Book Review

DarkMarket
CyberThieves, CyberCops and You

by Misha Glenny
Random House, London
2011, 296 pages
ISBN-9781847921260

Reviewed by Richard Shortt

If you want to learn more about the cyber threats we face in today's interconnected world, *DarkMarket* provides an ideal case study. Glenny, a journalist and historian takes the reader inside the cyber-enabled criminal domain and details how an internet site set up to service the connection and supply needs of cyber-enabled criminals from across the world worked.

The story is structured in two parts. In the first, Glenny sets the scene regarding internet enabled criminality and introduces the reader to the main characters. The section provides historical context about the development of cyber-enabled crime and some of those responsible for driving its development. The section also introduces the main cyber terms you need to come to grips with to gain—at the least—a moderate level of understanding of the cyber enabled criminal world, terms like: "phishing," "carding," "dump" and "hacking." On the issue of terms, I use the term "cyber-enabled" because the crimes described in this story are not new. They include old favourites like theft, burglary (i.e. break and enter), extortion and fraud. The difference in the cyber world is that they are enabled through technology, be it a computer, server, money-card skimming device, or computer network.

The criminals themselves are also not new. They are the opportunists, amateurs and career offenders that law enforcement has been encountering since the first laws were enacted and someone was charged with enforcing them. However, the difference is these criminals' ability to navigate and operate in a world that is as foreign to most as living on another planet, but which is more and more entwined with our lives. As Glenny points out, even our motor

vehicles now have embedded technology that requires a computer technician to fix—not a person with a spanner in their hand and oil under their fingernails—while providing the cyber-criminal with the ability to offend against them without the need for lock picking or window breaking. In fact, not even having to be near the vehicle.

In the second part, Glenny details how the *DarkMarket* site was compromised and finally closed through the efforts of law enforcement officials in a variety of countries. He details and exposes the challenges officials face in tackling a multi-headed, widely connected, loosely associated group of essentially anonymous people (or groups) who hide behind ego-driven monikers such as "Matrix," "JiLsi," Iceman," "Cha0" and "Lord Cyric" in a world with no restrictive boundary, such as a geographical jurisdiction or physical border. The criminals do, however, appreciate how such boundaries can affect them and how officials within the boundaries can be neutralised. For example, Russian cyber-enabled criminals avoided committing crimes against Russian targets, thereby avoiding the interest of their domestic intelligence and law enforcement agencies. Similarly, other cyber-enabled criminals focused on jurisdictions that did not display an aggressive desire to come after them, while targeting people and computer systems in countries to which they themselves had never been and which they had no intention of travelling too.

Working to thwart these criminals were a range of security and law enforcement organisations and officials in a variety of countries; from the United States, United Kingdom, France, Germany, and Turkey. Each agency held a small piece (or in some cases large amounts) of information, but ultimately needed the others to contribute their knowledge before a true picture of the criminal network could be built. Once that picture was known, then the identities and vulnerabilities of those involved could be plotted and their downfall orchestrated.

As Glenny traces the origins and operations of the *DarkMarket* site and its various "administrators" (a term used in this book which also means: criminal conspirator, crime boss, or just plain criminal), the non-cyber skilled reader comes to appreciate the complexity of this new operating environment. It challenges the sovereign state/domestic focus of traditional law enforcement jurisdictions and forces officials to engage in a mixture of cooperative, coordinated and collaborative arrangements, not just with official counterparts (which is reasonably common in law enforcement), but also in arrangements

with the private sector who own, operate and understand the systems and networks involved, and whose customers are ultimately the victims of the crimes being committed.

DarkMarket also exposes the lengths that modern law enforcement must go to in order to identify, track, and ultimately trap, cyber-enabled criminals. Again, nothing is really new, just the way it is done. Many law enforcers are versed in the techniques of sting operations, essentially helping the criminals show exactly what they are up to in the presence of law enforcement officials so that they can be lawfully stopped and, where possible, prosecuted. *DarkMarket* is a case study in just such a technique, and an example of how it can be effective against the cyber-enabled criminal. The book also details the difficulties such operations face where multiple jurisdictions have to be engaged for them to be successful.

This book is an easy read. I recommend it to anyone who would like to learn more about the challenges facing civil society from cyber-enabled crime (regardless of whether you have any security or law enforcement responsibilities). I particularly encourage people with responsibility for cyber-crime policy to consider reading this book because it provides the historical context and insider's insight into an issue that is not going to go away.

ABOUT THE REVIEWER

Richard Shortt, MPM, is a PhD Candidate with Charles Sturt University's Australian Graduate School of Policing and Security. He is a retired New Zealand Police officer, who has also worked as a national security policy advisor within government and managed a nationally focused, multi-agency, threat assessment unit. Richard's PhD research is into the nature of inter-organisational relationships between intelligence and law enforcement agencies when tackling "wicked issues" such as transnational criminality.

- o O o -