The Impact of the COVID-19 Pandemic on the Serious and Organised Crime Landscape:

Assessing the evolution of serious and organised crime during COVID-19 through the enterprise model

Tamara Schotte
Mercedes Abdalla
Europol

Abstract
Organised crime not only did not stop during the pandemic: on the contrary, it leveraged the situation prompted by the crisis, including the high demand for certain good, the decreased mobility across and into the EU, as well as the increased social anxiety and reliance on digital solutions during the crisis. Criminals have quickly capitalised on these changes by shifting their market focus and adapting their illicit activities to the crisis context. The supply of counterfeit goods and the threat posed by different fraud schemes, financial and cybercrime activities have remained significant throughout the crisis. The prolonged COVID-19 situation and related lockdown measures have exposed victims of crimes revolving around persons as a commodity to an even more vulnerable position. Recently, newly emerging criminal trends and modi operandi have emerged that are specific to the current phase of the pandemic that revolves around the vaccination roll-out and the wider financial developments of the crisis. In parallel, already known pandemic-themed criminal activities continued or criminal narratives further adapted to the recent developments in the pandemic and the fight against it.

Keywords: COVID-19, serious and organised crime, criminal networks

Introduction

Recent developments have demonstrated that global crises such as the COVID-19 pandemic do not hamper serious and organised crime. Instead, criminals again demonstrated their ability to adapt to external challenges. On the contrary, it has evolved in the pandemic context and exploited the crisis situation. The obstacles or challenges that societies have been confronted with have become an opportunity for both for criminal networks and opportunistic criminals. Criminals have leveraged several crisis-induced developments in the wider environment, including the high demand for certain goods, the decreased mobility across and into the EU, the increased reliance on digital solutions and the widespread social anxiety and economic vulnerability (Europol, 2020a, p. 3). Criminals have quickly capitalised on these changes by shifting their market focus and adapting their illicit activities to the crisis context. This paper aims at providing an overview of the key findings that affected the serious and organised crime landscape since the outbreak of the pandemic, looking at the developments through the theoretical lens of the enterprise model.

Research design

Europol has been monitoring the impact of COVID-19 on crime since the outbreak of the pandemic and developed a series of strategic assessments informing Law Enforcement partners, the general public and decision makers on the developments pertaining to the serious and organised crime and COVID-19. These assessments provided a general overview of the most impacted crime areas and zoomed into focal topics.

The analysis relied on operational data and strategic information provided by EU Member States ad Third Partners to Europol, as well as on a set of dedicated monitoring indicators. Where needed and applicable, in-house intelligence was complemented with open source information providing context to law enforcement's understanding of the serious and organised crime scenery in the EU.

The enterprise model of organised crime

The notion of the enterprise model applied to the study of serious and organised crime started garnering significance from the 1970's onward; following insights gained into the organisation of Mafia groups, scholars drew up the hypothesis that legal and illegal businesses operate in a similar manner. The main principle of the enterprise model of organised crime emphasises the profit-oriented nature of organised crime (Halstead, 1998, p. 2). In this context, illicit marketplaces operate according to the same logic as a legitimate business would– they adapt to market forces and respond to the demands of customers, suppliers, regulators and competitors (Arsovska, 2014). Criminal markets emerge and/or flourish in vacuums and loopholes of legal markets, which are heavily exploited by criminal networks. Consequently, niche markets emerge where

> *"(...) buyers, sellers, perpetrators, and victims interact to exchange goods and services consensually, or through deception or force, and where the production, sale and consumption of these goods and services are forbidden or strictly regulated"* (Tusikov, 2010, p. 7).

Other markets, including those for sexual exploitation, migrant smuggling and drugs have always operated outside state regulatory procedures, and the persistent presence of criminal markets is motivated by their long-lasting profitability. In essence, organised crime is driven and shaped by profit; criminals and criminal networks organise their activities around profitable opportunities and economic incentives. The COVID-19 pandemic underlined again how profit opportunities spark and drive unexpected shifts in criminal associations and reveal criminals' organic capability to adapt to their external environment (Europol 2021b).

Criminal business relies on processes to perpetrate crimes but and the parallel support infrastructure designed to ensure the success of illicit operations. The entire criminal infrastructures are built to enable, support and conceal the core crimes, or to expand resulting criminal profits. Examples of parallel services include money laundering, transportation services, document fraud, resource pooling, fencing, distribution of illicit commodities or provision of customized digital solutions, are examples of parallel services sustaining and shielding criminals' pipelines for profit (Europol 2021b).

