

PROSEGUR RESEARCH

Criminal technological innovation

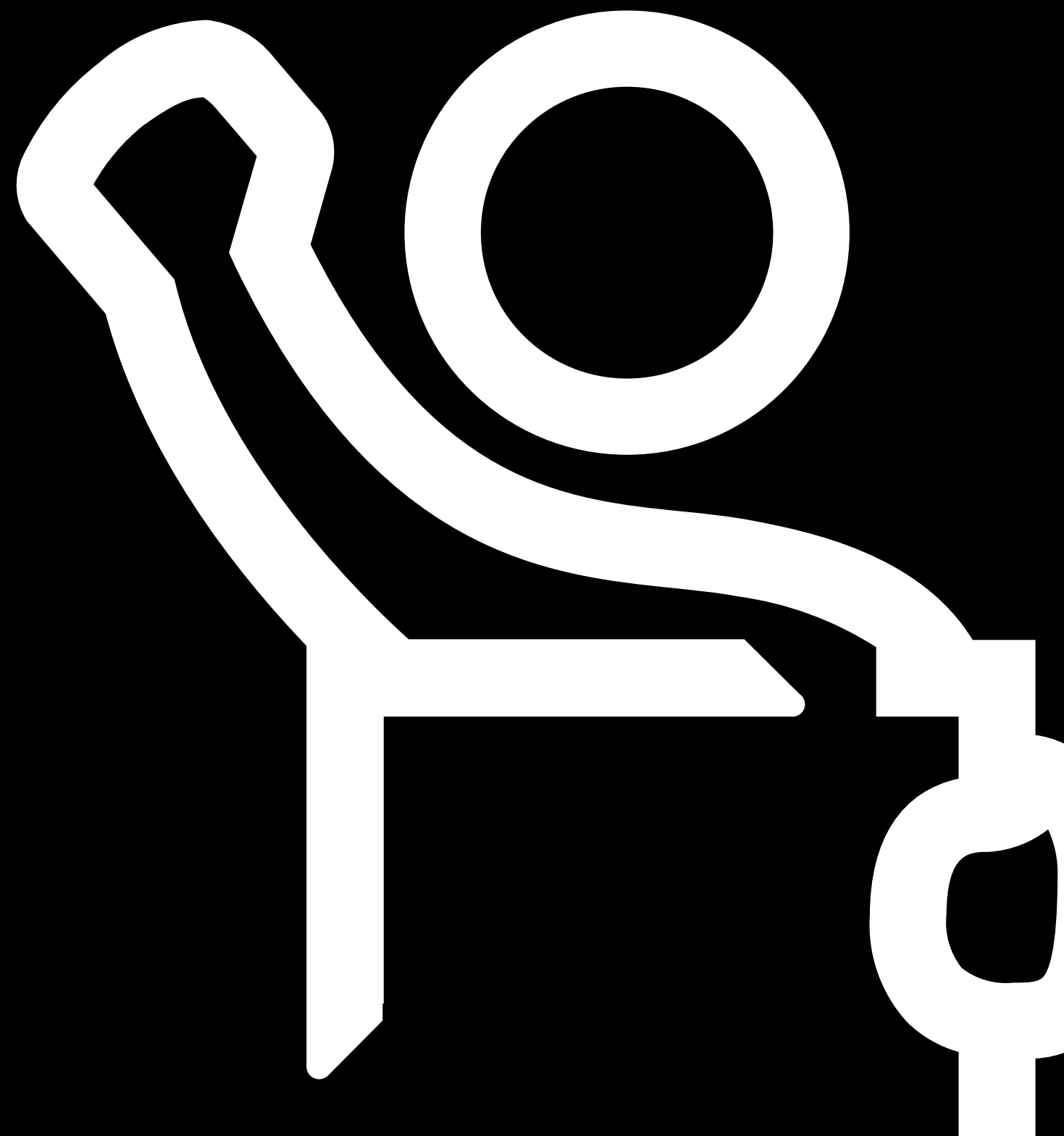
Index

This is an interactive document



01

Criminal
innovation





What is criminal innovation?

Creativity and imagination are inherent to human beings yet their usage for criminal purposes have not traditionally been studied in the world of criminology and security. In fact, The 9/11 Commission Report found that lack of imagination was partially responsible for the lack of prevention of the terrorist attack, whose materialization could be defined as radically different, disruptive and innovative.

Thus, it seems important to know how criminals innovate and to explore the formulas used so far. Innovation is defined as "the adoption of new patterns of behavior"¹; therefore, criminal innovation would be applicable when this behavior is criminal². Inspired by Lubrano³ (2021) we can define criminal innovation **as a process in which substantial components of pre-existing codes and norms, written or unwritten, that characterize the modus operandi of organizations or individuals for illegal purposes or means, are reformulated.**

This implies the consideration of innovation as a process and as a product. But creativity is not equivalent to innovation: while creativity is associated with the generation of new ideas or concepts, innovation implies the implementation of such ideas.

¹ Crenshaw (2010).

² An interesting concept is "malevolent creativity" o el "dark side of the creativity", as the creative effort to achieve goals by harming other individuals or groups.

