Jerry M. Couretas

An Introduction to Cyber Analysis and Targeting

Springer

An Introduction to Cyber Analysis and Targeting

Jerry M. Couretas

An Introduction to Cyber Analysis and Targeting

Springer

Jerry M. Couretas
Washington, DC

ISBN 978-3-030-88558-8 ISBN 978-3-030-88559-5 (eBook)
https://doi.org/10.1007/978-3-030-88559-5

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

The development of this book had many hands. Mr. Ed Waltz was key in the early discussions, feedback and support for this work. In addition, I would like to thank Vicky Pate and Pat Adrounie for reviewing each of the chapters during the writing phase.

I would like to dedicate this book to Monica, Sophie and Ella, for the time and patience they provided. In addition, I would also like to thank Jorge and Aida Carpio, for their support and mentoring. And finally, to my parents, Gus and Mary, for providing an example of persistence and faith.

Foreword

The cyber threat landscape has grown to pose risks to every facet of our lives – infrastructure, finance, communications, health, personal and social media, and even our smart homes and vehicles. As the complexity of the cybersphere has grown, even so have the threat vectors and targeting mechanisms. To defend a network, you must understand how the attacker strategizes, analyzes, and targets a network. This book uniquely describes the offensive analysis and targeting process as a set of conceptual models.

The book market is replete with books at the high, strategic level of cyber warfare and the deep, tactical level of hacking methods unique to enterprise systems. This book stands alone in providing conceptual models for addressing cyber *analysis and targeting* – the systematic analysis and prioritization of cyber entities considered for possible cyber engagement, and the planning of vectors for access.

The sophistication of the cyber-attack process has grown with the complexity of networked systems and their operations. The disciplines of cyber-Intelligence (CI) and cyber counterintelligence (CCI) conduct detailed analyses of the cybersphere and carefully select targets to exploit and conduct operations. Cyber operators, offensive or defensive, need to understand the methods to perform analysis of targeted networks and the means to select targets and then conduct cyber operations.

This book follows the traditional approach of introducing a new discipline: Grammar, Logic and Rhetoric. The grammar (unique terminology) of the cyber operational world is introduced throughout; next, the text describes the logic of how cyber analysis is conducted, how targeting selection is performed, and the means by which cyber operations are conducted. Finally, the rhetoric of cyber operations is narrated by real-world use cases that illustrate the mechanisms introduced throughout.

Jerry Couretas is uniquely equipped to introduce this subject because of his broad expertise in the fields of military and cyber operations, analysis, modeling, and simulation. Dr. Couretas has spent the last decade modeling and simulating cyber systems for network defense. As Editor-in-Chief of the *Journal of Defense Modeling and Simulation* (JDMS), Dr. Couretas produced over 20 special issues on subjects of national security importance simulating complex military operations. He has also served on the North Atlantic Treaty Organization’s (NATO) Modeling and Simulation Group 117 (NMSG 117), cyber modeling and simulation (M&S). Those who build computational models of systems and operations must know the details, and Jerry has that depth of knowledge in the cyber field. His experience encompasses cyber risk mitigation, cyber ops analysis, cyber analytics, and targeting. I have enjoyed working with Jerry for over 4 years as he conceived and prepared this text. His depth of understanding and expertise in explaining this topic is evident as he introduces defensive and offensive cyber operators to the state of the practice in cyber analysis and cyber targeting.

Ed Waltz

Contents

Chapter 1
Cyber Analysis and Targeting

The goal of this book is to describe cyber analysis and targeting for defensive applications. One objective of developing a cyber analysis and targeting methodology is to add information technology (IT) considerations into traditional military operations research (OR). For example, we will include cyber threats, cyber terrain, IT architectures, and other information-related capabilities (IRCs) in a developing cyber analysis and targeting methodology, accounting for the steady ingress of cyber into military operations through IT-based improvements in weapons systems, telecommunications, and online media. In developing this cyber analysis and targeting methodology, we will leverage use cases that span from analysis to modeling and simulation. This includes a look at assessment, for resilient systems development, along with using novel modeling and simulation approaches to describe the target as a discrete event process that we will use to estimate the effects from a cyber attack.

Policy applications for cyberspace generally focus on resilience, or defensive applications, for the United States, the United Kingdom, Canada, and Australia. Similarly, the information assurance (IA) community has distilled both rule-based approaches (e.g., SANS 20) and standards (e.g., NIST: US National Institute of Standards and Technology) to guide network engineers in the development of secure cyber systems. We will therefore review this body of developing cyberspace policy and doctrine, which covers the increasing use of information-related capabilities (IRCs), in Chap. 2.

While cyberspace is still developing, in terms of policy and doctrine, conventional military engagements, missions, and campaigns have a rich history to draw on for analysis and targeting exemplars. One scenario might be to use traditional military analysis and targeting to focus on, and describe, adversary order of battle (OOB). For example, the locations and movements of Soviet divisions were thoroughly analyzed, for conventional analysis and targeting, over the course of the Cold War. Similarly, targeting for this kind of conventional engagement focused on affecting an enemy's ability to maneuver, which includes controlling the lines of communication (LOC). This might consist of destroying (e.g., denial) transport

J. M. Couretas, *An Introduction to Cyber Analysis and Targeting*,
https://doi.org/10.1007/978-3-030-88559-5_1

techniques (e.g., trucks, rail, associated lines of communication), reducing the ability to communicate or perform command and control (C2), or direct targeting of enemy forces and weapons. In addition, attacking enemy C2 included using information-related capabilities to target both the availability (i.e., jamming) and integrity (i.e., trust) of communication between a command headquarters and units in the field.

Much of the current military analysis is still based on Cold War era operations research approaches, a time period before microprocessors were key components in the trucks, trains, and telephones that a modern force relies on to conduct war. Cyber analysis and targeting should therefore incorporate considerations for the information technologies (IT) included in every element of a fighting force's order of battle (OOB). The ubiquitous cyber in modern fighting forces is defined as follows:

Cyber "of, relating to, or involving computers or computer networks" (Merriam Webster).

Cyber is often not considered in current conventional analysis, which includes estimating likely adversary courses of action (COAs). While communications intelligence (COMINT) is a factor in performing engagement through campaign-level planning, this is usually high level, and does not include the scale or scope of cyber effects. For example, standard tabletop exercises and wargames consider equipment effectiveness, physical terrain, and command and control (C2), among other force components, when doing force-on-force simulations. In fact, one method of bringing cyber into current, conventional, military modeling, and analysis is to turn the communications off, which only provides denial; missing the cyber effects that accrue from compromising the confidentiality of data stores, or modifying the integrity of an organization's key data sets (e.g., orders, geo location). We can therefore define cyber analysis as follows:

Cyber Analysis (1) the process of decomposing cyber information to synthesize explanation of adversary actions, networks, and cyber objects; (2) describing the physical, logical, or persona target in terms of the full spectrum of confidentiality, integrity, and availability (CIA) effects achievable via cyber means.

