EUROPOL

The Unmanned Future(s)

The impact of robotics and unmanned systems on law enforcement

An Observatory Report from the Europol Innovation Lab

THE UNMANNED FUTURE(S)
THE IMPACT OF ROBOTICS AND UNMANNED SYSTEMS ON LAW ENFORCEMENT
An Observatory Report of the Europol Innovation Lab

PDF | ISBN 978-92-9414-064-7 | ISSN 2600-5182 | DOI: 10.2813/0022284 | QL-01-25-023-EN-N

Luxembourg: Publications Office of the European Union, 2025

Cite this publication: Europol (2025), The Unmanned Future(s), The impact of robotics and unmanned systems on law enforcement, Europol Innovation Lab observatory report, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.
www.europol.europa.eu

Contents

Glossary

UNMANNED SYSTEM: A device or machine that can perform physical actions without a human operator physically present.

AUTONOMOUS SYSTEM: A device or machine that can make its own decisions about performing physical or digital actions, including communication, without the assistance or interaction of a human operator.

ROBOT: A programmable machine capable of carrying out a series of actions automatically, often with a degree of autonomy.

ROBOTICS: The branch of engineering and science that deals with the design, construction, operation, and use of robots.

DOMAIN: A space or environment in which an unmanned system can operate in, such as space, air, land, the water surface or underwater. This also includes the digital domain and information domains.

UAS/UAV: Unmanned aerial system/vehicle. Unmanned system that operates in the air, most often with fixed wings or rotor blades.

UGS/UGV: Unmanned ground system/vehicle. Unmanned system that operates on the ground, most often with wheels, tracks or legs.

USS/USV: Unmanned surface system/vehicle. Unmanned system that operates on the water surface.

UUS/UUV: Unmanned underwater system/vehicle. Unmanned system that operates under the water surface.

DRONE: In this report, a smaller UAS, typically equipped with rotor blades.

DIGITAL TRANSFORMATION: The process of integrating digital technologies across all areas of a business, organisation, or society, fundamentally changing how it operates and delivers value.

PHYGITAL: The merging of physical and digital.

LIDAR: Light Detection and Ranging. A remote sensing technology that uses laser pulses to measure precise distances and create 3D models of an environment.

IOT: Internet of Things. A network of physical objects embedded with sensors, software, and connectivity, enabling them to collect and exchange data over the internet.

HAPS: High-altitude platform station, which can also mean high-altitude pseudo-satellite or high-altitude platform systems, also known as atmospheric satellite, is a long endurance, high altitude aircraft able to offer observation or communication services similarly to artificial satellites.

Executive summary

How might criminals or terrorists use drones and robots in three years from now? How might law enforcement police the air? And can or should the police develop their own RoboCop?

Unmanned systems are already widely used in various industries, including manufacturing, logistics, healthcare, agriculture, and more recently in warfare. Law enforcement agencies (LEAs) are increasingly adopting unmanned systems to enhance situational awareness, improve safety, and improve operational reach. However, the use of unmanned systems also raises concerns about safety and privacy, including issues related to technical limitations, data protection, regulatory challenges, and the need to ensure public trust.

Some of these concerns also relate to various security threats, such as the potential for unmanned systems to be exploited by malicious actors[1]. Over the past years, tactics and equipment used in warfare have spilled over into organised crime and terrorism, impacting law enforcement. There has also been a reported increase in the use of drones around European infrastructure, and there are examples of drone pilots selling their services online, transforming this criminal process from crime-as-a-service to crime-at-a-distance.

As unmanned systems become more and more integrated into everyday life, we have observed four converging trends, which will require LEAs to develop new strategies for policing and regulating these systems:

1. Unmanned systems are operating over increasingly vast distances.
2. Unmanned systems are acting with growing autonomy and coordination.
3. Unmanned systems are becoming progressively more capable.
4. Unmanned systems increase rapidly in number and variety.

With the advances in technology and increasing uptake in society, the future operational landscape for law enforcement will need to evolve to be able to monitor and act in all domains, from underwater to above ground, and develop ways to interact with new types of unmanned systems.

Robots and drones bring the digital world to the physical world, requiring adaptation to deal with automated crime and crime conducted in the public by actors out of physical reach for law enforcement.

With Artificial intelligence (AI), there is a before and an after to unmanned systems capabilities. **Experts expect physical, analytical and generative AI to drive the next wave of robotics, creating a "ChatGPT moment" for physical AI**[2]. There are already robots that charge themselves or change their own battery when needed and collaborate with others to solve complex, goal oriented, missions.

In order to prepare for the future operating environment, a number of concrete steps can, and should, be taken. These range from the development of a strategic intent, a clear will, and updating of tactical, operational and security paradigms regarding unmanned systems. European law enforcement would also benefit from coming together in testing and evaluating unmanned systems for policing and law enforcement use and countering of such systems in realistic settings. However, for this to happen, a regulatory framework must be established with clear guidelines that support law enforcement innovation and testing, alongside investments in training and education for personnel.

Additionally, the development of partnerships with European industry and academia will be crucial to leverage key technologies with citizen trust and stay ahead of emerging threats. Establishing and connecting competence hubs on national and European levels will further ensure that European law enforcement personnel have timely access to the necessary knowledge and skills to effectively use and police unmanned systems.

This foresight report provides an outlook on these ***unmanned futures*** and aims to raise awareness on the opportunities and threats that the technological progress in this field is expected to bring. Furthermore, the report aims to provide a robust and informed foundation for LEAs to make proactive decisions that shape the future.

Key insights

Changing needs, behaviours and services

As unmanned systems become more common, societies will have to adapt how they interact and adapt to this technology. This could have negative consequences, especially as these systems collect more detailed and personal information due to their growing presence in in our private lives.

From situational to systemic

Challenges and benefits from unmanned systems will change as their deployment paradigm changes from situational (deployed and operated when needed) to systemic (becoming a standard part of operating procedure). This change will be similar to how the use and impact of smartphones has changed over the years.

Fuelling of national security concerns

Recent conflicts have acted as drivers for innovation, accelerating the development and testing of novel unmanned systems, with both the technology and associated knowledge spreading quickly. National security concerns may also prevent law enforcement access to key technology.

Digital becomes physical – technology convergence

Unmanned systems operate using digital data but within the physical world. As several maturing technologies (such as AI, robotics, and high-speed data connectivity) converge, new capabilities emerge. By extending society's digital transformation into the physical realm, crimes can be committed remotely and on a larger scale, raising more complex issues of attribution and accountability.

From 2D to 3D policing

In our future societies, logistics and services will be available in the low altitude airspace. The operational environment for future law enforcement will expand in volume, going from a traditional two-dimensional responsibility to a three-dimensional, where crime can be committed in or from the air and law enforcement operations can be challenged from above. This will challenge traditional operational and tactical doctrine in law enforcement as well as security protocols.