³ Although this study is more focused on innovation in terrorist attacks, the framework we propose is applicable to any criminal actor.

Based on the formulas for change, we can identify different types of innovation.

Increasing innovation would be based on the need to overcome obstacles for committing crimes, such as beating security measures, or on the introduction of new developments that perfect or improve the original model. For example, drones used by criminal organizations for different purposes: they begin by being used as a means of surveillance of the authorities and later include explosives to scare off the police.

Radical innovation is a fundamental shift away from previous processes and products, such as the 9/11 terrorist attacks. It is short-lived because it is immediately imitated thus providing an incentive for incremental innovation. Radical innovation is, therefore, a driver of incremental innovation, which makes it possible to incorporate all those gray areas that exist in the conceptualization of innovation, especially when we talk about imitation, emulation or adaptation.

In his book, *The innovator's dilemma*, Christensen (1997) introduces the concept of **disruptive innovation**: one in which goods and services are provided that are less costly and more accessible, and eventually replace previous formats. It implies a total change compared to the previous situation in products, markets or sectors, such as the use of Artificial Intelligence to imitate the voice of executives during extortions of companies or the use of 3D printers to quickly generate keys.



What is criminal innovation?

Another interesting classification is that of **Crenshaw (2010)**, differentiates between tactical, operational and strategic innovation according to the scope of the change implemented.

- ▶ He considers **tactical innovation** to be that which focuses on adopting new technologies to address traditional objectives, while it would be strategic in nature when the aim is to address new objectives. It would therefore be defined as substantial changes in the execution of crimes that redefine patterns of behavior of an organization or individual. It focuses on the weapons and technologies used, objectives, time and location of the action and selection of crimes and targets.
- ▶ **Operational innovation**, called organizational by Crenshaw, refers to changes in the structures and institutions of an organization. It focuses on activities necessary to maintain operations: organizational structure, recruitment, financing, communication, propaganda, etc. Operational innovations can be the use of cryptocurrencies, encryption, the use of mobile communication applications or the DarkWeb.
- ▶ Finally, a **strategic innovation** is one that affects fundamental patterns of criminal challenges to political authorities, which implies either new objectives or a new way of developing their operations towards this objective.

⁴ As happened in December 2021 with log4j, a zero-day vulnerability of high severity.

⁵ Which generate fake audiovisual content thanks to Artificial Intelligence, until now practically impossible to differentiate from real content.

⁶ UEBA, User and Entity Behaviour Analytics, are tools for analyzing user behavior; also known as Insider Risk Management.

⁷ An automatic weapon that was more comfortable, faster and more accurate at close and medium range than other weapons on the market in the early 20th century, dubbed the Chicago Typewriter for its capacity of approximately 1,000 rounds per minute.

⁸ In the armament field, the use of innovative equipment by criminal organizations rather than by armies and police forces is widespread, given the process they must follow to get their governments to approve new weapons; as we have previously mentioned, not respecting the rules facilitates this type of anticipation.

⁹ Although these devices have existed since the 1990s, their use has increased in recent months, with between 30 and 40 being intercepted each year in Colombia alone.

Companies are not the sole innovators

We often highlight the best practices in terms of innovation implemented by companies and public bodies; the truth is that **criminals also innovate**, and possibly do it better.

There is an explanation for this: it is easier to design and implement innovations in a team on the fringes of the law, which systematically breaks all kinds of rules and takes risks beyond its capabilities. In addition to this **flexibility**, those on the other side of the law have more **time** to prepare their illegal initiatives and, sometimes even benefit from more **resources** if it is a highly profitable illegal business.