In defining cyber analysis, our first definition leans more toward the classical intelligence use of cyber for collection and determination of adversary intent. One of the current challenges is placing cyber alongside kinetic options when planning an operation. Definition (2) is therefore focused on the types of effects that the cyber analyst will be looking for when developing a target.

Both definitions of cyber analysis contribute to describing an order of battle, which can miss much of the cyber attack surface, or IT Achilles heel, of conventional C2 and maneuver elements. In addition, much of the targeting is based on traditional line of communication (LOC) elements, missing the more nuanced effects available via cyber. For example, cyber targeting is currently more likely to be thought of in terms of communications availability, and subsequent C2 challenges, than the longer-term effects that can result from confidentiality or integrity attacks. Chapter 3 will therefore address the scope of a cyber threat for both the individual components and the overall cyber system. This will include a use of cyber threat intelligence (CTI) to roll up the different elements of risk analysis in order to find and classify IT system vulnerabilities over the steps of a cyber attack process (Launius, 2019).

Chapter 4 transitions from the physical systems that hackers target to compromise data, to the human terrain. Information operations (IO) are used for strategic purposes to attack leadership and key personnel in order to create organizational friction via false information, potentially changing the course of their target's operations. One example was the outing of private e-mails in the 2014 Sony attack (Zetter, 2014a, b), causing Sony to cancel the release of a film that parodied the President of North Korea. In addition, we will look at the operation of cyber-based information operations (IO), including how popular news sources, including social media, were used to deliver "fake news" during the 2016 US Presidential Election, inciting dozens of riots within the United States (Mueller, 2019). For strategic effects, we will also look at how cyber operations compare to active measures from the former Soviet Union to create confusion and doubt. Similarly, for tactical effects, we will look at how cyber can be used to provide the wrong coordinates for a munition or mapping application, causing a bomb to hit the wrong target or a unit to go to the wrong location. IO therefore covers the overall spectrum described as information-related capabilities (IRCs) that govern current cyberspace operations.

As discussed in Chap. 4's use of social media to affect the news feeds and change the thinking of the general population, cyber means can also be used to collect and develop potentially compromising information on key decision makers. For example, in Chap. 5, we will look at how confidentiality attacks, where the acquiring of secure data (e.g., private keys, personnel information), can be used to unlock communication channels, determine centers of gravity (COG) (e.g., understand an organization's structure), or, in longer term, compromise key personnel with private information.

While Chap. 5 shows the detrimental effects that an intelligent adversary can have through the collection, and processing, of private information, Chap. 6 reviews security technologies that compose current cyber terrain. These end points, connections, and key nodes use security operations centers (SOCs) to secure an organization's data and key operating information. In addition to using component technologies for network protection, Chap. 6 will provide conceptual architecture techniques, including defense in depth, to layer the technologies and decrease the likelihood of attacker success. Similarly, we review implementation guidance, including denial and deception, to provide overall guidance in developing network security solutions.

While our primary focus is to use cyber analysis and targeting for defensive means, we can also look at the cyber threats in terms of well-developed attack models. One example is the Lockheed Martin Attack Cycle (Eric M. Hutchins, 2012), which provides a step-by-step map of how an attacker maneuvers from initial reconnaissance of a target to actions on objectives. This includes increasing knowledge across the steps. For example, the reconnaissance phase informs weaponization concerning the types of vulnerability evaluations that we perform in Chaps. 2 and 3, along with the intelligence, surveillance, and reconnaissance (ISR) development

(Chap. 5). In addition, we can use our understanding of defensive technologies (Chap. 6) to better understand target terrain.

Target analysis, as discussed in Chap. 7, will require information on appropriate delivery methods, and candidate techniques, for exploitation of target vulnerabilities and installation of the cyber weapon. We can therefore use the Lockheed Martin Attack Cycle to compare analysis and target intelligence development for kinetic and cyber munitions, at different stages of the attack life cycle. For example, we can look at "dumb bombs," precision-guided munitions (PGMs), unmanned autonomous systems (UAS'), and cyber, in parallel, to compare the information collection and support requirements across the spectrum of conventional, precision-guided, and cyber munitions (Fig. 1.1).

As shown in Fig. 1.1, analysis and targeting are done in advance of the mission for conventional "dumb bombs" and PGMs. With the introduction of drones (i.e., UAS'), and especially cyber, ISR is now part of the mission, a tool that operators use to refine the targeting solution both before attack cycle initiation and over the course of the attack. One advantage of UAS' and cyber is that they are more flexible for addressing dynamic, time-sensitive targets (TSTs). Conventional and "smart" munitions, on the other hand, maintain ISR as a decoupled, independent, process that occurs prior to the attack.

An additional challenge is that cyber also operates as a pseudo-kinetic actor, challenging analysis and targeting to assess effects that can take multiple forms over a range of time periods. Successful kinetic effects simply remove their targets from the battlefield. Cyber effects, however, span the compromise of information (i.e., confidentiality), the misuse of information (i.e., integrity), or the denial of information (i.e., availability). Quantifying any of these effects is still an art, with one source

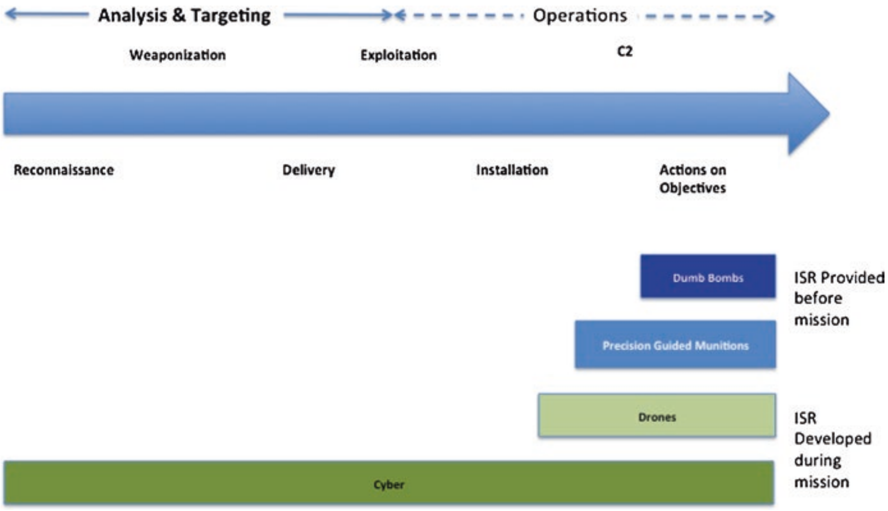

Fig. 1.1 ISR for analysis and targeting: "dumb bombs" to cyber operations

of inspiration coming from legacy joint munition effectiveness manuals (JMEMs), used to describe the performance of conventional bombs and guided munitions.

