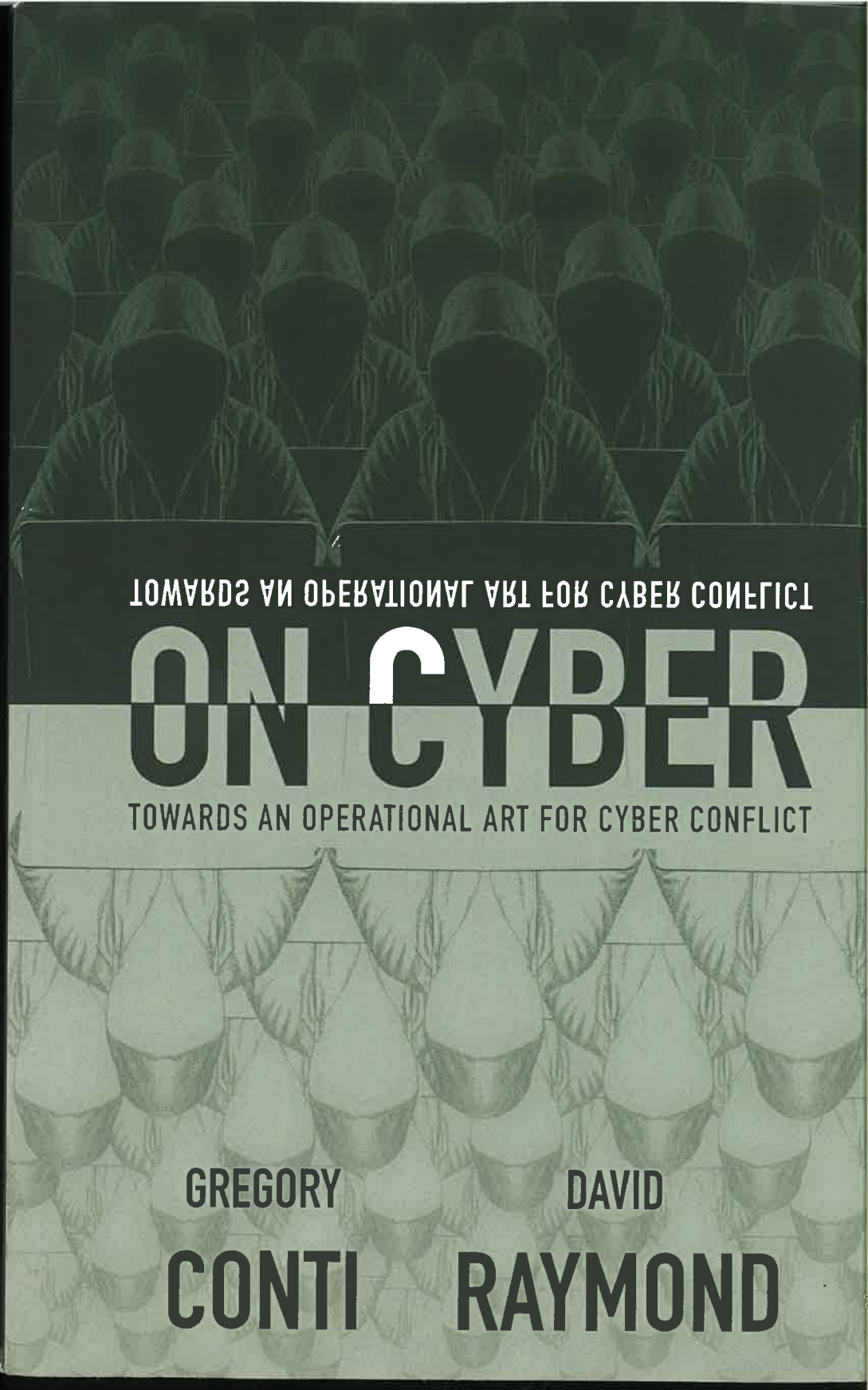

ON CYBER

TOWARDS AN OPERATIONAL ART FOR CYBER CONFLICT

GREGORY CONTI

DAVID RAYMOND

CONTENTS

1 INTRODUCTION

"Cyber is Conflict in Code for Control"
- Captain Roy Ragsdale[11]

Cyber conflict is ongoing now.[12] Actors of all stripes—from empowered individuals to nation-states—fight to achieve their goals in cyberspace. They do so by conducting cyberspace operations, either alone or in conjunction with physical operations. All future military engagements of any magnitude will likely include some aspect of cyber operations, which seek to achieve objectives in or through cyberspace.[13] Cyber conflict certainly isn't isolated to military organizations. Enterprises are facing nation state aggressors on a regular basis in this domain. This type of war isn't as physically destructive as kinetic conflict, at present, but it is certainly undermining the national security of the United States and other countries.

