## Then and Now: A Look Into the World of Espionage and the Impact of the Internet on Traditional Spying

GORDON CORERA, CYBERSPIES: THE SECRET HISTORY OF SURVEILLANCE, HACKING AND DIGITAL ESPIONAGE (Pegasus Books Ltd., 2016)

New York, New York 2016
Pegasus Books Ltd., 2015
ISBN: 978-1-68177-154-0
Price: $29.95, pp. 391

Key words: Cyber Espionage, Spying, Data, Hacking, Surveillance, Government

Reviewed by Ashley Berger
Journal of High Technology
Suffolk University Law School

---

*"Computers went from being a tool for espionage … to being the means of espionage itself: because they could talk to each other, one machine could steal another's secrets. This is the story of how that happened, what came next and why it matters."*[1]

Gordon Corera's Cyberspies: The History of Surveillance, Hacking and Digital Espionage delves into the history of traditional espionage and how that age-old process has adapted to modern cyber espionage. Cyber espionage is at the forefront of intelligence discussion and debate: how to monitor the ever growing internet of things and what the government and law enforcement to do within their legal boundaries to detain, arrest and shut down actors working behind a screen to stop them from obtaining the most private of secrets. This review will examine the scope of Corera's journey through time, beginning with the earliest of espionage and focusing on the impact that cyber espionage has on the government, the military and how society perceives the threats and affects of cyber espionage.

[1] *See* GORDON CORERA, CYBERSPIES: THE SECRET HISTORY OF SURVEILLANCE, HACKING AND DIGITAL ESPIONAGE 8-9 (Pegasus Books Ltd., 2016).

Hailing from Britain, Gorden Corera is not only an author and journalist but also acts as the Security Correspondent for the BBC News. Mr. Corera holds a degree in modern history from the University of Oxford as well as a graduate degree in United States foreign policy from Harvard University. Mr. Corera's resume includes working on the re-election campaign of former United States President Bill Clinton before joining the BBC in 1997 as a researcher and reporter. Since working for the BBC, Mr. Corera has presented documentaries focusing on secret intelligence, espionage and cyber space as well as authoring "The Art of Betrayal: Life and Death in the British Secret Service" and "Shopping for Bombs: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the A.Q. Khan Network", on the same subjects. Mr. Corera's accolades include being named the Information Security Journalist of the Year at the BT Information Security and Journalism Awards in 2014.

Cyberspies: The History of Surveillance, Hacking and Digital Espionage is a timeline of espionage beginning with the First World War and exploring major developments in both traditional espionage and cyber espionage since the beginning of the 1900's. Structured in eighteen chapters, each one provides a different insight to a different player in the game of cyber espionage, whether a state, an actor, an attack and how that event has impacted the current state of espionage. While each chapter has a slightly different focus, Mr. Corera does a fine job of tying all relevant elements of how history is truly a foundation for where society is now dealing with these issues as well as enforcing how impactful the potential effects of cyber espionage will be in the near future. The end of Mr. Corera's book is a lengthy set of endnotes, directing readers to the sources he relied upon to form his timeline and conclusions and for more background information.

Mr. Corera acknowledges early on in his book that “this was originally intended to be a narrower book about ‘cyber espionage’ … but as I tried to understand what it was an where it came from, it soon became clear there was a more interesting story to tell.”[2] Successfully, Mr. Corera does just that – hooks the reader in with a complete history of how cyber espionage came to be by relying on what traditional espionage was. The concept of cyber espionage would be moot to a reader if the background and hurdles of traditional espionage were first not adequately explained. Spying has been an age-old practice and technology has enhanced the abilities of spies and the governments they work for. Perhaps most importantly, Mr. Corera defines spying as “finding out secrets … that has involved establishing the intentions of another state, such as its plan and capabilities for waging war”[3] and then using that description to explore how espionage has developed into cyber espionage and hacking– for better or for worse – in the cyber domain.