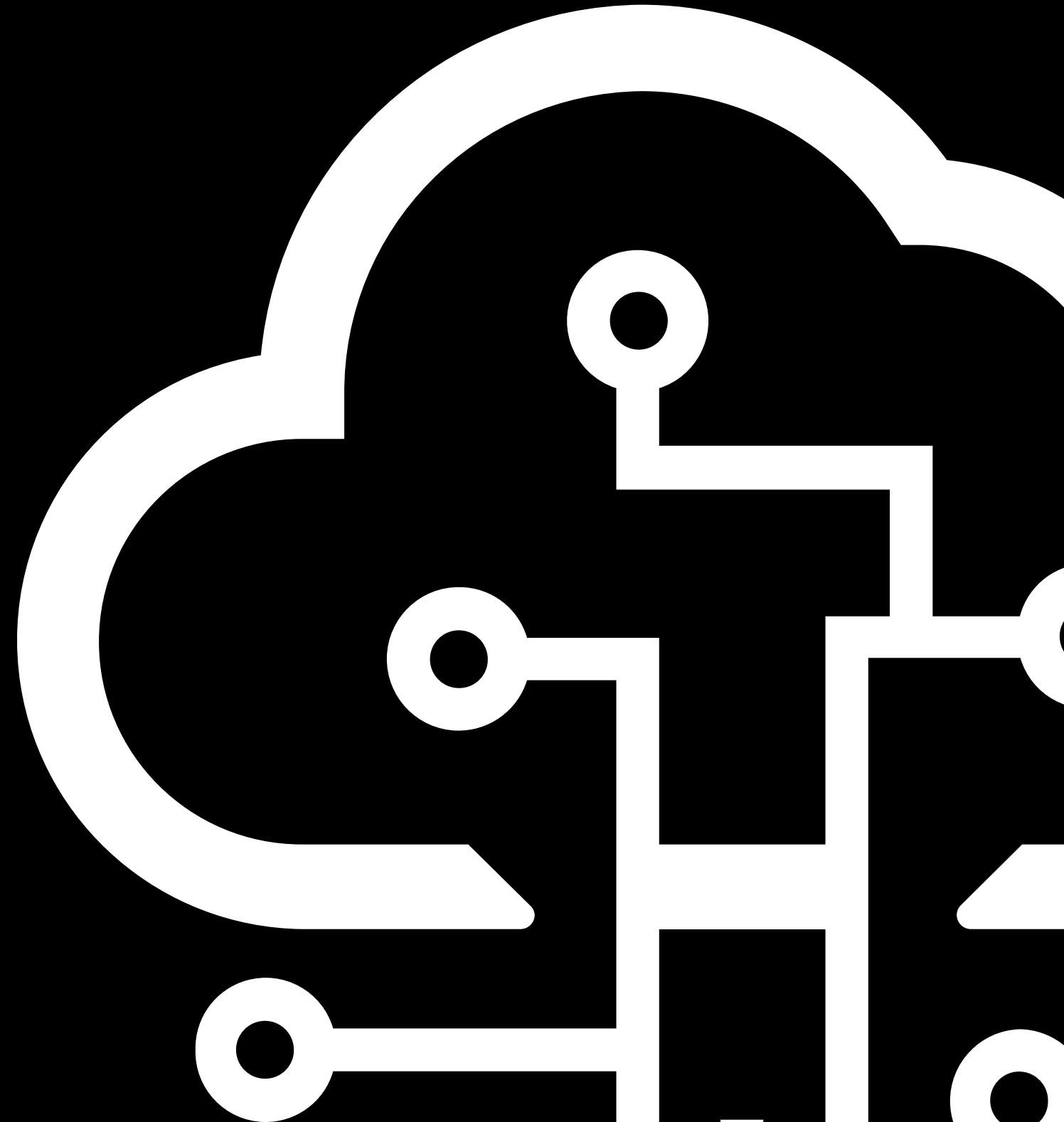
In this context, innovating without legal or ethical criteria allows criminals to exploit vulnerabilities and design deceptions to confuse both humans through social engineering via **phishing** and DeepFake⁵ technologies, and the tools themselves, acting stealthily by simulating human behavior to avoid UEBA⁶.

But criminal innovation is not unique to the current era; a good example of this was the **early use** of the Thompson⁷ submachine gun by the Mafia before the U.S. police in the Prohibition era⁸.

Criminal innovation is constant.

Even critical moments for societies are not an impediment for criminal groups, who know how to take advantage of opportunities to update their operations, guidelines and methods of action. COVID-19 is a good example of this: the restrictions on mobility and services led criminal organizations to look for new ways to continue their illicit activities. The use of narco-submarines to transport drugs from the Americas to Europe is just one example⁹.

02 Innovating from the dark side





How to innovate from the dark side?

We identify four dimensions from which we can analyze the main criminal innovations known today.

Taking advantage of technological advances

While technological progress has led to significant advances in civilization, it has also led to a significant expansion of the surface available for criminal activities¹⁰.

The key to their profitability lies in putting technological development and its widespread use at the service of criminals. Thus, we can state that cybercriminals are constantly innovating (*Europol, 2021*).

For example, since the first ATMs in the late 1960s, they have become an exponential part of our daily lives, becoming one of the main sources of attacks on financial institutions, both through **fraud** (user impersonation), often by skimming (card cloning), **logical attacks** such as jackpotting¹¹ through malware¹², and **physical attacks**, for example, by placing false mouths in the cash dispenser. These attacks continue to increase year after year, especially mobile Trojans, innovating for example with the use of 3D printers to replicate keys quickly at least for more than ten years, or the theft of tokens to circumvent MFA (Multiple Factors of Authentication).

¹⁰ Especially horizontal technologies, which are more widespread in terms of diffusion curve. This has happened largely thanks to the IoT (Internet of Things), the digitization of companies and the widespread use of the Internet, which represents a major opportunity for illicit enrichment through all kinds of cyber-attacks.

¹¹ This technique makes it possible to achieve up to 40 banknotes every 23 seconds.

¹² Especially mobile Trojans (Europol, 2021).





Undoubtedly, **Crime-as-a-Service**¹³ as an environment for the exchange of cybercriminal services has generated an authentic ecosystem of highly profitable innovation: from Malware-as-a-Service¹⁴ now very focused on mobile devices to Ransomware-as-a-Service¹⁵ aimed at reducing time-to-ransom for industrial espionage and data theft are examples of this¹⁶. Within this **ecosystem of criminal activities**, one way that has been found profitable for these groups is the 'outsourcing' of services to other organizations to carry out different activities, such as cocaine production in Latin American laboratories, with the aim of being more agile and efficient, as well as being able to save on production and logistics tasks and isolate the central nodes of organized gangs.

