EXPERT INSIGHT

Cyber Warfare – Truth, Tactics, and Strategies

Strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare

Foreword by:
Gregory J. Touhill
CISSP, CISM (Brigadier General, USAF ret.)

Dr. Chase Cunningham

Packt

Cyber Warfare – Truth, Tactics, and Strategies

Strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare

Dr. Chase Cunningham

Packt>

BIRMINGHAM - MUMBAI

Cyber Warfare – Truth, Tactics, and Strategies

Producers: Andrew Waldron, Jonathan Malysiak
Acquisition Editor – Peer Reviews: Divya Mudaliar
Content Development Editor: Ian Hough
Technical Editor: Aniket Shetty
Project Editor: Tom Jacob
Copy Editor: Safis Editing
Proofreader: Safis Editing
Indexer: Priyanka Dhadke
Presentation Designer: Pranit Padwal

First published: February 2020

Production reference: 1210220

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.
ISBN 978-1-83921-699-2

www.packt.com

This book is dedicated to all those digital warriors who operate in a never-ending game of digital cat and mouse. Warriors like Shannon Kent, Blake Mclendon, and countless others who have given all while taking the fight to the enemy. May God bless those select few that are engaged with the enemy in a boundaryless battlefield. Keep up the good fight brothers and sisters!

packt.com

Subscribe to our online digital library for full access to over 7,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

Why subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Learn better with Skill Plans built especially for you
- Get a free eBook or video every month
- Fully searchable for easy access to vital information
- Copy and paste, print, and bookmark content

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.Packt.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at customercare@packtpub.com for more details.

At www.Packt.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

Foreword

The last fifty years have witnessed a tremendous revolution. This revolution continues to rage all around us, threatening to redefine international borders; destroying long-cherished businesses and institutions; disrupting our social fabric and norms; challenging our privacy; and calling into question what is right and what is wrong. Often referred to as the "Information Revolution," this revolutionary technological transformation continues its relentless march around the globe.

As the Information Revolution transformed the world and the advent of the World Wide Web brought internet access into homes around the world, pundits came to adopt the "Cyber" moniker from William Gibson's 1984 novel *Neuromancer* to describe the new domain of human experience. As the World Wide Web continued its expansion in the 1990s, "Cyber" soon became a prefix added to words highlighting the impact of digital technology to everyday activities. Soon, internet cafes were rebranded as "Cyber Cafes," offering internet access to those who didn't have a computer or internet access. The explosive growth of internet connectivity throughout society saw new terms like cyberspace, cyberpunks, cyberbully, cybercrime, cyberstalker, cyberporn, and other like terms added to the lexicon.

It wasn't long before this newly minted "cyber domain" became a source of potential conflict, earning the interest of the world's military powers. For example, during my Air Command and Staff College classes in 1994, I penned a monograph positing a unified cyber command and describing how cyber capabilities could be used as an instrument of national power in lieu of kinetic strikes. Such thinking was not unique in military circles.

For example, in 1999, two Chinese People's Liberation Army colonels, Qaio Liang and Wang Xiangsui, wrote a seminal book on military strategy, *Unrestricted Warfare*, which highlighted how China could leverage non-traditional means to attack an opponent, including leveraging attacks in the networked digital world. Not long after, in December 2005, the United States Air Force added "cyberspace" as a warfighting domain to its mission statement, highlighting the importance of cyber operations in military doctrine. With that Air Force mission statement, "Cyber Warfare" came of age.

The infamous Prussian general and military theorist Carl von Clausewitz said, "War is politics by other means." A century later, the noted humorist and philosopher Julius "Groucho" Marx said, "Politics is the art of looking for trouble, finding it everywhere, diagnosing it incorrectly, and applying the wrong remedies." I submit that both Clausewitz and Marx's statements apply to today's so-called "Cyber Warfare."

Sadly, we have seen too many people declaring themselves as experts in "Cyber Warfare." I contend that anyone who says they are an expert isn't. The cyber domain is vast, incorporating numerous skills and specialties. During my decades of experience in the cyber domain, I have witnessed many so-called "Cyber Experts" whose non-technical background often leads them to fall victim to superficial analyses that invariably lead to inaccurate conclusions that are often passed on as gospel to others.