Due to the decoupling of ISR from kinetic strike, conventional munitions lend themselves to a more detached, technical assessment, with methods and techniques developed over decades. The Joint Munitions Effects Manual (JMEM) (US Army), for example, is used to document an explosive munitions' effects in engineering-level detail. A history of kinetic JMEMs defines weaponeering as follows:

> "… the process of determining the quantity of a particular type of weapon required to achieve a specific level of target damage by considering the effects of target vulnerability, warhead damage mechanism, delivery errors, damage criterion and weapon reliability, p. 1 of http://www.weaponeering.com/." (Weaponeering)

It is currently a challenge to provide this JMEM level of detailed engineering estimate for cyber munitions. For example, one of the analysis and targeting challenges for drones and cyber is that the process continues over the course of the mission, has the operator in the loop, and implicitly requires more operator assessment (Fig. 1.2).

As shown in Fig. 1.2, like conventional munitions, cyber requires a method to estimate effects. Because cyber effects usually include more than physical effects (e.g., information and psychological) and potentially cause effects at a wider scale, the description of all of these properties of cyber munitions is required before use. While kinetic effects have the Joint Munition Effectiveness Manual (JMEM), (US Army), cyber is still a challenge to describe as either an effects alternative (Mark Gallagher, 2013) (George Cybenko G. S., 2016), or an ISR complement, to conventional munitions. An additional difference is that cyber penetration and collection operations are often used for intelligence collection, as a strategic asset; with relatively few comparable effects measures.

Accounting for cyberspace operations' ill-defined effects in the application of information-related capabilities, or quantifying cyber, is a challenge that we will approach through currently known capabilities. One approach is to look at the application of cyber, either defensive or offensive, in terms of resource requirements, as an intermediate-term solution for describing cyberspace operations. For example, in Chap. 6 we describe network defense, along with component technologies and

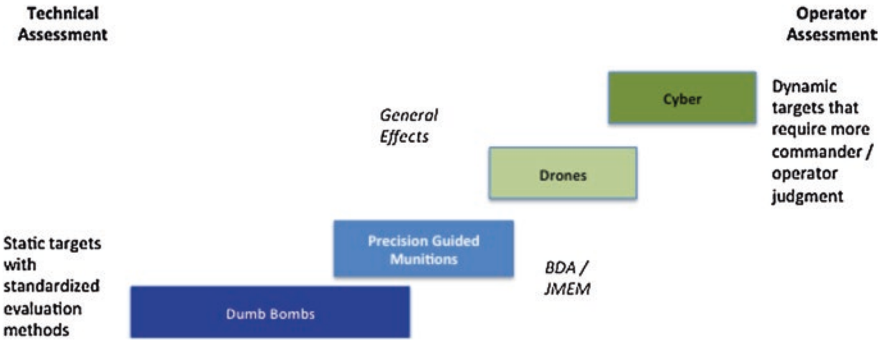
Technical Assessment
Operator Assessment
Cyber
Dynamic targets that require more commander / operator judgment
General Effects
Drones
Static targets with standardized evaluation methods
Precision Guided Munitions
BDA / JMEM
Dumb Bombs

Fig. 1.2 Technical/operator assessment of munitions: dumb bombs to cyber

architecture techniques. A natural question in planning a network defense architecture is the cost to purchase and maintain a secure network. Chapter 7 provides an example attack process methodology that estimates the time and cost for an attacker to successfully attack an objective network.

The introduction to network terrain in Chap. 6 also describes the challenges that a network attacker (e.g., penetration tester) will need to analyze prior to prosecuting a target. The attack processes in Chap. 7 therefore describe how an attacker will formulate and execute his targeting process. For example, we will review the CARVER—i.e., criticality, accessibility, recuperability, vulnerability, effect, recognizability—targeting matrix to analyze key nodes during initial operational planning. Developing the targeting solution includes reviewing computer network vulnerabilities over the Lockheed Martin Attack Cycle to identify the target elements for specific effects—effects that cyber is ideally suited to provide. We can now, therefore, provide a definition for cyber targeting.

Cyber Targeting the practice of selecting targets, and pairing up the appropriate collection plan or response to them, on the basis of operational requirements.

In addition, cyber targeting is the final step in the overall scheme of cyber operations described in Fig. 1.1, which includes the defensive, operational preparation, and offensive steps of a cyber engagement.

When looking at Fig. 1.1, it seems obvious that there is currently a need for cyber analysis and targeting. In Chap. 7, we estimate the people, process, and technology costs of maintaining a defensive portfolio against hackers, terrorist, or nation state adversaries. One of the differentiators between the respective groups includes resourcing in terms of research, ISR, and operations. For example, a hacker will be expected to have no research, ISR limited to his cognitive capability, and operational capacity based on his ability to hack. At the other end of the spectrum, a nation state hacker will be able to draw from top-notch universities, access to finished intelligence products, and have state of the art tradecraft. We can therefore compare a defended network in terms of its component technologies (e.g., security baseline) and its architecture (e.g., SOC policies) for the resources required by the respective groups to access the network and compromise a target.

The targeting methods in Chap. 7 culminate in the cyber process evaluator, a "simple" means of estimating the time/cost imposed on an attacker based on the policies, processes, and technologies that compose the defensive terrain (i.e., Chap. 6). Each of the components in the defensive system can also be described by software architectures, with well-developed frameworks available to describe the terms (i.e., reference architecture), functions (i.e., solution architecture), connections (i.e., logical architecture), or implementation (i.e., physical architecture). Describing a cyber system in terms of general artifacts provides the network defender with a method for ensuring that the respective components are up to date, in terms of individual components and overall system security. In addition, architectures help with organizing the respective network architecture elements for easier management by the Security Operations Center (SOC). We review an example cyber system architecture, including its solution architecture, in Chap. 8.

The example cyber system solution architecture, from Chap. 8, provides us with a basic structure for studying the development of metrics for a cyber system. For example, we will look at key performance parameters (KPPs) to describe the solution architecture as a system. This includes system characteristics (e.g., stealth and speed). Similarly, we will use measures of performance (MOPs) to describe cyber system operator characteristics. MOPs for cyber operations are likely the limit of what can be measured for individual cyberspace targeting engagements. As we move to cyber missions and campaigns, MOPs and measures of effectiveness (MOEs) are used to show the types of unique effects that a cyber system can provide for a military commander. In Chap. 9, we will review the KPPs, MOPs, and MOEs of a cyber system, showing their merits through a compare/contrast with an unmanned aerial system (UAS), and its measurable improvements over a piloted aircraft.

