Preface

The non-profit Privacy Rights Clearinghouse (PRC) maintains an ongoing chronology of significant data breaches in its efforts to raise awareness about consumer privacy issues. During 2011 alone, PRC reported 535 breaches compromising millions of records. The top six worst data breaches were criminal attacks on Sony, which compromised data related to its PlayStation Network and Qriocity music service operations in 101.6 records; the attacks on cloud based email provider Epsilon that breached between 50 to 60 million emails (which means as many as 250 million were affected in some way); the theft of nine servers from Health Net containing personal information on more than 1.9 million policy holders; the data breach at Sutter Physician Services and Sutter Medical Foundation that compromised the personal data of more than 3.3 million patients; the theft of backup tapes from Science Applications International Corporation (SAIC) containing healthcare patient data on 5.1 million active and retired members of the armed services and their families; and finally, the State of Texas Comptroller’s Office, where thieves accessed 2 to 3.5 million records from three different state agencies, including the Teach Retirement Center, the Texas Workforce Commission and the Employees Retirement System of Texas (Schwartz, 2011). In the age of the Internet, cybersecurity will necessarily remain a vital concern.

On July 26, 2012, the United States Senate passed a procedural motion to begin debate on what is known as the Cybersecurity Act of 2012. The most controversial component of the bill addressed information sharing between private entities and governments, with the intention to prevent unwanted cybersecurity threats. The legislation is only the most recent attempt by U.S. legislators to either control certain aspects of private cyberspace or to address various elements of cybersecurity. Cybersecurity has also taken center stage at the international level, with such efforts as the United Nations World Summit on the Information Society in 2003 and 2005, the annual Information Security Summits conducted by Asian World Summit, and the International Telecommunication Union (ITU) with its 2010 Plenipotentiary Conference and its 2012 World Conference on International Telecommunications. In 2007, the ITU also launched the Global Cybersecurity Agenda, a general framework for potential international coordination of efforts to address the technical and social aspects of cybersecurity.

Cybersecurity has grown tremendously over the past decade as private industry, public administration, commerce, and communication gained greater online presence. The discipline intersects a number of fields including information systems, computer science, criminology, economics, management, and political science, among others. Cybersecurity also represents a productive, but costly industry in the global economy. In contrast to traditional crime, cybercrime has the possibility to directly affect very large groups of individuals and businesses. In the cybersecurity literature, potential extra effects beyond those directly affected exist and are known as network effects (Gandal, 2006, p. 79).
This book presents a multi-faceted lens on Cybersecurity Policies and Strategies for Cyberwarfare Prevention. Such a review is a necessary step in the process of creating a cumulative culture for the continued growth of any field of research (Webster and Watson, 2002) and can make a substantial contribution when it reveals new avenues of research, frameworks, and operating theories (Rowe, 2012). This is especially relevant in the field of information systems, where cybersecurity is a subdomain that crosses the boundaries of multiple fields. The purpose of this book is to examine the current knowledge in the field and provide an accurate and current reference point from which further development may take place.

This book aims to provide a needed perspective on emerging policies, doctrines, strategies in cyberwarfare and cybersecurity. It highlights a structural framework within which to organize present cybersecurity and cyberwarfare literature, as well as a historical snapshot of its main analytical strands and related policy positions. The book intends to highlight the different dimensions of cybersecurity policies and economics, and collect different perspectives on cyberwarfare.

Given the sophistication of cybercriminals and their advantageous positions as attackers in cybersecurity, it is expected that future research will target modeling and prevention of attacks as well as mitigating the consequences of breaches and attacks when they do occur.

Furthermore, online transactions have become indispensable for public administration. This means that criminal networks will target these transactions for breach and fraudulent activities, and will continue to innovate in ways to infiltrate security systems. These innovations must be matched by academic and industry researchers in a cyber arms race of sorts so that they are not always one step behind criminal networks. A development spearheaded by some governments is to enforce cybersecurity standards as they apply to privately-run electric grids (Wright, 2012; Zhang, 2011). Since public infrastructure is vulnerable and poses wide economic and safety risks to societies, such standards may prove to be useful in the development of cost-effective and innovative information security products.

