Cybercrime and Espionage: An Analysis of Subversive Multivector Threats

By Will Gragido and John Pirc
Price: $59.95, pp. 272.

Reviewed by Kip Bodi
Journal of High Technology Law
Suffolk University Law School

“The enemy is within the gates; it is with our own luxury, our own folly, our own criminality that we have to contend.”¹

We currently live in an information age.² Nearly all of our personal information is now stored on computer networks.³ As the amount of personal, financial, and governmental data stored in electronic form has increased, so too have criminal activities seeking to access and make adverse use of that information.⁴ Will Gragido and John Pirc provide a timely overview of computer related crimes and espionage, and offer a new paradigm for the analysis of computer related threats and network security.

Will Gragido and John Pirc have a combined 25 years of information security experience.⁵ Cybercrime and Espionage, their debut book, summarizes the current state of cybercrime, network security, and computer-related espionage. The authors go far beyond just computer related crime and seek to establish new ways of thinking about security.

The authors begin with a broad discussion of humanity and its propensity for crime. Criminal behavior can be understood by looking at a risk to reward ratio; if a criminal

---

³ See SOLOVE, supra note 2, at 22 (detailing the increasing storage of personal information on the internet).
⁵ See GRAGIDO, supra note 1, at xv (describing author’s backgrounds).
opportunity exists and the risk of getting caught is low, it is likely that there will be criminal activity. 6 One early effort to maintain order in society was the code of Hammurabi. 7 Our world has changed greatly since the time of Hammurabi, and with the growth of networks and the internet it is more interconnected than ever. This creates new potential for criminal activity and exploitation. The number of incidents reported to the Internet Crime Complaint Center increases yearly, as does the amount of total losses attributed to cybercrime. 8 Recent trends such as social networking will see an increase in attacks as they become a target of opportunity. 9 Attackers are becoming increasingly sophisticated, and make use of distributed compromised personal computers (“bots”) or cloud computing resources to conduct their attacks. 10 All new avenues for criminal activity are quickly exploited.

An analysis of crime and espionage in the information age requires a look at the history of communication. 11 With every improvement in communications technology, there have been abuses. 12 The invention of the telegraph and telephone allowed gambling, bookmaking, and wire-fraud rings to become country-wide enterprises. 13 Today, physical location is no longer a requirement for the distribution and theft of information. 14 This lack of physical location decreases the risk of detection, and fuels the propensity to commit crime. 15

6 See GRAGIDO, supra note 1, at 6 (showing that this criminal opportunity is nothing new).
7 See GRAGIDO, supra note 1, at 4-6. The ancient code includes an early form of negligence law: “If a builder provides a house for someone, and does not construct it properly, and the house that he built falls in and kills its owner, then the builder shall be put to death.” GRAGIDO, supra note 1, at 5.
8 See GRAGIDO, supra note 1, at 10 (comparing reported cybercrime incidents with total losses).
9 See GRAGIDO, supra note 1, at 13-14 (discussing the rapid growth of online social networks).
10 See GRAGIDO, supra note 1, at 15 (mentioning the growing popularity of bot-networks).
11 See GRAGIDO, supra note 1, at 22-26 (providing the evolution of human communication, from cave writing to the printing press to the internet).
12 See GRAGIDO, supra note 1, at 27 (noting the “emergence of abuse (in lock step fashion) with technological progression”).
13 See GRAGIDO, supra note 1, at 29-31 (telling the story of Jacob “Mont” Tennes, one of the first people to use the nascent telegraph and telephone network for illicit means).
14 See GRAGIDO, supra note 1, at 33 (showing how today’s telecommunications infrastructure enables new forms of criminal activity).
15 See GRAGIDO, supra note 1, at 33 (indicating that information can now be stolen from anywhere).
Efforts at securing information have already been taken on a large scale, and many industries must abide by regulations for securing confidential information. Common standards include “reasonable and appropriate” measures for information security. The authors argue that these regulations may actually decrease information security. Corporations tend to do the minimum required for compliance, and what is considered reasonable and appropriate may vary greatly between two individuals.

The authors continue with an illustration of the divide between physical and logical security. In any company, the departments responsible for physical security and network security are usually entirely separate entities. However, locked cabinets and security guards are generally of no concern to the cybercriminal. Companies should ensure that physical and network security teams interact to ensure that a terminated employee no longer has access to the premises or data files stored on company computers.

