

CyberWar, CyberTerror, CyberCrime

By Julie E. Mehan

Ely, Cambs, UK: IT Governance Ltd., 2008, ISBN: 978-1-905356-47-8

Price \$69.95, pp. 268

Reviewed by: Robert PENCHUK

Journal of High Technology Law

Suffolk University Law School

*“Cybersecurity is not just a technical issue, but it is often handled as if it were. In reality, information security is a business and governance challenge . . .”*¹

Information technology (IT) increasingly affects every facet of our lives. As a result, there has been a dramatic rise in Cybercrime, encompassing everything from simple attacks on personal computers to threats to our national infrastructure. At one end of the spectrum, are unsophisticated “script kiddies” using readily accessible virus code.² At the other end are highly organized criminal organizations reminiscent of the Mafia.³ On the international front, rogue states directly sponsor Cyberterrorism groups.⁴

The central thesis of Dr. Mehan’s book, *CyberWar, CyberTerror, CyberCrime*, is that technology alone will not solve the problem of Cybercrime. Organizations need a standardized approach to IT governance, which is able to incorporate an industry’s best practices, adapt to the needs of the business, and evolve over time to respond to changing threats and business requirements. Dr. Mehan discusses IT governance in the context of a corporate enterprise; however, the principles are readily adaptable to organizations of all sizes including individuals, corporations, and nations.

¹ Julie E. Mehan, *CyberWar, CyberTerror, CyberCrime*, 86 (2008).

² Mehan, *supra* note 1, at 51 (describing “script kiddies” as novice hackers using readily available virus code from the Web).

³ Finjan Inc., *Know Your Cybercrime Enemy – Finjan Unveils the Latest Cybercrime Organizational Structures and Modus Operandi*, Press release (July 15, 2008) at <http://www.finjan.com/Pressrelease.aspx?id=1998&PressLan=1819&lan=3>.

⁴ Mehan, *supra* note 1, at 20; see also Tech. Sgt. A.J. Bosker, *SECAF: Dominance in cyberspace is not optional*, The Information Warfare Site (June 1, 2007) at <http://www.iwar.org.uk/news-archive/2007/06-01.htm>.

Dr. Mehan's expertise in IT security and governance is quite evident in this book. She is highly credentialed as an associate professor, business consultant, entrepreneur, and an active participant in numerous committees. She has served on the President's Partnership for Critical Infrastructure Security, Task Force on Interdependency and Vulnerability Assessments. In addition, she currently chairs the development of criteria for the International System Security Engineering Professional (ISSEP) certification, is a voting member for the board of development of the International Systems Security Professional Certification Scheme (ISSPCS), and chairs the Systems Certification Working Group of the International Systems Security Engineers Association.

CyberWar, CyberTerror, CyberCrime begins by defining the nature and scope of the problem we face. It is an excellent overview for all audiences, regardless of their technical background. Dr. Mehan then describes the fallible nature of people. This sets the stage for the discussion of why standards are essential to combat the problem of Cybercrime. The reader should consider her discussions on crime, terrorism, and warfare to be interchangeable since they share similar characteristics. The remainder of her book provides a more technical discussion regarding the framework for implementing standards.

While defining the problem to be addressed Dr. Mehan first draws a parallel between the development of societal norms and the attendant threats to show why past solutions are no longer effective. Prior to the information age, societal threats and information were more centralized than they are today. Just as the printing press enabled mass distribution of the book, the internet enabled mass distribution of electronic information.⁵ In addition, economies of scale have driven down the cost of new technology making it available to the masses.⁶ As a result, the new

⁵ Mehan, *supra* note 1, at 8.

⁶ Mehan, *supra* note 1, at 11.

internet society greatly increases our capacity to distribute and retrieve information rapidly, over great distances, and often with questionable data integrity.⁷ Additionally, we have become increasingly reliant on this questionable data, as we conduct our daily personal and business transactions. This makes IT an ideal target for criminals and terrorists alike.

