

Preface

It is imperative, going forward, that we broaden our understanding of the science that underpins cybersecurity.
—General (Ret.) Keith Alexander, Former Commander of U.S. Cyber Command¹

Modern society's increased reliance on computer systems, smartphones, and the Internet has provided a new target in a time of conflict. Indeed, cyber-warfare has already emerged as an extension of state policies—one needs to look no further than the headlines produced by Stuxnet, Aurora, or the cyber-attacks during the Russian-Georgian war than to gain an understanding of the emerging impact this domain has during a conflict.

While we have seen a plethora of advanced engineering concepts that directly affect cyber-warfare such as the inventions of the firewall, Metasploit, and even advanced malware platforms such as Flame, many of these concepts are built around best practices, rules-of-thumb, and tried-and-true techniques. While these inventions have been of high impact and significance, history has repeatedly taught us (in other disciplines) that the establishment of scientific principles leads to more rapid and remarkable progress.

Hence, this volume is designed to take a step toward establishing scientific foundations for cyber-warfare. Here we present a collection of the latest basic research results toward establishing such a foundation from several top researchers around the world. This volume includes papers that rigorously analyze many important aspects of cyber-conflict including the employment of botnets, positioning of honeypots, denial and deception, human factors, and the attribution problem. Further, we have made an effort to not only sample different aspects of cyber-warfare, but also highlight a wide variety of scientific techniques that can be used to study these problems. The chapters in this book highlight game theory, cognitive modeling, optimization, logic programming, big data analytics, and argumentation to name a few.

It is our sincere hope that this volume inspires researchers to build upon the knowledge we present to further establish scientific foundations for cyber-warfare and ultimately bring about a more secure and reliable Internet.

¹ <http://www.nsa.gov/research/tnw/tnw194/article2.shtml>.

Cyber Warfare

Building the Scientific Foundation

Jajodia, S.; Shakarian, P.; Subrahmanian, V.S.; Coyan, V.; Wang, C. (Eds.)

2015, XIII, 321 p. 83 illus., 49 illus. in color., Hardcover

ISBN: 978-3-319-14038-4