From devices to collective

Law enforcement need to create a collaborative and interoperable team of various unmanned systems, capable of understanding missions and working together with humans. This would expand operational reach, combine different capabilities and enhance traditional law enforcement operations in new and effective ways.

Introduction

Throughout history, humans have dreamed about unmanned systems taking on tasks that are "dirty, dull, and dangerous". This dream has never been closer to becoming a reality, with delivery drones, self-driving vehicles, and home automation appliances playing a growing role in society. Today, unmanned systems have become more sophisticated, widespread and accessible than ever before. As such, these systems are being applied to automate production processes to improve efficiency[3] in a wide range of industries, including manufacturing, warehousing, agriculture, healthcare, and logistics. Additionally, developments in materials in recent years have made it possible to develop robots that challenge our imagination. In the field of self-driving transportation, Waymo is now planning to introduce its "Robotaxi" in London, its first European destination after Tokyo and several US cities[4]. The convergence of robotics with key technologies, particularly AI, has driven rapid progress in the development of unmanned systems, enhancing components such as sensing, reasoning, learning, decision-making, planning and autonomy.

As unmanned systems become more advanced and autonomous, they are being introduced into the complex and unpredictable environment of everyday society. This has already led to some disruptive incidents such as birds attacking police drones[5], a chess-playing robot breaking its opponent's finger[6], and a law enforcement officer pulling over a car only to realise it is self-driving[7]. A key challenge includes ensuring the safe coexistence of robots with humans and animals, and guaranteeing reliability, usability, and safety. Law enforcement agencies, tasked with providing security and protecting citizens, must navigate this key challenge while also addressing the need for calibrated regulation, responsibilities, and capabilities.

2022 may well have been the turning point for organised crime to have used unmanned systems in all domains[8] and in 2024 the first ever all-robot assault took place in Ukraine[9]. The rise of unmanned systems will require LEAs to adapt to a rapidly changing operational reality. The digital transformation of society, driven by the internet and the subsequent digitalisation of products and services, has already led to the emergence and expansion of cybercrime and the development of policing capabilities in the cyber realm. The advent of robotics is now extending this digital transformation into the physical space, where mechanical entities interpreting digital data will interact with humans and animals. As a result, LEAs will have to develop new capabilities to address the unique challenges and opportunities presented by unmanned systems.

The exploitation of unmanned systems by criminal and terrorist networks presents a growing problem. A terrorism sentence in 2022[10] and recent plots in Europe indicate an ambition to use drones[11]. Criminals are increasingly using drones to smuggle illicit goods[12], monitor drugs labs, and even to attack the police[13]. These developments are concerning, highlighting the potential threats and vulnerabilities that law enforcement must be prepared to counter.

In response, we need to consider the broader context of unmanned systems development. The military's use of unmanned systems, for example, provides valuable insights into advanced technologies and operational strategies that can be adapted for public safety and crisis management. Additionally, understanding military applications can help law enforcement anticipate potential threats and develop effective countermeasures, as adversaries may adopt similar tactics and technologies. However, as most unmanned systems' development is focused on either purely civilian or military applications, we identify **a critical gap in the development of law enforcement specific capabilities**, especially at a systemic, interoperable level.

What does the emergence of criminal unmanned systems mean for law enforcement and how can resulting challenges be addressed? This report explores the impact of increasingly capable unmanned systems on the current and future operating environment for law enforcement in Europe. It does not detail specific unmanned systems, but rather focuses on the wider implications of having these systems integrated in our world and lives.

To broaden the foundation of this report, a diverse range of expert stakeholders were consulted, all of which are to some extent involved with, or impacted by, the developments in the fields of robotics and unmanned systems. These stakeholders included representatives of the various law enforcement communities in Member States as well as technical subject matter experts. Their input has significantly improved the comprehensive understanding of the challenges posed and the advantages offered by unmanned systems.

Current law enforcement use

While the actual uptake of unmanned systems in law enforcement as a whole is to date still somewhat limited, the use of drones, robots, and other autonomous technologies, is increasing and beginning to have a significant impact. Initially, law enforcement pilots used small and relatively simple drones for tactical surveillance and during rescue missions. Early ground robots were primarily used for high-risk deployments such as entering collapsed buildings to assess structural integrity and to search for victims, or to investigate suspicious packages. The state of the art has advanced significantly though, with commercially available drones being able to hover in place to hold a position, follow waypoints reliably and even to shadow an operator autonomously. Ground robots have also evolved, shifting from wheeled or tracked vehicles to legged robots, effectively branching out from *driving* into *walking*. Going forward, unmanned systems will also increasingly be able to operate in more than one domain, such as to combine flying, walking, driving or diving.

Figure 1: Different types of ground-based police robots employed by the Police North-Rhine Westphalia. Photo courtesy of the Landesamt für Zentrale Polizeiliche Dienste.

Surveillance and reconnaissance

Unmanned systems can be utilised to monitor and track suspects, vehicles, or objects, providing valuable real-time intelligence to support investigations and operations, and do so overtly or covertly. For instance, the real-time video transmission capability of unmanned systems can be used to support tactical operations and decision making, such as in SWAT team deployments, high-risk warrant services, hostage situations or in (potentially) hazardous areas. By providing a live video feed of the scene, unmanned systems can help tactical teams to gather intelligence, identify potential dangers, and develop a more effective plan of action. This can help to reduce the risk of injury or harm to officers, victims and witnesses, while also enhancing the overall safety and effectiveness of law enforcement operations.

Figure 2: A police drone. Photo courtesy of the Swedish Police Authority.

Furthermore, unmanned systems are used to monitor crowds and detect potential security threats, to enhance public safety and prevent potential incidents. The bird's eye view provides a valuable addition to on-the-ground monitoring systems and more expensive and scarce helicopters. Increasingly, advanced unmanned systems have begun to integrate automatic object detection and tracking capabilities, allowing for the more efficient identification and tracking, thereby providing valuable intelligence for surveillance and monitoring operations.

Occasionally, unmanned systems are used for waterborne surveillance by specialised teams, where they can be deployed to conduct operations in coastal areas, ports, or waterways. This provides law enforcement agencies new ways to monitor and respond to potential security threats from these environments.

Crime scene mapping and forensics

Unmanned systems can gather and analyse critical information for investigations, such as high-quality videos and still images. With additional sensors such as LiDAR[14], a crime scene can be mapped in 3D. This can be particularly useful in a range of scenarios from crime scene analysis to accident reconstruction.

