MARC LOSITO

MPP CANDIDATE '22
SANFORD SCHOOL OF PUBLIC POLICY
DUKE UNIVERSITY

PREPARED FOR:

OFFICE OF IRREGULAR WARFARE, USD-POLICY, DEPARTMENT OF DEFENSE

FACULTY ADVISORS:

DR. SIMON MILES
PROF. TIM NICHOLS

ABSTRACT

In the digital era, sabotage is an attractive tool to policymakers looking for strategic utility below the threshold of violence, with little to no interaction with the target nation, and a very low risk of escalation. This project analyzes sabotage policy and operations to provide the Office of Irregular Warfare with insight on "can, should, and how" the Department of Defense might approach sabotage in the digital era. The project utilizes chronological policy analysis to track the evolution of U.S. cyber policy from 2001 to 2021 and examines three case studies, selected from twenty-four possible, using a building block model to identify sub-theories on sabotage. In the analysis process, three characteristics of the digital era's nature of warfare are identified--the threshold of violence, interaction, and escalation. Finally, a sub-theory is presented comprised of intensity, speed, and control that is adapted to Clausewitz's Trinity of Warfare. This new sub-theory provides a novel approach to thinking about sabotage policy formation and operations. Finally, the project revisits the "can, should, and how" framework to provide a succinct summation of findings.

Keywords: Sabotage, Irregular Warfare, Policy, Department of Defense

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor Dr. Simon Miles of the Sanford School of Public Policy at Duke University. Without his assistance and guidance throughout this process, this project may have languished. Simon's door was always open when I wrestled with the concepts of the project, a problem with research, or struggles with putting thoughts into words. He consistently allowed this project to be my own work but steered me in the right direction whenever either of us thought I needed it. My sincerest thanks for your mentorship and friendship over these last two years with the hope of many years to come.

I would also like to show gratitude to Professor Tim Nichols of the Sanford School of Public Policy at Duke University as the second reader of this project. Tim's scholarship and course instruction in the field of national security policy made a strong impression on me as a student and shaped the development of this project from its inception. Thank you, Tim, and I look forward to your continued mentorship and friendship.

I would also like to acknowledge Mrs. Kathryn Lieb of the Richard B. and Kathryn C. Lieb Dean's Fellowship and Mrs. Marcia Carlucci and Mrs. Kristin Carlucci-Weed of the Marcia and Frank Carlucci National Security Fellowship. Their financial support was essential to my academic success at the Sanford School of Public Policy and allowed me to focus on scholarship and leadership. Thank you for all you do in honor of veterans, Duke University, and philanthropy.

This project would not be possible without the great people of The Office of Irregular Warfare and Counterterrorism. I would like to personally thank Ms. Milancy Harris and Mr. Daniel "Deak" Roh for sponsoring this project. I look forward to our paths crossing in the future and working on the nation's toughest problems.

Most importantly, this project required more than academic support, and I have to thank my children – Megan, Adeline, and Logan – and my partner, Mary Kate Bryant. My kids provide the single greatest respite from study that anyone could ask for. Anyone that follows my Instagram can attest that they keep me young, active, and beaming with pride and joy. My partner, Mary Kate, spent many months listening to (unsolicited) sabotage and great power theory. She provided much-needed humor and seemed to know when I needed to step away from the project. Cheese, her beloved Frenchie, has undoubtedly heard this project more than anyone else, hands down. Each of you has been my muse. My sincerest love and thanks to all of you.

PROJECT SNAPSHOT

In the digital era, what Irregular Warfare options are available to the DoD to compete below the threshold of violence with limited interaction while avoiding escalation?

OBJECTIVES

The Director of Irregular Warfare* (IW) is interested in the critical analysis of three policy questions.

1. Can the DoD conduct a campaign of sabotage in the digital era in lieu of armed conflict?
2. Should the DoD be bolder or more aggressive in the conduct of sabotage in the digital era?
3. How should the DoD analyze opportunities when considering sabotage in the digital era?

SCOPE

The "can, should, how" framework provides a blueprint for analyzing the foundations and gaps regarding:

1. Can We - do we have the requisite policy framework?
2. Should We - is sabotage a viable pursuit to national security ends below the threshold of violence?
3. How We - do we have a framework of strategic thought for sabotage policy and operations?

This project will address all three objectives. However, the project accepts limitations to address each component in its entirety, leaving ample opportunity for future work.

FUTURE WORK

"Can We"

Analysis of the legal regime and authority for the DoD to conduct sabotage outside of a declared state of war.

"Should We"

Analysis on DoD capabilities, readiness, and requirements to conduct sabotage in the digital era.

"How We"

Develop operational-level models to evaluate DoD sabotage campaigns and operations.

AT A GLANCE

Challenges

- Character of Warfare
- Technology Diffusion
- Intensity, Speed, Control

Opportunities

- Low-cost, High-yield
- Strategic Utility
- Turn Adversary Strengths to Weaknesses

"To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.."

Sun Tzu

The Art of War, Ch. 3

TABLE OF CONTENTS

INTRODUCTION

Executive Summary

Sabotage, a component of Irregular Warfare (IW), has been a historical and economic means to America's national security ends and is a core competency of the DoD.[1] The United States has executed sabotage with varying degrees of success and with varying degrees of integration with other national instruments of power. Likewise, geopolitical competitors have historically executed sabotage operations for various purposes and with varying degrees of success to achieve ends both complimentary and inimical to U.S. national interests.

Irregular warfare is an enduring, economical contribution to America's national security, and will remain an essential core competency of the U.S. Department of Defense.

Summary of the Irregular Warfare Annex to the National Defense Strategy

Technology has expanded the competitive space and accelerated the onset of "hybrid warfare" by offering adversaries the means to combine conventional and irregular capabilities. This construct challenges the U.S. comparative advantage below the threshold of war without provoking justified military action.

Short of war, and in careful coordination with U.S. partners and allies, sabotage remains a tool to address our primary, contemporary national security challenge: Great Power Competition. Particularly in cyber and space domains, sabotage is both a viable and effective tool to achieve U.S. strategic objectives without broaching the threshold of violence and mitigating escalation risks.

Great care should be taken to develop policy governing digital era sabotage and the operational employment of sabotage with an eye toward intensity, speed, and control. These three attributes interact in a Clausewitzian manner to form an interactive trinity that characterizes the nature of sabotage in the digital era.

PROBLEM STATEMENT

The digital era presents challenges to the conventional wisdom of warfare celebrated for centuries, namely in the nature and character of warfare.

The enduring nature of warfare – violence, interaction, and its being a fundamentally political endeavor – has been altered by the advent of the digital era and the implications of great power competition.[2] A core tenet of great power competition is to **employ nation-state tools below the threshold of violence and with limited interaction to the greatest extent possible to avoid confrontation and escalation**.[3] The digital era makes this possible, for all actors, in ways never before seen in warfare.

The character of warfare – described by Clausewitz as "more than a true chameleon that slightly adapts its characteristics to the given case" and "**the means by which war has to be fought**" – has been dramatically altered as technology diffuses traditional comparative advantages enjoyed by great powers.[4] Russia, China, Iran, and North Korea enjoy the proliferation of technology, as does the United States, disrupting the balance of power and leveling the balance of power dominated by the U.S. over the last century. Furthermore, as the digital era diffuses capability among great and rival powers, the character of warfare becomes more ambiguous in terms of the political and human dimensions while the existence of uncertainty expands to unparalleled heights.

In the digital era, what Irregular Warfare options are available to the DoD to compete below the threshold of violence with limited interaction while avoiding escalation?

As the DoD continues to adapt to the changing nature and character of warfare, priorities have shifted from counterterrorism to strategic competition. In concert with this shift, the Office of Irregular Warfare and the Assistant Secretary of Defense for Special Operations and Low-intensity Conflict seek options for low-cost, high-yield operations with strategic utility.

ASSUMPTIONS OF THE DIGITAL ERA

Warfare is Changing

The dawn of the digital era has altered the future operating environment, the character of warfare, and the very nature of warfare. State and non-state actors are able to blend conventional and irregular capabilities in new domains such as cyberspace and space.

Tech is Cheap

Technology once available only to large nation-states is becoming increasingly cheap and within reach of new adversaries. Financial, technical, and expertise barriers to acquiring advanced technology are diminishing.

Balance is Shifting

The digital era has expanded the ambiguity of the global landscape and disrupted the traditional balance of power between nation-states. Competing nations are using technology to challenge the international security dynamic and influence populations. Technology affords indirect approaches to challenge U.S. power without provoking international response while gaining influence in the regional balance of power.

The Enemy is Fast(er)

Rapid technology diffusion will allow adversaries to advance threats more quickly than ever before. The hyperconnected global battlefield provides adversaries with the opportunity to seize the initiative, offset U.S. strengths, minimize U.S. battlefield awareness, and pressure U.S. decision cycles. Access to technology allows nearly all actors to act first, fast, and adapt quickly.

A Core Assumption & Paradigm Proposal Intensity, Speed, and Control

Digital Era sabotage policy and operations will be subject to three interactive and negatively correlated attributes – intensity, speed, and control. Policy regarding sabotage operations in the cyber and space domains is relatively new and will struggle to find the optimal point of balance between these three attributes to meet the new characteristics of warfare – below the threshold of violence, limited interaction, and avoiding escalation. This project proposes a new paradigm of strategic thought for sabotage policy and campaigns through these three attributes, which are directly correlated to the outcomes of violence, interaction, and escalation.

METHODOLOGY

Research Design

There is a dearth of academic literature on sabotage, writ large. Sabotage, done well, is inherently difficult to detect and difficult to trace to its origin. As well, successful sabotage operations are likely undiscovered and contained in a classified environment. It is the cases of failure which loom largest. Given these challenges, the literature review for this topic is limited. This research is considered exploratory and follows a deductive research design.

This project will undertake two methods of analysis – chronological policy analysis and case study comparison.

First, the analysis of U.S. cyber policy during the digital era will set the policy landscape and provide an understanding of the "Can We" facet of this project.

Second, three case studies will be reviewed to provide a context of how sabotage has been used in the digital era and in great power competition providing an understanding of the "Should We" facet of this project.

The policy analysis and case studies will be examined through a building block theory design to identify and develop new sub-theories regarding sabotage policy and operations in the digital era.