Cyber conflict is harder to perceive since many effects occur in cyberspace alone, but there is no doubt that nations are active in cyberspace, stealing intellectual property on a massive scale, reading the U.S. president's email, placing backdoors at strategically important locations, subverting the supply chain of critical infrastructure, and attacking major corporations, including Sony, Sands Casino, HBO, and Saudi Aramco.[14] Much more is possible, but for now there are limited actors with both the will and the capability to do more damaging attacks, like take down power grids, disrupt stock markets, or shut down hospitals.[15] As we look to the future, cyber operations will certainly cause significant real world disruption, destruction, and even death. Over the past months we've seen attacks against the U.S. presidential election campaigns, allegedly by a foreign power, that directly influenced the U.S. election. Medical devices, automobiles, military weapon systems, satellites,

voting machines, and smart cities, all have proven vulnerable to cyber attacks. These attacks, both on the battlefield and at the national-level, are growing increasingly serious.

Technology's allure and potential efficiencies have drawn governments, businesses, militaries, and individuals *en masse* to adopt technical solutions that enable governance, commerce, and national security. You cannot live in modern times and avoid cyberspace. These digital systems are insecure, converging into risky monocultures, yet we depend on them. Nations that have a love affair with expensive weapon systems rely on them doubly so. Military systems that have a long procurement pipeline measured in years, or even decades, have vulnerabilities based on their use of dated software and hardware that must be addressed before they are exploited by their adversaries. Additionally, no nation has unlimited resources to dedicate to its military. The driving force behind new technologies is efficiency. It is unlikely that there are sufficient service members allocated to operate and maintain new, cyber-enhanced systems, and still maintain traditional "stubby pencil" back-up techniques for when those systems fail. Despite this constraint, training under degraded network conditions is absolutely necessary; all systems should have manual modes, and all units should occasionally train under constrained conditions in which they lack their technical tools. Every minute spent on technical training increases the unit's dependency on its digital systems.[16]

Actors who do not want to engage the United States and other powerful nations on a conventional battlefield will likely turn to cyberspace operations to wield power. The United States seeks unqualified dominance on the battlefield, but this isn't easy in cyberspace. The normal rules of military power do not apply. One cannot just count tanks on each side to determine the likely victor. The proliferation of technology, combined with a low cost of entry, allows non-traditional powers to arise and potentially impact everyone. Asymmetries abound, and we are seeing the rise of hybrid warfare that uses affordable and sophisticated technology and enables a threat actor to inflict disproportionate harm on its opponents.[17] Figure 1-1 depicts a military model of the spectrum of conflict and our assessment of the current state of cyberspace.

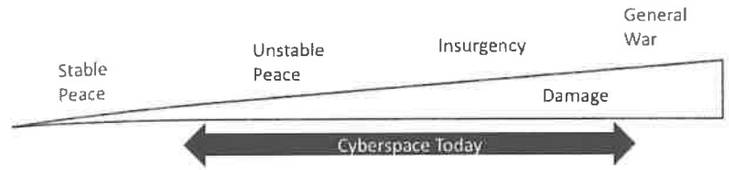

Figure 1-1: In military doctrine the spectrum of conflict ranges from a stable peace to all-out war. As depicted by the arrow, cyberspace today is unsettled at best, with spikes of destructive activity by nation-state actors against companies as well as in the hybrid warfare strategy employed during the Russian invasion of Ukraine.[18]

A Hacker's Apology

This book is written for an audience of military and civilian information security professionals. For our information security readers, we offer a short disclaimer. This book is about "cyber." We acknowledge that this phrase chafes at some, especially the hacker and information security communities. We were in the room when "cyber" won a DEF CON Recognize award for worst cyber security buzzword.[19] We get it. But we've lost the battle. The term "cyber" isn't going away anytime soon, not when there are entire armies organized around it and most of the world is following suit. Information security has its place, the defense of systems and information, penetration testing, reverse engineering, vulnerability scanning, social engineering, and other concepts, but cyber transcends InfoSec. Where InfoSec could be a component of the tactics employed in cyber operations, cyber is about thinking at scale. Cyber considers how to defend nations in cyberspace, how armies fight in the cyber domain, how a nation-state might conduct a cyber siege of a city, and how a combat division might integrate cyber effects with kinetic battlefield operations.[20]