By deploying unmanned systems equipped with high-resolution cameras, law enforcement agencies can gather detailed and accurate visual evidence, which can be used to support investigations, to identify suspects, and reconstruct crimes. UAS, for instance, can be used to capture overhead images of crime scenes, providing a bird's eye view of the area and helping investigators to identify potential evidence and piece together the events surrounding a crime.

This deployment of drones has the additional benefit of working faster than human officers on their own could, thus enabling a faster release of the scene. For example, in the case of car crashes, since this helps to minimise congestion and ensures that law enforcement staff are not occupied for extended periods.

Search and rescue

Unmanned systems are increasingly being used in search and rescue operations to help locate missing persons or survivors. By leveraging unmanned systems, search and rescue teams can rapidly survey affected areas, identify potential locations of missing individuals, and provide critical assistance in a timely manner. New developments, such as the ability to deploy larger platforms to uphold satellite communications and control, even in the absence of terrestrial infrastructure, will enable law enforcement to increasingly deploy unmanned systems for search and rescue purposes, even in extreme conditions.

Figure 3: A ground-based police robot employed by the Police North-Rhine Westphalia. Photo courtesy of the Landesamt für Zentrale Polizeiliche Dienste.

These systems are currently mainly deployed in aerial search and rescue operations in response to emergencies that are hard to reach, such as boat accidents or flooding, as well as natural disasters like hurricanes, earthquakes, or wildfires. While this use is still in a more experimental phase, this capability is particularly valuable in situations where divers may be unable to safely operate, such as in unstable ground conditions, strong currents or low-visibility environments. Unmanned underwater systems can be equipped with sonar, cameras, and other sensors to locate missing persons or survivors in underwater environments, providing a vital tool for search and rescue teams to respond to emergencies in these areas. By expanding the reach and capabilities of search and rescue operations, unmanned systems can help save lives and improve response times in emergency situations.

Explosive ordnance disposal and hazardous materials

Unmanned systems are being increasingly utilised in the critical areas of explosive ordnance disposal (EOD) and hazardous materials handling. One of the most important applications of these systems is in the inspection and disposal of explosive devices, such as ammunition, (hand) grenades, and improvised explosive devices (IEDs). Its benefits are evident: by deploying unmanned systems equipped with specialised sensors, cameras, and manipulator arms, bomb technicians can safely and effectively inspect and dispose of these devices, minimising the risk of injury or damage to people and property. EOD systems can be equipped with a range of sensors and tools, including X-ray machines, metal detectors, and robotic arms, allowing them to inspect and manipulate explosive devices in a safe and controlled manner. Additionally, unmanned systems can be used in a variety of environments, including urban and rural areas.

Figure 4: A bomb disposal robot. Photo courtesy of the Swedish Police Authority.

In addition to the explosive threat, unmanned systems are also being used to enter contaminated areas (hot zones) and to handle hazardous materials, such as chemicals, biological agents, and radioactive substances. These systems can be equipped with specialised sensors and manipulator arms, allowing them to safely and effectively detect, identify, handle, and contain hazardous materials, reducing the risk of exposure to officers and other personnel.

Technical limitations

Modern unmanned systems are often restricted by limited levels of control and autonomy. The drone is piloted by an officer, the operational deliverable from the device often goes to a screen, watched by humans, adding to a conventional decision-making process. Moreover, the collaborative capabilities between systems used today are very low and require human assistance and analysis to add value in a mission. This “effectively” ties down a lot of officers and teams of experts, often in several levels of the command structure, to digital devices performing narrow tasks in missions[15].

Current unmanned systems are often specialist systems, optimised to perform a specific task in a specific domain[16]. While they have proven effective in reducing danger and providing a different view or access to new domains, they are often directly controlled by human operators, requiring significant resources and infrastructure to deploy and maintain[17]. In addition, the operation of these systems requires some level of expertise and poses a significant cognitive load for the operator. As the situations in which these systems can be used are very specific as well as dependent on experts, their deployments are limited and, thereby, the efficiency of their use is limited. These factors also make their use more expensive.

Additional technical challenges include the limited battery life, the need to improve sensor and navigation capabilities to expand their operational reach, and the integration of diverse sensor data (such as thermal, LiDAR, and spectral imaging) into a unified intelligence picture. These challenges necessitate interoperability efforts between various systems and operating units across European Member States.

Finally, robotic systems may have relevant general capabilities, but still lack abilities to be meaningfully deployed in a law enforcement context. Industrial applications may be too narrow as the environment can be adapted to the robot to allow it to operate successfully in a factory or warehouse. This is impossible in most law enforcement use cases as the systems need to operate wherever operationally required, in less predictable environments. Therefore, a more general capability is needed. While military applications generally have to deal with a great variety of environments, they may lack certain specific skills, for instance non-lethal interventions and minimalisation of damage during operations.

Figure 5: A bomb disposal robot facing a staircase. Photo courtesy of the Swedish Police Authority.

Example box – opening doors

The lack of law-enforcement centric solutions is often linked to the limited number of suitable vendors, particularly in Europe. While many major robotics companies produce solutions that can and are used in the law enforcement domain, they are not developed for law enforcement specifically. An example of this is a robot that can open specific types of doors in a specific way – a common challenge faced by LEAs when entering unknown and potentially dangerous buildings. While an industrial user in a highly controlled environment, such as a factory, might be able to adapt and change the doors the robot needs to be able to open in order to move through the respective environment, law enforcement agencies do not enjoy such luxury. LEAs encounter a wide variety of doors and need to adapt to their environment, rather than the other way around. In addition, tactical considerations may require different ways of opening doors. As a result, LEAs currently need to adapt commercial solutions to their own needs, should they want to use them in operational settings.

Lack of independence from industrial suppliers

A significant cause for concern is the reliance on a limited number of manufacturers for commonly used unmanned systems. While this applies to a wide range of systems, the drone industry, in particular, is affected by non-European market dominance, with many law enforcement capabilities being built around a single manufacturer[18]. This “vendor lock-in” has created an important strategic vulnerability regarding hardware access, service, and data protection[19]. The lack of diversity in the market can limit the ability of LEAs to respond to emerging threats, compromise the security of sensitive information and eventually, public trust. Emerging concerns regarding the products of a non-European supplier, such as cybersecurity or data protection vulnerabilities, do not just present a costly challenge for law enforcement to mitigate potential issues. In some cases, it might simply not be possible to find an alternative, European supplier, which becomes even more of a concern when it comes to counter UAS systems (C-UAS). This makes European LEAs dependent on, and offers them only limited control over, technology provided by non-EU countries.