The output of this research will be a novel interpretation of Clausewitz's interactive trinity adapted to sabotage policy and operations in the digital era. This sub-theory will provide a framework of thought and understanding toward the "How We" facet of this problem set. This model is intended to guide strategic thought in the development of Department-level sabotage policy and in the ASD-level guidance of sabotage campaigns. Further work may include the adaptation of critical factors analysis to aid in the operational-level development of sabotage campaigns and operations.

ANALYSIS

Policy Analysis Overview

U.S. cyber policy, over the last two decades, has become increasingly offense-oriented in both law and policy. The dominant explanation for this trend is a reactive posture by U.S. legislators and policymakers responding to the last significant cyber event. Post-facto law and policy formation has not provided the desired defensive protections for future threats, which normalizes an offensive policy landscape. Seven qualified congressional or executive actions are analyzed to form a chronological accounting of modern U.S. cyber policy from 2001 to 2021. This chronological analysis indicates a marked string of policies leading to the offensive posture and forward-leaning nature of U.S. cyber policy.

Homeland Security Act of 2002

In response to the September 11th, 2001, terrorist attacks, the federal government rightly acknowledged the inadequacies in how the nation was postured to defend its citizens against terrorism and cyber-attacks. The U.S. responded with the creation of the Department of Homeland Security (DHS) and the Homeland Security Council; the largest reorganization of the federal government in more than half a century. The 9/11 Commission would canonize the phrase, “the system was blinking red,” as President Bush responded to an overpowering public sentiment to address enormous vulnerabilities in national defense.[5] Chief among these vulnerabilities were U.S. critical infrastructure sectors with special concern for cyberterrorism and securing cyberspace. Consequently, the Homeland Security Act of 2002 included the addition of a cybersecurity organization within DHS. The National Cyber Security Division (NCSD) was created as an amalgamation of previously existing federal directorates performing disparate functions without coordination or communication.[6]

Upon its inception, NCSD was plagued by organizational and leadership challenges. The Homeland Security Act of 2002 imbues the NCSD with inherent contradictions, likely the result of committee compromises required for passage. As the first significant restructuring of federal cybersecurity functions in the United States, the act fails to provide consistent language and delineate authorities pertaining to cybersecurity functions. Namely, the act identifies DHS’s first responsibility as preventing terrorism and cyberattacks in the United States, but only assigns DHS an analytical and advisory role for intelligence activities concerning terrorism and cyber activity. The act’s language makes clear the Federal Bureau of Investigation (FBI) maintains investigatory and prosecution authorities.

POLICY ANALYSIS (CONTINUED)

In this same vein, the act gives DHS a broad mandate to minimize damage to U.S. critical infrastructure but only limited authority to share information and coordinate with the private sector—a major stakeholder in the operation of U.S. critical infrastructure.

Moreover, the NCSD has struggled with leadership absenteeism and turnover. Richard Clark, the 2002 Special Advisor to the President on Cyber Security, refused the first-offered NCSD Director position, presciently citing concerns of "too many bureaucratic layers between NCSD and the Homeland Security director [Secretary] Tom Ridge." Clark keenly understood the leadership challenges presented by the Homeland Security Act of 2002 language, whereby NCSD was tucked under the organizational hierarchy of the DHS Office of Cyber Security and Communications. Charged with carrying out most of DHS's cyber protection responsibilities and statutorily responsible for activities within the Comprehensive National Cybersecurity Initiative (National Security Presidential Directive 54/Homeland Security Presidential Directive 23), NCSD leadership was fraught with the ineptitude that Clark feared as a result of being too far down the organizational chain of command. In fact, NCSD would see three leaders come and go within the first two years of its inception. Largely thought of as a powerless position, multiple resignations and abrupt departures from the NCSD directorship point to a symptom of a greater problem—the position does not have the legislative or organizational authority to set priorities, develop strategic plans, or provide effective leadership in cyber-related matters.

Cybersecurity Act of 2012 and Presidential Policy Directive 20

The Cybersecurity Act of 2012 was a comprehensive proposal seeking to protect both government and industry from foreign cyberattacks by achieving three ends: (1) new threat-information-sharing between government and private industry, (2) better protection of critical infrastructure, and (3) DHS authority to unite federal resources to lead U.S. cybersecurity.[7] Given the disjointed state of cybersecurity at the federal level, in part due to the Homeland Security Act of 2002, the overarching policy goals of the Cybersecurity Act of 2012 appear to right-size both legislation and policy toward a unified cyber defense.

POLICY ANALYSIS (CONTINUED)

The act would do this through two major overhauls of flawed legislation. First, the act amends the Homeland Security Act of 2002 to consolidate existing federal resources for cybersecurity within a DHS National Center for Cybersecurity and Communications. The act sets forth the duties of the Center, including managing efforts to secure, protect, and ensure the resiliency of the federal information infrastructure, supporting private sector efforts to protect such infrastructure, prioritizing efforts to address the most significant risks to the information infrastructure, and ensuring privacy protections. Second, the act amends the Federal Information Security Management Act of 2002 (FISMA) to revise information security requirements for federal agencies and provide for continuous monitoring of, and streamlined reporting of, cybersecurity risks.

Specifically, the Act directs DHS to, in consultation with owners and operators of critical infrastructure, the Critical Infrastructure Partnership Advisory Council, and other federal agencies and private sector entities, (1) conduct a top-level assessment of cybersecurity risks to determine which sectors face the greatest immediate risk, and beginning with the sectors identified as having the highest priority, conduct, on a sector-by-sector basis, cyber risk assessments of the critical infrastructure; (2) establish a procedure for the designation of critical infrastructure; (3) identify or develop risk-based cybersecurity performance requirements; and (4) implement cyber response and restoration plans. Further, the act sets forth a policy definition and requirements for critical infrastructure, including notification of cyber risks and threats and reporting of significant cyber incidents affecting critical infrastructure.

However, Congress missed this opportunity to strengthen U.S. cybersecurity within the existing civil-military relations framework. Instead, two months after the legislation was voted down in the Senate, President Obama signed Presidential Policy Directive 20 (PPD-20)[8], directing the Pentagon to take aim at our enemies with cyberweapons and set the stage for cyber operations into third countries not currently the site of active hostilities. This marked a wholesale shift in our cyber defense strategy from a "defense in depth" scheme to a "best defense is a good offense" scheme.

POLICY ANALYSIS (CONTINUED)

PPD-20 ensured the continuing framework of control, requiring presidential approval for all cyber operations, but also instituted intense interagency vetting. This ensured the scope and scale of operations were maximized for effect, coordinated with other instruments of national power, integrated into a coup de main stratagem, and considered on all facets for risk of escalation. PPD-20 did, however, sacrifice speed as a significant cost. The intense interagency process required multiple rounds of input across the national security community, which is detrimental in the digital age where opportunity is often fleeting.

Lastly, PPD-20 tacitly advanced the notion of the cyber domain as a battlefield requiring capabilities for the "full spectrum of conflict." This notion, as we will see, will crystalize in the 2018 National Cyber strategy as "continuous competition…in cyberspace" and in the Department of Defense Cyber Strategy in a concept to be known as "defense forward."

2018 National and DoD Cyber Strategies

The 2018 National Cyber Strategy and accompanying 2018 DoD Cyber Strategy reflect the changing political, technical, and cyber threat evolutions that occurred between 2015 and 2018.[9] Maturation and proliferation of cyberattacks at scale, such as Wannacry and Petya, and the inherent national security risks, such as the 2016 U.S. Presidential election meddling by Russia, exemplify the growing cyber threat confronting the United States during this time period.

The 2018 National Cyber Strategy draws attention and focus to great power competition, specifically with China, Russia, Iran, and North Korea. Within Pillar III —Preserve Peace through Strength—a throwback to President Ronald Reagan's Cold War mantra for increased military posturing, the National Cyber Strategy contextualizes a "continuous competition" with great powers and rogue states using cyberspace to challenge the United States, often with a recklessness they would never consider in physical domains.[10] As a national cyber policy document, the undertones of competition, conflict, and deterrence set the conditions—and potentially begged the question—for further military leadership of cyber policy and action.

POLICY ANALYSIS (CONTINUED)

Finally, the strategy's enumeration of the "Big 4" cyber competitors—China, Russia, Iran, and North Korea—would set the table for future legal considerations of cyberwarfare, as we'll see in the John S. McCain National Defense Authorization Act.

The 2018 DoD Cyber Strategy draws upon PPD-20 and the National Cyber Strategy to codify the offensive-oriented gains in U.S. cyber policy. The strategy cribbed the premise of PPD-20's call to military cyber action, by proclaiming the cyber domain as a warfighting domain. Specifically, the strategy uses elements of PPD-20 to characterize an armed conflict in cyberspace that requires the Joint Force to "employ offensive cyber capabilities…across the full spectrum of conflict."[11] More importantly, and previously foretold in PPD-20, the strategy crystalized the notion of "defense forward" to disrupt or halt malicious cyber activity at its source, foreign territory. Taken from the counterterrorism playbook, the grand idea of defense forward is to take the fight to the cyber enemy before they can reach U.S. critical infrastructure.

John S. McCain National Defense Authorization Act of 2019

In direct response to Russian election meddling in the 2016 U.S. Presidential election, the John S. McCain National Defense Authorization Act of 2019 (NDAA'19) placed the DoD firmly in charge of cyber activities abroad with post-facto oversight —referred to as "defense forward." Then-National Security Advisor John Bolton best summarized these changes when he outlined how the new National Cyber Strategy had replaced restrictions on the use of offensive cyber operations with a legal regime that enables the DoD and other relevant agencies to operate with a greater authority to penetrate foreign networks to deter hacks on U.S. systems. Bolton goes on to discuss the autonomy given to executive agencies, that "decision-making for launching [cyber] attacks will be moved down the chain of command from requiring the president's approval."[12]

The legal concept of "defense forward" builds on the offensive underpinning of PPD-20 and the policy pretexts of the national cyber documents; more importantly, it contemplates DoD cyberwarfare activities that are not part of an armed conflict. First, Section 1632 of NDAA'19 eliminates all doubt that DoD is precluded from conducting unattributed cyber operations with effects outside of combat zones.[13]

POLICY ANALYSIS (CONTINUED)

Historically, unattributed operations outside of combat zones required a covert action finding and congressional notification under Title 50. Therefore, Section 1632 is unequivocal in categorizing DoD offensive cyber operations outside of combat zones as Traditional Military Activity (TMA) which does not require a finding or prompt congressional notification. Second, Section 1642 of NDAA'19 provides expressed authority—referred to as "active defense"—for DoD "to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter" cyberattacks involving China, Russia, Iran, and North Korea, previously enumerated as the "Big 4" cyber competitors.[14]

Finally, the notification and reporting requirements levied by NDAA'19 for cyber warfare activities considered "active defense" provides for an element of speed. NDAA'19 requires Commander, U.S. Cyber Command to provide a quarterly, post-facto summary of cyber warfare activities to congressional defense committees and an annual, post-facto summary to congressional intelligence committees and the Senate Foreign Relations Committee. Speed is often quoted as the quintessential element of preparedness against cyberattacks.