Fortunately, we have those like Dr. Chase Cunningham who indeed can and should be considered a "Cyber Expert." With deep experience in cyber operations, forensics, research, and domain leadership, he understands the broad cyber domain and is able to (to paraphrase Groucho) discern what is trivial versus what is real trouble. He uses his real-life experience to diagnose it properly, and has the technical heft to apply the right remedies. In an era rife with self-declared cyber experts, Chase Cunningham is the real deal and presents this much-needed book to help the reader truly understand Cyber Warfare.

In my book, *Cybersecurity for Executives: A Practical Guide*, I state that cybersecurity is a risk management issue and not just a technology problem. I highlighted that people, process, and technology are all critical parts of any cybersecurity program. In this great book, Dr. Cunningham provides outstanding analysis and description of the cyber domain in a manner that even a cyber-neophyte (Yes, I note the irony of me deliberately using a cyber-prefixed word) would understand.

The chapters presented are crisp and clear; each worthy of a college class. In Chapter One, he describes the continually evolving threat landscape and the strategic implications of this dynamic threat environment. Chapter Two is logically placed in the discussion as Dr. Cunningham explains why the traditional castle moat-like perimeter defense model has become obsolete and how this challenges our strategic risk and investment decisions. From there, in Chapter Three, he discusses how adversaries are adapting their tactics, techniques, and procedures to gain a strategic advantage to achieve their goals as well as what we can and should do to thwart them.

Those who do not have deep technical background will benefit to pay particular attention to the next three chapters. Chapter Four discusses influence operations, where attackers seek to manipulate the reader's views and persuade them to make certain decisions favorable to the attacker's objectives. This cyber warfare topic is highly relevant in today's hotly-contested political environment where charges of influence operations in the 2016 US presidential election remain part of the daily discourse. Chapter Five presents a fascinating discussion of how "DeepFakes" and Artificial Intelligence/Machine Learning technology are the next cyber battleground. Chapter Six demonstrates how cyber adversaries are increasing sophisticated in their operational employment of advanced campaigns. Here Dr. Cunningham forecasts what are the most likely courses of action and identifies what remain "science fiction."

The next three chapters provide practical analysis and guidance of great value. Chapter Seven highlights the importance of strategic planning to thwart future cyber threats. Chapter Eight discusses the types of cyber tools that are used to conduct cyber operations.

Some readers may be surprised to find that many are what I call, "dual-use tools," that is, tools that can be used for both offensive and defensive purposes. Chapter Nine is a seminal discussion of how tactics, when properly applied, enable strategy in cyber warfare.

At the beginning of this foreword, I stated that the Information Technology revolution threatens to redefine international borders; to destroy long-cherished businesses and institutions; to disrupt our social fabric and norms; to challenge our privacy; and call into question what is right and what is wrong. As he concludes this book, Dr. Cunningham addresses these conditions, discusses the future of cyber warfare and forecasts how it will impact society, governments, and technology. I believe his projections are noteworthy, and ones we all should be paying particular attention to. As such, *Cyber Warfare – Truth, Tactics, and Strategies* is a necessary handbook for all who seek to understand cyber operations and the world we live in.

"Si vis pacem, para bellum." ("If you wish peace, prepare for war." Quote from Publius Flavius Vegetius Renatus.)

GREGORY J. TOUHILL, CISSP, CISM
Brigadier General, USAF (ret)

Contributors

About the author

Dr. Chase Cunningham focuses on helping senior technology executives with their plans to leverage comprehensive security controls and the use of a variety of standards, frameworks, and tools to enable secure business operations. His work focuses on integrating security into operations, leveraging advanced security solutions, empowering operations through artificial intelligence and machine learning, and planning for future growth within secure systems.