Additionally, the use of military jargon in computer security is starting to gain the same disdain that "cyber" has gained. People in the InfoSec community, particularly those in marketing, often misappropriate and oversimplify military terminology. Nonetheless military terminology and concepts are extremely powerful if employed correctly, an assertion this book seeks to prove.

With our disclaimer in place let's define *cyber* as we use it in this book.[21] We use *cyber* to mean attacking, defending, or collecting information from other computers, where *computers* is used broadly to mean electronic systems that collect, process, store, and communicate information.[22] We consider

cyberspace as the sum of the computing systems, networks, and data which permeate our global environment. These systems and networks are usually interdependent and include the Internet and isolated computing networks all the way down to the sensors, chips, and code that run individual devices.[23] *Electronic warfare* intersects with cyber operations, but focuses on military actions that use electromagnetic and directed energy to control the electromagnetic spectrum or to attack an adversary.[24] *Information Technology* (IT) operations are the provisioning, use, and maintenance of information technology infrastructure that we use day-to-day.[25]

In this book we use the language of warfighting because at its heart our book is about how nations fight wars in cyberspace. The inception of this book was based on a conversation we had with an information security friend who frequently encountered nation-state teams attacking his networks. He described a situation when he was forced to decide whether to cut off an intruder in his network or allow the intruder to continue to operate so he could collect additional information about the attacker's tactics and techniques. He lamented that there ought to be a term to describe this condition. We told him there is, it is called *intel gain/loss*, which led to a discussion about the military and intelligence community having concepts that are very applicable to the information security practitioner in industry. This random encounter at the ShmooCon hacker conference started our chain of thinking that took us through multiple conference talks and ultimately led to this book's creation. The military does indeed have terms and concepts useful for cyber security. The book will sound aggressive and warlike, which unfortunately is the nature of war. We will use appropriate military language throughout the book, but strive to make it accessible to a non-military audience. The military lexicon will help information security practitioners think differently, and at the right level of scale, when facing nation-state enabled threat actors.

This book isn't solely about how the military approaches cyber operations, although we think the military should use some of our ideas more often. Rather, it also describes how military thinking can be used to improve the way other organizations approach their own cybersecurity. Meticulous planning, detailed training, and deliberate decision-making are hallmarks of military operations, and many outside the military can learn valuable lessons from these standard practices. This book takes many of these military processes and planning techniques and applies them to cyber in a way that hasn't been done before—not even by the military.

"A serious problem in planning against American doctrine is that the Americans do not read their manuals, nor do they feel any obligation to follow their doctrine."
- Attributed to Unknown Cold War-era Soviet Author[26]

A Soldier's Apology

For our military readers, this book is about military and nation-state cyber operations. By necessity, it isn't a doctrinal manual. For those unfamiliar with the military, doctrine is codified in the manuals and frameworks upon which military units operate. For some military personnel, doctrine is holy writ, and for others, something to be ignored. Most are somewhere in between. At present, military doctrine for cyberspace operations is unsettled and ranges from muddled[27] to a "great start."[28] There is not, and may never be, a canonical "right" answer. That means we are free to choose, extend, or ignore models and frameworks from the military doctrines of any nation. Most importantly, we are free to challenge doctrine before our adversaries do and, ideally, to get ahead of doctrine in order to improve future iterations.

At present, militaries are largely moving blindly into the era of cyber. Traditional doctrine doesn't always fit, and many aspects of cyber operations are counterintuitive to those with limited technical expertise. Our goal is to help provide a glimpse into future possibilities by providing an overarching framework with which to analyze and understand cyber operations and their impact on warfighting, as well as enterprise defense and national security. With that goal in mind, this book uses the language of technology and information security. At times, this language will be unfamiliar, but it is necessary to describe cyber operations with precision. We will attempt to define new terms as we go; however, we do ask that you meet us halfway and look-up terms you are unfamiliar with, lest the book become a primer on InfoSec and not a book on how nations fight wars in cyberspace today and in the future. For someone, who hasn't interacted with the information security community and studied its rich body of work, you may be surprised to find that much about cyber conflict is in the public domain.

