Polish Political Science Yearbook vol. 46 (1) (2017), pp. 350–353
DOI: 10.15804/ppsy2017125 PL ISSN 0208-7375

Natalia Ciszewska
Nicolaus Copernicus University in Toruń (Poland)

Is Technology Threatening Us?

Book Review: Marc Goodman, *Zbrodnie przyszłości. Jak cyberprzestępcy, korporacje i państwa mogą używać technologii przeciwko Tobie*. Gliwice: Helion, (pp. 504). ISBN 978–83–283–1729–1. Price: 49.99 PLN.

Marc Goodman is considered to be an authority in the field of global security with over 20 years of experience and his cooperation with the Interpol, the North Atlantic Treaty Organisation, the United Nation and the government of the United States, including the Federal Bureau of Investigation. He is a founder of the Future Crime Institute and presently serves as a Chair for Policy, Law, Ethics at Silicon Valley's Singularity University.

The book consists of three parts. In the first part Goodman explores present-day cybercrime reality. The second part addresses cybercrime underground, development of new types of technology, and criminal activity which is getting more innovative and creative. Then, in the third part the writer includes recommendations for consumers, government agencies and technological companies about ensuring the security in the cyberspace.

In the first chapter of the book Goodman analyses the condition of contemporary cybercrime and its evolution over the years. Comparison of cybercrime and common crime presented in this chapter is both interesting and educational. Subsequently, the author presents a historical overview of computer security and provides the reader with a sort of tutorial about malicious software (malware). In the latter part of this section the author outlined basic threats exemplifying them with real life instances. At the end of this chapter Goodman queried the reader, "Think, does your on-line world is safe? Think one more time!". Such measure compels us to reflect and encourages to continue

reading. To sum up, the first chapter constitutes a reference point for the entire first part of the book in which the author thoroughly analysed crime activities concerned with technology we use in our daily lives (in communication, entertainment, health care or work). Also worth mentioning is the dark side of all free Internet services such as e-mail, Internet browsers and social networks revealed by Goodman. The author enumerates many examples where companies such as Facebook, Google, LinkedIn provide free services in exchange for obtaining user data which later they use as they deem appropriate. Moreover, the fact that the majority of the users is not aware of further fate of their data should be emphasized; they do not know who purchases them and in which way they are used.

When the reader realizes how often it is naive to use various Internet services Goodman moves the narrative from the victims to the offenders. The second part emphasizes that perpetrators will always be pioneers of new means of using technology in a malignant manner. This trend is accelerated every day by emergence of new electronic gadgets. In *Future Crimes* the author described in detail the organizational structure of the cybercrime in the reference to the reporting models, specialization models, outsourcing models and the black market (the Dark Web). In the respective chapters of this part Goodman explained the usage of monetary mules, the communication of cybercriminals via the Dark Web and the significance of the digital currency such as Bitcoin. Interestingly, the writer also featured the average prices for the numbers of the stolen credit cards, fake documents, and even the cost of renting a hitman.

As the title of the book suggests, the third part is concerned with future crimes connected primarily with the growing Internet of Things (IoT), which allows to combine resources of computational, networking and mass memory technologies with capabilities of the consumer and industrial objects. Goodman is a supporter of the Internet of Things, that is why he highlighted many potential benefits as well as threats posed by loopholes in the software of these intelligent objects of everyday use. For instance, implanted medical devices (IMDS) such as pacemakers and insulin pumps can be remote-controlled and monitored by doctors. This would ensure the improvement of the health care and the drop in costs. However, on the other hand, unsecured IMDS could be also used in criminal activities. There may be a case where thousands of diabetic patients with implanted insulin pumps connected to the Internet is blackmailed with the lethal dose of the insulin unless they pay 1000 USD. Goodman provide numerous examples of the future crimes that present dire prognoses such as a situation when we lose control of your life because of using too much technology.

Undoubtedly, the present book is not devoid of flaws. Recommendations concerning improvements of safety in the cyberspace proposed by Goodman in the last part

are more than a little evident, they do not introduce any novelty. Moreover, after reading *Future Crimes* one can have the impression that the author may be slightly paranoid; in every aspect of the Internet activity he sees evil and opportunity to commit a crime. This impression is compounded by the fact that the author does not give any positive aspects of online activities. Worth mentioning is also the fact that the abundance of the examples presented by Goodman, which without a doubt aim at confirming his observations, are occasionally lengthy and repetitive. For instance, the book recounts the 2008 attack in Mumbai and describes in detail how terrorists took advantage of technologies such as cell phones, GPS, and real-time access to news feeds. Another example presented the story of a website, *PatientsLikeMe*, focused on connecting people with chronic illnesses. In my opinion it was unnecessary, too long and distracted the attention from the main thread.

In spite of these several faults I think that the book is worth reading. Many views of the author regarding various types of the cybercrime are accurate, which is undoubtedly an advantage. However, the biggest asset of the discussed publication is its scope; it would appear that on approximately 400 pages Goodman discussed nearly every aspect of the subject (consumer, industrial, medical technologies, etc.). Moreover, from the given examples of the criminal activities the author skilfully deduced future tendencies in this area.

The book appears to be an excellent textbook for those who study national security, internal security, criminology, law, etc. In the absence of studies on the policy of cyber security one must admit that Goodman filled the gap, which is especially recognized by the academic staff. In this volume the writer brilliantly underlined relevant aspects of the security in the given research area. In my opinion, due to the interesting approach to the problem this publication is recommendable not only for students and lecturers but also for every person interested in learning about nuances of the cyber security, and, particularly, for entrepreneurs from the IT sector and for professionals who ensure the security in the cyberspace. Relevance, the rank of undertaken issues and the level of expertise are the most exceptional qualities of this book. Moreover, the logical approach to the problem, accurate division and compelling content deserve recognition. Furthermore, the author's argument is clear; he explained new terms, their applications and then moved to using these concepts in the problem-solving context. It should also be noted that apart from the interesting content this book is characterized by accessible language which facilitates its reception.

References:

Buchy, J. (2016). "Cyber Security vs IT Security: Is There a Difference?". *George Mason University. School of Business*. Retrieved from: http://business.gmu.edu/blog/tech/2016/06/30/cyber-securit-it-security-difference.

Chabrow, E. (2010). "Cybersecurity Vs. Information Security". *Information Security Media Group: Government Info Security.* Retrieved from: http://www.govinfosecurity.com/blogs/cybersecurity-vs-information-security-p-711.

Goodman, M. (2016). *Zbrodnie przyszłości. Jak cyberprzestępcy, korporacje* i państwa *mogą używać technologii przeciwko Tobie.* Gliwice: Helion.

Titchener, J. (2013). „Are information security and cyber security the same thing?". *IT Governance Ltd.*. Retrieved from: www.itgovernance.co.uk/blog/are-information-security-and-cyber-security-the-same-thing.

Author

Ms Natalia Ciszewska

Nicolaus Copernicus University in Toruń, Faculty of Political Sciences and International Studies. Contact details: ul. Batorego 39L, 87–100 Torun, Poland; e-mail: natalia.ciszewska@interia.pl.