freepik.es

Juan Manuel Aguilar Antonio*

Cybercrime, the New Global Challenge and Its Impact in Mexico

Cybercrime's Global Impact

In 2021, the United Nations Office on Drugs and Crime (UNODC) published the first issue of the *Digest of Cyber Organized Crime*.[1] The report is significant because it presents a series of case studies about organized cybercrime in different regions. It should be noted that the compendium has a global scope to ensure equitable representation.

It is divided into five chapters and the cases organized in tables. Among the issues touched on are the kinds of organized cybercriminal groups, as well as their structure and organization; their tools; and procedural issues related to the investigation, prosecution, and adjudication of cases linked to organized cybercrime.

The study covers more than 130 events in thirty countries, with their respective jurisdictions and different *modus operandi*. It also presents the ways that each nation investigates, prosecutes, and judges this activity. It is a key tool for familiarizing oneself with criminal organizations and contributes to improving procedural issues in this area; identifying challenges to investigating, judging, and adjudicating cases; and identifying the lessons learned by professionals in the administration of justice, including challenges in dealing with this kind of crime.

Since the Covid-19 pandemic, this kind of surveillance has heightened because intensified use of information and communication technologies (ICTs) has impacted organized crime's operations. In fact, ICTs have had a huge impact on illicit activities, on the profiles of participating individuals, on the kinds of crimes committed, and their *modus operandi*. I should underline that some conventional criminals have completely immersed themselves in cybercrime, while others limit themselves to operating through cyberspace and do not need to become more involved to generate income.

* Juan Manuel is a fellow in the CISAN for the UNAM Post-doctoral Fellows Program; you can contact him at alchemistffvii@hotmail.com.

The UNODC report underlines the fact that certain criminal groups like drug traffickers and local or national mafias tend to increasingly associate with cybercriminals with technical skills and capability in order to take advantage of their talent to commit crimes on the Internet. Among the main kinds of professionals they seek out are code writers, malware and exploit developers,[2] and others who have the tools that are useful for their purposes.

It is also important to analyze how apps and their links to ICTs have transformed criminal organizations' structures and organization: using cyberspace eliminates the need for face-to-face contact and allows people who do not know each other well to work and coordinate their activities from anywhere in the world. They can even use aliases, thus minimizing the risk of revealing their identities and locations to other members of the group. This has facilitated the creation of new criminal groups and networks that operate completely on the Internet; this, together with apps and ICTs, has eliminated the barriers to access to illicit markets, which are no longer limited by geographical location.

Cybercrime in Mexico: The Case Of Online Loan Sharking Networks

On August 17, 2022, the Cyber Police of Mexico City's Ministry of Public Security carried out a surgical operation in coordination with the City Attorney's Office. The next day, at 11:29 a.m., the then-head of Mexico City's government, Claudia Sheinbaum, held a press conference to explain the operation's details, which included raids on twelve locations due to the abnormal increase in complaints about loan applications available through smart phones. This was the debut performance of a public security institution that had fought against a complex criminal network that used cyberspace to commit cybercrime.

Certain criminal groups like drug traffickers and local or national mafias tend to increasingly associate with cybercriminals with technical skills and capability in order to take advantage of their talent to commit crimes on the Internet.

This event shows the legal scope that these groups can have in the country, using legal loopholes, institutional deficiencies, and the lack of awareness about cybersecurity. Let us look at some key points about these loan sharking networks that have been able to impact the Mexican population.

What Are Online Loan Sharks?

These are groups that practice fraudulent financial practices and extortion, taking advantage of the rise in financial technology and the growing demand for loans in the country's big cities. Of course, they operate in the shadows, often offering quick loans through mobile apps downloadable to cell phones. Their *modus operandi* involves promoting these services online, especially in social media, to attract people looking for loans without strict prerequisites. They promise to grant loans immediately without verifying credit history.

In this sense, they are particularly dangerous because of their lack of transparency and the fact that they are not authorized by the country's financial authorities. When doing a thorough investigation, it is difficult to find verifiable information about these organizations or persons (address, history, contact numbers, or legitimate news about their activities). The real threat lies in their requests for loan applicants' personal, sensitive information. To approve the loan, they demand delicate information such as our full name and date of birth (often used in personal passwords), cell phone number, access to our contacts, photo gallery, and, sometimes, to users' social media accounts.