NDAA 2020

The National Defense Authorization Act of 2020 is an example of Congress achieving small victories, however unrecognized, to build a domestic framework to govern military cyber operations. The Act refines the definition of "Sensitive Military Cyber Operations" (SMCO) to establish that these operations do not constitute covert action for purposes of U.S. domestic law even when conducted on a deniable basis. They are however subject to a notification process modeled on the 48-hour "covert action notification" without the interagency notification requirement and with the oversight running through the Armed Services Committees instead of the Intelligence Committees.[15]

This small but significant adjustment to U.S. cyber policy eliminates interagency friction in obtaining approval for U.S. Cyber Command operations, even if they have the qualities of covert action. This fine-tuning of the policy affords significant speed to military cyber operations, but may sacrifice control and scale of effects as a trade-off.

CASE STUDY ANALYSIS

The case studies selected for this project will examine historical instances of sabotage in the digital era. Twenty-four Case studies have been screened for six selection criteria. All case studies are drawn from publicly available information and verifiable sources. There is an acknowledgment that public knowledge of sabotage operations may connote a constraint to less than successful sabotage operations; sabotage operations, by their very nature, are covert at best, clandestine by necessity, and compromised at worst. Public knowledge of sabotage operations does not indict an operation as a failure but indicates the operations may have earned a less than pristine evaluation.

First, the case study must involve a sabotage event where a status quo (SQ) and non-status quo (NSQ) nation-state are identifiable (or alleged). This ensures each case study can identify, to some extent, the state that prefers to keep things the way they are and the state that is revisionist. Second, the act of sabotage is conducted by a nation-state or state-sponsored organization under some modicum of control by the nation-state. This ensures the act of sabotage is likely tied to a national end. Third, the SQ and NSQ countries must be peer entities, as characterized by the Organisation for Economic Co-operation and Development (OECD). This ensures the act of sabotage is conducted between two relatively equal opponents in a multi-polar setting. Fourth, the act of sabotage must be part of an identifiable coup de main strategy, as opposed to an individual act of sabotage. This is important to understand the value of sabotage as a campaign or as part of a larger strategic campaign involving sabotage. Fifth, the threshold of violence and/or interaction must be identifiable. This is important in evaluating the interaction and value of sabotage as a tool below the threshold of violence. Sixth, escalation or confrontation must be identifiable, which is important in evaluating the risk of sabotage operations as an escalatory measure.

Criteria one through three are straightforward, easily identifiable as a matter of public record, and do not require in-depth evaluation. Criteria four through six are identifiable but require qualitative evaluation to determine their degree and overall impact on the utility of the operation. These immediate findings are provided at the conclusion of the case study section.

CASE STUDY 1 - SIBERIAN PIPELINE

President Francois Mitterand greets President Ronald Reagan

In July of 1981, French President Francois Mitterand offered President Ronald Reagan an opportunity to collaborate on a spy effort, codenamed Farewell. Colonel Vladimir Vetrov (Farewell) was a KGB defector that provided the French *Direction de la Surveillance du Territoire* (DST) with approximately four thousand classified documents from 1981 to 1982.[16] The documents contained soviet organizational secrets, intentions, capabilities, and technical data. More important to this case study, the dossier contained information on operations conducted by Line X and intelligence provided to Directorate T within the KGB. Line X was the KGB's operational effort to steal technology and software from the West in support of the ongoing arms and space races. Directorate T was the organizational element overseeing KGB scientific and technical collection from the West.

Colonel Vladimir Vetrov

Farewell, an engineer assigned to evaluate the technical "take", provided the French DST with information on Line X operations, Line X operative identities, and Directorate T technical requirements. Among these technical requirements, colloquially termed "the shopping list," counterintelligence and sabotage operations seemed plausible. All in all, Line X had been successful in fulfilling two-thirds of its technology intelligence requirements, an impressive feat.[17] The Farewell Dossier shook the confidence of the CIA and immediately brought technology transfer to the fore of the intelligence community's radar. The CIA established the Technology Transfer Intelligence Center and the Pentagon established small cells to assess the damage Line X had already caused. The CIA and National Security Council, represented by Gus Weiss and Thomas Reed, respectively, saw an opportunity in Russia's desire for Western technology and the LineX shopping list.[18] Line X and Directorate T's hunger for Western technology might overshadow any question about the provenance of its origin.

SIBERIAN PIPELINE (CONTINUED)

As the Farewell Dossier reached the CIA and the NSC, U.S. rhetoric regarding a planned Trans-Siberian gas pipeline was growing increasingly caustic. There was substantial fervor surrounding the European financial backing being given to Moscow for the project, which would transport natural gas from Siberia to Europe. The United States' geostrategic fear was that the project would give the Communists control over European energy supplies and funnel Western capital and dual-use technologies into Russian research and armament programs.[19] The U.S. estimate of economic capture was approximately USD$8 billion and it was projected the revenue would be used to finance satellite research.[20]

The Farewell Dossier provided an opportunity to take action against an economic target of U.S. political concern. The Line X shopping list included, among other items, pipeline turbines and software for (1) supervisory control and data acquisition (SCADA) and (2) distributed control systems (DCS).[21] The CIA now had three points of entry, one hardware and two software, to sabotage the Trans-Siberian pipeline through a concerted sabotage operation.

"U.S. Intelligence, tipped by Farewell, and in cooperation with some outraged Canadians, 'improved' the software before sending it on."

Thomas C. Reed

In 1982 and in concert with the French and Canadians, the United States took action and initiated a sabotage plot. The CIA allowed Line X to steal SCADA and DCS pipeline control software from a Canadian company. Unbeknownst to the Russians or the Canadian commercial proxy, the CIA included a logic bomb in the software.[22] The logic bomb was designed to run during a pressure test of the pipeline and double the normal pressure while maintaining safe but misleading readings. In June of 1982, the plan worked brilliantly, causing an explosion in the Trans-Siberian pipeline so great in magnitude that it could be observed from space.[23]

SIBERIAN PIPELINE (CONTINUED)

The sabotage operation had two immediate effects. The first was economic and cut to the core of the Soviet leviathan. By creating an explosion with the power of a three kiloton nuclear weapon, the US disrupted supplies of natural gas and the consequential foreign currency earnings it was intended to reap, at approximately USD$8 billion.[24] Moreover, the anticipated revenue could not be funneled into arms and space research, which was defining the Cold War and shaping great power status. The sabotage of the Trans-Siberian pipeline was cold-eyed economics, meant to inflict a price on the Soviets.[25]

Second, the project also had important psychological advantages in the battle between the two superpowers. Line X had been in the business of pilfering U.S. technology and thought they had been successful in their pursuits. The Trans-Siberian pipeline explosion placed doubt as to how many more ticking timebombs were lurking in stolen technology. The Soviets had no way of knowing which equipment was sound; all equipment was suspect, which was the intended endgame for the entire operation.[26]

Finally, the economic and psychological effects were amplified by coordinated actions of national power. The CIA, in concert with European and NATO intelligence services, used the Farewell Dossier to expel or compromise approximately 200 Line X operatives, worldwide. This not only blinded KGB technical intelligence collection efforts but created far more moving pieces for the Soviets to address while reeling from the sabotage. To this point, the sabotage and Line X compromises took place just as President Reagan was announcing the largest U.S. technical effort to date, the Strategic Defense Initiative (SDI), and the introduction of stealth aircraft into U.S. forces.

CASE STUDY 2 - GEORGIAN WAR 2008

The war between Georgia and Russia (and the Russian-backed breakaway provinces of South Ossetia and Abkhazia) is regarded as the first European war of the 21st century.[27] It is also unique in that it is the first known occurrence of cyber-sabotage being used as an element of combined arms warfare.[28]

Map of the Russo-Georgian War

The conflict between Georgia and Russia dates back hundreds of years and is complicated by intertwined ethnic populations sharing culture, language, and religion. These ethnic populations have been subject to the Mongols and the Russian Empire, and have been geographically divided by the Bolshevik Revolution and the fall of the Soviet Union, to name a few. The 2008 crisis was a product of an increasingly Western-leaning Georgia exercising liberal energy and trade policies antithetical to the Russian ends.[29] In 2008, Georgia's desire to join NATO pushed Russia to declare support for the separatist populations of South Ossetia and Abkhazia. A series of diplomatic, military, and economic maneuvers by both Georgia and Russia escalated the confrontation to a full-blown crisis in August of 2008.[30]

At the strategic level, the Russian cyberspace reconnaissance and probing attacks began weeks prior to the actual inception of virtual and physical combat, akin to Phase 0 operations in preparation for war. The cyber probing actions began with the Georgian President's website coming under a Distributed Denial of Service (DDoS) attack from Russia's state hackers in July 2008.[31] There are several practical reasons to conduct probing attacks at this scale and level. First, the probe target must have been significant enough to warrant a reaction to gauge the real-time response from the Georgian cyber authorities. Second, the DDoS attack on President Saakashvili's website permitted Russian cyber elements to observe response measures and evaluate Georgian cyber defenses.

GEORGIAN WAR 2008 (CONTINUED)

Finally, Russia may have needed to evaluate the impacts on Georgian internet infrastructure for future, planned cyber actions in the impending combined arms war. Georgian internet infrastructure was relatively undeveloped, so the scale and effect of cyber warfare may have been unknown to Russian war planners. Following this probe attack, Russian websites, chat rooms, and networks discussed the upcoming attacks for several weeks prior to the first shot being fired.