In contrast to the UAS market, the bomb disposal robot market has a more diverse range of manufacturers[20] providing law enforcement agencies with greater flexibility and options[21]. These companies have developed a range of purpose-built products, from small, portable robots to larger, more advanced systems. However, this field is heavily influenced by military specifications, which can result in high pricing and limited availability and relevance. As a result, law enforcement agencies often have to balance the need for advanced capabilities with the constraints of limited budgets and resources.

While hardware access presents a strategic challenge, the emergence of open-source robotics can play an important role in lowering development barriers and enabling innovation across various stakeholders, including smaller players in the robotics domain. Platforms like the Robot Operating System 2 (ROS 2), for instance, provide a flexible, modular, and scalable software framework for developing and integrating AI-driven, sensor-rich, and autonomous systems[22]. ROS 2's support for real-time communication, security, and distributed systems makes it particularly well-suited for multi-robot coordination, autonomous navigation, and swarm operations. As such, open-source robotics could be at least one possible response to counter a European lack of technological autonomy.

The lack of strategic technological sovereignty for European LEAs presents a critical challenge. Without European alternatives, there is a significant risk of being vulnerable to dependencies, cybersecurity and data protection vulnerabilities, as well as losing control over the ability to deploy technological solutions in accordance with the values of the European Union. Consequently, those factors could pose as a serious barrier to an effective uptake and deployment of unmanned systems by European law enforcement in the future.

Threat from unmanned systems

Criminal and terrorist groups are often early adopters of technology to gain advantages. As a long history of technology abuse has demonstrated, malicious actors will use any technology that is good, cheap, and easy enough to use while at the same time being freely obtainable on the consumer market. The rapid commercial rise of unmanned systems, specifically of hobby drones, meets and continues to accelerate these criteria. In a study made by the Hague Centre for Strategic Studies[23], they suggest that new vulnerabilities can be detected by using the *Routine Activity Theory*[24]. The theory emphasises that crime occurs when three elements converge: (1) a motivated offender, (2) a suitable, attractive target, and (3) the absence of a capable guardian. The study suggests that if the value desired by a motivated offender is more efficiently acquired by using a drone, this vulnerability will be exploited by the offender. As unmanned systems challenge the capability of security authorities to protect and respond accordingly, the threat stemming from unmanned systems is of particular concern.

Although the malicious use of unmanned systems, particularly drones, can lead to criminal or terrorist activities, a growing concern is that these actions can originate from state-sponsored sources. Unmanned systems are particularly attractive in the context of hybrid threats as the increasingly autonomous nature with which they can be operated can offer state actors certain plausible deniability. This can complicate attribution and lead to a (mis-) categorisation of these activities as mere criminal acts[25]. Suspected drone sightings over Danish[26] and German[27] airports in September and October 2025 underlined capability gaps within both military and law enforcement but also political ambition to increase law enforcement capability to better police the problem.

The criminal use of drones has been reported since around 2010[28], making 2025 a 15-year learning process for criminal innovators and early adopters. Organised crime actors are now capable of producing professional and advanced drones in an artisanal way, and in 2022 the first known instances of unmanned underwater drones, deployed for nefarious purposes, were discovered[29]. This, together with the widespread use of drones in Russia's war against Ukraine, suggests 2022 as the turning point for a wide spread antagonistic use of unmanned systems in all domains. The attacks on Israel by Hamas on 7 October 2023 involved extensive use of UAS[30], both, for the purpose of intelligence and situational awareness or to deliver payloads. This further emphasises the potential and relevance of these systems for criminal and terrorist purposes.

Figure 6: Drone operator. Photo courtesy of the Swedish Police Authority.

The criminal exploitation of unmanned systems is following the general trend towards common societal use of cheap and simple drones. This malicious use mostly involves opportunistic, remote-controlled, commercially available and easily obtainable UAS for reconnaissance (information) and smuggling[31] or delivery (logistics)[32.] This allows both the successful conduct of these operations as well as offer a means to further distance people from the act, providing greater anonymity. **A new form of "crime-at-a-distance" can emerge from today's "crime-as-a-service"**[33]. For example, a criminal network might hire an experienced drone operator to supply real-time information on locations and movements of police officers, to attack a rival gang with homemade explosives or to smuggle drugs across a border. There are already cases of drone pilots selling their services online, flying someone else's drone from a distance[34], for example in October 2025 an unmanned "narco submarine" with a Starlink satellite antenna was seized off the coast of Colombia.

The use of drones for said smuggling purposes is particularly prevalent in rural and uninhabited border areas in Europe[35]. However, a potentially greater threat is the ability of these systems to gather information, which can be used to support a wide range of criminal, terrorist, or hybrid operations[36]. This intelligence-gathering capability is particularly concerning because it is difficult to detect, can be used repeatedly over time, and can provide long-term value to malicious actors, making it a more significant and enduring threat than the smuggling itself.

All of these developments are boosted by the accessibility of information on how these systems may be deployed and modified. This development has been exacerbated by the fact that the Russian war on Ukraine has led to a wide spread competence in drone construction and modification[37]. This is further supported by similar resources on supporting technology like 3D printing for the modifications, crypto currency for anonymous trade, and encrypted communications to evade law enforcement detection.

The threat from unmanned systems is a growing concern as criminal and terrorist groups increasingly adopt and modify these technologies to carry out illicit activities, and the future may hold even more sophisticated and anonymous operations as technology continues to advance and become more accessible. As we move forward, the capability to deploy effective countermeasures and strategies to address these threats will become increasingly critical for law enforcement[38].

Countering unmanned systems

Despite the growing use of unmanned systems in law enforcement, the capability to counter them at scale is limited. **The relative distance between the threat and the capability to mitigate and protect has grown into a substantial gap.** This gap is not only technological but also relates to regulations, training, data sharing and infrastructure.

The increasing accessibility and versatility of drones as well as rapid, continuous innovation, (particularly displayed in Russia's war on Ukraine) have led to serious security concerns. In response, governments, defence agencies, and private sector companies are heavily investing in C-UAS solutions to detect, identify, track, and neutralise (rogue) unmanned aerial vehicles.

Incidents involving suspected drone activity require a structured and consistent approach to information management. Experience shows that reports of unidentified aerial objects can quickly attract significant media attention and lead to the mobilisation of considerable resources, even when later analysis indicates that the observations likely concerned conventional aircraft or other benign phenomena. To ensure an efficient and proportionate response, initial assessment and information handling are of critical importance.[39]

When a suspected drone observation is reported, the first step is to determine whether the incident is genuinely abnormal or falls within the range of expected air activity. Relevant data sources, such as Air Traffic Control (ATC) primary radar[40], military radar, and Automatic Dependent Surveillance–Broadcast (ADS-B) information[41], should be consulted to validate the report, supported by established communication channels with the owners or operators of these systems. Information relating to large, long-range drones should be clearly distinguished from that concerning small, short-range drones, as the likelihood of connection between incidents varies significantly. Applying this structured and data-driven process reduces the risk of misinterpretation, ensures the effective use of operational resources, and contributes to a more accurate overall situational picture[42].