Exploiting the increased demand for goods and information

Given the profit-oriented nature of organised crime, opportunistic criminals and criminal networks have evidently exploited the pandemic-induced shortages in the consumer market. Since the outbreak of the pandemic, counterfeiters have engaged in the production and supply of personal protective equipment, counterfeit pharmaceuticals, sanitary products taking advantage of the persistently high demand and occurring shortage in the supply of these goods. Offers have appeared on the Darknet, but mostly on the surface web, as the latter has more potential to maximise criminals' reach. Online non-delivery scams have persisted during the crisis, ranging from selling non-existent personal protective equipment or pharmaceuticals allegedly treating COVID-19. COVID 19-related changes have driven an increase in demand for other goods too; criminals leveraged additional market opportunities as well, offering more counterfeit or illicit COVID-19 test kits, test certificates and vaccines as well as orchestrating related scams (Europol 2020e, p. 15; Europol, 2020h). Fraudulent offers and/or offers for counterfeit or sub-standard commodities will likely also extend to other test- or vaccination-related material such as PCR tests.

Criminals also exploited the introduction of COVID-19 certificates and vaccination passes. As demand for those has sharply risen given their mandatory use for travelling and accessing certain facilities in some countries, the production and distribution of fraudulent test

and vaccination certificates has similarly increased (Europol, 2020g).

Given that in today's global economy, information has become a key commodity, with the Internet at its epicentre (Lengel, 2009), it comes as no surprise that criminals turn information and the need for it similarly into profit. Pandemic-themed cyber criminality persisted throughout the pandemic, partially exploiting people's increased need for information and the widespread reliance on digital means during the lockdown.

Different cybercrime schemes have been adapted to the pandemic narrative, including phishing attacks, the distribution of malware and business e-mail compromise schemes (Europol, 2020a, p. 4). Most recently, cyber criminals have capitalised on current headlines and have been using the vaccination and unemployment/financial aid narrative to lure victims. Online fraudsters have continued to defraud victims by distributing COVID-19 related spam e-mails and hosting scam campaigns on bogus websites and by offering speculative investments related to COVID-19 (Europol, 2020a, p. 7). Recently, fraudsters have adapted their known schemes to the vaccination roll-out often posing as health authorities and targeting individuals with false vaccine offers.

Capitalising on the vaccination roll-out and the high demand for the newly manufactured vaccines against COVID-19, new large-scale fraud typologies emerged. In a new criminal trend, fraudulent offers of vaccine deliveries were made by so-called intermediaries to public authorities responsible for the procurement of vaccines. Several Member States were impacted by this scheme (Europol information).

Continued profit from illicit markets for exploitation

Although trafficking activity for sexual exploitation has dropped as the demand for services with direct contact has decreased, traffickers proved to be resourceful with the aim of maintaining profit. As offers of virtual sexual encounters have become increasingly popular among clients, traffickers have also intensified the digitisation of sexual exploitation, moving several of their illicit activities to the online sphere (Europol, 2020e). During the COVID-19 pandemic, a considerable share of trafficking of human beings for sexual exploitation has moved to the online domain as the crisis generally facilitated increased online presence, also opening new opportunities for recruitment of victims online (Europol, 2021).

The production and online supply of child sexual abuse material has remained a grave threat during the pandemic. It has been observed that the production and circulation of child sexual abuse material (CSAM) has generally increased during periods of lockdown, taking advantage of more time spent at home, both by the victims and the offenders.

Despite an initial set back of migrant smuggling activities in the beginning of the crisis, no significant disruption of migratory flows has been noted. The market for smuggling services remains sustained due to its profitability and presents a key threat to the EU with some alterations in smugglers' activities emerging during the pandemic (Europol, 2020e, p. 12). Much of the crime area has moved to the online domain. Virtually all phases of migrant smuggling - including recruitment campaigns run on social media, selling maps to irregular migrants and providing indications via instant communication platforms – have moved online (Europol, 2021b). Taking advantage of the circumstances, where an illicit journey may be perceived as more dangerous compared to pre-pandemic times, migrant smugglers turned it into a business opportunity and have increased the prices for their illicit services (Europol, 2020e, p. 12).

Maximising profit in times of crises

Criminal networks strived to maximise their profit during the crisis, underlying once again the profit-oriented nature of organised crime.