Russian Cyber Sabotage Comparing President Saakashvili to Adolf Hitler

Meaningful sabotage of Georgia's Internet infrastructure began on July 20, a full ten days before the first shot was fired.[32] The cyber phase began with a coordinated DDoS attack overloaded and effectively shut down Georgian servers. Alleged Russian cyberattacks impaired Georgian communications and media companies, the National Bank, and transportation companies. Russia maintained plausible deniability throughout the initial campaign by using Russian and Turkish commercial servers to route traffic and attacks. These extensive preparatory actions imply a strategic planning process that began long before July 2008, to incorporate cyber warfare into the combined arms model. By the time the first artillery round fell on August 1, 2008, Russia had successfully muffled Georgia's ability to coordinate a wartime response, coordinate with allies and sympathizers, mobilize needed resources, and communicate with itself and its people.[33]

During active hostilities, Russian cyber-sabotage efforts were able to simultaneously attack thirty-eight Georgian government and financial websites, connoting a centralized control of the attack. The attacks included the defacing of websites (hacktivism), web-based Psychological Operations (PsyOps), a fierce information warfare campaign, and continued DDoS attacks on political and economic targets. [34] Lastly, the attacks were occurring at a localized level that coincided with the Russian troop movement inside Georgia, suggesting government and military coordination of the attacks in a combined arms maneuver. Russia's ability to coordinate cyber sabotage with irregular and conventional operations amplifies the effects of the sabotage as a coup de main component.

GEORGIAN WAR 2008 (CONTINUED)

Finally, while Russia's cyber sabotage efforts in before and during the Georgian War were crude, they were effective. No country had ever before so openly combined hacker disruption tactics with traditional warfare. Georgia was the first crude experiment in a new flavor of hybrid warfare that bridged the digital and the physical.

CASE STUDY 3 - OLYMPIC GAMES

Operation Olympic Games, and the associated Stuxnet worm, are thought to have been a joint cyber-sabotage operation between the U.S. and Israel, targeting Iran's nuclear centrifuges. However, to the date of this project, there has been no official credit or evidence to assign attribution to a nation-state. Stuxnet, the computer worm associated with Olympic Games, is thought to have been developed as early as 2005 and was discovered in 2010. Stuxnet was considered a game-changer as the first worm of its kind--a discriminant, weaponized cyber sabotage tool targeting precise subsystems of industrial control systems.

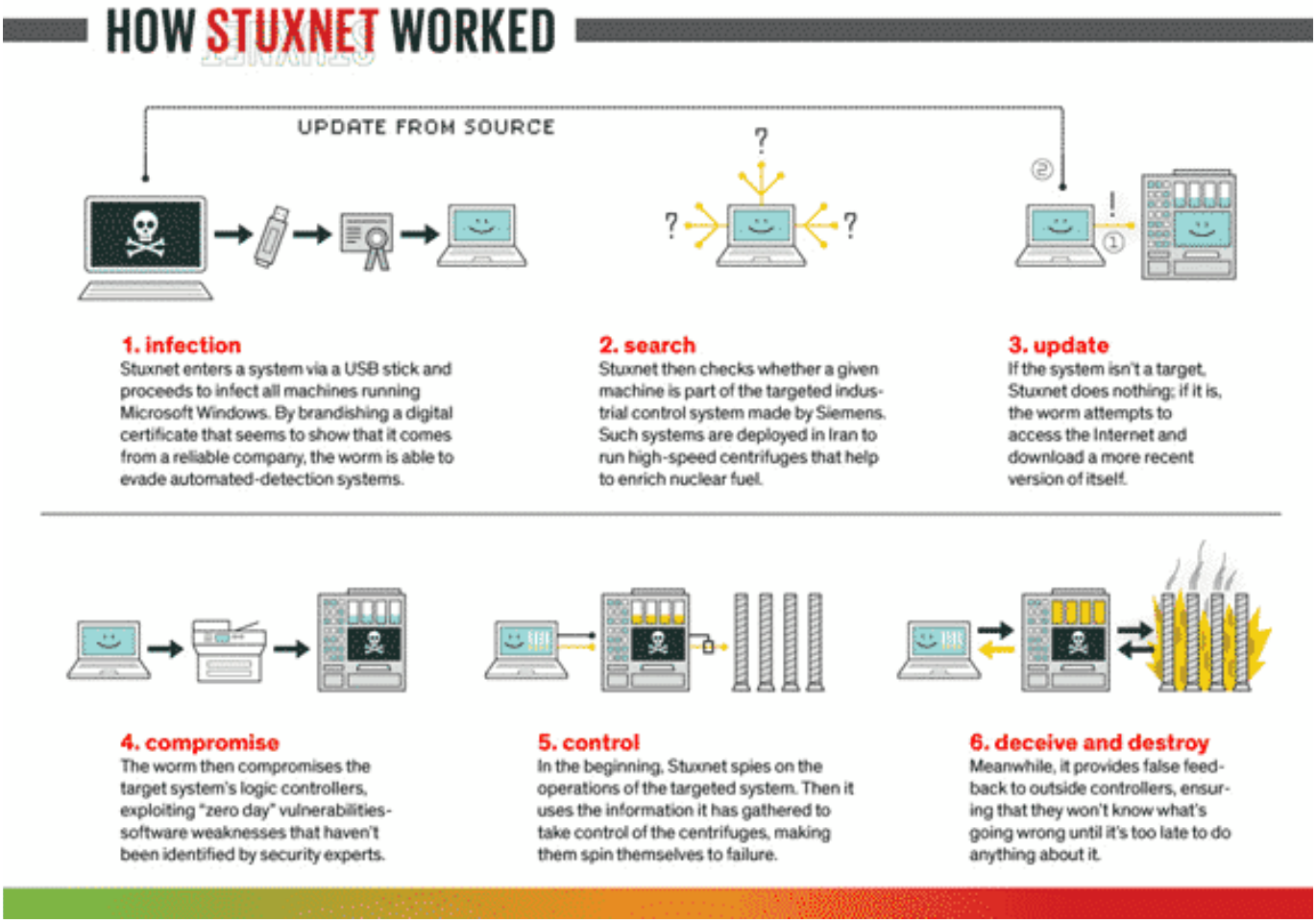
The genius of Stuxnet was in its multi-module composition, criteria-based infection, and criteria-based attack. Stuxnet modules are identified as the (1) worm module, (2) link module, and (3) rootkit module.[35] Upon introduction into the target environment, the worm module targeted zero-day vulnerabilities to establish a beachhead in the operating system and execute a criteria-based infection scheme. The link module repeatedly replicated the worm to propagate itself across the network. The rootkit module executed operations to hide malicious code and activity, preventing the detection of Stuxnet.

About thirteen days after infection, the virus turned itself on and began spreading and executing criteria-based infections.[36] Although the worm was promiscuous by nature, Stuxnet was programmed to become inert if it did not satisfy three progressive infection criteria – meaning the worm must satisfy each criterion, in order, or it would become dormant. The target criteria were identified as (1) a Windows-based operating system, (2) the presence of Siemens WinCC/PCS7 SCADA software (also known as STEP7), and (3) the presence of one or more Siemens S7 Programmable Logic Controllers (PLC).[37] PLCs allow for automated control of electromechanical processes for industrial systems, such as centrifuges. This combination of criteria ensured Stuxnet infected specific target systems with a high degree of probability of intention.

OLYMPIC GAMES (CONTINUED)

Finally, Stuxnet employed selective attack criteria – meaning that the absence of any single criterion would preclude the attack. The attack criteria were identified as (1) connection of variable-frequency drives to the PLC, (2) variable-frequency drives must be produced by Vacon (Finnish vendor) or Fararo Paya (Iranian vendor), and (3) the frequency of attached motors must be between 807 Hz and 1,210 Hz (this range is well beyond the operational capacity of most industrial motors, except those of centrifuges).[38] This combination of attack criteria ensured Stuxnet was highly selective in its attack. Together, between infection and attack criteria, Stuxnet was a precision weapon with a highly refined target profile: Iranian centrifuges.

Once operational, Stuxnet modulated the speed of the centrifuges from 1,410 Hz to 2 Hz to 1,064 Hz.[39] Such a dramatic change in speeds creates a significant stress on the components of the centrifuge, causing them to destroy themselves. The sabotage was so sophisticated it was able to unfold without showing any signs of problems with monitoring systems used by officials at the Iranian facility. During the attack, the rootkit module would return a loop of normal operating system values, giving the operator no reason to suspect the software as the culprit for the destruction.



IEEE Diagram of Stuxnet Operational Model

OLYMPIC GAMES (CONTINUED)

All in all, the cyber-sabotage operation dismantled approximately one thousand Iranian centrifuges or twenty percent of Iran's nuclear enrichment capability. Specifically, the operation targeted the Natanz Nuclear Facility and degraded operations at that location by at least thirty percent.[40] The impacts and effects, however, were greater than this physical damage. Stuxnet demonstrated that the opponents of Iran's nuclear program (believed to be the U.S. and Israel) were deep inside Iran's systems. After discovering multiple variants of the worm in their systems, the Iranians had to believe that not only were they deeply penetrated but the attackers could keep coming back – Iran could not lock the door.

Additionally, Iran had no way of knowing for certain which systems had been corrupted from those that had not; the rootkit module was performing its function very well. Out of fear, Iranian engineers took many more centrifuges offline than had been infected.

Moreover, there was an insidious fear growing within the Iranian bureaucracy and the Iranian engineering community. Before the discovery of the virus, the destruction of the centrifuges appeared to be either faulty equipment or incompetent engineers. The Iranian bureaucracy began to develop a lack of confidence in their nuclear program's supply chains and scientific leadership. Several senior scientists and engineers were arrested by state police for suspicion of treason and sabotage. Due to the uncanny timing of the assassinations of several leaders in the Iranian nuclear program, Iranian scientists and engineers began fleeing the country, creating a nuclear brain drain effect. The psychological impacts of Stuxnet may be incalculable in terms of money but were effective in slowing down Iranian nuclear progress.