Inside the military there are many naysayers[29] who tend to believe that cyber is the domain of "REMFs," soldiers in the rear echelon, people you can ignore. Believe this if you will, but you would be naively wrong. We are always in real or imminent contact with adversaries in cyberspace. We argue that militaries should focus on strategic threats in cyberspace and not be drawn to their comfort zone of focusing heavily on the tactical battlefield. Battlefield innovation is important, but it pales in comparison to the

cyberspace as the sum of the computing systems, networks, and data which permeate our global environment. These systems and networks are usually interdependent and include the Internet and isolated computing networks all the way down to the sensors, chips, and code that run individual devices.[23] *Electronic warfare* intersects with cyber operations, but focuses on military actions that use electromagnetic and directed energy to control the electromagnetic spectrum or to attack an adversary.[24] *Information Technology* (IT) operations are the provisioning, use, and maintenance of information technology infrastructure that we use day-to-day.[25]

In this book we use the language of warfighting because at its heart our book is about how nations fight wars in cyberspace. The inception of this book was based on a conversation we had with an information security friend who frequently encountered nation-state teams attacking his networks. He described a situation when he was forced to decide whether to cut off an intruder in his network or allow the intruder to continue to operate so he could collect additional information about the attacker's tactics and techniques. He lamented that there ought to be a term to describe this condition. We told him there is, it is called *intel gain/loss*, which led to a discussion about the military and intelligence community having concepts that are very applicable to the information security practitioner in industry. This random encounter at the ShmooCon hacker conference started our chain of thinking that took us through multiple conference talks and ultimately led to this book's creation. The military does indeed have terms and concepts useful for cyber security. The book will sound aggressive and warlike, which unfortunately is the nature of war. We will use appropriate military language throughout the book, but strive to make it accessible to a non-military audience. The military lexicon will help information security practitioners think differently, and at the right level of scale, when facing nation-state enabled threat actors.

This book isn't solely about how the military approaches cyber operations, although we think the military should use some of our ideas more often. Rather, it also describes how military thinking can be used to improve the way other organizations approach their own cybersecurity. Meticulous planning, detailed training, and deliberate decision-making are hallmarks of military operations, and many outside the military can learn valuable lessons from these standard practices. This book takes many of these military processes and planning techniques and applies them to cyber in a way that hasn't been done before—not even by the military.

"A serious problem in planning against American doctrine is that the Americans do not read their manuals, nor do they feel any obligation to follow their doctrine."
- Attributed to Unknown Cold War-era Soviet Author[26]

A Soldier's Apology

For our military readers, this book is about military and nation-state cyber operations. By necessity, it isn't a doctrinal manual. For those unfamiliar with the military, doctrine is codified in the manuals and frameworks upon which military units operate. For some military personnel, doctrine is holy writ, and for others, something to be ignored. Most are somewhere in between. At present, military doctrine for cyberspace operations is unsettled and ranges from muddled[27] to a "great start."[28] There is not, and may never be, a canonical "right" answer. That means we are free to choose, extend, or ignore models and frameworks from the military doctrines of any nation. Most importantly, we are free to challenge doctrine before our adversaries do and, ideally, to get ahead of doctrine in order to improve future iterations.

At present, militaries are largely moving blindly into the era of cyber. Traditional doctrine doesn't always fit, and many aspects of cyber operations are counterintuitive to those with limited technical expertise. Our goal is to help provide a glimpse into future possibilities by providing an overarching framework with which to analyze and understand cyber operations and their impact on warfighting, as well as enterprise defense and national security. With that goal in mind, this book uses the language of technology and information security. At times, this language will be unfamiliar, but it is necessary to describe cyber operations with precision. We will attempt to define new terms as we go; however, we do ask that you meet us halfway and look-up terms you are unfamiliar with, lest the book become a primer on InfoSec and not a book on how nations fight wars in cyberspace today and in the future. For someone, who hasn't interacted with the information security community and studied its rich body of work, you may be surprised to find that much about cyber conflict is in the public domain.