Throughout the book, Mr. Corera alludes to the notion that with each new event, such as Titan Rain, the KGB’s 1980’s attack and most recently, the Stuxnet debacle in Iran, governments are surprised at how hackers are able to infiltrate and explore systems and data. Instead of being surprised though, Mr. Corera suggests that the infrastructure should be better secured and enforces how easy it is for hackers to get into systems that are supposedly “secure.” He attributes this to the weak foundation that the Internet was built upon, because creators never could have imagined the explosion and ultimate reliance on computers all hooked up to a network, a network with many holes.

Repeatedly, human nature and history have shaped the field of cyber espionage, but the end goal of espionage has not changed at all. Espionage has been carried out in all

[2] *See* Corera, *supra* note 1, at 9.
[3] *See* Corera, *supra* note 1, at 9-10.

other physical spaces, the development of the computer has simply provided a new tool by which to spy. Clearly and logically throughout this book, Mr. Corera emphasizes that computer abilities may be changing, but that human nature is not. Where the computer provides a major tool to learn and dissect its users secrets, the purpose of gaining access to those secrets is to use them against the holder for the hackers gain.

Time and time again, Mr. Corera refers to the fine line between legality and illegality in the scheme of espionage and cyber espionage. This question first arises in Mr. Corera's discussion of telegrams and if it was legal then for the National Security Agency (the "NSA") to be reading telegrams. It seems that these intrusions were excused then in the name of patriotism. Nearly with every described incident, underlying the science and technology behind each hack or actor, there are various legal questions stemming from 'is this legal' to 'how far can something go before it becomes illegal.' Within this discussion, Mr. Corera does a great job of keeping the reader engaged by referring to and acknowledging recent scandals and their legal outcomes, such as the Edward Snowden and Wikileaks debacle and the violations of espionage committed by Bradley (now Chelsea) Manning.

One of the major problems with the Internet and the regulation of it, is that the physical structures are generally privately owned by companies but the necessary response would have to come from the government and the military, so there is a disconnect between who is the recipient of the attack and what entity is able to appropriately response. The companies expect the government and military to protect their data, but with so many anonymous players, that task is quite great to take on. One of the themes in the book is that cyber espionage doesn't seem to fit into something that the military can protect against, but also something that law enforcement does not have the full capabilities to guard against either because of the nature of cyber espionage. This "crime" includes elements of traditional criminal activity but that this type of spying can also escalate to threats against national security and lead to physical destruction. Throughout the book, it seems that cyber espionage is investigated and dealt with in the United States by a variety of governmental agencies including the NSA, the Central Intelligence Agency (the "CIA") and the Federal Bureau of Investigation (the "FBI").

Late in the book, Mr. Corera delves into the issue of "cyber weapons" and questioning if the Stuxnet virus and this new class of weapons provide a state with the ability to act in self-defense. This new technology, resembling the first atomic bomb in the sense that something similar has never been used before, may have catastrophic legal consequences for states if acted upon incorrectly. Mr. Corera seems to wrestle with what body has the power to determine what rises to a level of necessary self-defense and what does not as well as what foreign states have the capabilities to launch such an attack. Mr. Corera makes it a point to distinguish between cyber spies infiltrating networks to learn information about the enemy from hackers actually launching some sort of attack.

The book achieves its goal of providing the reader with an exceptionally detailed history and explanation of cyber espionage. Generally the book is easy to follow, though a reader with a basic understanding of technology and coding would probably find this a more interesting read than one without a technological background. Likewise, Mr. Corera adequately provides a background legal discussion about the issues that have surrounded new technology and actors potentially abusing the benefits of that technology. These include potential acts of war and legally how a state can respond as well as the probably more common data theft and how companies should be better protecting their data but also who can be held liable for this thievery, an entire state? A particular actor? A competing company? These seem to be questions that are asked but not fully answered, likely because those questions have not been adequately addressed in the real world yet.

While the book seems lengthy, the simple language, individualized chapter breakdown and chronology make the story not only engaging, but also easy to follow. While the book does include some references to very technical coding terms, the usage and descriptions of such do not lose or intimidate the reader. Rather, the informative tone of Mr. Corera's writer seeks to and successfully educates a reader who may not have a solid basis for understanding the history, technological advancements or legal implications for modern day cyber espionage. By interweaving history and current events, Mr. Corera's book reads like a novel, keeping the reader, be him or her a history buff, a lawyer, a student or coder, fully engaged and interested.