Finally, Stuxnet worked in concert with other instruments of national power to accomplish two ends: (1) avoid direct military action and (2) pursue diplomatic negotiations. These two ends worked hand-in-hand with each other to avoid escalation. In simple terms, Stuxnet was a viable alternative to strategic deep strikes by the U.S., and more importantly by Israel. Also, Stuxnet "bought time" by delaying the Iranian nuclear program and providing space for economic sanctions and diplomatic actions to take shape. In the diplomatic effort, the centrifuge sabotage operation shaped two interrelated messages for the Iranian leadership.

OLYMPIC GAMES (CONTINUED)

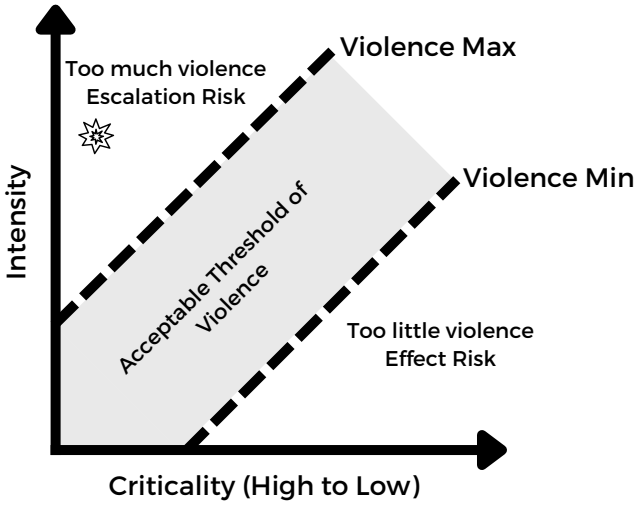
First, if the U.S. and Israel were willing to go to these lengths to disrupt centrifuges, what lengths would they be willing to go to stop a bomb from being produced?[41] Second, their nuclear program may be more valuable as a bargaining chip than a bomb-making system.[42] In the aggregate, Stuxnet gave the Obama administration crucial time to bring Iran to the bargaining table, culminating in a nuclear deal (Joint Comprehensive Plan of Action) in 2015.[43]

CASE STUDY IMMEDIATE FINDINGS

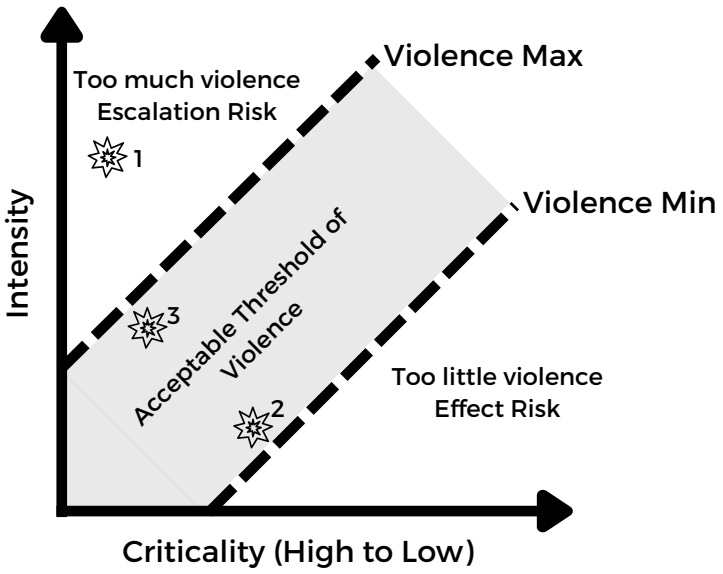
Coup de Main

The Department of Defense defines a coup de main as an offensive operation that capitalizes on surprise and simultaneous execution of supporting operations to achieve success in one swift stroke. The operative elements of a coup de main sabotage operation follow this definition closely in that it must maintain the element of surprise, be offensive in nature, and be conducted in concert with actions of other national instruments of power. In the analysis section, each case study has been identified as having a coup de main component.

Threshold of Violence



An adapted model for acceptable thresholds of violence will be used to evaluate the case studies.[44] The y-axis qualitatively measures the level of violence in terms of intensity corresponding to thex-axis measuring target criticality beginning with high at the origin and extending to low. An example is provided to demonstrate a high-intensity case of applied violence to a high-value critical target, resulting in an operation above the acceptable threshold of violence incurring escalation risk. The model visualizes the inverse relationship between intensity and criticality while acknowledging there must be a minimum level of violence to achieve the desired effects/impacts and there exists a maximum level of violence where escalation risk becomes unacceptable.



1 - Siberian Pipeline 2 - Georgian War 2008 3 - Olympic Games

CASE STUDY IMMEDIATE FINDINGS

The U.S.-sponsored sabotage operation of the Siberian Pipeline case study ranks high in intensity, due to causing the equivalent of a three kiloton nuclear explosion. The operation also ranks high on criticality, given the economic importance of the pipeline to the USSR's domestic economic woes and the pipeline's profit value to USSR arms race research programs. The resulting evaluation is above the acceptable threshold of violence.

The Soviet-sponsored sabotage operations of the Georgian War case study rank low in intensity, given they were primarily hacktivism and DDoS attacks. The attacks rank medium to high in criticality given their targeting of political and economic infrastructure preventing a coordinated response at the onset of physical combat. The resulting evaluation is within the acceptable threshold of violence, nearing the violence minimum.

The sabotage operations of the Olympic Games case study rank low to medium in intensity, given they caused physical damage to Iranian centrifuges but did so with prejudicial precision and avoided collateral damage. The attacks rank medium-high to high on the criticality scale, given Iran believes nuclear weapons are a guarantee to their national security. The resulting evaluation is within the acceptable threshold of violence, nearing the violence maximum.

Escalation

Escalation is defined as a qualitative response to an increase in intensity (vertical escalation) or scope (horizontal escalation) of a conflict that crossed a threshold considered significant by one or more of the participants. In each case study, the act of sabotage is easily identified in space and time, and each case study is evaluated for a qualified response of escalation. The only case study to exhibit any form of escalation is the Georgian War 2008 case.

Case Study	SQ / NSQ Countries	State Sponsored Control	Peer Entities	Coup de Main	Threshold of Violence	Escalation
Siberian Pipeline	SQ: US/FR NSQ: USSR	US/FR	YES	YES	TOO HIGH	NO
Georgian War 2008	SQ: GE NSQ: RU	RU	YES	YES	ACCEPTABLE	YES
Olympic Games	SQ: US/IS NSQ: IR	US/IS	YES	YES	ACCEPTABLE	NO

A NEW TRINITY

In the 19th century, Carl von Clausewitz proposed a theory of interaction that defined warfare through the modern age, the Clausewitzian Trinity. Literally writing the book on war, *On War*, Clausewitz's theory provides a useful framework of thought for this project. Clausewitz hoped his theory would serve as a source of illumination, a means by which the constituent elements of war could be broken down and further analyzed. In this way, his theory "acts as a guide for anyone who wanted to learn about war from books," helping to avoid pitfalls.[45] Following a brief description of the original theory, two new adaptations are presented to illustrate the unique nature of policy and sabotage in the digital age.

Clausewitz's trinity comprises three specific elements. The identity of those elements is readily evident to anyone who actually reads the first paragraph of his description: It is "composed of primordial violence, hatred, and enmity, which are to be regarded as a blind natural force; of the play of chance and probability within which the creative spirit is free to roam; and of its element of subordination, as an instrument of policy, which makes it subject to reason...." This set of elements is usually labeled "emotion/chance/reason"; sometimes "violence/chance & probability/rational calculation"; or, even more abstractly, "irrationality/nonrationality/rationality."[46]

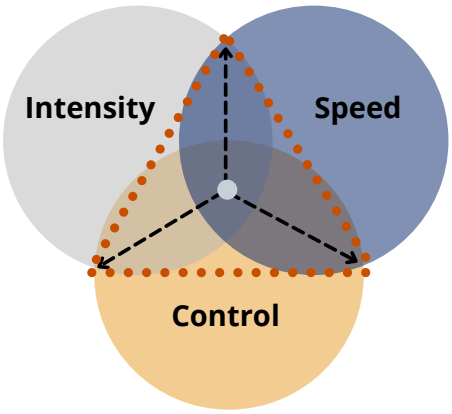
Clausewitz's theory rests upon these three intangible attributes that, despite uncertain conditions, persist in every case. Together, they act as a keystone upon which all further analyses should gain strength and stability. Clausewitz concludes that the "task...is to develop a theory that maintains these three tendencies" and creates a "conception of war...that will be the first ray of light into the fundamental structure of the theory."[47] His conclusion winks at his principle that war is "more than a mere chameleon that slightly adapts its characteristics to the given case," and begs the reader to adapt and apply the complexities that shape their understanding of the nature of war.[48]

Sabotage policy and the act of sabotage, itself, can be analyzed through three intangible, interactive attributes--intensity, speed, and control--that amplify their Clausewitzian trinity counterparts. These attributes will be adapted to the policy process governing sabotage and the evaluation of sabotage operations.

A NEW TRINITY (CONTINUED)

The Sabotage Policy Trinity

The overarching policy governing sabotage in the digital era is most discernable in the post-9/11 era and beyond, as will be covered in the policy analysis. The interaction between intensity, speed, and control in the context of policy evolution represents a constant trade-off between the three variables.



Losito Trinity for Sabotage Policy and Operations

- Intensity is defined by scope and scale. Scope concerns the policy's ability to maximize resources across agencies and departments to yield the greatest effect. Scale concerns the policy's ability to achieve multiple effects in terms of targets or types of effects (political, diplomatic, economic, military). Intensity is best represented through policy by Presidential Policy Directive 20, wherein there was an intensive interagency and legal regime applied to cyber sabotage operations, and through the Operation Olympic Games case study, whereby the sabotage operation was coordinated through multiple instruments of national power for maximum effect.

- Speed is defined by the time required, by virtue of the policy's ease or restrictions, from the inception of an operation until it produces the desired effect. The policy impact on speed is most commonly associated with preauthorized measures of action or the determined level of authority required to approve a sabotage operation. Speed is best represented by the John S. McCain National Defense Authorization Act of 2019, Section 1642, as discussed in the policy analysis portion, and through the Georgian War 2008 case study, whereby the Russians were able to coordinate their sabotage operations to the precise moment of active hostilities.