Law enforcement agencies must, in collaboration with other relevant actors and partners, develop comprehensive strategies to monitor unmanned systems effectively, detect misuse and counter them when needed. Guidance on developing such strategies can be found in resources like the European Commission's Handbook on UAS protection of critical infrastructure and public space, which provides a five-phase approach for C-UAS stakeholders, covering detection, tracking, identification, and neutralisation[43].

Additionally, this means investing in new technologies, training personnel, and establishing clear protocols and procedures. Several LEAs are starting to, or have already, established dedicated units, sometimes in collaboration with the military, to counter unmanned systems to address this, with a unit that includes personnel trained in drone detection and mitigation[44, 45].

Most detection systems utilise a combination of radar, radio frequency (RF) analysers, acoustic sensors, and optical cameras enhanced with artificial intelligence to accurately identify and classify drones among other flying objects[46, 47]. Advanced algorithms improve the ability to differentiate between legitimate UAS operations and potential threats, reducing false alarms[48].

On the mitigation front, several technologies are available and under development to counteract unauthorised drones. Electronic countermeasures like RF jamming and GPS spoofing can disrupt a drone's communication links, causing it to land or return to its operator[49]. However, if drones are controlled via fibre-optic cable, some of this mitigation mechanisms are ineffective.

Kinetic solutions involve physically intercepting drones using nets fired from specialised guns or deploying interceptor drones designed to capture or collide with the target[50]. Additionally, directed energy weapons, such as high-powered microwaves and lasers, are being developed to disable drones by damaging their electronic components or airframes[51].

Most of the C-UAS applications are military applications which are solely addressing the threat of the drone and stopping it. However, this is much more complicated as the safety of the surroundings is a primary concern for law enforcement as they are generally tasked with stopping threats with minimal damage to the source of the threat. For example, cars are usually stopped, not destroyed – similarly, a drone may have to be stopped. Furthermore, from a forensic perspective, it is essential to have the drone as intact as possible to extract data in order to investigate what it was doing, as well as identify who controlled it, for intelligence and evidence purposes.

Since much of the development is focused on military use, law enforcement finds itself in a challenge since systems deemed not effective enough in military conditions may be the only relevant systems in peacetime urban situations.

Finally, the term counter-UAS (C-UAS) is a military term but for law enforcement, the ability to counter unmanned systems is actually the ability to police a society with unmanned systems as a component.

Public trust & regulation

Next to the regulatory environment, **public trust is key for legitimacy of law enforcement and its capabilities.** For instance, the New York City Police Department used robot dogs to investigate a collapsed building. While the use of the unmanned system was generally considered to be effective, it raised fear among some citizens and advocacy groups of privacy violations and indiscriminate surveillance. The criticism further highlighted the need for more transparency and assurance on responsible use[52.] The use of the robot dog, as well as its subsequent criticism, came after previous deployments had to be retired due to significant public backlash over fears of robots as an 'alienating' presence, specifically with regards to the potential use of violence[53]. These fears stem from widely publicised debates and actual uses of lethal robots for police operations[54].

In another case, a police robot deployed to patrol an area near Los Angeles, California, was unable to assist a bystander in calling the police in response to a heated argument. Highlighting a clear gap in public expectations and the real capabilities a police robot can provide[55]. Public trust, particularly when viewing the law enforcement deployment of a specific technology through the lens of a trade-off between privacy and security – is much harder to ensure when the promised added value provided by the technology is insufficient to offset potential concerns. These examples are not limited to the deployment of novel robotics in law enforcement.

The already widespread use of police drones, for instance, such as for surveillance purposes, has repeatedly been met with public scepticism related to fears of surveillance, lack of transparency, concerns over misuse, and a perceived dehumanisation of policing. Research into this dynamic has highlighted that the public acceptance of police use of drones is significantly dependent on perceptions of fairness and justice in their deployment[56]. Understanding public fears is essential as technological solutions must address emotional and social dimensions, in addition to those related to safety and legal compliance alone.

This trust for the use of technology is based on historic and general performance of law enforcement as well as understanding of the technology and its use by law enforcement. As unmanned systems are still relatively novel in the public domain and in particular in a security-related context, there is a lack of awareness of and exposure to these systems. This results in a lack of reference points for the general public. Lacking a real reference of actual police use and a clear understanding of police operations, regulation and processes in this field, public reactions often default to regulating against potential abuse.

In order to address such concerns, and help law enforcement agencies evaluate new technologies in a structured approach with a view to upholding fundamental rights and public trust, Europol has published a dedicated framework, entitled 'Assessing Technologies in Law Enforcement'[57]. This framework offers a method for ethical decision-making that can help ensure that the adoption of new technologies align with core values, such as transparency, fairness, privacy, and accountability. If the use of unmanned systems by law enforcement agencies is to increase, it is important to carefully consider the implementation and communication about such deployment, as well as involve the public actively (such as via public consultations and workshops) – ideally before citizens start seeing robots patrolling their neighbourhoods or drones hovering overhead.

Figure 7: A drone operator. Photo courtesy of the Swedish Police Authority.

European law enforcement agencies face several challenges when adopting new technologies. First, they must provide transparent, knowledge-based, and trustworthy explanations to the public about why these technologies, such as drones or robots, are necessary for policing. Second, their ability to use such tools depends on legal frameworks that are often still under development. Because technology evolves faster than legislation, this creates grey or temporarily unregulated areas. At the same time, European regulations governing the use of unmanned systems have been advancing to address safety, security, and privacy concerns while supporting innovation and technological progress. These regulations span a wide range of sectors, from aviation to industrial automation and public space management.

The primary regulation governing drones is the *EU Drone Regulation*, comprising two main pieces of legislation: *Regulation (EU) 2019/947: Operational Requirements and Regulation (EU) 2019/945: Technical Requirement*. This regulatory framework categorises aerial drones based on risk into three main categories:

- **Open:** includes low-risk operations that do not require prior authorisation. For instance, a local police unit can use a drone to monitor foot traffic in a local park.
- **Specific:** encompasses medium-risk operations that necessitate a risk assessment and, in some cases, operational authorisation.

For instance, police may deploy a drone to monitor (and fly over) a crowd during a large-scale event.

- **Certified:** comprises high-risk operations, such as transporting people or dangerous goods, which require certification of the drone, operator, and remote pilot. For instance, police may use a large, fixed-wing drone to monitor critical infrastructure for counterterrorism purposes.