This has hurt many people, since the loan sharks often charge exorbitant interest rates and use extortion tactics to get the money back. In addition, applicants are in danger of their personal and financial information being used fraudulently in the future.

Transnationality and the Lack of Regulation

During the aforementioned Mexico City cyber police operation, twenty-four people were arrested, five of whom were of Asian extraction. It is important to understand the national and international scope of the network: it was

operating in eight of Mexico City's mayoralties and eight states of the union (Jalisco, Sinaloa, Nuevo León, Hidalgo, and Querétaro, among others) and also made use of call centers subcontracted from Colombia and China to extort customers. This defines it as a translational network that took advantage of the Internet's ubiquitousness.

This was one of the first big operations against these mid-sized gangs that use new technologies and take advantage of the lack of a data protection culture among the general populace to exploit their weaknesses. This means the raid was an important precedent.

The Murky Field of the Administration of Justice

Despite that, one of the main weaknesses exploited by cybercriminals is the lack of experience of litigating and defense attorneys in Mexico in dealing with cybercrime complaints. This is due, in part, to the almost non-existent coverage of this issue in national and state penal codes, despite the fact that legislators both in the Chamber of Deputies and the Senate have pushed for bills to be passed on cybersecurity, for example, the National Cybercrime Law.

Given this state of affairs, the legal vacuum was better used by the online loan sharks because there was no regulatory and verification body to check the apps promoting loans available on Google Play and in the Mac Store for Mexican users. This contrasts with the situation in a large number of European and North American nations, where apps must pass muster in a verification process to show that they are safe for users, that they are not purveyors of fraud, and that they comply with minimum data protection requirements. Mexico lacks such an authority, and this has facilitated proliferation of the apps among the population.

In addition, the extorsion schemes used a complex network of social engineering. When users registered on the app, the loan sharks were able to identify their Facebook, Twitter [or now, X], or Instagram page and download their photos and personal and family information to extort them. With that material, the cybercriminals sent modified photos and videos with the faces of their victims. They could also send fake videos of supposed armed commandos of the criminal organizations to intimidate them.

Loan sharks are groups that practice fraudulent financial practices and extortion, taking advantage of the rise in financial technology and the growing demand for loans in the country's big cities, they operate in the shadows, often offering quick loans through mobile apps downloadable to cell phones.

The Potential for Expansion

The online loan shark schemes have high potential for expanding to a large number of important urban areas in the country, such as Monterrey, Guadalajara, León, and Tijuana, among others. However, doubts continue to exist about the investigative and containment capabilities of local law enforcement. The cyber police and Mexico City Ministry of Public Security experience should be an example that the rest of the states follow to improve their crime prevention and prosecution. The online loan shark could be just the tip of the iceberg in the sea of Mexico's cybercrime.

This brings up many questions about the issue. Among them are: What about ransomware attacks?[3] What about information breaches or the theft of intellectual property in cyberspace in Mexico? How do cybercriminals move through the deep web and the dark net and what will happen if cybercriminals attack critical national infrastructure or government databases and networks?

We know very little about this. However, we have to celebrate the success of this first operation and begin to build a road toward the generation of resilience and dissuasive capabilities in Mexico's legal institutions and among users in order to make cyberspace safe. VM

Notes

1 United Nations Office on Drugs and Crime, *Digest of Cyber Organized Crime* (Vienna: UNODC, 2021), https://www.unodc.org/documents/organized-crime/tools_and_publications/21-05344_eBook.pdf.[Editor's Note.]

2 Malware is a kind of software designed to damage or steal information or carry out actions in computer and operating systems or networks without users' consent; an exploit is a fragment of code or a series of instructions designed to take advantage of a specific vulnerability in a program, operating system, or device.

3 Ransomware is a program that restricts access to certain parts or files of an infected operating system; the criminals demand ransom in exchange for freeing up the system again. [Editor's Note.]