Leveraging Chap. 9's cyber system metrics, Chap. 10 will include a discussion of modeling and simulation for cyber analysis and targeting. Chapter 10 will look at the inherent parallelism in cyber systems, providing conceptual models, along with example analytics, to describe how we might compute the risk associated with performing courses of action (COAs) at different portions of a generalized cyber attack cycle. These generalized operational approaches are complimented by a discussion of a cyber target as a dynamic, discrete event system, for operational effects estimation.

1.1 Key Cyber Analysis and Targeting Questions

Cyber currently provides unique value with effects that are comparable to both intelligence collection systems and munitions, occupying a strange space between the previously separable domains of spies and bombs. This presents a challenge in measuring cyber's effects, beyond relatively straightforward information collection.

Each cyber operation, whether it is used to perform intelligence collection or to provide effects, has a relatively fixed process over which it occurs. Therefore, we will use a few example questions to guide us as we progress through the development of this analytical framework:

- Which policies and doctrine are specifically written for cyber operations? (Chap. 2)
- How does cyber threat intelligence (CTI) contribute to analyzing cyber? (Chap. 3)
- How are information operations (IO) currently executed via cyber means? (Chap. 4)
- How is intelligence, surveillance, and reconnaissance (ISR) performed both through cyber and to develop cyber-specific effects? (Chap. 5)
- How do current security technologies make up cyber terrain? (Chap. 6)
- Which key targeting processes lend themselves to cyber operations? (Chap. 7)

- What are the tools and technologies that can be used for designing cyber systems? (Chap. 8)
- What are examples of cyber system metrics? (Chap. 9)
- How is modeling and simulation used for cyber analysis and targeting? (Chap. 10)
- What is a summary of the use cases in this book? (Chap. 11)

We will now look at the overall organization of this book.

1.2 Organization of This Book

This book comprises three major sections, as shown in Fig. 1.3.

Chapter 2 will provide an overview of policy, doctrine, and tactics, techniques, and procedures (TTPs). This will include a review of current policies from multiple countries, current cyber doctrine use, and TTPs applied by cyber defenders on a daily basis.

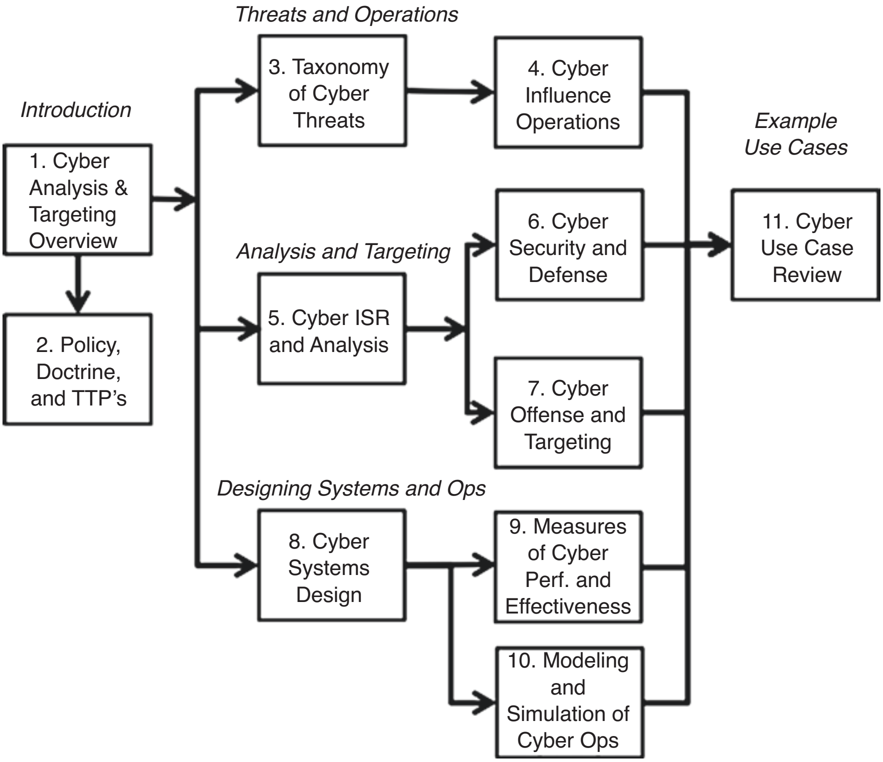
Threats and Operations
Introduction
1. Cyber Analysis & Targeting Overview
2. Policy, Doctrine, and TTP's
3. Taxonomy of Cyber Threats
4. Cyber Influence Operations
Example Use Cases
Analysis and Targeting
5. Cyber ISR and Analysis
6. Cyber Security and Defense
7. Cyber Offense and Targeting
11. Cyber Use Case Review
Designing Systems and Ops
8. Cyber Systems Design
9. Measures of Cyber Perf. and Effectiveness
10. Modeling and Simulation of Cyber Ops

Fig. 1.3 Chapter flow of cyber analysis and targeting

Chapter 3, looking at the taxonomy of cyber threats, will discuss government industry standard cyber threat frameworks (e.g., NIST, MITRE), describing how they are used to facilitate cyber analysis and targeting.

Chapter 4 will describe influence operations, providing the reader with a general framework for analyzing information operations, providing current examples of point and area targeting in cyber influence operations.

Chapter 5 will compare current cyber to mature intelligence, surveillance, and reconnaissance (ISR) frameworks and techniques. This will include a look at how current cyber data collection and aggregation can be used for analysis and targeting.

Chapter 6 will review defensive cyber operations methodologies (e.g., DHS resilience framework, Australian eight-step approach) and evaluate current techniques, along with suggesting methods for increasing probability of detection, while decreasing false alarm rates.

Chapter 7 will expand on the targeting doctrine discussion in Chap. 2, looking at the overall people, process, and technology elements of a cyber system to guide the reader through targeting components of socio-technical stack of a cyber system.

Chapter 8 will expand on cyber systems as described by architectural products. This includes the development of an example cyber collection system via an architecture description method.

Chapter 9 will expand on effects evaluation using a comparison between cyber and autonomous systems. This will include looking at the cyber collection system architecture from Chap. 8 to develop metrics for the example cyber system.

Chapter 10 will provide a review of cyber modeling and simulation, discussing the parallel and series elements of a cyber system. This will include using a discrete event system to describe an example target process, introducing Cohen's *d* for effect estimates. We will also discuss the current state of constructive modeling.

Chapter 11 will provide use cases, referenced throughout the chapters, to capture key analysis and targeting insights.

Bibliography

9/11 Commission. (2004). *The 9/11 Commission Report.* Retrieved 8 4, 2019, from https://www.9-11commission.gov/report/911Report.pdf

Acton, J. M. (2017). Cyber weapons and precision guided munitions. In A. L. G. Perkovich (Ed.), *Understanding cyber conflict*. Georgetown.