Dr. Cunningham served as a director of cyber threat intelligence operations at Armor. He was the computer network exploitation lead for Telecommunication Systems and the chief of cyber analytics for Decisive Analytics. Dr. Cunningham is a retired U.S. Navy chief with more than 20 years' experience in cyber forensic and cyber analytic operations. He has past operations experience, stemming from time spent in work centers within the NSA, CIA, FBI, and other government agencies. In those roles, he helped clients operationalize security controls, install and leverage encryption and analytic systems, and grow and optimize their security operations command systems and centers.

Chase holds a Ph.D. and M.S. in computer science from Colorado Technical University and a B.S. from American Military University focused on counter-terrorism operations in cyberspace.

I want to thank all the visionaries and innovators that I have had the luck of coming across over the years. Those insightful leaders who help shape our collective future and hopefully lead us all to a more secure and prosperous future.

About the reviewer

Glen D. Singh, CEH, CHFI, 3xCCNA (cyber ops, security, and routing and switching) is a cyber security instructor, author, and consultant. He specializes in penetration testing, digital forensics, network security, and enterprise networking. He enjoys teaching and mentoring students, writing books, and participating in a range of outdoor activities. As an aspiring game-changer, Glen is passionate about developing cyber security awareness in his homeland, Trinidad and Tobago.

Glen is also the lead author of the following books:

- Learn Kali Linux 2019
- Hands-On Penetration Testing with Kali NetHunter
- CompTIA Network+ Certification Guide
- CCNA Security 210-260 Certification Guide

I would like to thank Divya Mudaliar for having me as part of this project, Tom Jacob and Ian Hough for their continuous support during this journey, and the wonderful people at Packt Publishing, thank you everyone.

Table of Contents

Preface v

Chapter 1: A Brief History of Cyber Threats and the Emergence of the APT Designator 1

- Hackers aren't what Hollywood shows us 1
- The Battle of the Beams 4
- Modem hacks 5
- Anti-virus growth 6
- The dawn of Advanced Persistent Threats (APTs) 7
- Early APT attacks 12
- Confusion in cyber defense 14
- US and allied cyber defense establishment 14
- The cyber shot heard round the world 15
- Tit-for-Tat cyber warfare 19
- Pandora's box busts open 20
- Conclusion 23
- References 24

Chapter 2: The Perimeter Is Dead 25

- A scenario detailing holes in the model 26
- A global perimeter falls 28
- Even compliant organizations' perimeters fail 32
- Governments' perimeters fail 34
- Users, BYOD, and the obliteration of the perimeter 36
- Applications add to insecurity 40
- Authentication methods failed 41
- IoT devices poke holes in any perimeter 45
- You can't fix stupid, or evil 47
- Conclusion 53
- References 53

Chapter 3: Emerging Tactics and Trends – What Is Coming? 55
Attacks move downstream 56
Autonomous vehicles…Bad data, bad day 59
Drones…Death from above 64
Threat actors combine tactics to optimize attack effectiveness 71
Ransomware goes mobile 76
DDoS reaches weapons-grade refinement 80
Conclusion 83
References 84
Chapter 4: Influence Attacks – Using Social Media Platforms for Malicious Purposes 87
The new cyber onslaught 88
Cyber combat is changing 89
#Hashtag or ammunition? 90
Influencing the influencers 98
Conclusion 103
References 104
Chapter 5: DeepFakes and AI/ML in Cyber Security 107
From big screen to smartphone – the dawn of DeepFakes 108
Defining DeepFakes 108
GANs power DeepFakes 109
Applied DeepFakes, AKA DeepMastersPrints 116
Hacking voice using ML, AKA DeepVoice 119
ReadFakes 125
Breaking news may mean breaking bad 127
When data and AI "studies" go awry 129
Conclusion 132
References 133
Chapter 6: Advanced Campaigns in Cyber Warfare 135
Cyber warfare campaigns 137
Indian Nuclear Plant campaign 139
Chinese manufacturing campaign 140
The US and Libya election interference campaign 142
False flags corrupt campaign attribution in cyberspace 144
Mapping campaigns to matrices 145
Threat groups avoid attribution intentionally 150
Modifying command and control for confusion 151
Naming the beast 152
Sometimes it doesn't add up 153
Chaos is the goal 153