Operators of drones must adhere to specific requirements, including registration, pilot competency, and operational limitations. For instance, all drone operations must be conducted within visual line of sight (VLOS) and at a maximum height of 120 metres above ground level. Additionally, registration is mandatory for all drones equipped with cameras or sensors that are not considered toys. Furthermore, drones are prohibited from flying over assemblies of people. Nevertheless, several pilot projects in Europe are testing the use of remotely piloted drones as first responders.

In October 2023 the European Commission published a policy document, titled “Communication on countering threats posed by unlawful and dangerous use of drones” (COM(2023) 659), which sets out a comprehensive EU counter-drone policy framework. The document outlines key actions for EU-wide coordination, a harmonised policy approach, and aims to address the growing security risks from non-cooperative drones. It was published alongside two handbooks providing practical guidance on risk assessment and protection measures.

There are still gaps in the current regulatory framework for drones. One significant concern is that these regulations primarily address remotely piloted systems, leaving a void in terms of fully or even partially autonomous operations. There are no clear guidelines for autonomous operations, including fail-safes and human oversight requirements, which will challenge accountability assumptions and compliance with existing laws. Other gaps include the inconsistent application of regulations across Member States, such as beyond visual line of sight (BVLOS) operations. There is also ambiguity regarding consent and data handling for unmanned systems equipped with cameras or sensors. Moreover, the lack of mandatory remote identification systems hinders tracking, prevention, and investigation of drone-related incidents. Finally, there are no standardised geofencing requirements to prevent drones from entering restricted areas, which poses a significant risk to safety and security.

The regulatory frameworks for humanoids, unmanned ground vehicles and unmanned surface or underwater vehicles are even less developed compared to those for UAS. While there have been attempts to establish standards and interoperability, civilian applications of UGS and USS/UUS lack comprehensive EU-wide regulation, resulting in a fragmented approach across Member States. In the absence of a comprehensive, overarching regulation for unmanned ground vehicles and robots in Europe, they are governed by a combination of regulations related to product safety, labour, privacy, and sector-specific standards.

The EU Machinery Regulation, adopted in 2023[58], broadened a previously existing Directive to include novel and evolving robots[59], including robotic autonomy and self-evolving systems. It addressed human-robot interactions, acknowledging that robots are moving from factory settings into everyday human environments. However, inadequately covers the impact of AI and autonomy, and lacks clear mandates for human oversight, thereby posing the risk of diminished accountability and potential harm[60]. The regulation further is not aligned with the AI Act[61], which is relevant for unmanned systems where AI is used for autonomous decision making. While the AI Act follows risk-based approach to AI regulation, with high-risk systems (such as healthcare and public services) subject to strict requirements, ground-based robots may not clearly fall into these categories, leading to regulatory ambiguities. Finally, both, drones and robots, being connected devices, fall under the scope of the *Cybersecurity Act*[62] (Regulation EU 2019/881), which establishes a framework for the certification of cybersecurity products and systems.

Going forward, a key uncertainty in the regulation of unmanned systems is going to be the impact of the use of unmanned systems in geopolitical conflicts. As the vast majority of these regulations were put in place several years ago, before 2022, they might not be calibrated to the current state of the technology and its rapid evolution. If experience and innovation in the use of these systems from conflict zones spills over into the European internal security domain, potential regulatory gaps may cause further challenges for law enforcement. This includes the current lack of legislation for law enforcement on countering unmanned systems. At the same time, law enforcement is lacking clear regulatory clarity on how emerging technologies in the field of unmanned systems can effectively be used in operational deployments – especially where improved autonomy and decision-making are experiencing rapid technological progress.

As the field has technologically and practically developed rapidly over the last few years, it is necessary to review and update legislation on the general use of unmanned systems as well as law enforcement specific legal guidance for the use and countering of unmanned systems. One example on market adaptation to regulation, is the exemption from direct identification (Remote ID) for very light drones (C0 class) below 250 grams[63], which has led to publicly available drones weighing 249 grams. Law enforcement input to support balanced and effective regulation is a continuous need.

Key trends shaping the future

The future of robotics and unmanned systems will be shaped by four key trends:

1. Artificial intelligence and technological convergence.
2. The expansion of the robotics industry.
3. The growing integration of robotics in society.
4. War as a driver for innovation.

These trends are leverage points that will play an important role in shaping the future of robotics and unmanned systems. The following chapter provides a brief explanation of each trend and where it might lead to in the future, before going deeper into the future operating environment.

Below, these trends are explained from a current perspective and a future perspective.

Artificial intelligence and technological convergence

In the future…

By 2035, the convergence of robotics and technological breakthroughs, especially AI, has led to a seamless integration of intelligent machines into every facet of daily life and industry. Robots, equipped with advanced language and vision models, intuitively understand and anticipate human needs, learning new tasks from observation or simple verbal instructions. In homes, personal assistant robots manage chores, provide companionship, and support elderly care, while in hospitals, AI-powered machines handle everything from surgery and diagnostics, to patient mobility and sanitation with unmatched precision and empathy.

In industry, we have autonomous robots and collaborative cobots working alongside humans, optimising production lines, logistics, and agriculture, all while minimising waste and energy consumption through sustainable design. Human-robot interaction have become natural and emotionally intelligent, with machines recognising and responding to social cues, personalising experiences, and supporting education and entertainment. Meanwhile, drone swarms have moved from the battlefield to the internal security domain, as open-source AI models allow criminals and terrorists to control hundreds of drones simultaneously.

The trend towards AI in robotics is a game changer. By leveraging diverse AI technologies, robots can perform a wide range of tasks more efficiently and the International Federation of Robotics expects physical, analytical and generative AI to drive the next wave of robotics, creating **a "ChatGPT moment" for physical AI.**[64]

Today, the merging of several technologies is pushing innovation and advancement at faster rate than has previously been witnessed. As AI, modular design, advanced power sources, multi-domain operations, sensor technology, and advanced materials continue to evolve and intersect, they are creating new opportunities for unmanned systems to be used in a wide range of applications, from surveillance and reconnaissance to search and rescue, environmental monitoring, and beyond. The synergy between these technologies is enabling the development of more sophisticated, adaptable, and effective unmanned systems that can operate in complex and dynamic environments, and providing users with greater flexibility, autonomy, and decision-making capabilities.

The convergence of these technologies is also driving the development of new concepts and capabilities, such as swarming[65], autonomous navigation, real-time data analysis and collaboration. As unmanned systems become increasingly interconnected and interoperable, they are enabling the creation of complex systems of systems that can operate in a coordinated and autonomous manner, providing much higher levels of situational awareness, decision-making, and operational effectiveness.

Figure 8: "*Royal Marines using Malloy TRV150 drone swarms*" – Crown Copyright, used under the Open Government Licence v1.0. Source: Wikimedia Commons.