During the pandemic, there was an increase noted in national COVID-19 subsidy schemes reported in several Member States (Europol information). With the release of the EU funds allocated under the Recovery and Resilience Facility, it is likely that criminal groups will attempt to siphon off EU funds through fraudulent procurement procedures.

Orchestrated theft of vaccines – supposedly with the aim of reselling them on the black market - in the different stages of distribution chain during the transportation process, at the storage facility or at hospitals presents an additional significant threat (UNODC, 2020). Unsuccessful attempts of burglary in vaccination centres have already been reported (Europol information).

With regards to cybercrime, healthcare organisations and institutions in the public sector continued to be targeted by ransomware and distributed denial of service (DDoS) attacks (Europol, 2020b, p. 6). Entities involved in COVID-19 research, testing, vaccine development and administration both the private and the public sector, have become also victims of different forms of cyber-attacks. In these schemes, criminals targeted critical infrastructure during the crisis. Due to their crucial role in the fight against the pandemic, victim of such attacks were more prone to pay ransomware in order to regain control over their systems. Such attacks included phishing, ransomware and DDoS attacks as well as data breach (Politico, 2020; ZDNet 2020; ZDNet 2021).

Conclusion

Criminal networks strive in times of crises. The COVID-19 pandemic has once again demonstrated that criminal networks are resourceful and operate for financial gains. Just as legal business entities, these illicit enterprises and entrepreneurs respond to market forces, maximise profit and leverage criminal business opportunities. It is essential to further the research on criminal networks and bring together different stakeholders in order to prevent them emerging stronger in the post-COVID-19 reality.

References

- Arsovska, J. (2014) 'Organised Crime', *The Encyclopedia of Criminology and Criminal Justice,* doi: https://doi.org/10.1002/9781118517383.wbeccj463
- Europol (2020a) An assessment of the impact of the COVID-19 pandemic on serious and organised crime and terrorism in the EU. The Hague: Europol.
- Europol (2020b) Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU. The Hague: Europol.
- Europol (2020c) Catching the virus: cybercrime, disinformation and the COVID-19 pandemic. The Hague: Europol.
- Europol (2020d) Exploiting isolation: offenders and victims of online child sexual abuse during the COVID-19 pandemic. The Hague: Europol.
- Europol (2020e) How COVID-19 related crime infected Europe during 2020. The Hague: Europol.
- Europol (2020f) The challenges of countering human trafficking in the digital era. The Hague: Europol.
- Europol (2020g) The illicit sale of false negative COVID-19 test certificates. The Hague: Europol.
- Europol (2020h) Vaccine-related crime during the COVID-19 pandemic. The Hague: Europol.
- Europol (2020g) Viral marketing. Counterfeits, substandard goods and intellectual property crime in the COVID-19 pandemic. The Hague: Europol.
- Europol (2021a) Digitalisation of Migrant Smuggling. Intelligence Notification. [Europol Unclassified – Basic Protection Level]. The Hague: Europol.
- Europol (2021b) Serious and Organised Crime Threat Assessment. The Hague: Europol.
- Halstead, B. (1998) 'The Use of Models in the Analysis of Organized Crime and Development
- of Policy', *Transnational Organized Crime,* 4, pp. 1-24.
- Lengel, L. (2009) 'The information economy and the internet', *Journalism and Mass Communication* 2.
- Politico (2020) *Belgian coronavirus test lab hit by cyberattack.* Available at: https://www.politico.eu/article/belgian-coronavirus-test-lab-hit-by-cyberattack/
- Tusikov, N. (2010) The Godfather is Dead: A Hybrid Model of Organized Crime, In: G. Martinez-Zalace, S. Vargas Cervantes, & W. Straw (eds.) Aprehendiendo al Delincuente: Crimen y Medios en América Del Norte. Media at McGill, pp. 143-159.
- UNODC (2020) COVID-19 vaccines & corruption risks: preventing corruption in the manufacture, allocation and distribution of vaccines.
- ZDNet (2020) *Hackers have leaked the COVID-19 vaccine data they stole in a cyber attack.* Available at: https://www.zdnet.com/article/hackers-have-leaked-the-covid-19-vaccine-data-they-stole-in-a-cyberattack/
- ZDNet (2021) *Oxford University lab with COVID-19 research links targeted by hackers*. Available at: https://www.zdnet.com/article/oxford-university-biochemical-lab-involved-in-covid-19-research-targeted-by-hackers/#ftag=RSSbaffb68;