- Control is defined as the extent of oversight afforded by a particular policy. Control can be exerted through a required notification prior to execution, through post-hoc notification, or a regularly scheduled reporting requirement. Control is best represented by Presidential Policy Directive 20, whereby President Obama reserved execution authority for all cyber operations at the Presidential level. Control (or lack thereof) is also represented by the Siberian Pipeline case study, where the "gifted" logic bomb was entirely out of U.S. control, even though there was high certainty it was going to be used for the Trans-Siberian Pipeline.

A NEW TRINITY (CONTINUED)

These three attributes are negatively correlated – meaning, an increase in one attribute creates losses in at least one of the other two attributes. For example, if policymakers hedge toward speed (setting authorities low to act fast) they lose control and potentially incur significant reputational risk. If they hedge toward control (setting authorities high to reduce risk) they lose speed, initiative, and potentially foreclose on intensity (scale and scope of effect).

The Sabotage Operational Trinity

While not the aim of this project, and with potential for follow-on research, the case study selection hints at cyber sabotage's strategic utility in and outside of declared hostilities. Strategic utility refers to measurable contributions toward a state's political goals or shifts in the balance of power. The case studies herein demonstrate cyber sabotage being deployed at the operational level for tactical effects and strategic ends, unifying all levels of conflict but remaining below the threshold of war. Finally, sabotage operations are inherently clandestine (the act itself is obscured), which is to say the effect is intended to be perceived as something other than sabotage. For example, in the Operation Olympic Games case study, the sabotage was intended to be perceived as faulty equipment or incompetence among the nuclear scientists and engineers. This characteristic, of being clandestine by nature, yields yet another trinity of interaction between intensity, speed, and control.

- Intensity is again defined by scope and scale but in terms of effects. Scope concerns the overall impacts on the intended target, sometimes measured as recoverability. Scale concerns the number of targets affected and thus the scale of impact.

- Speed is again defined as the time required to execute an operation and achieve the desired effect but in terms of the conduct of the operation from reconnaissance to withdrawal.

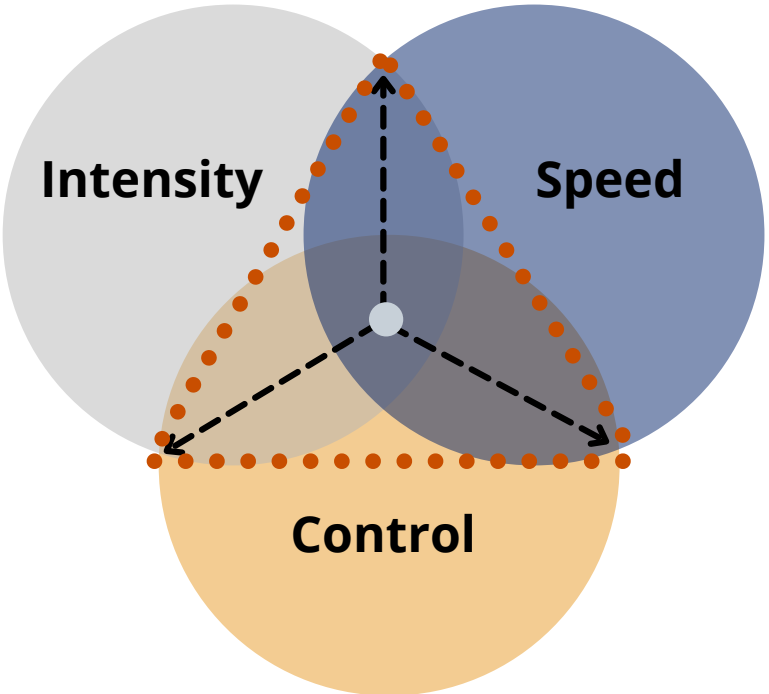
- Control is defined by the extent the saboteur has control over the sabotage tool, the targeted system, and the desired effect.

A NEW TRINITY (CONTINUED)

The inherent, clandestine nature of sabotage distinguishes it from warfare and diplomacy, the two classic instruments of power in security competition. This characteristic offers two significant advantages to the policymaker; it lowers states' escalation risks and reputation costs for intervening in their adversary's affairs. Sabotage offers a less expensive and less risky alternative to warfare as a means to actively interfere in their adversary's affairs and attempt to shift the balance of power when diplomacy falls short.

However, this secrecy characteristic that offers the promise of sabotage also impacts sabotage's operational effectiveness across the three interactive attributes. By its very nature, secrecy limits the intensity of impact to avoid compromise. The intensity of impact must be right-sized so as to maintain a plausible and ostensible cause other than sabotage. Additionally, secrecy slows the speed at which operations proceed as a safeguard against compromise. This is not always the case, as sometimes speed can be accelerated to avoid discovery paraphrased as "speed is security." Finally, efforts to maintain clandestinity can preclude control. While the action is not covert (the identity of the actor is obscured), exerting too much operational control can spoil the clandestine nature of the sabotage, colloquially showing one's hand.

Lastly, the clandestine characteristic creates operational trade-offs among these three attributes in the same manner as the policy trinity. Deductively, an increase in control likely results in a decrease in speed and possibly intensity.

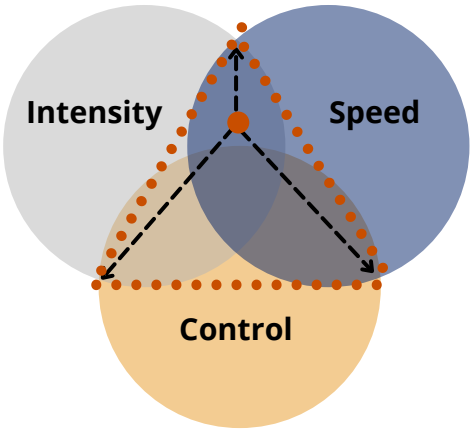


Losito Trinity for Sabotage Policy and Operations

EVALUATION

The Siberian Pipeline

Evaluation of the Siberian Pipeline case study using the Trinity for Sabotage Operations reflects the case study's analysis in terms of intensity, speed, and control. The operation ranks high in both speed, given the operation occurred in less than a year It ranks high in intensity due to both the physical and economic value of the target. However, the operation lacked control over the sabotage tool, which may have resulted in a lack of control over the intensity. A greater degree of control, as demonstrated in the Olympic Games case, may have resulted in an acceptable threshold of violence.

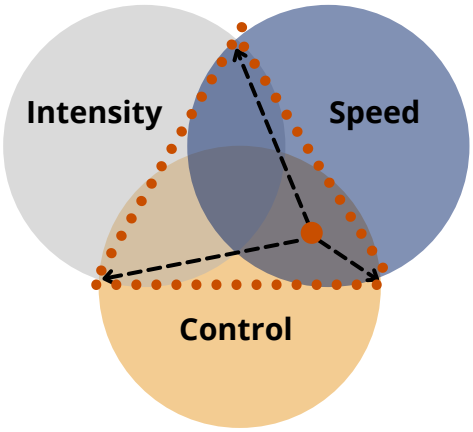


Trinity for Sabotage Operations - Siberian Pipeline

Case Study	SQ / NSQ Countries	State Sponsored Control	Peer Entities	Coup de Main	Threshold of Violence	Escalation
Siberian Pipeline	SQ: US/FR NSQ: USSR	US/FR	YES	YES	TOO HIGH	NO

Georgian War 2008

The Georgian War case study evaluated through the Trinity for Sabotage Operations reflects an operation reliant on speed and control. Speed and control allowed for the precise launch of simultaneous cyber-sabotage effects at the moment of physical combat. However, the sabotage operations were largely low intensity, below the violence minimum, and required increased violence. While not causal in this case, there is a correlation between the lack of intensity and escalation.



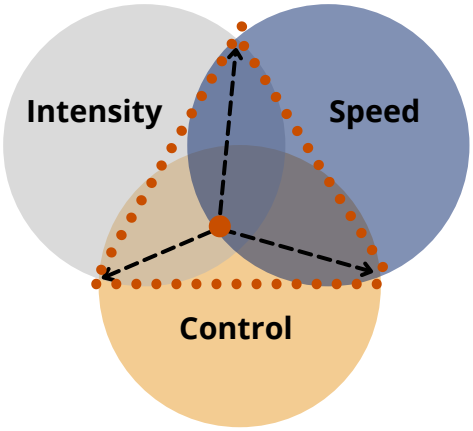
Trinity for Sabotage Operations - Georgian War

Case Study	SQ / NSQ Countries	State Sponsored Control	Peer Entities	Coup de Main	Threshold of Violence	Escalation
Georgian War 2008	SQ: GE NSQ: RU	RU	YES	YES	ACCEPTABLE	YES

EVALUATION (CONTINUED)

Olympic Games

The Olympic Games case represents the most well-balanced operation when applied to the Trinity for Sabotage Operations. Slightly erring toward control, it largely sacrificed speed taking years to deliver effects. However, the control over the Stuxnet virus produced an acceptable threshold of violence due to its precision and target discrimination. Likewise, Olympic Games was the most successful case in terms of coup de main, violence, and escalation criteria, producing very few unintended effects.

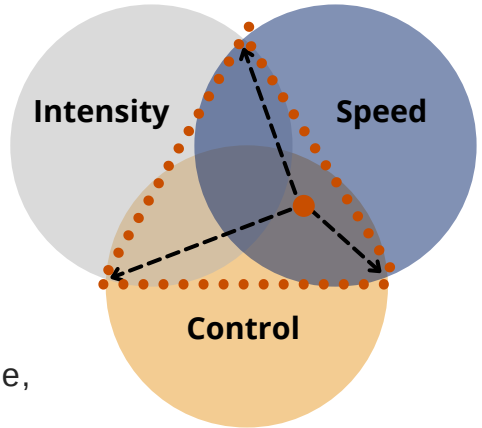


Trinity for Sabotage Operations - Olympic Games

Case Study	SQ / NSQ Countries	State Sponsored Control	Peer Entities	Coup de Main	Threshold of Violence	Escalation
Olympic Games	SQ: US/IS NSQ: IR	US/IS	YES	YES	ACCEPTABLE	NO

U.S. Policy and Sabotage

Reactionary policymaking in the wake of cyber-sabotage has not produced the desired balance of speed, intensity, and control exerted through policy. The evolutional arc of policy regarding sabotage in the digital era has trended toward speed and offensive posturing. In doing so, it is likely to sacrifice policy intensity by failing to achieve i ntegration with other instruments of national power and acting as a part of a larger coup de main strategy. Likewise, prioritizing speed over control introduces a potential for escalatory risk. The current state of U.S. policy regarding sabotage in the digital era is represented on the Trinity for Sabotage Policy, to the right. This evaluation is very similar to the evaluation produced for the Georgian War case study that resulted in escalation. Consequently, it is recommended to institute policy controls such as authority levels, approval levels, and oversight to increase control and bring U.S. policy into greater balance.