Andrei Soldatov, I. B. (2015). *The red web - the struggle between Russia's digital dictators and the new online revolutionaries*. Public Affairs.

Barton Whaley, & Susan, S. A. (2007). *Textbook of political-military counterdeception: Basic principles and methods*. National Defense Intelligence College.

BBC. (2016, October 27). *18 revelations from Wikileaks' hacked Clinton emails* . Retrieved 21 Aug 2018, from BBC: https://www.bbc.com/news/world-us-canada-37639370

Ben Collins, G. R. (2018, 3 1). Leaked: Secret documents from Russia's election trolls . Retrieved 9 9, 2018, from Daily Beast: https://www.thedailybeast.com/exclusive-secret-documents-from-russias-election-trolls-leak?ref=scroll

Bennett, C. (1995). *How Yugoslavia's destroyers harnessed the media.* Retrieved 8 27, 2018, from PBS frontline: https://www.pbs.org/wgbh/pages/frontline/shows/karadzic/bosnia/media.html

Bernstein, J. (2017). *Secrecy world - inside the Panama papers investigation of illicit money networks and the global elite*. Henry Holt and Company.

Bowden, M. (2011). *Worm - the first digital world war*. Atlantic Monthly Press.

Carr, J. (2012). *Inside cyber warfare: Mapping the cyber underworld*. O'Reilly Media.

Cleary, G. (2019, 6). Twitterbots: Anatomy of a propaganda campaign. Retrieved 7 6, 2019, from Symantec: https://www.symantec.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation

David Leigh, L. H. (2011). *WikiLeaks - inside Julian Assange's war on secrecy*. Public Affairs.

Department of Defense. (n.d.). Operation desert fox. Retrieved 6 24, 2020.

Diresta, R. (2018, 3 8). *How Isis and Russia won friends and manufactured crowds*. Retrieved 7 7, 2019, from wired.: https://www.wired.com/story/isis-russia-manufacture-crowds/

Doman, C. (2016, 7 6). The first cyber espionage attacks: How operation moonlight maze made history. Retrieved 8 4, 2019, from Medium: https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7

Domscheit-Berg, D. (2011). *Inside Wikileaks - my time with Julian Assange at the World's Most dangerous website*. Crown.

Dustin Volz, J. F. (2016, March 24). *U.S. indicts Iranians for hacking dozens of banks*. Reuters.

Economist. (2007, 7 12). *A world wide web of terror.* Retrieved 8 11, 2019, from Economist: https://www.economist.com/briefing/2007/07/12/a-world-wide-web-of-terror

England, R. (2019, 8 13). *UN claims North Korea hacks stole $2 billion to fund its nuclear program.* Retrieved 8 18, 2019, from Engadget: https://www.engadget.com/2019/08/13/un-claims-north-korea-hacks-stole-2-billion-to-fund-its-nuclear/

Ferguson, N. (2018). *The square and the tower - networks and power, from the freemasons to Facebook*. Penguin.

FireEye. (2014). *APT28: A Window Into Russia's Cyber Espionage Operations?* Retrieved 9 9, 2018, from FireEye: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

FireEye. (n.d.). *APT 29*. (FireEye, Producer). Retrieved 9 9, 2018, from APT 29: https://www.fireeye.com/current-threats/apt-groups.html#apt29

Gallagher, M. (2008). *Cyber analysis workshop. MORS*. MORS.

George Cybenko, G. S. (2016). Quantifying covertness in deceptive cyber operations. In V. S. S. Jajodia (Ed.), *Cyber deception: Building the scientific foundation*. Springer.

George Cybenko, J. S. (2007). Quantitative foundations for information operations.

George Perkovich, A. E. (2017). *Understanding cyber conflict - 14 analogies*. Georgetown.

Global Security. (2005). Global security. Retrieved from Letter from al-Zawahiri to al-Zarqawi: https://www.globalsecurity.org/security/library/report/2005/zawahiri-zarqawi-letter_9jul2005.htm

Michael R. Gordon, H. C. (2017, 4 6). *Dozens of U.S. Missiles Hit Air Base in Syria.* Retrieved 8 21, 2019, from New York Times: https://www.nytimes.com/2017/04/06/world/middleeast/us-said-to-weigh-military-responses-to-syrian-chemical-attack.html

Harris, G. (2018, 3 4). State Dept. was granted $120 million to fight Russian meddling. It has spent $0. Image. Retrieved 9 9, 2018, from New York Times: https://www.nytimes.com/2018/03/04/world/europe/state-department-russia-global-engagement-center.html

Hayden, M. V. (2016). Playing to the edge: American intelligence in the age of terror.. Peguin.

Heli Tiirmaa-Klaar, J. G.-P. (2014). *Botnets*. Springer.

Eric M. Hutchins, M. J. (2012). *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.* Retrieved 8 6, 2019, from Lockheed Martin.: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Katelyn Polantz, S. C. (2018, 7 14). 12 Russians indicted in Mueller investigation . Retrieved 9 9, 2018, from CNN: https://www.cnn.com/2018/07/13/politics/russia-investigation-indictments/index.html

Koblentz, G. D., & B. M. (2013). Viral warfare: The security implications of cyber and biological weapons. *Comparative Strategy, 32*(5), 418–434.

Koerner, B.I. (2016, October 23). Inside the cyberattack that shocked the US government. Retrieved September 7, 2018, from Wired: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

Lamothe, D. (2017, 12 16). How the Pentagon's cyber offensive against ISIS could shape the future for elite U.S. forces. Retrieved 8 27, 2018, from Washington Post: https://www.washingtonpost.com/news/checkpoint/wp/2017/12/16/how-the-pentagons-cyber-offensive-against-isis-could-shape-the-future-for-elite-u-s-forces/?utm_term=.8cce44e017f9

Launius, S. (2019). Evaluation of comprehensive taxonomies for information technology threats. Retrieved 3 7, 2019, from SANS: https://www.sans.org/reading-room/whitepapers/threatintelligence/evaluation-comprehensive-taxonomies-information-technology-threats-38360

Lewis, D. (2015, March 31). Heartland Payment Systems Suffers Data Breach. *Forbes*.

Lewis, J. (2012). *Significant cyber incidents since 2006*. Center for Strategic and International Studies.

MacEslin, D. (2006). Methodology for determining EW JMEM.. TECH TALK.

Mark Gallagher, M. H. (2013). Cyber joint munitions effectiveness manual (JMEM). *Modeling and Simulation Journal*.

