



Cyber

Commander's Handbook

The Weaponry & Strategies of Digital Conflict

technolytics

Preface

As stated in *The Art of War*, one of the oldest and most successful books on military strategy, written by Sun Tzu in the 6th century BC, the key to success in any type of battle is having information about your adversary. For centuries the world's militaries have used scouts for reconnaissance to gather information about the enemy and intelligence about their operations. Today, this strikes at the very core of modern day military strategy and the rapidly evolving era of digital conflict. Understanding your adversary through cyber intelligence has become a critical capability for military planners. Gathering information about an enemy – their systems, processes, and background – is as valuable as knowing what kind of weapons they possess. This concept, called “Know Your Enemy,” has become a well established military and computer hacker philosophy.

Very few organizations today really know who their enemies are, how they might attack, when they might attack, and, perhaps most importantly, the attack modality that might be used. By coupling together “Know Your Enemy” with Scenario-Based Intelligence Analysis (SBIA) and Trans-disciplinary Intelligence Engineering (TIE) techniques, the result provides the ability to derive substantial intelligence about potential attacks, role-play responses, and defensive measures, creating a wealth of knowledge.

Understanding that a new threat exists from cyber warfare and cyber spies is critical to our nation's security. The United States House of Representatives Armed Services Committee has ordered the U.S. Defense Department to facilitate the increase of formal cyber

Cyber Commander's Handbook

warfare training for U.S. troops. The Department of Defense is establishing a professional force of cyber operators and developing cyber career paths for officers, enlisted personnel and civilians. The new Air Force Cyber Command and the Air National Guard are among the focal points of the plan. As many as 40,000 cyber warfare specialists will be trained “as warriors, advocates and visionaries” for cyber operations.

This handbook is a strategic guide that can be used by cyber commanders to understand this threat of cyber warfare and current cyber spying techniques. The content of this handbook has been gathered and synthesized using the techniques mentioned above. Our intent is that this information is put to good use to help today's cyber commanders keep our nation safe.

“The United States is under cyber attack virtually all the time, every day.”

U.S. Defense Secretary

Robert Gates

Table of Contents

- Preface
- Chapter 1 – Introduction
- Chapter 2 – Setting the Stage
- Chapter 3 – Cyber Espionage
- Chapter 4 – Cyber Terrorism
- Chapter 5 – Cyber Intelligence
- Chapter 6 – Cyber Weapons
- Chapter 7 – Disrupters
- Chapter 8 – Cyber Attack Process
- Chapter 9 – Cyber Doctrine and Strategy
- Chapter 10 – Cyber Warfare Infrastructure
- Chapter 11 – Conclusion
- Appendix A – Important Facts & Figures
- Appendix B – Cyber Attack Case Study
- Appendix C – Recent Cyber Intelligence
- Appendix D – Formal Training Program About Technolytics

Electronic high value targets are networks, servers, or routers, whose disruption would have symbolic, financial, political, or tactical consequences.

About Technolytics

The Technolytics Institute (Technolytics) was established in 2000 as an independent executive think-tank. Our primary purpose is to undertake original research and develop substantive points of view on strategic issues facing executives in businesses, government and industry around the world.

Our strategic goals focus on improving critical measures of performance, creating sustainable competitive advantage, delivering innovation and technology, and managing security and risk. We operate three centers: [Business & Commerce] – [Security & Intelligence] and [Science & Technology].

Two strategic issues for businesses, governments and militaries are the rapid evolution of cyber acts of aggression and forecasting what the future of cyber warfare will be. These two important issues are why the Technolytics Institute has dedicated significant resources to understanding this critical area and preparing stakeholders at all levels, through education and advisories, for the current and future challenges of cyber security.

CONTACT INFORMATION

Technolytics
4017 Washington Road
Mail Stop #348
McMurray, PA 15317
info@technolytics.com



Cyber Commander's Handbook

The global reliance on computers, networks and systems continues to grow. As our dependency grows so do the threats that target our military's Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) systems as well as the operational components and electronic controls for our critical infrastructure. Over the past decade we have experienced a substantial rise in the complexity and sophistication of cyber attacks as well as a frightening increase in the impact of some of the attacks. Every computer is a potential cyber weapon waiting to be loaded and used by extremists, criminals, terrorists and rogue nation states.

As the world becomes more and more dependent on computers and information technology, the greater the risk of cyber attacks. Government and military leaders now face this fact and our critical systems and infrastructure remain at great risk! This risk has made the ability to defend these critical systems and direct cyber attacks core capabilities required for the modern military. In the age of cyber conflict, leaders need to understand the weapons and strategies used to wage this rapidly evolving type of warfare.

This handbook will provide the background needed to understand the new world of cyber warfare, define the tools and techniques for offensive and defensive action, and provide insight into the strategies behind building a dynamic and relevant cyber warfare capability.



\$29.95
ISBN 978-0-578-03935-0
52995 >

9 780578 039350