They also know how to take advantage of cryptography as a self-protection¹⁷ formula, anonymizing their identity when committing illegal activities on the Internet, for example, by surfing the **deepweb** and the **darkweb** or the lucrative abuse of the privacy offered by **cryptoassets** for money laundering, scams and extortion. In this sense, the use of **drones to monitor** police or vigilantes is known, as MS13 members did in Honduras in 2020, or drones with explosives to scare off the police as the CCJNG did in Mexico this same year. Occasionally octocopters have allowed organized crime to smuggle contraband (drugs, phones and even blades) into high security prisons **high security prisons**.

Somewhat simpler and more efficient is the use of **vehicles as weapons** in recent years. Current security protocols are vulnerable to the usage of official vehicles, such as **ambulances**, and take advantage of the free access they have to almost all restricted spaces and the trust they inspire among the population and members of law enforcement agencies since they are part of the emergency services¹⁸.

We have also seen the use of **semiconductor technology for industrial espionage** through reverse engineering in order to illegally obtain all kinds of information, especially with the intention of infringing intellectual property rights.



¹³ By its acronym CaaS, it implies the existence of a real cybercrime industry.

¹⁴ MaaS enables the purchase of malware services.

¹⁵ RaaS offers illegitimate Ransomware programs to extort money from individuals and companies.

¹⁶ They are constantly renewing themselves, maximizing profits and minimizing risks, customizing the services offered as much as possible: if they want to attack a specific person, they are designed ad hoc with the latest technology.

¹⁷ As the latest Europol reports indicates. Encrypted applications and devices seem to have become the main form of communication, due to the guarantees they offer against detection.

¹⁸ The fact is that, since 2001, a total of 19 cases have been identified in which an **ambulance was used as a VBIED** ambulance was used as a VBIED in terrorist attacks: 14 in the Middle East and the remaining 5 in Southeast Asia.



Boosting organized crime markets

Technology offers a wide range of ways to improve the exchange of goods and services; something that, logically, organized crime is taking advantage of in the increasingly lucrative black market.

Improvements in production, such as the refinement of **cultivation techniques** that reduce the surface area of cocaine plantations while increasing production, the use of larger **mobile laboratories** with better conversion mechanisms, as well as the production by the groups of their **own precursors** such as potassium permanganate, are examples of the criminal groups' constant attempts to optimize their processes, resources, and services.

The sophistication in **self-protection** such as is the usage of drones to move drugs across borders¹⁹ or prisons or the design of narco-drones and narco-submarines²⁰ for transatlantic travel. To improve trafficking, drugs are also transported in **concrete blocks, liquid** or **cream** cocaine, and sold on the Internet through **cryptomarkets**²¹, especially on the darkweb and deepweb.

These formulas allow criminal organizations to **increase efficiency and maximize their profits** while taking less risk by reducing their visibility and the traceability of their activities. Other illegal markets²² have also benefited from these technological innovations for self-protection, such as the arms market, with the establishment of arms **manufacturing workshops using 3D printers**.

¹⁹ Such as between US and Mexico in 2014.

²⁰ As identified in Spain with cargo from Brazil in 2021.

²¹ Platforms that, of course, are in full growth, as there is a great imbalance between the time it takes to locate and close a platform of these characteristics and the time it takes to create a new one, which is undoubtedly an advantage for criminal gangs.

²² Also, for example, of human trafficking and child sexual abuse material.





Optimizing terrorist attacks

Terrorism's pledge towards innovation and exploring new ways of perpetrating attacks, such as the use of vehicles, VBIEDs and even formulas for coordination with technological means, has broken with the tactics of classic terrorism. Moreover, until the emergence of DAESH, traditional terrorist activity on Western²³

soil mainly involved the use of explosive charges (both remotely²⁴ triggered and detonated by suicide²⁵ operatives). Three innovative formulas therefore stand out:

A

The use of conventional vehicles as weapons to attack large groups of civilians

Despite the fact that the use of conventional vehicles as a weapon had already been put into practice on some occasions prior to 2016²⁶, and although the possibility of these attacks has been contemplated for decades, for example, by **reports** collected by the U.S. Department of Justice, DAESH's innovation in focusing its offensive on this modus operandi, taking advantage of its simplicity, low cost, high impact and high difficulty of detection²⁷, has led to security forces being surprised by the magnitude and unpredictability of the attacks, with serious consequences for the population²⁸.

In this same innovative line, the assault on Mosul by DAESH in 2014 (weeks before the proclamation of the Caliphate), was based on the coordinated use of several **suicide VBIEDs**²⁹ equipped with **rudimentary** armor, which were detonated against the city's defenses at **different points simultaneously**. These devices had a great effect on the defenders, who overestimated DAESH forces and resources, and ordered a retreat, leaving the city at the mercy of DAESH's forces which led to the beginning of 3 years of local rule by the group³⁰.

²³ With the expansion of the insurgency in Syria and Iraq - especially since the beginning of the loss of control over the territory in 2015 - and based on the lessons learned on the battlefield, the DAESH terrorist group compensated for its offensive limitations and its loss of war material by adopting an innovative posture that implied, since 2016, a change in the modus operandi of the group and a modification of the tactics used by its followers both to attack Europe and the United States, and to maintain its insurgent activity in its areas of influence.