Inside the military there are many naysayers[29] who tend to believe that cyber is the domain of "REMFs," soldiers in the rear echelon, people you can ignore. Believe this if you will, but you would be naively wrong. We are always in real or imminent contact with adversaries in cyberspace. We argue that militaries should focus on strategic threats in cyberspace and not be drawn to their comfort zone of focusing heavily on the tactical battlefield. Battlefield innovation is important, but it pales in comparison to the

existential threats we face at the national level. When was the last time we faced an armored division in head-to-head combat? There might not be a next time because we might cease to exist as a nation if we fail to secure our critical infrastructure. If you are uncomfortable with technology and you won't believe in cyber unless an adversary's hands reach out from your monitor to choke you, then we ask that you reconsider. We must not ignore this slow bleed happening in the United States.

Combat Power

Militaries fight by bringing combat power—including leadership, information, and the forces at their disposal—to bear against an adversary with the objective of eliminating the enemy's will to fight. These tools include intelligence, fires and effects, logistics, protective measures, and maneuver, all under a unifying command and control architecture.[30] At any given time, combat power is the sum of all of the combined destructive, constructive, and information capabilities a military unit can muster.[31] These powerful concepts apply equally well to cyberspace and cyber/kinetic operations. In this book, we'll examine each element of combat power in depth in the context of the cyber and cyber/kinetic domains.

Cyberspace is a battlespace impacted by a number of factors, including policy, economics, diplomacy, and military operations. For those of us familiar with the inception of the Internet and its accompanying nobly egalitarian goals, we wish that cyberspace wasn't a battleground, but the strategic value of the Internet has grown to such an extent that it can no longer simply be a garden for intellectual discourse and a playground for hackers. Cyberspace is too important to be ignored by those in power, and there they vie for dominance. Militaries seek to maintain freedom of action for themselves and deny the same to their enemies.[32] Freedom of action means the ability to operate as you wish without impediment, with the ultimate objective being to achieve cyberspace superiority and, by extension, superiority in the air, land, sea, and space so that your side has a decisive advantage in military operations. The extent that "freedom of action" and "cyberspace superiority" can actually be achieved in practice is yet to be determined.

Levels of War

Militaries organize their actions into three primary levels: Strategic, Operational, and Tactical.[33]

- Strategic: The strategic level employs the elements of national power to accomplish national and multi-national objectives.
- Operational: The operational level is the art and science of employing tactical operations, allocating resources, and assigning tasks and missions to achieve objectives. It is at this level we think of "campaigns," which are a planned series of operations, over time, designed to accomplish these objectives.
- Tactical: The tactical level is compromised of the planning and executing of battles, engagements, and other activities to achieve low-level objectives.

These three levels are useful in the context of cyber operations as well (see Figure 1-2). Information security operates primarily at the tactical level and is of short duration. Nation states take a longer-term perspective, implementing their strategies as a series of campaigns. InfoSec defenders who think in terms of campaigns are more effective than those who constrain themselves to tactics and isolated incidents.[34]

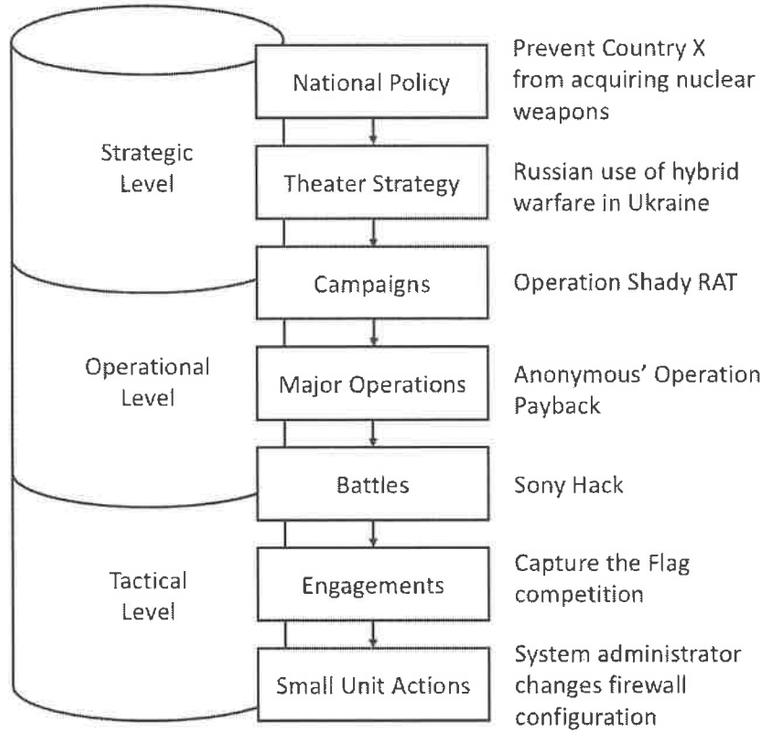

Figure 1-2: The levels of war: strategic, operational, and tactical mapped to major aspects ranging from national policy down to small unit actions, and annotated with representative cyber operations examples.[35]