Trinity for Sabotage Policy - Present Day

EVALUATION (CONTINUED)

"Can We"

Can the DoD conduct a campaign of sabotage in the digital era in lieu of armed conflict?

Twenty-four case studies were screened from 1982 to present-day and evaluated for their threshold of violence and escalation. Two case studies, including the 2008 Georgian War study, included other activities above the threshold of violence and/or escalation. Some of the highest yield sabotage case studies have been conducted by the U.S. or its allies. Integration of the sabotage operation with other instruments of national power in a coup de main stratagem is a key variable of success.

Do we have the requisite policy framework?

The Department's current policy framework is built for speed and sacrifices intensity and control. The optimum point of balance is debatable, but the case studies demonstrate that operational scope and scale are maximized when policy intensity is integrated. It appears that NDAA 2020 corrected any misperceptions of the legal regime restrictions for military cyber operations in areas other than declared hostility, but I recommend further legal review of Sensitive Military Cyber Operations, the 48-hour reporting requirement, and any scenarios that might trigger covert action regulation and a Presidential finding.

"Should We"

Should the DoD be bolder or more aggressive in the conduct of sabotage in the digital era?

In a word, yes. The Department has the policy framework and the tools to conduct sabotage in the digital era, at scale. The Department should establish more aggressive directives for the conduct of sabotage in the cyber and space domains. These directives should incorporate principles of policy intensity and policy controls. Additionally, an evaluation of the capacity of the Office of Irregular Warfare should identify any resource gaps to manage such a departmental effort.

EVALUATION (CONTINUED)

Is sabotage a viable pursuit of national security ends below the threshold of violence?

Yes. Sabotage, particularly in the cyber and space domains, is demonstrated through case studies to have high strategic utility in competition. Policymakers are likely to see sabotage in as a low-cost, high payoff, and low-risk operation that is exempt from the covert action notification rules. This makes sabotage an incredibly versatile and agile tool in the pursuit of national security ends.

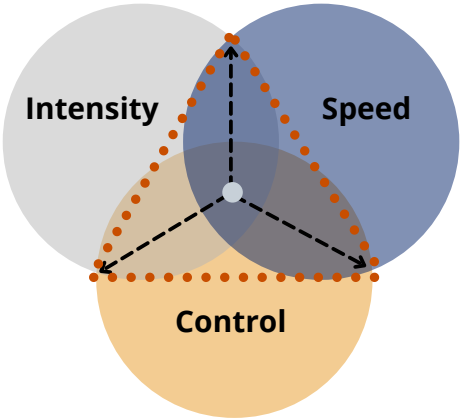
"How We"

How should the DoD analyze opportunities when considering sabotage in the digital era?

This is an area for further research. The Department requires two models (perhaps one integrated model) to assess opportunity and risk. At the operational level, models such as MSHARPP and CARVER are ideal for assessing opportunity, but the Department will likely require an adaptation of these models to assess strategic opportunity while integrating with other national instruments of power.

Do we have a framework of strategic thought for sabotage policy and operations?

This project puts forth a new paradigm for strategic thinking about sabotage policy and operations in the digital era. The three interactive and negatively correlated attributes of intensity, speed, and control have a direct impact on the digital era characteristics of warfare – violence, interaction, and escalation. This adaptation of the Clausewitzian Trinity provides a novel way of thinking about sabotage in the digital era.



Losito Trinity for Sabotage Policy and Operations

ANNEX A - FURTHER RESEARCH

- The Department of Defense does not have an official definition for sabotage. The DoD Dictionary of Military and Associated Terms mentions sabotage six times in the definitions of other terms, which is problematic. Each use of the term sabotage is in reference to protecting U.S. interests from foreign sabotage.
  - The lack of common terms prevents clear policy, universal planning, organization, training, and execution of sabotage across the Joint Force.
  - According to the Summary of the Irregular Warfare Annex to the National Defense Strategy, sabotage is not relegated to Special Operations only. The annex proclaims irregular warfare, and thereby sabotage, is a common task across the joint force. The lack of a definition for sabotage creates an institutional chasm that can have knock-on effects on operations, integration, approvals, policy, and strategy.
  - Policymakers likely have differing conceptions or preconceived notions of sabotage. The absence of a standard term permits confusion between operational and strategic levels of understanding.
- Of the twenty-four case studies examined, two were conducted within a declared state of war. This project presupposes the DoD has the authority to conduct sabotage operations below the threshold of conflict.
  - Following suit with the lack of common terminology, there is no clear resource to determine if DoD has the legal authority to conduct sabotage outside a declared state of war. This is of paramount concern in great power competition since a large part of U.S. policy is to refrain from entering a declared state of war.
  - Fully understanding authorities will enhance the understanding of cost-benefit and risk decisions regarding sabotage operations.
  - Finally, understanding DoD's authorities to conduct sabotage outside a declared state of war will assist Policymakers in understanding the conduct of sabotage in a rapidly evolving environment.
- Contemplating sabotage in the digital era requires a paradigm shift of risk analysis. The current DoD risk framework is not designed for waging sabotage in the digital era. Risk to mission, risk to force, and risk management frameworks for cyber systematically push the system to buy down risk in the wrong areas. A more comprehensive model for evaluating sabotage operations would involve risk of detection, attribution, retribution, political blowback, reputation cost, asset compromise, repeatability, and control.

ANNEX B - ENDNOTES & REFERENCES

[1] Department of Defense, “Summary of the Irregular Warfare Annex to the National Defense Strategy,” 2020, https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF.

[2] Carl von Clausewitz, On War, Wordsworth (Ware, England: Wordsworth Classics of World Literature, n.d.).

[3] Kimberly Amerson and Spencer Merideth III, “The Future Operating Environment 2050: Chaos, Complexity and Competition | Small Wars Journal,” accessed September 17, 2021, https://smallwarsjournal.com/jrnl/art/the-future-operating-environment-2050-chaos-complexity-and-competition.

[4] Clausewitz, On War.

[5] The System Was Blinking Red - Content Details - GPO-911REPORT-14,” accessed March 17, 2021, https%3A%2F%2Fwww.govinfo.gov%2Fapp%2Fdetails%2FGPO-911REPORT%2FGPO-911REPORT-14.

[6] “Homeland Security Act of 2002,” Department of Homeland Security, August 17, 2006, https://www.dhs.gov/homeland-security-act-2002.

[7] Joseph I. Lieberman, “S.2105 - 112th Congress (2011-2012): Cybersecurity Act of 2012,” legislation, February 16, 2012, 2011/2012, https://www.congress.gov/bill/112th-congress/senate-bill/2105.

[8] Office of the President of the United States, “Presidential Policy Guidance 20 - U.S. Cyber Operations Policy Guidance” (The White House, September 2018).

[9] “The 2018 DOD Cyber Strategy: Understanding ‘Defense Forward’ in Light of the NDAA and PPD-20 Changes,” Lawfare, September 25, 2018, https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes.

ANNEX B - ENDNOTES & REFERENCES

[10] Office of the President of the United States of America, “2018 National Cyber Strategy,” Trump White House, September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[11] Secretary of Defense, “2018 Department of Defense Cyber Strategy,” September 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[12] “The Law of Military Cyber Operations and the New NDAA,” Lawfare, July 26, 2018, https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa.

[13] Elias Groll, “Trump Has a New Weapon to Cause ‘the Cyber’ Mayhem,” Foreign Policy, https://foreignpolicy.com/2018/09/21/trump-has-a-new-weapon-to-cause-the-cyber-mayhem/.

[14] “The Pentagon’s New Cyber Strategy: Defend Forward,” Lawfare, September 21, 2018, https://www.lawfareblog.com/pentagons-new-cyber-strategy-defend-forward.

[15] Robert Chesney, “Military Cyber Operations: The New NDAA Tailors the 48-Hour Notification Requirement,” Lawfare, December 18, 2019, https://www.lawfareblog.com/military-cyber-operations-new-ndaa-tailors-48-hour-notification-requirement.

[16] Gus W. Weiss, “Duping the Soviets: The Farewell Dossier,” Studies in Intelligence 39, no. 5 (1996): 121–26.

[17] Weiss, “Duping the Soviets: The Farewell Dossier.”

[18] Thomas Reed, At the Abyss (Penguin Random House), https://www.penguinrandomhouse.com/books/139848/at-the-abyss-by-thomas-c-reed/.

[19] Weiss, “Duping the Soviets: The Farewell Dossier.”

[20] Weiss, “Duping the Soviets: The Farewell Dossier.”

ANNEX B - ENDNOTES & REFERENCES

[21] Weiss, “Duping the Soviets: The Farewell Dossier.”

[22] Reed, At the Abyss by Thomas Reed.

[23] Reed, At the Abyss by Thomas Reed.

[24] Weiss, “Duping the Soviets: The Farewell Dossier.”

[25] Reed, At the Abyss by Thomas Reed.

[26] Reed, At the Abyss by Thomas Reed.

[27] David Hollis, “Cyberwar Case Study: Georgia 2008,” n.d., 10.

[28] Sarah P White, “Understanding Cyberwarfare: Lessons from the Russia-Georgia War,” Modern War Institute, 2018, 28.

[29] David Hollis, “Cyberwar Case Study: Georgia 2008,” n.d., 10.

[30] Government of Georgia, “Russian Cyberwar on Georgia,” 2008, https://lawlordtobe.files.wordpress.com/2018/03/cyberwar-georgia.pdf.

[31] David Hollis, “Cyberwar Case Study: Georgia 2008,” n.d., 10.

[32] White, “Understanding Cyberwarfare: Lessons from the Russia-Georgia War.”

[33] White, “Understanding Cyberwarfare: Lessons from the Russia-Georgia War.”

[34] David Hollis, “Cyberwar Case Study: Georgia 2008,” n.d., 10.