²⁴ As it occurred with the first attack on the World Trade Center in 1993, or in the case of some of the explosives detonated in the attack of tourist facilities in Bali (Indonesia) in 2002.

²⁵ As in the case of the 11-M attacks in Madrid in 2004, attributed to an Al-Qaeda suicide commando.

²⁶ For example, in the attacks carried out on December 21st and 23rd 2014 in the French towns of Dijon and Nantes, respectively, which resulted in no fatalities.

²⁷ In the case of other types of attacks, such as those perpetrated with firearms or homemade explosives, both the weapons and the explosives precursors may be subject to tracking, given that they are not conventional items.

²⁸ For example, the attacks in Nice (2016), Berlin (2016), London (Westminster in March and London Bridge in June 2017), Stockholm (2017), Levallois (2017), Barcelona (2017) and Murcia (2021) were perpetrated using vehicles.

²⁹ Vehicles equipped with improvised explosive devices.

³⁰ The experience derived from the use of these means on the battlefield has tried to be exported unsuccessfully to Europe, at least in the following cases: i) Barcelona, 2017: as indicated by police investigations carried after the attack on the Ramblas in Barcelona revealed that the explosion of a detached house in the town of Alcanar in the hours prior to the attack took place while a jihadist commando was manufacturing homemade explosives with the intention of introducing them in a van with which, first, to run over civilians and, then, to carry out a detonation in the vicinity of the Sagrada Família. ii) Paris, 2017: a jihadist rammed a Gendarmerie van with a car loaded with explosives, but the planned deflagration did not occur and the only fatality was the assailant.



B

Use of drones to carry explosives and carry out attacks or assaults

During the last few years, there has been an increase in the **use of homemade drones modified to carry improvised explosives**, hand grenades, 40mm grenades and small mortar shells during several **insurgencies active** in the wars in Syria, Ukraine, Libya, Iraq or Yemen and also present in countries such as Mexico or Colombia, among others.

The first record of the use of domestic or homemade drones **use of domestic or homemade drones** for the commission of attacks dates back to 2014³¹. Since then, other incidents have been recorded, such as the attack by a **swarm of homemade explosive drones** against a Russian base in Syria in January 2018; the **attack** by Houthi rebels³² against the Yemeni army

headquarters in January 2019 and the **drone attacks** during in the context of the conflict between the Jalisco Cartel New Generation (CJNG), the **United Cartels** (Familia Michoacana, the Knights Templar and the Viagras) in January 2022, or the **DAESH** operations in Syria and Iraq.

While drone innovation has been decades in the making, the adoption of the concept of "*drone warfare*" and its adaptation to the constraints of criminal and insurgent groups is an innovative approach that has resulted in an enormous security challenge. This is due, in part, to the fact that most air defense systems³³ are designed to confront threats of a very advanced military engineering level (such as rockets, missiles, fighter planes or state-of-the-art drones) and are not suitable, or optimal, for the interception of **small homemade drones**. In addition, the cost of shooting down each drone is sometimes infinitely higher than the cost of the device itself³⁴.

C

Innovation to improve coordination

The terrorist actions that took place in the city of Bombay in November 2008 incorporated an **innovate modus operandi** with respect to the modalities used by radical Islamic groups such as Al Qaeda and its derivatives in previous attacks.

The innovation registered in the extreme coordination in the concatenation of the **actions**, their **magnitude and intensity** made the work of the security forces difficult and guaranteed the impact of the previously planned actions.

The attacks, allegedly planned from Canada and Pakistan, included shootings in infrastructures with a large influx of civilians, specifically selected due to the difficulties of control by the authorities, as well as in emblematic establishments in the city of Bombay. The terrorists also used GPS for targeting and

resorted to BlackBerry devices and satellite phones to ensure coordination of their actions and to guarantee that the previously studied plan was carried out in a **comprehensive** manner.

³¹ When Hezbollah guerrillas (Shiite militant group based in Lebanon) managed to carry out a successful terrorist action against an Al Qaeda building on the Lebanese-Syrian border.

³² The Houthis employ drones of greater sophistication, which cannot be considered homemade, including: Samad-1 (3.5 m wingspan, 500 km range, surveillance), Samad-2 (UAV-X, 4.5 m wingspan, 500 km+ range, surveillance or payload) and Samad-3 (4.5 m wingspan, 1500 km range, payload).

³³ As in the case of the Phalanx C-RAM or the S-300/400.

³⁴ As an example, it is noted that the cost of a Patriot missile (surface-to-air) ranges from 1 to 6 million dollars, while a modified homemade drone can range from 100 to 3,000 dollars. Despite this low cost, a homemade drone has the potential to cause significant property damage, loss of life and psychological impact. Along these lines, laser devices capable of detecting and destroying devices with a surface area of up to 0.002 m² have appeared in recent years.





Hacking the mind

Social engineering, an innovation that increases annually, is highly profitable. The fact is that **human error is the source of 95%** of security breaches today making it an enormously valuable attack vector.