The current development of unmanned systems is heavily driven by advancements in AI and sensor technology. The integration of AI enables robots to navigate and interact with their environment more effectively, while sensor technology provides the necessary data for robots to make decisions[66]. The use of large language models and multi-modal AI models is expected to further enhance the capabilities of unmanned systems, enabling them to understand and interact with their environment in more sophisticated ways[67]. As a natural progression of this trend, it is likely that future unmanned systems will not only interact with their environment more effectively but also interact with humans more directly, and indeed, the team of "NATO HFM-SCI-ET-219" is currently laying the groundwork for a NATO wide alignment in standards and best practices for human-swarm interaction. In addition, the industry is pushing for the development of more advanced robotic forms, such as humanoid robots, that can engage with people in a more personal and intuitive manner[68].

Given the importance of AI in the development of robotics, companies with capabilities in this area are becoming increasingly relevant stakeholders in pushing technological boundaries[69,70]. NVIDIA, for instance, is driving the development of intelligent robots through its NVIDIA Isaac platform. This platform provides a comprehensive set of tools and technologies for building, testing, and deploying autonomous robots, including simulation software, AI models, and hardware acceleration. With NVIDIA's Isaac platform, developers can create more sophisticated robots that can learn from their environments, adapt to new situations, and perform complex tasks autonomously. Other companies leverage expertise from existing products. Google's Gemini models allow robots to respond to text, images, audio, and video[71]; Tesla's experience in AI for autonomous driving is now being applied to build humanoid robots[72], and Boston Dynamics integrates advanced AI to enhance robot mobility and decision-making in real-world environments[73].

Despite advancements, challenges remain in the development and deployment of AI-powered robotics. First, AI models trained in simulations often face difficulties when transitioning to real-world environments, where conditions are more complex and unpredictable (Sim-to-Real Transfer). Second, the increased use of AI robotics raises concerns about job displacement, particularly in industries like manufacturing and logistics. And finally, AI robots that collect and process personal data, especially in the law enforcement context, raise significant privacy and security concerns.

In addition to the development of AI as a key driver of robotics development, a number of supporting technologies that enhance capabilities and applications are experiencing rapid developmental growth and, critically, are converging to benefit from one another:

- Modular unmanned systems are at the forefront of innovation, providing greater adaptability through interchangeable components. This allows operators to tailor systems to specific missions, whether by altering sensor packages, swapping out batteries, or changing propulsion units. Hybrid unmanned systems are combining various propulsion methods, such as electric motors paired with combustion engines, to enhance range, flexibility, and performance in different operational environments. For instance, aerial drones may employ hybrid designs to undertake long-duration flights with varied payloads, while modular UGS can be reconfigured for diverse tasks ranging from surveillance to bomb disposal.
- The endurance of unmanned systems is being advanced by new power sources. High-capacity, lightweight battery technologies, such as solid-state and lithium-sulphur batteries, are extending

operational times and reducing recharge intervals. Solar power is becoming more practical for smaller unmanned systems, with high-efficiency photovoltaic cells contributing to energy independence. Additionally, hydrogen fuel cells are emerging as a clean, long-endurance power source, particularly for UAS and UGS that require longer mission profiles without the logistical footprint of traditional fuel.

- Unmanned systems are increasingly designed to operate seamlessly across multiple domains. Amphibious drones can transition between aerial and maritime environments, while all-terrain UGS can handle diverse landscapes, from urban settings to rugged off-road scenarios. The integration of environmental-specific sensors and navigation technologies enables these platforms to collect data and function autonomously across these varied domains.
- Advancements in sensor technology are providing unmanned systems with enhanced situational awareness and data collection capabilities. High-resolution cameras, LiDAR, multispectral sensors, and synthetic aperture radar (SAR) are some examples that allow for detailed observation and analysis. In terms of communication, mesh networking and anti-jamming technologies are ensuring reliable data links even in contested or challenging environments.
- The use of advanced materials such as carbon fibre composites and 3D printing technologies in manufacturing unmanned systems is reducing weight and improving durability. This not only enhances performance but also allows for rapid prototyping and customisation of unmanned systems for specific missions.

The robotics industry – affordability and market dominance

In the future...

By 2035, the landscape of the tech industry has undergone a profound transformation, as many of the dominant AI companies of the 2020s have fully transitioned into robotics powerhouses. These firms, primarily headquartered in the U.S. and East Asia, leveraged their leadership in foundational AI models to develop sophisticated, autonomous robotic systems that now dominate sectors from logistics and manufacturing to eldercare and urban infrastructure. With their massive data reserves, compute infrastructure, and capital, these companies rapidly scaled production and distribution, leaving little room for smaller competitors. Robotics is no longer a standalone industry but an extension of AI empires, creating an ecosystem where AI and physical automation are deeply integrated—and tightly controlled by a few global players.

Europe, despite its early ambitions in ethical AI and digital sovereignty, has fallen behind in the robotics race. While some EU states have established local innovation clusters, the continent *remains critically dependent on foreign firms for advanced robotic hardware and software. Nowhere is this dependency more visible than in European law enforcement and public security. National agencies routinely source critical robotic systems, from surveillance drones to autonomous security patrol units, from a narrow selection of American and East Asian tech conglomerates. This reliance has sparked concern within EU institutions about digital autonomy, data governance, and national security, as law enforcement tools are increasingly shaped by the priorities and update cycles of companies outside Europe's jurisdiction. The situation underscores not only a technological lag but also a growing strategic vulnerability, forcing the EU to confront difficult questions about how to reclaim control in an industry increasingly dominated by external forces.*

Today, the robotics industry is experiencing substantial growth, with significant funding and growing interest which is accelerating progress. One direct consequence of this development is a broader societal integration of robotics as more industries – from healthcare to hospitality – expose more parts of the population to robots.

The synergy between AI and robotics, referenced earlier, has led to a collaboration between and, in some cases, a convergence of AI and robotics companies, leading to increasingly capable robotic systems. This rapid progress, has led to tensions between innovation and regulation, with much of the robotics industry exhibiting a tendency to resist regulatory measures that might limit its growth. This resistance highlights a key question: how can the ethical, accountable, and safe use of robotics be balanced with interests to continue progress in this field?

The sub-trends within the industry point to several areas of concern and opportunity. Europe's reliance on foreign resources and technology, particularly from dominant players outside the EU, highlights the need for increased supply-chain autonomy and the risks associated with dependency. The example of certain companies' market dominance in the drone sector illustrates how innovation, mass production, and competitive pricing can lead to significant market power. As the industry advances, the demand for robotics expertise is also growing, implying a crucial need for education and training in these fields – including for law enforcement.

