Foreword

WHY A BOOK ON CYBER WARFARE IS IMPORTANT

> *". . . it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation," Obama said, adding, ". . . we're not as prepared as we should be, as a government or as a country" [1].*

According to the Director of National Intelligence James Clapper, "The cyber warfare threat facing the United States is increasing in scope and scale and its impact is difficult to overstate" [2]. A variety of educational institutions, both military and civilian, are grappling with the question, "What should we teach each and every one of our students about cybersecurity?" When these students take their places as leaders and officers in the defense of our country, they need to be aware of this persistent threat.

Today's threatscape is constantly changing, adapting to our countermeasures and continuing to successfully pursue various missions ranging from identity theft, to criminal and nation-based corporate espionage, and, in the case of a worm called Stuxnet, to sabotage. Only a decade ago we had kids attacking systems for the thrill of it; then it was criminals attacking identities. Now it appears to be more about social media, ideology, and insider threats. This book provides great graphics for the threatscape and challenges we are facing today.

In May, the Atlantic Wire reported China was winning the cyberwar, in part because they had accessed US physical war plans. Also last week Edward Snowden claimed the United States and Israel co-wrote the Stuxnet worm to damage the Iranian Nuclear program; today, we are still trying to figure out exactly how Stuxnet worked. And while WikiLeaks and Anonymous (the ideology-driven group intent on punishing organizations that did not support WikiLeaks) have been in the news of late, the theft of RSA two-factor authentication intellectual property is especially chilling. If access control fails, everything fails. Identity theft is so commonplace that it is no longer newsworthy. How many people in the United States have had their identity stolen? Many experts say all of them. There is just so much stolen data that the criminals have not yet figured out how to use them all. But they will. Criminal groups are hiring computer scientists to run their cyber-based scams and mine the results. The term *cyber warfare* is becoming part of discussions on national security. Cybersecurity is an issue that can impact us at the personal level as users of the Internet and at the national defense level as an advanced, persistent threat.

WHY SHOULD YOU READ THIS BOOK

Everyone needs to understand the risks to our information so that we can make an informed decision regarding the steps that we might take to secure it.

The Internet connection in your home that you use to talk to friends with Skype, play games, and send email may also be used to conduct crimes, undertake international espionage, and quite possibly fight a new kind of war.

This new Wild West of the Internet matters to each of us at both the personal and national levels. *Cyber Warfare* is focused more on the national level and what the Department of Defense (DoD) has done and is doing.

A week doesn't go by without a story of a cyber attack, hacker group causing a data breach or malcode spreading across the Internet. Cyber Warfare puts the threatscape into context by showing how the threat operates as well as how all the different stories relate to one another.

If you work with the US government, or want to know what the US government is doing to organize and respond to the cyber threat, *Cyber Warfare* lays it out in comprehensive detail. The authors will show you how cyber attacks and defense intersect with each of the classic warfighting domains of land (Army), sea (Navy), air (Air Force), space (Joint, with Air Force in the lead), and cyber (ubiquitous, with US Cyber Command [USCYBERCOM] just getting organized).

Cyber Warfare covers the doctrine being developed today and lays out the tactics, techniques, and procedures of Computer Network Operations (CNO) including attack, defend, and exploit (the military term for reconnaissance or spying), plus the new aspect of social engineering. On a personal note, it is easy to read about social engineering and think "yeah, yeah, yeah," but I, among many others, friended Robin Sage, a fake personality created by a security researcher to see how much data could be collected, on Facebook.

Switching from the "what" to "how" in the later chapters, *Cyber Warfare* considers the "why," as the authors explore the ethics and legal issues of this new battlefield. Then the book defines and analyzes the challenges facing cyberspace. Finally, it looks at trends in this arena.

Cyber Warfare will provide readers with a strong foundational understanding of a threat they see every week in the news. Here is why that matters: In the beginning of this Foreword, I said my head was spinning. Why? Because there is so much new stuff that I can't keep track of? Actually, no. What amazes and scares me is that we are having the same conversations we had 13 years ago when I was chief for information warfare at the Ballistic Missile Defense Organization. Granted, today there are more acronyms, and more money is involved. But none of the fundamental issues have changed. Back then, the Russians were pursing international agreements to treat cyber attacks as strategic weapons. We did not listen, I think, because we thought our technology and techniques were superior. In addition, a lot of people were in denial—"Is this cyber attack stuff really an issue?" And far more people just did not have a clue. If it did not have to do with the Redskins or Cowboys, it could not possibly matter. But we forgot something. We had the most to lose. The United States has more information online than any other country, and that makes us the biggest target. We had an opportunity more than a decade ago to begin the dialog of government–private industry partnerships. We had an opportunity to begin to establish international agreements. We largely squandered those opportunities. Now they have returned. Compelling evidence suggests that there is a cyber threat. We need to educate ourselves, do our part, and encourage our legislators to engage. We need to hold the government accountable to spend our tax dollars wisely in the cyber warfare realm, not to just throw dollars in the air and hope they will land where they will do some good. *Cyber Warfare* will allow you to educate yourself, to form an opinion on where the nation should be moving and the risks we face if we take no action. More than a decade ago we missed our opportunity to take comprehensive action, and we have paid a terrible price. What are we going to do this time around?

Stephen Northcutt

References

[1] President Barack Obama. Remarks by the president on securing our nation's cyber infrastructure [home page on the Internet]. Washington, DC: The White House, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/; 2010 [accessed 15.02.10].

[2] Allen V. Cyber warfare threats to U.S. are increasing: top spy [home page on the Internet]. New York: Thomson Reuters, http://www.reuters.com/article/2011/02/10/us-usa-intelligence-cyberspace-idUSTRE7194E320110210; 2010 [accessed 15.02.10].