Phishing scams include sophisticated methods such as the use of **chatbots** pretending to be real users or **deepfake**, even **artificially generating faces** that are more reliable than human ones.

A good example of criminal innovation was the imitation of the voice **of the CEO** of an energy company using Artificial³⁵ Intelligence to extort money from a supplier in 2019, a technique known as **vishing**³⁶.

Many innovations in scams take advantage of the seasonality of campaigns in which people let their guard down: at the tax return deadline with a fake email from the Spanish Tax Agency³⁷, on Valentine's Day pretending to be a user of a dating website³⁸, etc.

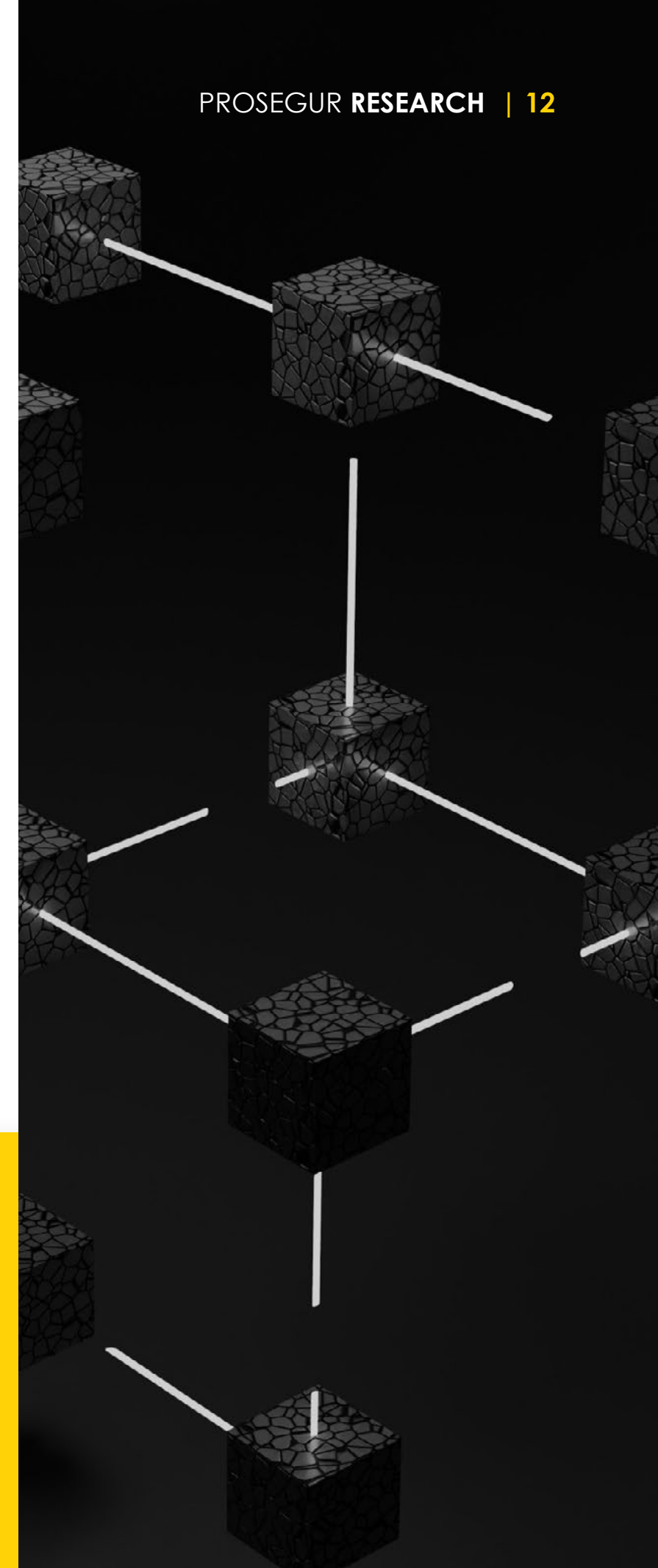
The use of **social networks** and the most popular **video games** of the moment are also powerful recruitment channels for **terrorism** and **organized crime**, under the promise of living authentic adventures or for the **trafficking and exploitation** trafficking and exploitation of people through sextortion or falsely offering a job or a stable love relationship.

³⁵ This scam is carried out through algorithms that work with RGAs (antagonistic generative networks) that analyze voice recordings and allow new phrases to be generated from them.

³⁶ A voice message phishing scam.