Readiness[36]

To fight and win, militaries must be ready. Readiness means that units are well trained, fully staffed, and equipped with the best available tools. They must constantly listen and learn to be more lethal, professional, and technically competent than their adversaries. To accomplish these goals, leaders must take care of their troops. These kinetic-centric dictums align closely with the needs of military cyber units, although the challenges are greater. Leaders must fight through a critical shortage of cyber talent,[37] overcome slow acquisition systems, adapt to constantly evolving technology, track agile adversaries, and ignore alluring private sector opportunities, to create an environment where the best people want to stay and build the most skilled and powerful cyber force.

Automated Combat

War is one of the most physically taxing activities possible. During conflicts, humans struggle to plan battles and campaigns using imperfect intelligence on very tight timetables, usually hours or days for tactical engagements and weeks or months for campaigns. Tools such as the Military Decision Making Process (MDMP) provide frameworks to make the best decisions despite imperfect information, fatigue, and limited time.[38] As technologies advance, however, humans will become increasingly distant from real-time decision making. We don't believe we will be seeing truly automated war as seen in the famous *Star Trek* episode *A Taste of Armageddon*, in which computers simulate battles and citizen "casualties" step into disintegration booths. At present, we see augmented human decision-making through battlefield command and control systems, predictive analytics, and semi-autonomous weapons systems such as the Phalanx close-in weapon system, used to defend against anti-ship missiles. Some online and physical battles will always occur at human speed, but we will absolutely see fighting online and in the physical world at speeds that far exceed human perceptual and cognitive processing abilities. Humans will be simply too slow. Perhaps the closest analog is that of high frequency and algorithmic trading on Wall Street.[39] The days of a sweaty command post filled with laboring staff officers driving all decisions are numbered, as was the trader-filled floor of the New York Stock Exchange of the twentieth century. Machine-speed attacks at a grand scale require integrated machine speed responses.

Multidisciplinary Cyber

Many mistakenly think that cyber is purely an InfoSec problem and squarely in the domain of expert technologists, particularly computer scientists. They don't understand that cyber is inherently multidisciplinary. To be honest, we did not buy into this idea at first, but we are now believers. Every discipline has some intersection with cyber (see Figure 1-3). Natural starting points are the disciplines of computer science, computer engineering, and electrical engineering. These people write the code and design and build computing systems, the ones with hands-on immediacy. But political scientists apply the rich toolset of international diplomacy and policy to tackle cyber-related challenges. And legal scholars and attorneys apply the law to enable legal cyber operations and punish transgressors. Political scientists and lawyers make up much of the nation's senior leadership who create law and policy to complement technical cyber security solutions. Much of information security revolves around economics. Economists study such things as malware economies to identify and help correct perverse incentives, analyze the impact of crypto currencies like Bitcoin, and trace back through complicated funding streams to identify online threat actors. Psychologists strive to create usable security and understand what causes people to perform unsafe online actions. Military science practitioners study strategy and tactics and act as cyber mission planners. Linguists study threat actor languages, including slang and jargon, to enable improved information collection. Historians bring us wisdom about the past, applying rich knowledge of warfare and technology so that we aren't doomed to repeat mistakes.

We have not fully plumbed the depths of the intersection between each discipline and how its tools and domain knowledge can be applied to both securing cyberspace and the conduct of cyberspace operations. Specialists are necessary to push the state of the art, but we also envision cyber leaders who have a solid technical foundation as well as advanced skills in policy, law, psychology, and a mix of other disciplines in the right amounts. We are still too early in the experimentation phase to get this ideal balance right.