Cyber attack campaigns for the coming decade **154**
Hoaxing 155
Conclusion **160**
Chapter 7: Strategic Planning for Future Cyber Warfare **163**
Everyone has a plan until they get punched in the mouth **164**
What type of strategy? **165**
When the nature of combat demands a change in strategy **167**
Infiltration does not equal dominance 168
Leaders need to have their "boots on the ground" 170
The environment determines what works, not the equipment 171
Intelligence and "Intel" may not be the same thing 174
Too much may be too much 175
Big walls can mean big problems 177
The mission was not accomplished… 179
What does an effective strategy in cyberspace look like? **184**
Changing strategic concepts 185
Strategically defending the "Edge" 186
Eat the elephant 189
The orchestration enables the strategy 191
Conclusion **193**
Chapter 8: Cyber Warfare Strategic Innovations and Force Multipliers **195**
Defensive tooling and strategic enablers **196**
Meet the Monkey 197
More offerings from the Infection Monkey 201
Advanced uses of the Infection Monkey 203
The Software-Defined Perimeter 206
Application whitelisting 213
Offensive tooling and strategic enablers **216**
Why kill the password? 217
WhatBreach 218
SNAP_R 223
Running the SNAP_R attack (sample commands) 224
Comment faking for influence 225
Conclusion **227**
References **228**
Chapter 9: Bracing for Impact **229**
Disclaimer **230**
Micro-segmentation is a key to survival **230**
What is micro-segmentation? 231

Micro-segmentation tools and technologies 233
A pragmatic application for SDN 235
Possible pitfalls in micro-segmentation 237
Reclaiming the "high ground" 239
Kill the password, limit the pain 244
Intelligence collection 251
Conclusion 256
References 257
Chapter 10: Survivability in Cyber Warfare and Potential Impacts for Failure 259
What good are laws in war? 260
"Law 1" – Default means dead 262
"Law 2" – Think strategically, move tactically 267
"Law 3" – Details, details 270
"Law 4" – Kill the password 271
"Law 5" – Limit the blast radius 276
Impact from failure 280
Compromising healthcare 281
Bringing down ICS (Industrial Control Systems) 282
Threatening the fates of nations 283
Threat scenario – DeepFakes 284
Threat scenario – Data manipulation 285
Threat scenario – Attacking democratic processes 285
Conclusion 286
Appendix – Major Cyber Incidents Throughout 2019 289
Other Books You May Enjoy 301
Index 305

Preface

This book is for all those cyber security professionals who seek to know the truth behind the history of cyber warfare and are working to secure their infrastructure and personnel for the future. The aim of this book is to cover the topics around cyber warfare tools, tactics, and strategies.

Who this book is for

This book is for any engineer, leader, or professional with either a responsibility for cyber security within their organizations, or an interest in working in this ever-growing field. In particular, CISOs, cyber security leadership, blue team personnel, red team operators, strategic defense planners, executives in cyber security, and cyber security operations personnel should benefit from the insights and perspectives offered in this book.

What this book covers

Chapter 1: *A Brief History of Cyber Threats and the Emergence of the APT Designator* – This chapter will dive into the real history of cyber threats and their emergence in the space and provide some background on nation state APT designations.

Chapter 2: *The Perimeter Is Dead* – In this chapter, we'll go through all the intricacies and details that prove that the perimeter-based model of security failed years ago.

Chapter 3: *Emerging Tactics and Trends – What Is Coming?* – This chapter will be a journey down the rabbit hole into the future of cyber warfare tools and tactics and will provide examples of the new trends in this ever evolving space.

Chapter 4: *Influence Attacks – Using Social Media Platforms for Malicious Purposes* – In this chapter, we will cover the ways in which social media and influence can be weaponized for cyber warfare tactics.

Chapter 5: *DeepFakes and AI/ML in Cyber Security* – In this chapter, you will learn about the reality of AI and ML in cyber security and delve into the practical applications of these often-misunderstood technologies.

Chapter 6: *Advanced Campaigns in Cyber Warfare* – In this chapter, we will get into the types of attack campaigns and their real-world implications.