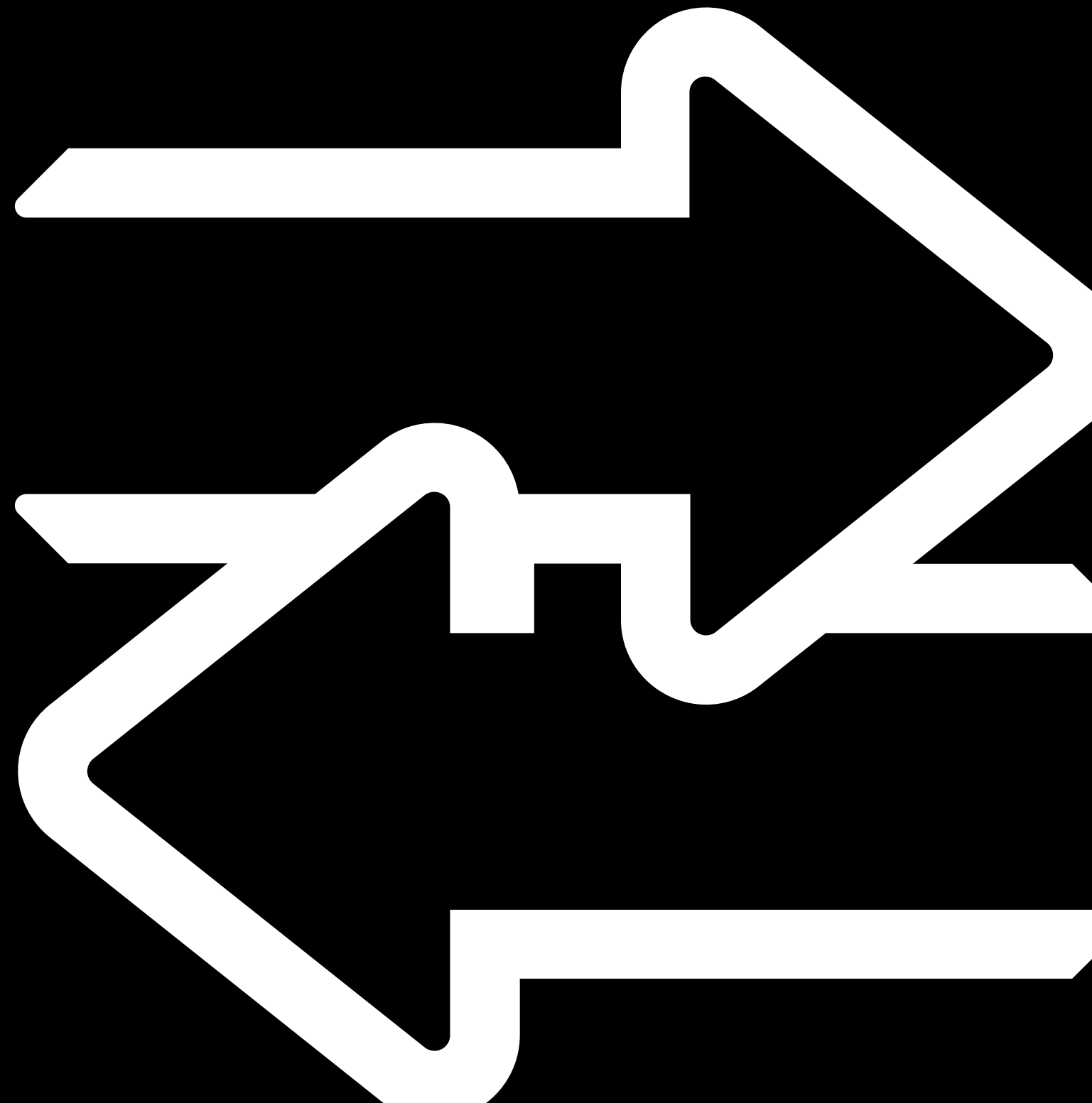
³⁷ Or any similar tax agency.

³⁸ Like popular TV series whose themes attract victims to cyberattacks and scams.



03

What's next?





What's coming now?

We may know only a small fraction of all the criminal innovations currently underway, and this limits us our capability to identify trends on the dark side. However, we can point to some possible lines of criminal innovation with great potential.

We will see more and more alliances between criminal organizations, terrorists and **cybercriminals**, who will capitalize on advances in terms of innovation by sharing products and ideas.

Everything-as-a-Service markets will continue to grow with major criminal innovations for supply chain attacks, the cloud, massive IoT (MIoT), currently undergoing expansion.

The expansive development of Artificial Intelligence and robotics will make it possible to manufacture better weapons and criminal robots or soldiers, that is autonomous weapons and even criminal nanorobots³⁹.

In turn, this global technological development represents a mighty environment in which new cyberattacks are designed against people who increasingly interact with the digital setting and companies in the process of digitization.