Future work in modeling attack and defense, especially that based on Varian’s (2004), suggests that information security is best optimized by companies when software developers hire fewer but more skilled programmers, use many testers, and acquire security architects with the greatest expertise. Since this early work, analytical research has further captured and defined externalities present in information security investment decisions whereby security level is a public good while defensive costs are private. Future research on attack and defense will continue to develop models of security hardening that takes into account costs and benefits. As these models are refined based on emerging attack data, organizations can tailor their information security hardening to their particular needs.

As Internet and communication technologies continue to change and evolve, cybersecurity and cyberwarfare will remain a vital area of research.

Regardless of the research avenue and particular focus in cybersecurity, future research will focus on the social, political, technical, and economic challenges that are considered when making security investment decisions. Wider policies on information security rely on sound information and empirical research evidence, which will prompt many industry individuals, legislators, and politicians to stay ahead of the curve in anticipating the impact of security breaches and attacks. Ultimately, a coordination of effort among researchers, private industry, consumers, and other intermediaries is necessary in navigating the complex, interrelated world of cybersecurity.
ORGANISATION OF THE BOOK

The book is organized into three sections and fifteen chapters. A brief description of each of the chapters follows:

Section 1 – Introduction to Cybersecurity and Cyberwarfare principles

Chapter 1 - Toward Principles of Cyberspace Security. This chapter outlines a set of cybersecurity principles that aim to identify strategies to assure operations in contested environments in the face of increased dependence, complexity and vulnerability.

Chapter 2 - Cyber Warfare: The State of the Art. This chapter provides a concise overview of cyberwarfare topics (in its politics, social, legal and technical dimensions.

Chapter 3 – Attribution. This chapter highlights that attribution is not only technical and brings a focus on political factors constraining attribution.

Section 2 – Cybersecurity at stake: monitoring threats, managing risks and defensive measures

Chapter 4 - Security Monitoring of the Cyber Space. This chapter defines the cyberspace trap-based monitoring systems, and presents the state-of-the-art in terms of techniques, tools and technologies.

Chapter 5 - The Rigorous Security Risk Management Model: State of the Art. This chapter presents the security concepts terminologies and present the state of the art of security risk management models.

Chapter 6 - Cybersecurity Requires a Clear Systems Engineering Approach as a Basis for Cyberstrategy. This chapter demonstrates why a systems engineering approach is best suited for large and complex cybersecurity information systems.

Chapter 7 - Towards protecting critical infrastructures. This chapter addresses Critical Infrastructure Protection (CIP) paying particular attention to the risk alert exchange among Critical Infrastructures.

Chapter 8 - Cyber-attacks, retaliation and risk: Legal and technical implications for nation-states and private entities. This chapter examines key legal and technical issues that arise when an adversary considers strategic retaliatory countermeasures in response to a cyber-attack.

Section 3 – National Issues, strategies and policies

Chapter 9 - Developing Confidence Building Measures (CBMs) in Cyberspace between Pakistan and India. This chapter outlines the usefulness of CBMs in preventing wars and facilitating conflict resolution.

Chapter 10 - Cyber Attacks and preliminary steps in cyber security in national protection. This chapter study cyberwarfare prevention in the context of Turkey cybersecurity strategy.

Chapter 11 - Conflict in the cyberspace, the case of the middle east. This chapter highlights the various cyber strategies in the Middle East Area.

Chapter 12 - Information Warfare in the 2013-2014 Ukraine Crisis. This chapter focuses on information warfare tactics used in times of crisis.
Section 4 – Concluding remarks and Reflections on the essence of cyberwarfare

Chapter 13- The Islamist Cyberpropaganda Threat and Its Counter-Terrorism Policy Implications. This chapter examines four Islamist cyberpropaganda cases studies, and outlines recommendations for counter-terrorism policy.

Chapter 14- Thinking Systemically about Security and Resilience in an Era of Cybered Conflict. This chapter argue that cybered conflicts cannot be resolved by military or intelligence organizations. Rather, it emphasizes that cybersecurity will require systemic thinking that enlists the full range of government and private organizations.

Chapter 15- Cyberinsecurity and Cyberwarfare: the Case for Social Science and Philosophical Approaches. Reflections from Asia. This chapter draw attention to the social grounding of cyberspace and the need to employ traditional social science and philosophy to examine cyberspatial politics.

Jean-Loup Richet
University of Nantes, France

REFERENCES