Maurer, T. (2016, 12 17). *'Proxies' and Cyberspace.* Retrieved 8 17, 2019, from Carnegie Endowment for International Peace: https://carnegieendowment.org/2016/12/17/proxies-and-cyberspace-pub-66532

Maurer, T. (2018, 7 27). Cyber proxies and their implications for Liberal democracies. Retrieved 8 17, 2019, from WASHINGTON QUARTERLY : https://carnegieendowment.org/2018/07/27/cyber-proxies-and-their-implications-for-liberal-democracies-pub-76937

Mazetti, M. (2018, July 13). 12 Russian agents indicted in Mueller investigation.

McGee, M. K. (2017, January 10). *A New In-Depth Analysis of Anthem Breach*. Retrieved September 7, 2018, from Bank Info Security: https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

McGlasson, L. (2009, 1 21). *Heartland Payment Systems, Forcht Bank Discover Data Breaches*. Retrieved 9 9, 2018, from Bank Info Security: https://www.bankinfosecurity.com/heartland-payment-systems-forcht-bank-discover-data-breaches-a-1168

Merriam Webster. (n.d.). *cyber.* Retrieved from https://www.merriam-webster.com/dictionary/cyber

Middleton, C. (2018, 6 25). Cyber attack could cost bank half of its profits, warns IMF. Retrieved 8 22, 2018, from Internet of Business: https://internetofbusiness.com/fintech-cyber-attack-could-cost-bank-half-of-its-profits-warns-imf/

Mueller, R. (2019). *Report on the investigation into Russian interference in the 2016 presidential election*. U.S. Department of Justice.

Nakashima, E. (2012, 9 12). *Iran blamed for cyberattacks on U.S. banks and companies.* Retrieved 8 18, 2019, from Washington Post: https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html?noredirect=on

Nakashima, E. (2018, 10 23). *Pentagon launches first cyber operation to deter Russian interference in midterm elections.* Retrieved 3 12, 2019, from Washington Post: https://www.washingtonpost.com/world/national-security/pentagon-launches-first-cyber-operation-to-deter-russian-interference-in-midterm-elections/2018/10/23/12ec6e7e-d6df-11e8-83a2-d1c3da28d6b6_story.html?utm_term=.8c47d573557b

Nakashima, E. (2019, 2 27). *US disrupted Internet access of Russian troll factory on day of 2018 midterms.* Retrieved 3 12, 2019, from Washington Post.

Nancy A. Youssef, S. H. (2017, 11 25). *Why did team obama try to take down its NSA Chief?*. Retrieved 8 27, 2018, from The Daily Beast: https://www.thedailybeast.com/why-did-team-obama-try-to-take-down-its-nsa-chief

Newman, L. H. (2017, September 8). *THE EQUIFAX BREACH EXPOSES AMERICA'S IDENTITY CRISIS*. Retrieved September 7, 2018, from Wired: https://www.wired.com/story/the-equifax-breach-exposes-americas-identity-crisis/

Nichols, M. (2019, 8 5). North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report. Retrieved 8 17, 2019, from Reuters: https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyber-attacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX

Parham, J. (2017, 10 18). Russians posing as black activists on FACEBOOK is more THAN fake news. Retrieved 8 22, 2018, from Wired: https://www.wired.com/story/russian-black-activist-facebook-accounts/

Paul Ducheine, Jelle van Haaster (2014). Fighting power, targeting and cyber operations. Retrieved 8 4, 2019, from CCDOE - 2014 6th International Conference on Cyber Conflict: https://www.ccdcoe.org/uploads/2018/10/d2r1s9_ducheinehaaster.pdf

Pegues, J. (2018). *Kompromat - how Russia undermined American democracy*. Prometheus.

Richard, A. C., & Robert, K. (2012). *Cyber war: The next threat to National Security and what to do about it*. Ecco.

Richard Clarke, R. K. (2011). *Cyber war: The next threat to National Security and what to do about it*. Ecco.

Riley, C. (2019, 7 9). *UK proposes another huge data fine. This time, Marriott is the target.* Retrieved 8 21, 2019, from CNN: https://www.cnn.com/2019/07/09/tech/marriott-data-breach-fine/index.html

Sanger, D. E. (2016, 4 24). U.S. cyberattacks target ISIS in a new line of combat. Retrieved 8 27, 2018, from New York Times: https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html

Sanger, D. E. (2017). Cyber, drones and secrecy. In A. E. G. Perkovich (Ed.), *Understanding cyber conflict*. Georgetown.

David E. Sanger (2018, July 15). Tracing Guccifer 2.0's many tentacles in the 2016 election. Retrieved September 9, 2018, from New York Times: https://www.nytimes.com/2018/07/15/us/politics/guccifer-russia-mueller.html

David E. Sanger, Eric Schmitt. (2017, 6 12). U.S. Cyberweapons, used against Iran and North Korea, are a disappointment against ISIS. Retrieved 8 27, 2018, from New York Times: https://www.nytimes.com/2017/06/12/world/middleeast/isis-cyber.html

Stoll, C. (2005). *The Cuckoo's egg: Tracking a spy through the maze of computer espionage*. Pocket Books.

Strategy and Tactics of Guerilla Warfare. (n.d.). Retrieved 9 9, 2018, from Wikipedia: https://en.wikipedia.org/wiki/Strategy_and_tactics_of_guerrilla_warfare

Catherine A. Theohary, John Rollins (2011, 3 8). Terrorist use of the internet: Information operations in cyberspace. Retrieved 8 22, 2018, from Congressional Research Service: https://digital.library.unt.edu/ark:/67531/metadc103142/m1/1/high_res_d/R41674_2011Mar08.pdf

U.S. Joint Forces Command. (2011, 5 20). Commander's handbook for attack the network. Retrieved 8 4, 2019, from https://www.jcs.mil/Portals/36/Documents/Doctrine/pams_hands/atn_hbk.pdf

U.S. Justice Department. (2019, March). Report on the investigation into Russian interference in the 2016 presidential election. Retrieved May 9, 2019, from U.S. Justice Department: https://www.justice.gov/storage/report.pdf

US Army. (n.d.). Joint Technical Coordinating Group for Munitions Program Office.

Weaponeering. (n.d.). History of the joint technical coordinating Group for Munitions Effectiveness. Retrieved 8 19, 2019, from Weaponeering: http://www.weaponeering.com/jtcg_me_history.htm

Wikipedia. (n.d.). Chaos computer Club. Retrieved 9 9, 2018, from Wikipedia: https://en.wikipedia.org/wiki/Chaos_Computer_Club

Zetter, K. (2014a). *Countdown to zero day - Stuxnet and the launch of the World's first digital weapon*. Crown.