Chapter 7: *Strategic Planning for Future Cyber Warfare* – In this chapter, we will break down the specifics around how to better plan for cyber warfare and why strategy matters in digital combat.

Chapter 8: *Cyber Warfare Strategic Innovations and Force Multipliers* – This chapter is going to provide specific examples of what tools and technologies there are on the market that can help exponentially increase an organizations defensive posture.

Chapter 9: *Bracing for Impact* – In this chapter, you will be offered examples of how to apply tooling, tactics, and strategies to brace for the impact of a cyber attack and ways in which your organization can better respond when things go awry.

Chapter 10: *Survivability in Cyber Warfare and Potential Impacts for Failure* – In this chapter, we will cover essential ideas for defensive strategic planning and provide real-world examples of what may happen when cyber warfare tactics go big.

Appendix: *Major Cyber Incidents Throughout 2019* – A list of recent major cyber incidents throughout 2019, categorized by the class of attack, as presented in *Chapter 6*.

To get the most out of this book

- Existing cyber security planners and strategists will gain insight into the reality of the space and will be better able to understand how future innovations part of that future state will be.
- This is not a how-to guide; the author does not wish to provide readers with knowledge that could potentially be turned to malicious purposes, but rather this book aims to provide the reader with a new perspective, to see and prepare for what is coming, rather than to be blinded by the threats that are more imminent.
- Cyber security experience is assumed; however, the book also features introductory concepts, which even beginners can take advantage of.

Download the color images

We also provide a PDF file that has color images of the screenshots/diagrams used in this book. You can download it here: `https://static.packt-cdn.com/downloads/9781839216992_ColorImages.pdf`.

Conventions used

`CodeInText`: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. For example: "`Changeme.py` focuses on detecting default and backdoor credentials, and not just common account credentials."

Bold: Indicates a new term, an important word, or words that you see on the screen, for example, in menus or dialog boxes, also appear in the text like this. For example: "The first, and arguably most important, technology is commonly called **Software-Defined Networking** (**SDN**)."

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book, mention the book title in the subject of your message and email us at `customercare@packtpub.com`.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book we would be grateful if you would report this to us. Please visit, `http://www.packt.com/submit-errata`, selecting your book, clicking on the Errata Submission Form link, and entering the details.

Piracy: If you come across any illegal copies of our works in any form on the Internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `http://authors.packtpub.com`.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions, we at Packt can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about Packt, please visit `packt.com`.

1

A Brief History of Cyber Threats and the Emergence of the APT Designator

"I think most people today understand that cyber clearly underpins the full spectrum of military operations, including planning, employment, monitoring, and assessment capabilities. I can't think of a single military operation that is not enabled by cyber. Every major military weapon system, command and control system, communications path, intelligence sensor, processing and dissemination functions – they all have critical cyber components."

– Gen. William L. Shelton, Commander, Air Force Space Command

Hackers aren't what Hollywood shows us

The common perception of a "hacker" is usually that of some individual at home or working in a basement somewhere, cloaked in a cheap hoodie and ingesting copious amounts of caffeine, while hammering away at code sprawled across at least three different monitors or displays.

In these Hollywood representations, the malicious actor is usually smiling and talking to themselves as they craft unique singular exploits that might be used to take down a bank or some world-ending computer system. These overhyped mythical "hackers" are almost always introverts and technical geniuses that are anti-social, anti-government, and often woefully ignorant of the totality of their actions.

In truth, this is not the reality behind the keyboard in the real world of cyber warfare operations. Certainly, in some instances, there must be a "hacker" somewhere that is a representation of this stereotype, but more often than not, the personas behind some of the most malevolent and vicious attacks in cyberspace look nothing like this. In many cases, those malicious actors are wearing a uniform and are paid, protected, and trained by their government – or in some cases, governments. They are exceptionally bright, well trained, highly focused, and creative individuals that have found a niche in their ability to engage in espionage and combat operations anywhere in the world, with any adversary. They are the tip of the digital spear for what is to be the dominant combat environment for the future, and they are the front-line warriors that are constantly engaged in a game of binary cat and mouse that rivals all other wars.

