mapub.org/mapeh

MAP Education and Humanities

Volume 5

MAP Education and Humanities (MAPEH) is a scholarly peer-reviewed international scientific journal published by **MAP** - *Multidisciplinary Academic Publishing*, focusing on empirical and theoretical research in all fields of education and humanities.

E-ISSN: **2744-2373**

BOOK REVIEW

DARK WIRE:THE INCREDIBLE TRUE STORY OF THE LARGEST STING OPERATION EVER

Senka Sojkić [1]

[1] ***International Burch University***, *Sarajevo, Bosnia and Herzegovina*

Correspondence concerning this article should be addressed to Senka Sojkić, International Burch University, Sarajevo, Bosnia and Herzegovina. E-mail: senka.sojkic@gmail.com

ABSTRACT

At the end of the 20th and the beginning of the 21st century, there was a significant increase in organized crime, which was contributed to by the advancement of technology and globalization. Organized crime groups have become increasingly sophisticated, using encrypted communications applications like SkyECC and ANOM to avoid detection and prosecution by law enforcement.

“Dark Wire: The Incredible True Story of the Biggest Sting Ever” by Joseph Cox delves deep into the secret world of criminal enterprise and the extraordinary measures law enforcement agencies take to combat this type of crime. Cox explores the convoluted narrative by analyzing its historical context, investigative journalism, and the sting operation’s broader implications for law enforcement tactics and civil liberties. The book not only provides a stunning account of one of the largest sting operations in history, but also raises pertinent questions about the ethical and legal ramifications of such covert activities.

Keywords: Organized crime, Globalization, Encrypted Communication Applications, SkyECC, ANOM

Multidisciplinary Academic Publishing

MAP EDUCATION AND HUMANITIES

Volume 5

ISSN: 2744-2373/ © The Authors.
Published by **MAP** - *Multidisciplinary Academic Publishing.*

Article Submitted: 18 February 2025
Article Accepted: 02 March 2025
Article Published: 03 March 2025

Publisher’s Note: ***MAP*** *stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.*

https://doi.org/10.53880/2744-2373.2024.5.123

MAP EDUCATION AND HUMANITIES
Volume 5

HOW TO CITE THIS ARTICLE

Sojkić S. (2025). **Dark Wire:The Incredible True Story of the Largest Sting Operation Ever**. MAP Education and Humanities, 5, 123-126. doi: https://doi.org/10.53880/2744-2373.2024.5.123

© The Author(s). **Open Access Article**

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

OPEN ACCESS
ARTICLE

The book "Dark Wire: :The Incredible True Story of the Largest Sting Operation Ever"is the first published book dedicated to sophisticated encrypted applications for communication, which delves deep into the world of criminal enterprises and extraordinary measures taken by law enforcement agencies around the world, with the aim of breaking or deciphering these applications. Well-known investigative journalist Jospeh Cox, who is also the owner of the web page Vice, detailed the daring and elaborate operation undertaken by law enforcement agencies around the world to infiltrate and dismantle a sophisticated criminal network. As an investigative journalist, Cox devoted a large part of his career to researching cyber security and fighting crime, in such a way that he followed the work of sellers of sophisticated encrypted communication devices, who promised members of the criminal milieu that they could not be eavesdropped or caught by the police.

At the end of the 20th and the beginning of the 21st century, there was a significant increase in organized crime, which was facilitated by the advancement of technology and globalization. Organized crime groups have become increasingly sophisticated, using encrypted communications applications and the dark web to avoid detection. Cox paid special attention to certain decrypted applications for communication, the way they were created, the expansion among various organized criminal groups on a global level, emphasizing the challenges that law enforcement agencies face when trying to decipher these applications. Law enforcement agencies have had to devise a response to this phenomenon, so they have adopted more aggressive and covert strategies to combat these evolving threats, emphasizing innovative methods used to gather intelligence.

As an investigative journalist, Cox showed amazing courage through the narrative, where several stories from several organized criminal groups and their participants in several countries around the world are interwoven, and which then show the degree of connection and coordination. Cox paid special attention to the main characters of the book, from the members of organized crime groups to the agents who were involved in this sting operation, emphasizing the importance of the sting operation, but ignoring the danger of revealing the identity of the agents who were involved in these narratives from the beginning. All the actors are described vividly, and the conversations, interviews and information that the author collected from them gave authenticity to the said book.