Zetter, K. (2014b, 12 3). SONY GOT HACKED HARD: WHAT WE KNOW AND DON'T KNOW SO FAR. Retrieved 9 9, 2018, from Wired: https://www.wired.com/2014/12/sony-hack-what-we-know/

Chapter 2
Cyber Policy, Doctrine, and Tactics, Techniques, and Procedures (TTPs)

The purpose of this chapter is to present a general background on cyber policy, doctrine, and tactics, techniques, and procedures (TTPs) and describe their role in providing guidance for cyber analysis and targeting. This will include a listing of national cyber policies, a look at the current cyber doctrine, and a review of TTPs as both examples and frameworks that capture analysis and targeting in cyberspace operations.

Policy, Doctrine, and TTP Questions to be Addressed in Chapter 2

1. What are the definitions of policy, doctrine, and TTPs? What are cyber examples of each?
2. How is cyber policy used for both defensive and offensive cyber operations?
3. What are the key drivers for cyber doctrine?

2.1 Background

Policy, doctrine, and TTP development over the last century directly influence both the composition and operation of current cyber systems and provide a framework for cyber analysis and targeting. For example, cyber policy protections span from national infrastructure to an individual's privacy rights when using the Internet. Similarly, doctrine, in providing guidance for future cyber operations, distills the "lessons learned" from successful employment of particular TTPs. In getting started, we will review foundational definitions before going into examples of policy, doctrine, and TTPs in current usage for cyber.

- Policy: usually cyber protection
- Doctrine: leverage existing targeting documents as they apply to cyber
- Tactics, techniques, and procedures (TTPs): developing; unique to cyber due to novel/fungible maneuver space

J. M. Couretas, *An Introduction to Cyber Analysis and Targeting*,
https://doi.org/10.1007/978-3-030-88559-5_2

2.1.1 Policy, Doctrine, and TTP Definitions

We will start this chapter with definitions for cyber policy, doctrine, and TTPs. As shown in Fig. 2.1, policy provides overall direction for moving toward an end-state. Doctrine describes lessons learned and best practices, or teachings in the field. And TTPs provide the attack process, style, and specific steps taken during both cyber analysis and targeting.

As shown in Fig. 2.1, policy provides the overall scope for an organization's approach to an issue. We use the following definition for policy:

Policy A course or principle of action adopted or proposed by a government, party, business, or individual. Also, a high-level, overall, plan, embracing the general goals and acceptable procedures, especially of a governmental body (Merriam-Webster)

While policies are organizational practices, or a deliberate system of principles, to guide decisions and achieve rational outcomes, doctrines are beliefs, developed through experience, that are taught as a form of institutional knowledge.

Doctrine A principle or position or the body of principles in a branch of knowledge or system of belief (Merriam-Webster)

While doctrine provides teachings, and policies represent organizational practices, TTPs provide details concerning how, specifically, an individual goal is achieved.

Tactics, Techniques, and Procedures (TTPs): The term tactics, techniques, and procedures (TTPs) describes an approach for analyzing an actors operation or can be used as means of profiling behavior (e.g., MITRE CARET (MITRE)).

Tactics: outline the way the actor chooses to operate over a course of action (COA). For example, tactics are associated with the achievement of short–/

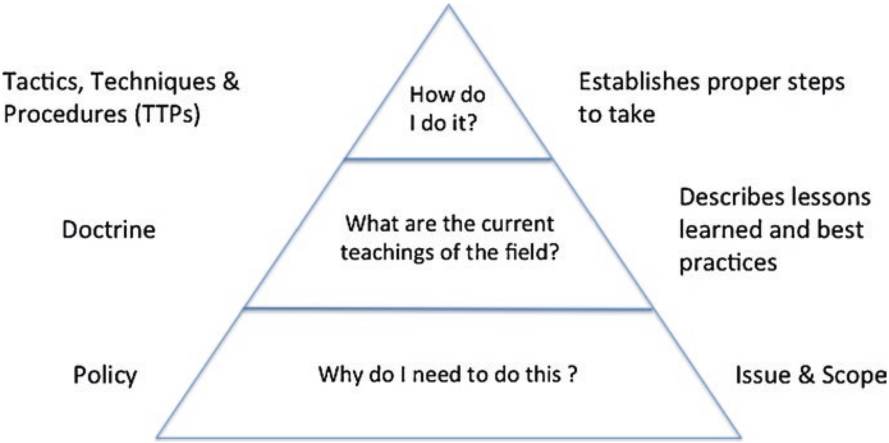
Tactics, Techniques & Procedures (TTPs)
How do I do it?
Establishes proper steps to take
Doctrine
What are the current teachings of the field?
Describes lessons learned and best practices
Policy
Why do I need to do this ?
Issue & Scope

Fig. 2.1 Policy, doctrine, and TTP triangle

medium-term goal(s) via one out of many possible ways that involve human factors as the subject and means of these tactics.

Techniques: related to the target, its technicalities, and specific details, which imply or suggest a specific way to get something done; for example, installing/uninstalling a backdoor to an information system, performing a scan, etc.

Procedures: more prescriptive; procedures are the steps to get something done.

Another definition for TTPs is that tactics are means to implement strategies. Techniques are means to implement tasks. Procedures are then the standard, detailed steps that prescribe how to perform a specific task.

In tracing the development of current operational guidance and procedures, we will review examples that illustrate current national, and international, policy/doctrine /TTP implementation.

2.2 Introduction

Mass networked government, business, and personal computers emerged in the mid-1990s. The 1990s to present is therefore the time period that we have to cite examples, case studies, and lessons learned that provides the current corpus of guiding cyber policy, doctrine, and best practices for cyber analysis and targeting. Because of this relatively short history of networked computers, or cyber systems, especially for operations, the terminology for cyber analysis and targeting policy, doctrine, and TTPs are often borrowed from legacy fields (e.g., radio).

Cyber policy is used to protect information systems. Estonia's recent passing of the "Huawei Law," (Reuters, 2020) as a means of providing telecom gear reviews, is an example of using policy, via law, to protect their information infrastructure. In addition, resilience, defined as "the capacity to recover quickly from difficulties, or toughness," is the foundation for many national cyber policies. This is similar to ensuring continuity of government through any other national emergency (e.g., hurricanes, power outages).

Many National Cyber Strategies, or policy implementations, focus on the security aspects of cyber, in accord with the legacy of maintaining secure radio communications. This is often called cyber resilience, or an entity's ability to sustain operations in a cyber-contested environment. In addition to this focus on resilience, some national strategies (e.g., the United States and Canada) include commercial considerations for expanding the use of cyberspace. The US Department of Defense (DoD) is a pioneer in discussing cyber as a contestable operational domain, potentially challenging the other warfare domains (e.g., Space, Air, Sea, Land) with denied or inaccurate information transmissions.