The command of cyberspace in the 21st century is as decisive and impactful as the command of the sea was in the 19th century and the command of the air in the 20th century. Cyberspace is, in all truth, the battlefield on which the war of the future is currently being fought. It is the arena for the New Cold War. An arena in which every nation on Earth, every criminal enterprise, and indeed almost every human on the planet, holds interests and resides. Never in the history of man has there been a location in which global conflict is actively raging in the same space as every business and organization on the planet.

With only about 50 years of history behind it, the internet and global connectivity are expanding at an extraordinary speed. More connections and more data were created and shared or distributed in the last 5 years than in the whole of human history previously.

Cyberspace is now the new platform for political, economic, military, and cultural interactions and engagements. This will be the domain wherein impacts on social stability, national security, economic development, and cultural communication will be made in the next century.

Computer security and the study of computer threats and exploitation have not always been at the forefront of computer science, however. It has only been in the last few decades that the need for, and the power of, cyber espionage and warfare tactics have been realized at an international level. In order to understand the power and efficacy of these digital warriors and the operations in which they hone their craft, it is imperative that we understand where computer exploitation came from, and analyze the evolution of this space; an evolution from a focus on innovation by any means necessary in order to benefit businesses and the consumer, to one of strategic combat on a global scale.

There are a variety of "early instances" of cyber threat activities and operations, and if you were to cobble together 50 different experts on the topic, you would likely have 50 different incidents to discuss as the beginnings of cyber warfare. It is therefore pointless to argue over the absolute particulars of specifics on what was the first or most influential of these attacks throughout time. What is important is to point out and detail a few major exploits and threat activities that stand out as seminal points in time to help us better understand the reality of this space and its evolution toward its future state.

For clarity's sake, in common definitions, a cyber-attack and cyber-defense could be conducted at any scale: from the state level by the military to a major organization, right down to the personal level involving a singular individual. It could be a simple hacking attack, focused mainly on nuisance type outcomes, or the attack could be a long-term, multi-year, large-scale state-launched operation that is aimed at damaging the physical infrastructure of an enemy state. There is no unequivocal "gospel" definition of a cyber-attack, or a cyber threat operation or operator.

However, in most circles familiar with the topic area, it generally refers to *an unauthorized intrusion into a computer or a computer network in such forms as tampering, denial of service, data theft, and server infiltration*. Additionally, there is no real consensus on what constitutes the actual "first" ever cyber-attack, be it by a nation state or a lone operator. Many cite the Morris Worm as one of the first real attacks, while others cite the attacks on the federal network in the early 1980s as the first real appearance of dedicated cyber threat actions. Regardless of the specific chosen threat action in history, in truth, there are so many possible referenceable actions that have occurred that there is no real right answer. What is more important to understand is the reality that the ways in which attacks have occurred in and around cyberspace have evolved from their earliest iterations, and that they are continuing to change and adapt as technology develops.

The Battle of the Beams

One of the earliest attacks leveraging communication- and electron-related conduits was not on a computerized system; those did not exist at the time. While not often widely considered as a direct part of cyberspace operations, signals espionage – an early form of cyberspace warfare, due to its use of communication media and electronic systems – was used to achieve specific operational objectives as far back as World War 2. In one of the earliest instances of leveraging a specific communication medium as a means of conducting espionage for warfare-focused outcomes, the United States and Great Britain launched an attack that would befuddle and confuse the German adversaries for years.

In what would come to be known as "the Battle of the Beams," German bombers navigated from continental Europe to Great Britain by following a radio signal transmitted from a point of origin (Manners, 2016). The German pilots would know they were above their targets when they intercepted a second beam, also transmitted from continental Europe. That system ensured that German night raiders found their targets in the dark and returned home safely – until it was "hacked," that is.

British engineers discovered the German use of radio-frequency telemetry and coordination for the German combat runs and developed countermeasures that would modify the German command signals.