Although some phones and applications functioned in a secret, encrypted way, they were eventually discovered by law enforcement agencies, and in such a way that the founders of the companies that sold these devices with installed encrypted communication applications were first arrested, and who then agreed to cooperate with the prosecution and the police. During the cooperation, they would mostly declare that they sold the mentioned phones to members of the criminal milieu to enable them to communicate easily between members of the group, and that these devices promised the complete impossibility of access by law enforcement agencies to these communications. The sellers of these phones also offered members of the criminal milieu and a promise that if they are still caught by the police or the prosecutor's office, that they have the possibility to delete the contents of the phone (and therefore all communications) in a very simple way. You only need to press the panic button and enter the pre-determined password for this occasion.

The book is structured in such a way that each new chapter reveals a new part of the secret operation, connecting in this way members of organized criminal groups around the world, the way in which they mutually arrange cooperation and deals, but at the same time the author describes the cooperation of law enforcement agencies that strive to discuss the best ways to tackle this problem. For a moment it seems as if it is one of the world's bestsellers that provides a fictional story about undercover police operations, but Cox references his sources throughout the narratives of each chapter, ensuring that the information presented is accurate and credible.

"Dark Wire" explains the intricate activities of a sting operation carried out in cooperation with several law enforcement agencies, where the different phases of the operation are explained through different chapters, from the initial planning and intelligence gathering to the execution and final elimination of organized criminal groups. The use of sophisticated decrypted communication applications is a key factor, which has been an excellent technique for gathering evidence against these groups on a global scale. Cox was also involved in researching the psychological tactics that agents used to gain the trust of criminals and thus obtain current information, describing the ethical dilemmas that agents faced during the operation.

Although Cox expresses his admiration for the topic throughout the narrative, he also considers the ethical issues of using the applications, wondering whether members of law enforcement agencies may have exceeded the limits of their jurisdiction and authority in these operations, and what implications this has for privacy and civil liberties. The use of special investigative actions, special techniques and tactics, which include the use of such applications, implies an examination of the legal frameworks that regulate the aforementioned areas, which Cox focuses on, and which encourages readers to think critically about security and privacy in the digital age.

"Dark Wire: The Incredible True Story of the Largest Sting Operation Ever" is a kind of detailed report on an extraordinary operation conducted by law enforcement agencies on a global level in the fight against organized crime. The book consists of 4 parts, where each part has a certain number of chapters that provide detailed and interesting narratives on two sides, organized criminal groups, but also on the side of law enforcement agencies.

In the first chapter, the development of organized crime at the end of the 20th and the beginning of the 21st century is shown, as well as the development and expansion of the company Phantom Secure, based in Vancouver, Canada, who was the first to design ultra-secure phones for the needs of clients. Those phones had special features such as erasing the contents of the phone remotely in emergency situations, if the phone fell into the wrong hands or if it was confiscated by law enforcement. This model was interesting because it was sold only to members of the criminal milieu, and through the analysis of the case of a fellow dealer who distributed cocaine in the US and Australia, the way in which he and other members of organized criminal groups obtained encrypted communication devices was described. These phones gained popularity in 2014 when the media in Australia reported that Phantom Secure phones were linked to certain murders but that the police could not access the contents of the phones to read the messages. In 2018, the director of Phantom Secure was arrested and convicted of conspiracy to extort for knowingly selling these phones to members of the criminal underworld. "The phones landed everywhere crime syndicates could be found, from cocaine production labs to drug safe houses. The users were corrupt police and government officials, hitmen for hire, and artisanal drug smugglers", said Cox.

Already in the second chapter, Cox includes in the story individuals who worked on the side of the law to implement this operation, from prosecutors in the US Attorney's Office for the Southern District of California and FBI agents, who were already familiar with Phantom Secure Phones.

Given that organized criminal groups in the US and Australia have already largely used these phones, it has already become clear for law enforcement in Australia and the FBI office in San Diego that they must join forces and work together on this problem to gather evidence against these groups. They held a meeting in 2016 attended by members of the Australian Federal Police (AFP) and San Diego team, prosecutors and FBI agents with discussion how to move together as one against Phantom Secure. Cox described the details of the meeting in Chapters V and VI, describing the dilemmas that law enforcement members faced during that period.

Given that the director of Phantom Secure had already been arrested, the distributors of this phone were wondering what to do next and how to avoid the FBI. One of the distributors, who was very technically educated, decided to offer the FBI to establish his own company that would sell encrypted phones, and in exchange for help, his fine would be reduced. Thus, ANOM was born and Cox begins Act II of the book.