Dr. Mehan further defines why past solutions are no longer effective by describing the evolution of warfare. War began as a disorganized effort and then evolved into professional armies engaged in what the author describes as symmetrical warfare.⁸ Both sides had an equally strong balance of force with similar cost/benefit decisions. The traditional solution was to match force with opposing force. With the new information age, Dr. Mehan believes warfare has become asymmetric.⁹ Relatively small terrorist groups can engage with large entities with very little cost, yet with considerable effect should they succeed. Similar to terrorism itself, the barriers to perpetrating Cybercrime are very low, yet the impact may be very substantial.¹⁰ The traditional approach is no longer effective against an asymmetric threat, thus the need for a new solution as proposed by Dr. Mehan.

Historically wartime defenses consisted of hardened perimeters, fortress walls, and moats. Short of permissively entering through the front gate as described in the story of the Trojan horse, these defenses were largely effective. However, the pervasive nature of the internet makes every employee a potential gateway through this perimeter. Indeed, the aptly named Trojan virus exploits this concept by relying on the human fallibility of a single employee who makes an inadvertent single click of the computer mouse.

The probability of error increases further due to our increasingly mobile society. The

⁷ Mehan, *supra* note 1, at 11.

⁸ Mehan, *supra* note 1, at 23.

⁹ Mehan, *supra* note 1, at 24.

¹⁰ Mehan, *supra* note 1, at 41 (estimating damage from Hurricane Katrina of 2005 at \$63 billion, while “So Big” virus was \$30 billion).

author opines that solutions must originate within the enterprise and begin with the employees themselves. People are the weakest link, since we are inherently fallible.¹¹ Dr. Mehan devotes the first half of her book sensitizing the reader to the extent of the threat. The remainder of her book provides a foundation to enable the reader to begin to implement standards to counter this threat. Although the book does not purport to describe these standards in detail, (such treatment would span multiple treaties) it provides a solid foundation with excellent references for further follow-up. There is no “one size fits all” when it comes to these standards, since business needs vary. To keep these standards relevant, the author suggests the use of a business method called Plan-Do-Check-Act (PDCA), which essentially is a continuous learning business process.¹² The PDCA method attempts to modify business practices to adapt to the changing needs of the business and evolving Cybercrime threats.

Corporate quality systems frequently use the concept of standards based corporate governance coupled with PDCA “continuous improvement” cycles. One example is ISO 9000, which in its simplest form requires employees to say what they do, and do what they say.¹³ When used properly standards based systems will greatly reduce the Cybercrime threat. Criticism of standards based governance as overly bureaucratic occurs when users lose sight of the initial objective. Standards can take on a life of their own, but this need not be the case. By ensuring that business needs drive the standards, and not the converse, these standards provide an important safety net against human error. Similar to terrorism where a single oversight by a security guard can result in disaster, Cybercriminals exploit a single employee who forgets to

¹¹ Mehan, *supra* note 1, at 49.

¹² Mehan, *supra* note 1, at 116; *see also* Paul Arveson, *The Deming Cycle*, Balanced Scorecard Institute (1998) at <http://www.balancedscorecard.org/TheDemingCycle/tabid/112/Default.aspx>.

¹³ Sapient Management Consulting, *ISO – International Organization for Standardization*, Home Page (2003) at <http://www.sapientmgmt.com/ISO.htm> (describing ISO9000 as a quality system that enables continuous improvement through standardization).

install a security patch or connects to an unsecured Wi-Fi hotspot in a café in a moment of inattention.

The method of using standards and continuous improvement to fight Cybercrime is a valid approach. When used correctly, it will provide an essential first line of defense against an ever-increasing threat, which shows no signs of abating. *CyberWar, CyberTerror, CyberCrime* is an excellent reference not just for IT professionals but for the legal community as well – the first few chapters being the most apposite. These first chapters provide an astonishing exposure to the extent of the threat we face. The later chapters touch upon familiar legal standards such as Sarbanes-Oxley, Healthcare data privacy (HIPAA), and Gramm-Leach Biley.¹⁴ The legal community should consider the value of this book as an aide in understanding their clients' exposure to Cybercrime, as well as their own firm's exposure and potential liability should there be a failure to take adequate protective measures.

¹⁴ Mehan, *supra* note 1, at 215.