Attacks via computer networks may be initiated by a variety of actors, and amateur involvement is increasing. Many attacks occur with the victim’s willing involvement via social engineering. The unsuspecting recipient is enticed to click a link in an email, which

---

16 See GRAGIDO, supra note 1, at 36-45 (detailing common regulatory frameworks for information security). One regulation that requires “reasonable and appropriate” standards is the Health Insurance Portability and Accountability Act (HIPAA). Regulations for the payment card industry are quite detailed, whereas those for student loan information provide little guidance. See GRAGIDO, supra note 1, at 42-44.

17 The authors recommend that corporations go “above and beyond” when addressing their information security needs. See GRAGIDO, supra note 1, at 47. Measures that meet these criteria are provided – but you have to wait until the end of the book!

18 See GRAGIDO, supra note 1, at 47 (concluding that interpretation of regulatory standards is a “silent killer.”)

19 See GRAGIDO, supra note 1, at 52 (discussing the practice of “siloed” security domains).

20 See GRAGIDO, supra note 1, at 51 (highlighting that most cybercriminals never see the facility or an armed guard).

21 One example is Dong Chul Shin, who was terminated from a large Texas power company but retained access to his corporate laptop for several days. See GRAGIDO, supra note 1, at 56. Mr. Shin changed a file on the corporate servers that led the company to lose $26,000 as it was unable to accurately forecast the ability to transmit energy. See GRAGIDO, supra note 1, at 56.

22 See GRAGIDO, supra note 1, at 66 (discussing motives at play in amateur involvement).

23 See GRAGIDO, supra note 1, at 68 (detailing types of social engineering tactics, including pretexting, diversion theft, and phishing).
opens a web page that downloads a malicious program to the recipient’s computer. Both Facebook and ExxonMobil have been targeted in this manner.

The authors move into a discussion of state-sponsored intelligence and espionage. Espionage, the practice of spying or using spies, has been used in nearly every culture of the world. Traditional forms of intelligence gathering include ‘human’ intelligence, which focuses on the identification and compromise of people in important places for the purpose of gaining valuable intelligence. Notable examples include Julius and Ethel Rosenberg, convicted of providing information about the atomic bomb to the Soviet Union and Robert Hanssen, a computer systems expert at the FBI who sold classified information to Russia for a period of 22 years. While somewhat out of place in a book about cybercrime, this review of traditional intelligence helps to illustrate motive, whether for political or financial gain.

There are various actors at play in computer network infiltration, from the relative novice, to the hacker-for-hire, to experts working for the State department. Attacks range in sophistication from phishing and baiting activities, to highly advanced efforts such as the “Stuxnet” worm. Cybercrime has proven to be extremely profitable, and the FBI has noted that it has surpassed drug trafficking in some measures. Known cybercrime groups include the Russian Business Network and Honker Union of China. Hezbollah, a state-sponsored terrorist

---

24 See GRAGIDO, supra note 1, at 74 (providing an example of phishing).
25 See GRAGIDO, supra note 1, at 74-75 (discussing “Koobface” Facebook worm and phishing emails targeting ExxonMobil). No matter how enticing, if you receive an email or message entitled “Nice! Your body looks awesome in this video!” you probably should not click it – especially at your place of employment.
26 See GRAGIDO, supra note 1, at 82.
27 See GRAGIDO, supra note 1, at 97.
28 See GRAGIDO, supra note 1, at 100-101.
29 See GRAGIDO, supra note 1, at 108-111.
30 See GRAGIDO, supra note 1, at 118-119. Stuxnet targeted Siemens Program Logic Controllers, the same models used by Iran. Stuxnet is credited with severely retarding the development of Iran’s nuclear program, and may have been introduced via an infected USB drive.
31 See GRAGIDO, supra note 1, at 123 (analyzing criminal cybercrime syndicates).
32 See GRAGIDO, supra note 1, at 124-26 (highlighting activities taken by several cybercrime organizations, including an attack on the White House website).
group in Lebanon, is classified as having moderate offensive cyber capabilities.\textsuperscript{33} Many countries also boast formidable cyber defense resources, including China, Russia, and Iran.\textsuperscript{34} The U.S. Department of Defense has taken cyber threats seriously since 1998, when a military field test was able to exploit the vulnerability of critical infrastructure, communications, and defense agencies.\textsuperscript{35}