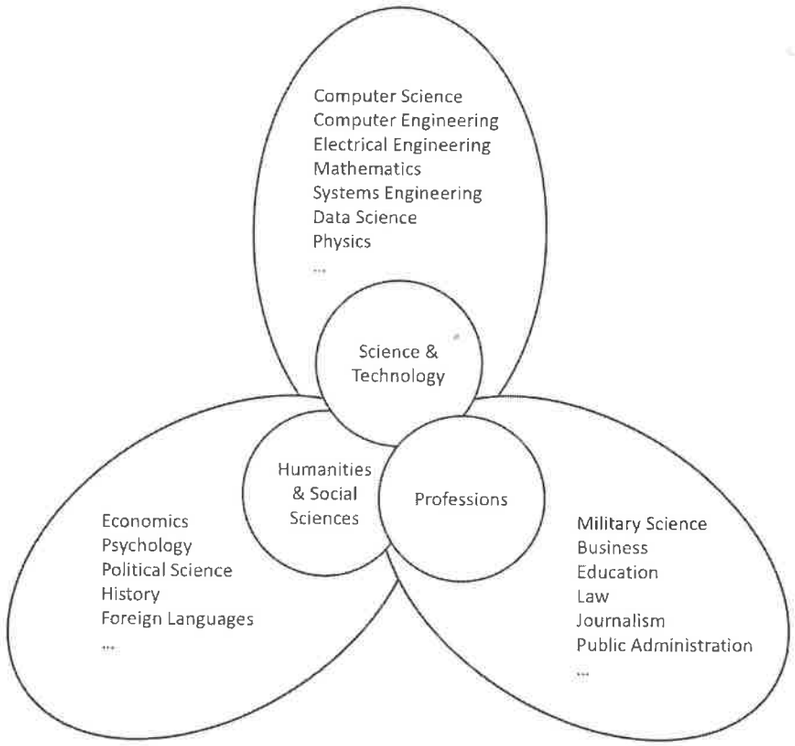

Figure 1-3: Cyber is inherently multidisciplinary. Every discipline has important tools and domain knowledge that can be brought to bear against cyber security challenges and enable the conduct of cyber operations.

Cyber operations can be covert and hard to detect, or noisy and deliberately disruptive. Much of the historical cyber operations occurring online have been quiet, with the exception of a few high profile attacks on Sony Pictures Entertainment, Saudi Aramco, and the Sands Casino, among others. Recently, we've seen the cyber operations employed by Russia in its incursions into Ukraine and their take down of the power grid.[40] Fueled by technological advancement, the rate of change in cyber warfare is much faster than advances in kinetic warfare. As a result, militaries are continually moving into unknown territory. Agile and innovative actors have the distinct advantage here. It is in the best interest of militaries to establish forward-looking organizations that are staffed by multidisciplinary cyber experts to continually explore over the horizon and prevent strategic surprise. The U.S.

Army did this by founding the Army Cyber Institute.[41] In a time of resource constrains, dedicating resources to explore the future may feel painful, but is doubly necessary for cyberspace operations.

Conclusions

Make no mistake: Cyber conflict is raging now. Much goes on unseen, but we see glimpses of the larger picture in the headlines every day. The military has many useful tools and frameworks for coping at scale with a spectrum of conflict, but militaries have a long way to go and may never catch up given the relentless press of Moore's Law and technical advancement. Most of these military tools need tailoring to be useful in the cyber domain, but we've presented several adapted examples and will add more throughout the book, as well as numerous new additions that we've designed ourselves based on our understanding of existing military doctrine. Militaries are designed to fight other militaries and are used to fighting at scale. Unfortunately, enterprises today are regularly attacked by nation-state enabled threat actors, and they need military grade strategies and tactics to survive. As we mentioned, military doctrine for cyber operations is immature, as evidenced by the litany of embarrassing military and government compromises and data spills that populate today's news headlines. However, traditional kinetic military thinking about fighting wars is mature and time-tested. In this book, we've worked hard to map and extend these robust kinetic principles to cybersecurity and cyber operations in novel and useful ways for both the enterprise and the nascent military cyber operations community.

The strength of the military's way is wrapped up in the process: deliberate planning, deliberate training, and highly structured decision-making. Most organizations don't plan their security operations. Instead, they rely on "heroes" (those highly knowledgeable and productive individual masterminds who save the day for everyone), best practices, and vendors. Just as the military cannot rely on its officers to all be Napoleons, organizations need a way to squeeze performance from insufficient cybersecurity resources. Flexible organizational structures and adaptive teams make this possible, not just talented individuals with exceptional intellectual capacity.