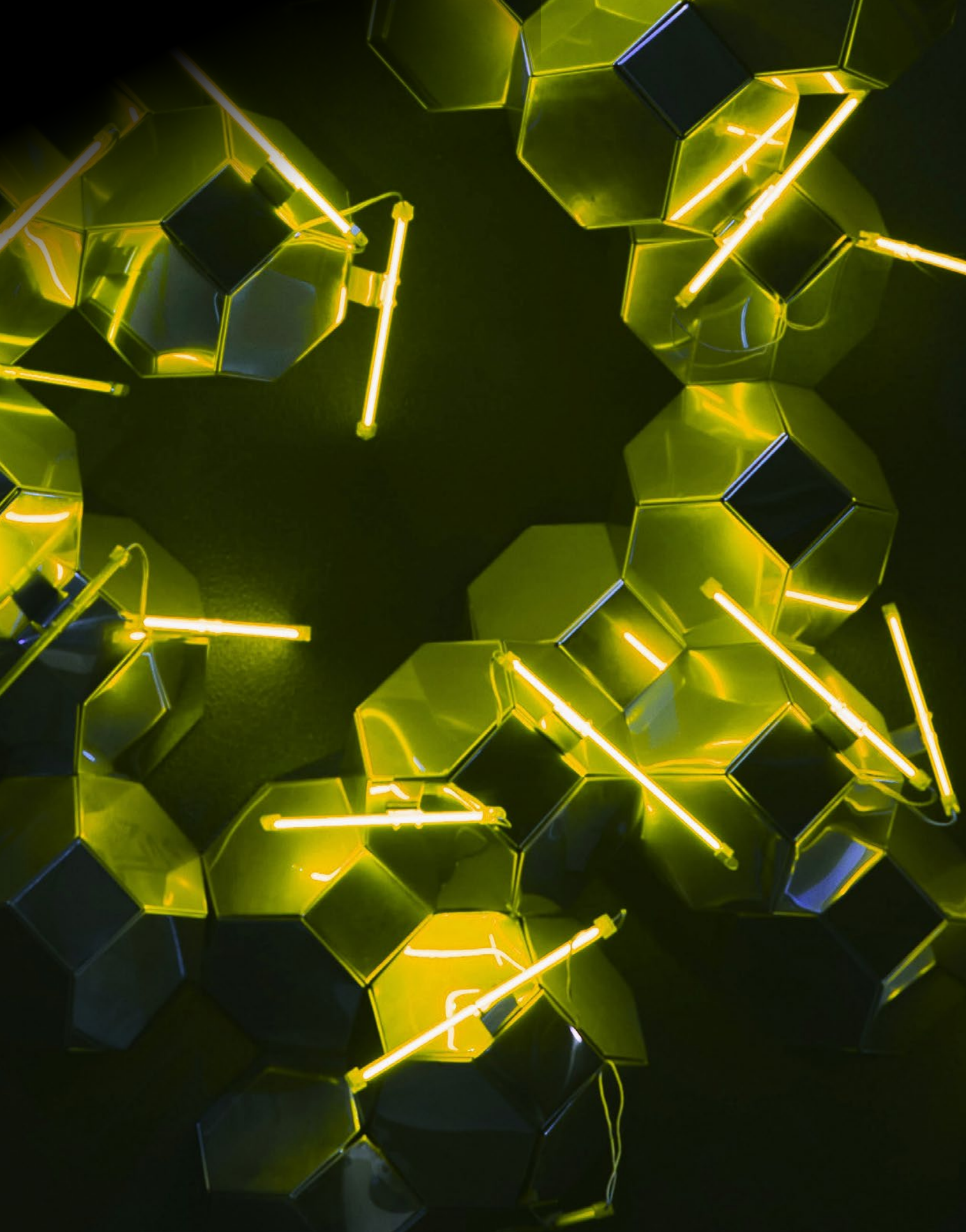
Among the possible uses of drones, in addition to physical attacks consisting of crashing drones into people or property, are logical attacks⁴⁰ through access points.

The detection of possible vulnerabilities in open-source components, used for example in autonomous vehicles, can lead to cyberattacks that generate significant physical damage and harm to the integrity of people.

³⁹ Very small machines in the service of criminal or terrorist organizations as long as they improve the price, accessibility and specialization needs of their technology.

⁴⁰ Setting up a fake mobile Wi-Fi network or a rogue access point in order to intercept network traffic from smartphones in range to capture sensitive information from users or take control of their devices, be they cell phones, computers, cars, etc.





4D technology or Next Generation Bioprinting (NGB) which achieves more flexible objects whose structures can be programmatically transformed in response to a stimulus, currently applied to the bioprinting of living tissues but has also potential in the field of production of drugs.

Advances in areas such as quantum computing or eHealth will enable a major leap forward in terms of criminal innovation. For example, in the first case, reaching processing capabilities that challenge the cryptographic protection tools used to date; in the second, gene editing techniques, hitherto known to be used in healthcare, can be used to improve drug design or even **bioterrorism**.

The development of the metaverse has been postulated as one of the major attack vectors for cybercriminals in the future of the Internet⁴². The user could experience an enormous diversity of risks or attacks⁴³, such as identity theft, theft of personal information (biometric or navigation data, for example), extortion, fraud or harassment. For all these reasons, the metaverse, and the digital environment in general, has become a new playground for criminal innovation.

Criminal innovation, which is closely linked to the ability to creatively take advantage of technological developments, will continue to be oriented towards high-return, low-risk investments. In this sense, trends will be marked by the accessibility of technologies that, while they represent positive improvements for humanity, they also bring creative business opportunities for criminals.

⁴¹ Specifically, the CRISPR technique that changes a specific gene sequence.

⁴² As an immersive virtual universe, the metaverse is based on virtual socialization, with the aim of interacting with other users, represented by avatars.

⁴³ A hypothetical economy based on NFTs (non-fungible tokens), which is based on blockchain technology, could give rise to attacks such as ransomware or other types of crimes related to money laundering, especially when data protection and intellectual property would not be clearly defined.



We guarantee the safety of people,
businesses, and society as a whole.