The Anom application could not be found and downloaded on the Google Play Store like most other applications, but the ANOM company "loaded the app onto phones itself and then sold these phones to corporations that wanted to keep their internal communications secure." Due to the demand of its clients, ANOM had to have a solution for archiving messages, which it used.

After the first distributor of ANOM phones was found in the field, he did not focus on corporations, but sold these phones to people from the criminal milieu, from the Italian mafia to drug dealers in Australia. In chapter eleven, Cox described in detail the characteristics of ANOM phones and how they were a better version than Phantom Secure, which additionally confirmed that Cox had extremely good sources that guaranteed him the authenticity of the entire story. Other encrypted phones did not have a camera and microphone, which was not the case with ANA.

Throughout the entire narrative, the ethical dilemmas that law enforcement agencies face during the entire operation and the way they were resolved are emphasized. One of the problems that arose for law enforcement was that certain countries such as Australia were not legally able to share data collected in this way with other countries, and the solution was to find a European partner who could do it for them. Thus, was born an operation the FBI called Trojan Shield, which Cox described as an "investor in the criminal underworlds latest startup."

Act III in his book Cox begins with a separate encrypted phone company, Encrochat, which had some of its servers in France, but the French police were able to retrieve these messages in the update process, several times, even after the company realized what happened. After that, the company closed Encrochat and sent a message to its customers that the phones are no longer safe for communication.

In the following chapter, Cox also described the Ironside operation, which was carried out by the AFP in Australia using data from ANOM, to confront the Calabrian Mafia. In one of the chapters, he also focuses on Dubai, which he defines as a paradise for people from the criminal milieu, who want to avoid persecution by law enforcement agencies, stating that in Dubai protection can be provided very easily because it is only necessary to have money, and Another reason why Dubai is a "paradise for criminals" is that there is no extradition.

The fourth part of the book represents the sublimation of all activities related to sophisticated encrypted applications for communication and is perhaps the simplest for readers, considering that the previous parts "jump" from topic to topic, which is difficult for readers who do not know the subject to understand at first reading.

Chapter 26 describes the events in February 2021, when police agencies decided to disclose that they had access to SkyECC, and thus began mass arrests in many European countries, primarily the Netherlands and Belgium, after which the users of the application began to send messages to each other: "Sky is down." Cox believed that only a few knew that the hack of Sky was part of the much grander master plan to force criminals over to ANOM. The operation wasn't so much about arrests that day. It was might happen next, said Cox, leading readers to see the operations as a certain conspiracy theory. After the arrest, US authorities confiscated Skys web domains, and the owner was indicted for providing Encrypted Communication Devices to help international drug traffickers avoid law enforcement. The eartquake of Sky's closure created a tsunami and tidal wave of users who needed a new encrypted phone headed straight in ANOM's direction. That's how the expansion of the ANOM application began, but also the story that it is one of the most secure applications for communication.

It described the hectic work that the FBI team in San Diego was doing every day, as well as the EUROPOL team, trying to cope with the ever-increasing flow of intelligence that came in every day, and preparing for the arrests of almost 800 people around the world. Agencies around the world-built cases based on this information, but as good as this information was, it was still insufficient to serve as evidence and guarantee a conviction at trial. Now it was time for ANOM, which was mainly an intelligence weapon, to change into an evidence-gathering tool, one that could be used to prosecute those drug traffickers in court. Investigators combined these messages with special investigative actions, physical surveillance, data from social networks, trying to identify ANOM users and to create a rich picture of exactly what crimes they committed, and to provide evidence for it.

Just as organized criminal networks now operated without borders, the officers inside EUROPOL did the same. They instantaneously collaborated, their own borders practically meaningless, concluded Cox.

In the book's epilogue, Cox described how the FBI and a member of Europol traveled to other countries and made available to law enforcement agencies information from the ANOM application that related to their area, which included Bosnia and Herzegovina, Serbia and Montenegro.

"Dark Wire: The Incredible True Story of the Largest Sting Operation Ever", by Joseph Cox, is a fascinating story about the emergence and use of sophisticated encrypted applications for communication that leaves every reader breathless, providing an insight into the detailed description of them, and the way they are used by organized criminal groups but also by law enforcement agencies on a global level.

The book emphasizes the role of technological innovations in the digital age in law enforcement, where the use of cutting-edge technology has made it easier for organized crime groups to commit crimes, but it is precisely this modern technology that has enabled law enforcement agencies to come up with creative investigative techniques thanks to which impressive operations are carried out. in the fight against organized crime, such as the operations featured in "Dark Wire."