[35] Mariusz Antoni Kamiński, “Operation ‘Olympic Games.’ Cyber-Sabotage as a Tool of American Intelligence Aimed at Counteracting the Development of Iran’s Nuclear Programme,” Security and Defence Quarterly 29, no. 2 (June 25, 2020): 63–71, https://doi.org/10.35467/sdq/121974.

ANNEX B - ENDNOTES & REFERENCES

[36] David Sanger, The Perfect Weapon (Penguin Random House), accessed November 27, 2021, https://www.penguinrandomhouse.com/books/547683/the-perfect-weapon-by-david-e-sanger/.

[37] Kamiński, “Operation ‘Olympic Games.’ Cyber-Sabotage as a Tool of American Intelligence Aimed at Counteracting the Development of Iran’s Nuclear Programme.”

[38] Kamiński, “Operation ‘Olympic Games.’ Cyber-Sabotage as a Tool of American Intelligence Aimed at Counteracting the Development of Iran’s Nuclear Programme.”

[39] Kamiński, “Operation ‘Olympic Games.’ Cyber-Sabotage as a Tool of American Intelligence Aimed at Counteracting the Development of Iran’s Nuclear Programme.”

[40] Sanger, The Perfect Weapon by David E. Sanger.

[41] Kamiński, “Operation ‘Olympic Games.’ Cyber-Sabotage as a Tool of American Intelligence Aimed at Counteracting the Development of Iran’s Nuclear Programme.”

[42] Kamiński, “Operation ‘Olympic Games.’ Cyber-Sabotage as a Tool of American Intelligence Aimed at Counteracting the Development of Iran’s Nuclear Programme.”

[43] Sanger, The Perfect Weapon by David E. Sanger.

[44] Eric Wendt, “Strategic Counterinsurgency Modeling,” Special Warfare (Naval Postgraduate School, 2005); Paul Tompkins Jr., “Threshold of Violence,” Assessing Revolutionary and Insurgent Strategies (The Jophns Hopkins University Applied Physics Laboratory), accessed April 28, 2022, https://www.soc.mil/ARIS/books/pdf/thresholds-violence.pdf.

[45] Christopher Bassford, “Teaching the Clausewitzian Trinity,” https://www.clausewitz.com/readings/Bassford/Trinity/TrinityTeachingNote.htm.

[46] Bassford

[47] Bassford

[48] Clausewitz, On War.

ANNEX B - ENDNOTES & REFERENCES

115th Congress of the United States of America. “John S. McCain National Defense Authorization Act for Fiscal Year 2019,” January 3, 2018. https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf.

Amerson, Kimberly, and Spencer Merideth III. “The Future Operating Environment 2050: Chaos, Complexity and Competition | Small Wars Journal.” Accessed September 17, 2021. https://smallwarsjournal.com/jrnl/art/the-future-operating-environment-2050-chaos-complexity-and-competition.

Andersen, Brett. “Clausewitz’s Continued Relevance and Foundation for Educating Critical Thinking Skills.” U.S. Army War College, 2012. https://apps.dtic.mil/sti/pdfs/ADA560832.pdf.

Bassford, Christopher. “Teaching the Clausewitzian Trinity.” Accessed April 18, 2022. https://www.clausewitz.com/readings/Bassford/Trinity/TrinityTeachingNote.htm.

Chesney, Robert. “Military Cyber Operations: The New NDAA Tailors the 48-Hour Notification Requirement.” Lawfare, December 18, 2019. https://www.lawfareblog.com/military-cyber-operations-new-ndaa-tailors-48-hour-notification-requirement.

Chesney, Robert. “The 2018 DOD Cyber Strategy: Understanding ‘Defense Forward’ in Light of the NDAA and PPD-20 Changes,” September 25, 2018. https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes.

Chesney, Robert. “The Law of Military Cyber Operations and the New NDAA,” July 26, 2018. https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa.

Clausewitz, Carl von. On War. Wordsworth. Ware, England: Wordsworth Classics of World Literature, 1997

Department of Defense. “Summary of the Irregular Warfare Annex to the National Defense Strategy,” 2020. https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF.

ANNEX B - REFERENCES (CONT)

Dunlap, Charlie. “Cyber Operations and the New Defense Department Law of War Manual: Initial Impressions.” Lawfare, June 15, 2015. https://www.lawfareblog.com/cyber-operations-and-new-defense-department-law-war-manual-initial-impressions.

Featured Commission Report. The 9/11 Commission Report. Accessed March 17, 2021. https%3A%2F%2Fwww.govinfo.gov%2Fapp%2Fdetails%2FGPO-911REPORT%2FGPO-911REPORT-14.

Gazula, Mohan B. “Cyber Warfare Conflict Analysis and Case Studies,” n.d., 100.

Government of Georgia. “Russian Cyberwar on Georgia,” 2008. https://lawlordtobe.files.wordpress.com/2018/03/cyberwar-georgia.pdf.

Groll, Elias. “Trump Has a New Weapon to Cause ‘the Cyber’ Mayhem.” Foreign Policy (blog). Accessed March 17, 2021. https://foreignpolicy.com/2018/09/21/trump-has-a-new-weapon-to-cause-the-cyber-mayhem/.

Handel, Michael I. “Clausewitz in the Age of Technology.” Current News (Washington, D.C. : Special Edition), no. 1475 (1986).

Hollis, David. “Cyberwar Case Study: Georgia 2008,” n.d., 10.

Department of Homeland Security. “Homeland Security Act of 2002,” August 17, 2006. https://www.dhs.gov/homeland-security-act-2002.

Joint Chiefs of Staff. “Joint Publication 1-02,” 2016. https://irp.fas.org/doddir/dod/jp1_02.pdf.

Joint Chiefs of Staff. “Joint Publication 3-0,” 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf.

Kamiński, Mariusz Antoni. “Operation ‘Olympic Games.’ Cyber-Sabotage as a Tool of American Intelligence Aimed at Counteracting the Development of Iran’s Nuclear Programme.” Security and Defence Quarterly 29, no. 2 (June 25, 2020): 63–71. https://doi.org/10.35467/sdq/121974.

ANNEX B - REFERENCES (CONT)

Kannewurff, Brandon T. von. “Undermining ‘The Deal of the Century’: The Siberian Natural Gas Pipeline & the Failure of American Economic Pressure on the Soviet Energy Industry.” James Blair Historical Review 9, no. 2 (2019): 25.

Kapusta, Philip. “The Gray Zone,” 2015. https://www.soc.mil/SWCS/SWmag/archive/SW2804/GrayZone.pdf.

Maneuver Self Study Program. “Nature and Character of War and Warfare.” U.S. Army Maneuver Center of Excellence, 2018. https://www.benning.army.mil/mssp/Nature%20and%20Character/.

Markoff, John. “Before the Gunfire, Cyberattacks.” The New York Times, August 12, 2008, sec. Technology. https://www.nytimes.com/2008/08/13/technology/13cyber.html.

Maschmeyer, Lennart. “Why Cyber War Is Subversive, and How That Limits Its Strategic Value.” War on the Rocks, November 17, 2021. https://warontherocks.com/2021/11/why-cyber-war-is-subversive-and-how-that-limits-its-strategic-value/.

Meegan, Daniel. “Breaking Other People’s Toys: Sabotage in a Multipolar World.” Naval Post Graduate School, 2020.

Meyer, Joel. “Supervising the Pentagon: Covert Action and Traditional Military Activities in the War on Terror.” Administrative Law Review 59, no. 2 (2008): 463–78.

Office of General Counsel. “Department of Defense Law of War Manual,” 2016. https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190
.

Office of the President of the United States. “Presidential Policy Guidance 20 - U.S. Cyber Operations Policy Guidance.” The White House, September 2018.

ANNEX B - REFERENCES (CONT)

O'Harrow Jr., Robert, and Ellen McCarthy. "Top U.S. Cyber-Security Official Resigns." Washington Post, October 2, 2004. https://www.washingtonpost.com/wp-dyn/articles/A64915-2004Oct1.html.

Powell, Alexander. "A Blast from the Past? The Role of Maritime Sabotage in Strategic Competition." Modern War Institute, February 3, 2022. https://mwi.usma.edu/a-blast-from-the-past-the-role-of-maritime-sabotage-in-strategic-competition/.

Reed, Thomas. At the Abyss. Penguin Random House. Accessed November 27, 2021. https://www.penguinrandomhouse.com/books/139848/at-the-abyss-by-thomas-c-reed/.

Rizzo, Jennifer. "Cybersecurity Bill Fails in Senate - CNN Politics." CNN, August 2, 2012. https://www.cnn.com/2012/08/02/politics/cybersecurity-act/index.html.

Rold, Ana. "The Digital Battlefield and the Future of War." Diplomatic Courier, 2018. https://www.diplomaticourier.com/posts/the-digital-battlefield-and-the-future-of-war.

Sanger, David. The Perfect Weapon. Penguin Random House. Accessed November 27, 2021. https://www.penguinrandomhouse.com/books/547683/the-perfect-weapon-by-david-e-sanger/.

Weinstein, Dave. "The Pentagon's New Cyber Strategy: Defend Forward," September 21, 2018. https://www.lawfareblog.com/pentagons-new-cyber-strategy-defend-forward.

United States Army Special Operations Command. "USASOC Strategy 2035," 2016. https://www.soc.mil/AssortedPages/USASOCStrategy2035.pdf.

United States Congress. "National Defense Authorization Act 2020," 2020. https://docs.house.gov/billsthisweek/20191209/CRPT-116hrpt333.pdf.

ANNEX B - REFERENCES (CONT)

Violand, David. “Adapting Clausewitz to the Information Age: How Traditional News Media and Social Networking Are Combining to Expand the Triangle.” Naval War College, 2011. https://apps.dtic.mil/sti/pdfs/ADA546364.pdf.

Wall, Andru. “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action.” Harvard National Security Journal 3 (2011). https://www.soc.mil/528th/PDFs/Title10Title50.pdf.

Weiss, Gus W. “Duping the Soviets: The Farewell Dossier.” Studies in Intelligence 39, no. 5 (1996): 121–26.

White, Sarah P. “Understanding Cyberwarfare: Lessons from the Russia-Georgia War.” Modern War Institute, 2018, 28.