Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It

Marc Goodman (Doubleday, 2015), 392 pp., index

Reviewed by Jay R. Watkins

The digital tidal wave is revolutionizing our lifestyles in many positive ways. Yet are we as aware as we should be of the perils that lurk beneath? *Future Crimes*, by Marc Goodman, presents a dystopian world in which our daily activities are monitored, monetized, and stolen or sold to advertisers, criminals, and governments alike. We become junkies, tempted by enticing apps and data clouds that open an amazing new universe of information to us. While availing ourselves of these accesses, we also click "accept" to a Faustian deal in which we surrender our identity and anonymity in perpetuity.

The author, Marc Goodman, is a senior technology futurist in residence with the FBI, senior adviser to Interpol, and consultant to the Los Angeles Police Department and the US Secret Service. He founded the Future Crimes Institute and chairs the Policy, Law, and Ethics track at Silicon Valley's Singularity University, an institution that bills itself as a "benefit corporation" hosting graduate and executive learning programs and incubators for new business.

Future Crimes, which has been on the *New York Times* best seller list, reads like science fiction but is based on hard facts. In a single comprehensive volume, Goodman provides a tour d'horizon of the cyber ecosystem and presciently describes trends in telecommunications, robotics, nanotechnology, digital manufacturing, artificial intelligence, wearable computers, and synthetic biology and how they will affect us.

This book has as much to do with the intelligence business as it does with law enforcement. It exposes how vulnerable we are as individuals and society to the technologies we have created. It has profound implications for intelligence tradecraft. Those engaged in the technical offensive and defensive worlds of cyber and counterintelligence may already know of many of these threats; however this book brings them all together in a compelling narrative. Goodman's prose is conversational, straightforward, and technical terms are simply explained. The reader will gain new vocabulary by reading about "botnets," "rootkits, "crowdsourcing," and "baseband" and "man-in-the-middle" attacks, to name a few. The author cites many relevant case studies and compelling real-life examples of cyber vulnerabilities and penetrations. He also address terrorists' extensive exploitation of cyber for targeting, recruitment, operational planning and support. He cites, for example, the use social media Lashkar-e-Taiba to verify targets in their Mumbai attacks in 2008. Goodman's posits a litany of other worries:

- State-sponsored cyber espionage is ubiquitous, with more than 100 countries actively hacking the systems of other countries and businesses. China alone has developed an army of 180,000 cyber spies and warriors, he claims, mounting an "incredible ninety thousand computer attacks per year" against US Defense Department networks alone. (31)

- Foreign government hackers have compromised information on vital US defense and government systems, including the F-35 strike fighter, Patriot missile system, and AEGIS ballistic missile defense system. Top secret plans for the US president's Marine One helicopter were found online in 2002, listed on a peer-to-peer (P2P) network in Iran. These P2P networks allow for easy decentralized file sharing and are often associated with distribution of pirated films and music. (119)

- Foreign spy services regularly use social media (LinkedIn, Facebook, and Twitter) to identify and target employees to recruit as spies for commercial and government espionage. The resulting losses to intellectual property rights and development costs have been hundreds of billions. (102–104)

- A wake-up call for analysts of the world scene in understanding the potential of social media data aggregation came in January 2011 with the spontaneous

All statements of fact, opinion, or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

Tunisian “Arab Uprising.” Meanwhile, repressive governments like deposed Ukrainian President Viktor Yanukovich in 2014 used cell phone data to monitor street demonstrators. His security service intimidated demonstrators by sending them text messages accusing them of unlawful behavior and threatening them with imminent arrest. (122)

- Encryption protocols can be compromised, as evidenced by the Heartbleed security bug in early 2014. Sites affected included: Instagram, Pinterest, Facebook, Tumblr, Google, Yahoo!, Etsy, GoDaddy, Foursquare, TurboTax, Flickr, Netflix, YouTube, USAA, and DropBox. The base operating systems of mobile devices (e.g., SSL) have been compromised. Developers assume because they are so embedded in the phone that no one will be able to figure them out. As the author points out, criminals and foreign intelligence services are often steps ahead of consumers in exploiting technology for their gain. (166–167)

- We are overreliant on GPS devices. They can be disrupted easily with devastating consequences to air, sea, and land transportation. North Korea routinely jams GPS signals in South Korea. The largest attack occurred in 2012 and ran for 16 days, disrupting 1,106 aircraft and 254 ships. (152)

- And what about those Google cars plying the streets taking pictures at street view for Google Maps? They are also collecting IP addresses from mobile devices as they pass by. (107)

- And there is much more: the “Internet of Things,” the risks of wireless networks, drones, and devices to collect metrics about human behavior and bodily functions. (224–225; 248–252)

This book has no shortage of evidence to illustrate the perfidious ways in which users of computers and devices can be compromised. Short of unplugging from the global grid, Goodman offers practical advice on how to mitigate the chances of succumbing to the “IEDs” on the Internet and foreshadows the connected world we face.

❖ ❖ ❖