By broadcasting similar signals at precise times on specific German frequencies, British cyber warfare operators fooled the German bombers, causing them to drop their ordnance at a location chosen by the British. Additionally, the British cyber-attacks made return trips nearly impossible for the Germans, many bombers never finding their home base, and a few even landing at Royal Air Force fields, their pilots thinking that they had returned home (Manners, 2016). This use of the frequency spectrum (a critical portion of what is now commonly referred to as cyberspace) created effects that illustrate the operational power of cyberspace half a century before it was to be considered a warfighting domain.

Modem hacks

The first focused instances of computer threat research and exploitation studies actually began during the 1970s and were not even related to computers; they were instead noted as a problem in the telephone-switching network. The phone system was growing so fast and becoming so large that the system had to be integrated and automated to survive. This first automated phone system was built to serve a large test environment, and immediately many problems were discovered. Calls originated and ended on their own, phone numbers were allocated to persons without phones, and a myriad of other issues came to light.

These initial issues were not actually considered a threat as much as they were thought to be a problem for the owners of the systems and those administering the networks. In the 1980s, the modem became the powerhouse means of connecting and managing the large networks that were becoming more and more commonplace, and as such modems became the primary point of compromise from which systems could be hacked.

While there are many different opinions about the first real virus on a computer system, the reality of this becoming a problem for computers did not become prevalent in public literature until the computer became a household item in the mid-1980s. During the "age of modems," groups like the 414s, a group of modem hackers whose name came from their area code, were identified and arrested by the FBI (Hansman, 2003).

The 414 group targeted and exploited the phone networks and modems of Los Alamos National Laboratory and a center for cancer research, using a combination of malicious code and a deep understanding of the flaws in the automation technology that was used by the phone companies at that time. Not long after this first noted computer threat campaign was finalized, the federal government passed the Computer Crime and Abuse Act (CISPA 2010). This legislation detailed what constituted a protected computer and the resulting punishment for those who sought to conduct malicious actions against any protected system (Grance, Kent, & Kim, 2004).

Anti-virus growth

Only a few innovative and industrious companies understood the possible maliciousness that could be wrought by activities such as those conducted by hackers and hacker groups.

Consequently, it was during this time that companies such as Symantec and IBM began to research and study viruses and malware to isolate and mitigate the threat. The malware and anti-virus company McAfee was established during this era. John McAfee noticed that many of his friends' and associates' computers were acting abnormally and running very slowly. After some research, he was able to discern that programs had either been installed and were intentionally causing detriment to the system, or programs had begun to simply degrade and harm the system on which they were running.

After some technical research and development, McAfee was able to write specific technical signatures for the anomalies within those programs, and the signature-focused malware and anti-virus system was born (Hutchins, Cloppert, & Amin, n.d.). McAfee's system of signature recognition and anomalous behavior detection was immediately recognized as a pivotal point in mitigating and detecting these newly recognized threats. Overnight, companies began to follow suit and corporate defensive cyber security operations were effectively "born."

It was not until 1987 that the federal government began to take notice of this type of activity and instituted the first **Computer Emergency Response Team** (**CERT**) (Grance et al., 2004). By the early 1990s, the rate of annual computer virus detection grew to over 1,000 instances per month. As the detection and isolation of computer viruses became a practice area within computer science, the detection and signature generation for viral programs also increased exponentially. By 1995, more than 250,000 viruses or variances of viruses had become commonplace. All of these incidents of early exploits and attacks paled in comparison to the growth of cyber threats that would emerge in the early 21st century.

The dawn of Advanced Persistent Threats (APTs)

The field of specific targeted cyber threats and especially cyber threat research did not truly exist in any real formality prior to the early 2000s, beyond that of what was in practice within the US government and other nation state agencies. The first mentions of cyber threats and cybercrime outside of government arenas appeared in 2001 during an unclassified briefing from the National Security Agency (Werlinger, Muldner, Hawkey, & Beznosov, 2010). This report was actually supposed to be focused on the issue of securing a network as large as that of the **Department of Defense** (**DoD**). However, thanks to leaks and the unclassified nature of the report, the spread of the threats that were becoming common knowledge within the DoD came to light in public circles.