The DoD Cyber Strategy (Department of Defense (DoD), 2018) provides policy guidance to several Joint Publications (JP) as doctrinal guidance for cyber operations; the primary documents are:

- JP 2-0, Joint Intelligence: describes the role of cyber-related intelligence collection and analysis in developing an overall intelligence picture.
- JP 2-01.3, Joint Intelligence Preparation of the Operational Environment (JIPOE): defines the role of cyber in describing the operational environment.
- JP 3-12, Cyber Operations: defines effects (e.g., denial, integrity), along with discussing the different missions over which cyber operations should be considered.
- JP 3-0, Joint Operations: the top-level publication for military operations that shows how cyber fits into the context of all military operations.
- JP 3-12: describes military operations in cyberspace.
- JP 3-13, Information Operations: where a broader view of potential cyber applications is considered for operations.
- JP 3-13.2, Military Information Support Operations (MISO): describes the role of MISO to collect, analyze, and disseminate information, including over cyber channels.
- JP 3-13.4, Military Deception: explains the role of deception principles and mechanisms that are delivered to targets over channels; cyber is but one channel used to deliver deception to military targets.
- JP 3-60, describes the integration of cyberspace operations in joint targeting.

For example, JP 3-12, Cyber Operations, defines effects (e.g., denial, integrity), along with discussing the different scenarios /TTPs over which cyber operations should be considered. JP 3-12 is complimented by JP 3-13, Information Operations (IO), where a broader view of potential cyber applications is considered for operations. This includes using both MISO for intelligence collection and the use of deception for prosecuting a military target. JP 3-60, Joint Targeting, provides the overall process for any targeting operation, including cyber.

In addition to military use of cyber operations, there are “best practices” that are derived from observing tactics, techniques, and procedures (TTPs), in the form of use cases that occur frequently enough to be categorized together. The SANS Critical Security Controls (CSCs) (SANS, 2016), 20 best practices, in order of priority, is one example of practical knowledge, distilled from known TTPs, to provide defensive cyber personnel with step-by-step approaches for securing cyber infrastructure from possible attack. In addition, the SANS CSCs are a bottoms-up view of providing cyber defenders with “doctrine” for defending our networks. Cyber policy, providing broader guidance than the use case based implementation of current cyber doctrine, benefits from a historic look at naval policy formation and implementation.

2.3 Policy

Using policy for cyber analysis and targeting provides a general view. One approach for looking at cyber policy is to compare it to a similar issue we faced almost a half a millennia ago—maritime threats (Table 2.1).

As shown in Table 2.1, cyber (in)security has similarities to maritime analogies through which we get the majority of our goods and services. In addition, the rapid growth of computer-based systems, or cyber, as a business and socialization tool, is paired with its adoption across supply chains that transparently underpin many of our day-to-day transactions. Because of the risk of cyber threats to these transactions, cyber policies have been adopted by many major governments (Table 2.2).

As shown in Table 2.2, most of the national cyber strategies focus on defense, or resilience. An additional policy introduced by the European Union is the General Data Protection Regulation (GDPR), a general law on data protection and privacy (European Union, n.d.). Slightly different than the national-level policies provided in Table 2.2, the GDPR provides more individual protections, sometimes fining organizations for unauthorized release of private data (Riley, 2019).

The US DoD, however, concerns itself with performing operations in a cyber-contested environment, which includes maintaining resilience of supporting infrastructure (e.g., critical infrastructure). In addition to the documents given in Table 2.2, multiple executive orders (EOs) (White House) and doctrine have been published to provide more specific steps to mostly defend current cyber equities (U.S. National Archives) (George Washington University).

As shown in Table 2.3, multiple executive orders (EOs) address cyber from both a personnel and technical standpoint. However, the frequency of EOs increased rapidly in the mid-2010s, and accelerated after Russian involvement in the 2016 US presidential election, with additional EOs designed to manage foreign participation in the US telecommunication sector (Trump, 2020). An additional EO was signed just before this book's publishing in response to the recent Solar Winds software supply chain attack (Trump, 2020).

While EOs add national-level emphasis to a particular thread of cyber defense, a key challenge to developing policy for cyber analysis and targeting is the ability to understand an adversary, especially with respect to attributing an attack. As shown in Table 2.1, the range of attackers spans from individuals to nation states. While civil and criminal laws are the domain for individual perpetrators, the line between crime and war is fuzzy for cyber actions. This is a challenge because a cyber

Table 2.1 Comparison between actors on the sea and in cyberspace (Egloff, 2017)

Actor type	Sea	Cyberspace
State actors	Navy (including mercenaries; e.g., blockades)	Cyber operators, intelligence analysts, contractors, tool/capability providers (e.g., denial of service botnets, specialty information operations developers)
Semi-state actors	Shipping/transportation; mercantile companies	Major telecommunications companies, technology developers, security vendors
	Privateers	Patriotic hackers, some cyber criminal elements (e.g., exfiltrations)
Non-state actors	Pirates (e.g., theft)	Hackers, cyber criminal elements (including organized crime; e.g., exfiltrations)

Table 2.2 Cyber policy documents (White House, International Partners, Department of Homeland Security [DHS], and DoD)

Title	Description
National Cyber Strategy (White House, 2018)	Leverage cyber to accomplish 4 pillars
	Pillar I Protect the American People, the Homeland and the American Way of Life
	Pillar II Promote American Prosperity
	Pillar III Preserve Peace through Strength
	Pillar IV Advance American Influence
UK National Cyber Security Strategy 2016–2021 (HM Government, 2016)	Document describing vision for 2021 is that the UK is secure and resilient to cyber threats, prosperous, and confident in the digital world.
Australian Cyber Strategy (Australian Government, 2018)	Achieve five themes of action
	1. A national cyber partnership
	2. Strong cyber defenses
	3. Global responsibility and influence
	4. Growth and innovation
	5. A cyber smart nation
Canadian National Cyber Security Strategy (Government of Canada, 2018)	Engage in the Cyber Domain via
	1. Security and Resilience
	2. Cyber Innovation
	3. Leadership and Collaboration
Singapore's Cyber Security Strategy (Singapore, 2016)	Engage in the Cyber Domain via
	1. A Resilient Infrastructure
	2. A Safer Cyberspace
	3. A Vibrant Cybersecurity Ecosystem
	4. Strong International Partnerships
Cyber Security Strategy (Department of Homeland Security (DHS), 2018)	Leverage cyber to accomplish 5 pillars
	Pillar I Risk Identification
	Pillar II Vulnerability Reduction
	Pillar III Threat Reduction
	Pillar IV Consequence Mitigation
	Pillar V Enable Cyber Scenario Outcomes
Department of Defense (DoD) Cyber Security Strategy (Department of Defense (DoD), 2018)	The Department's cyberspace objectives are
	1. Ensuring the Joint Force can achieve its missions in a contested cyberspace environment

(continued)