The authors describe how themes from Sun Tzu’s *The Art of War* are directly applicable to computer network security—specifically the concept of the converted spy, or double agent.\textsuperscript{36} The use of subversion and deception is integral to a spy’s activities, just as it is for the cybercriminal.\textsuperscript{37} The authors use this opportunity to define a new class of threat that is growing and will become pervasive over the next decade: the Subversive Multivector Threat (SMT). A SMT will use a crippling, deceptive, and systematic approach, utilizing multiple paths and courses to achieve its goal.\textsuperscript{38} Examples of SMT’s include several prosecutions brought under the Economic Espionage Act of 1996,\textsuperscript{39} which involved Chinese nationals using and exploiting people, processes, and technology to provide secret information to the People’s Republic of China.\textsuperscript{40}

After leaving us with a bleak outlook on the future of information security, the authors conclude that all is not lost and provide recommendations on how companies and individuals can

\textsuperscript{33} See GRAGIDO, *supra* note 1, at 128 (providing an example of a subnational entity with a heavy investment in cyber warfare).
\textsuperscript{34} See GRAGIDO, *supra* note 1, at 129-31 (listing the offensive cyberwarfare capabilities of several countries). During the altercation between Russia and Estonia, Russia was able to shut down Estonia’s internet access. See GRAGIDO, *supra* note 1, at 130. It is unclear whether Estonia’s productivity was negatively impacted.
\textsuperscript{35} See GRAGIDO, *supra* note 1, at 161-64 (providing an account of “Eligible Receiver 97,” a large scale military field exercise designed to test the nation’s infrastructure).
\textsuperscript{36} See GRAGIDO, *supra* note 1, at 136 (summarizing Sun Tzu’s advocacy of the use of spies).
\textsuperscript{37} See GRAGIDO, *supra* note 1, at 138 (noting the parallels between information and physical warfare).
\textsuperscript{38} See GRAGIDO, *supra* note 1, at 149 (defining the SMT).
\textsuperscript{40} See GRAGIDO, *supra* note 1, at 139-143 (discussing the cases of Chi Mak, Greg Chung, Hai Lin, Kai Xu, and Noshir Gowadia). Filial loyalty to the People’s Republic of China was the root cause for several of these cases. See GRAGIDO, *supra* note 1, at 141.
protect themselves from cybercrime. Legacy security devices such as traditional firewalls are insufficient. Antivirus programs are still necessary, but the choice of vendor is important as many new malware programs are released each day. Advanced systems are needed for both intrusion detection and prevention. The authors describe a framework for assessing risks that involves understanding the motives and techniques of potential actors, and suggest continually reviewing a network security plan. A next-generation security framework is discussed, and the authors show how a network analysis tool can be used to monitor and analyze suspicious activity in real time.

Mr. Gradigo and Mr. Pirc’s book succinctly summarizes the challenges regarding network security in the information age, and states standards that can be used to evaluate criminal activity in this age and beyond. However, the book feels a little unpolished. The authors often fail to define terms such as “cyberkinetic” or include seemingly irrelevant information. Occasionally there are typos. There are few concrete examples, though still more than most other books or articles on the subject. Nevertheless, the book is a good review of the current challenges facing humanity in dealing with cybercrime and espionage in the information age. Cybercrime and Espionage is recommended for students interested in learning more about cybercrime as well as network security professionals seeking to understand network security needs at a higher level.

41 See GRAGIDO, supra note 1, at 224. For example, a firewall is often forced to open several ports for services like the web or email. See GRAGIDO, supra note 1, at 224. Attackers may use vulnerabilities in these ports to infiltrate a network. See GRAGIDO, supra note 1, at 224. Additionally, social engineering tricks such as enticing a user to click on a link in an email will also defeat the firewall. See GRAGIDO, supra note 1, at 225.
42 See GRAGIDO, supra note 1, at 224 (stating continuing importance of antivirus protection).
43 See GRAGIDO, supra note 1, at 226 (discussing growing need for real-time network monitoring).
44 See GRAGIDO, supra note 1, at 229-34 (describing the MOSAIC framework).
45 See GRAGIDO, supra note 1, at 236-44 (describing a next-generation security framework composed of core technologies, advanced meta-network security analysis, and information event management).
46 These include the full Greek, Hebrew, and Archaic Etruscan alphabets along with seven pages devoted to the insignia of various state intelligence organizations. See GRAGIDO, supra note 1, at 24-25, 84-90.
47 The authors describe how certain subversive activities were linked to Hezbollah because of “antisemetic language.” See GRAGIDO, supra note 1, at 129.