The role of AI in accelerating scientific research across a wide range of disciplines indicates that interdisciplinary collaboration could enable the unlocking of new frontiers. In addition, as major AI companies invest in robotics, we are witnessing a shift in the power dynamics within the tech industry, with the potential for increased market concentration and influence.

Growing integration of robots in society

In the future…

By 2035, service robots have become a fixture of daily life across Europe, gliding silently through shopping centres, delivering parcels to fifth-floor flats, and cleaning public transit platforms by night. While many citizens have grown used to their presence, nodding politely to automated crossing guards or receiving prescriptions from pharmacist bots, frustration simmers beneath the surface. In economically strained regions, displaced workers protest outside automated warehouses, chanting slogans at tireless machines behind reinforced glass. A spate of " bot-bashing" incidents in city centres, ranging from graffiti to targeted arson, has prompted debates about "robot rights" and the psychological toll of widespread automation. In this uneasy climate, even minor malfunctions, such as a hospital care robot administering the wrong medication, are magnified into national scandals, fuelling populist calls to "put people first."

Law enforcement now finds itself caught at the intersection of technological adaptation and social tension. Police officers investigate crimes by robots—such as drones used as tools in theft or automated vehicles causing pedestrian injuries—and against them, including sabotage, tampering, or hate-driven destruction. As AI and robotics replace routine policing tasks like patrolling or traffic management, some departments face internal pushback from officers who fear obsolescence or diminished purpose. At the same time, the rise in economic dislocation caused by automation has contributed to an uptick in cybercrime, vandalism, and organised theft, often targeted at robotic infrastructure. Agencies are under pressure to both modernise and humanise—balancing the efficiency of unmanned systems with public trust, and equipping officers not just with new tools, but with new roles in a society where "protect and serve" increasingly applies to both humans and machines.

Today, the growing adoption of robotics by various industries and sectors means that more and more members of society will be exposed to, and interact with, this technology. While an increased frequency of encountering different types of robots in everyday life may lead to greater familiarity and acceptance, there is a risk of societal alienation, frustration, and resistance towards robots. These reactions can be the result of robotic malfunctions leading to unintended harm (i.e., crashing autonomous taxis or service robots in hospitals), or simply disapproval of their very existence (i.e., nuisances caused by drone flights or surveillance concerns linked to police patrol robots).

War as a driver for innovation

In the future…

By 2035 the improvised-yet-sophisticated lessons of Ukraine's "garage drone" revolution have fully migrated into Europe's criminal underground. Small extremist cells now field pocket-sized AI-guided quadcopters and shoebox-sized tracked UGS built from globally available CAD blueprints and 3D-printed composite armour. Old school fibre-optic "leash reels" or the newer short-burst laser links let these machines remain invisible to jammers until moments before impact, enabling coordinated attacks on critical infrastructure and spectacular prison-yard extractions. Last winter's multi-city blackout, triggered when a swarm of €600 kamikaze FPVs dived into high-voltage switchyards, illustrated how cheaply physical force can be bought in the post-industrial hobby marketplace—and how quickly tactics can mutate once shared on encrypted maker forums.

European law-enforcement agencies, denied the luxury of military-grade rules of engagement, have responded by hardening the urban air-ground interface rather than the sky alone. "Quiet grids" of passive acoustic masts map every micro-rotor within a kilometre; sidewalk bollards and street lights conceal microwave point-defence pods that fry inbound guidance modules in milliseconds; and patrol officers carry RoboFreezer guns and throw-down nano-net grenades that bloom like dandelions to snare a rogue rotorcraft. Yet the cat-and-mouse cycle accelerates: criminals continuously flash new firmware patches harvested from distant battlefronts, while public pressure mounts over the privacy costs of ubiquitous counter-drone surveillance. The border between warfare innovation and everyday policing, once distinct, has blurred into a restless, rapid-fire ecosystem where advantage is measured in software sprints and printable parts, not in years.

War is an unfortunate driver of technological innovation. Recent conflicts, chief among them the Russian war of aggression against Ukraine, have demonstrated novel uses of UAS, USS and UGS that is reshaping how war is fought. An illustrative example of this novel dimension of warfare is the Ukrainian "Spiderweb" operation, that allowed Ukrainian drones to strike key targets deep inside Russian territory[74].

A key factor in this regard is the tremendous speed on display in developing innovative concepts and improving products. This knowledge is widely spread among a significant number of users – and observers – and risks spilling over to criminal and terrorist use in an EU internal security context.

Figure 13: *"UA 72nd Brigade drone bomber"* by the Ministry of Defence of Ukraine, used under CC BY 4.0. Source: mil.gov.ua / Wikimedia Commons.

Ukraine's drone industry has undergone a remarkable transformation, with the country exponentially increasing its drone manufacturing output in an extremely short amount of time. In 2024, over 1.5 million first-person-view (FPV) drones were produced[75], with plans to manufacture up to 4.5 million drones in 2025[76]. This surge is supported by a network of over 200 domestic companies and civilian workshops[77], often operating from homes and garages. The integration of AI has further enhanced the effectiveness and autonomy of Ukrainian drones, with approximately 10,000 AI-enhanced drones acquired in 2024[78, 79].

At the same time, batteries are becoming increasingly advanced, holding more charge while being lighter, which has led to drones being mass-produced and utilised as a readily available resource, similar to grenades. The industry is undergoing significant evolution, not only in terms of researching greater autonomy but also in its ability to mass-produce units. This advancement has made it accessible for individuals with relatively limited technical knowledge to build and program a drone to perform entirely automated flights – either with GPS or, in case communication is unavailable, with slightly more advanced image software. Without a control connection to the pilot, it becomes extremely challenging for law enforcement to stop the drone or locate the operator.

The development of electronic warfare-resistant drones has been another key area of innovation, with Ukraine creating fibre-optic-controlled drones that are immune to radio signal jamming[80], as well as the use of 3D printing and readily available materials to produce cost-effective kamikaze drones, capable of destroying high-value targets like tanks or airplanes, at a fraction of the cost of traditional weaponry[81].

A critical role in the success of Ukraine's drone industry has been played by the grassroots involvement of civilians and small enterprises that are actively contributing to the development and production of drones. Initiatives like the 'People's FPV' program enable individuals to build and supply drones directly to military units, which has led to the establishment of a decentralised and highly responsive production model[82]. This approach has not just allowed Ukraine to rapidly adapt to the challenges of combat, but also to set new precedents in military technology.

There are two key implications of Ukraine's drone innovation for law enforcement agencies:

- The country's experience demonstrates how conflict can drive innovation, with potential applications for non-lethal use cases in areas like surveillance, drone defence or search and rescue. The decentralised production model employed by Ukraine's drone industry, in particular, might provide valuable lessons for law enforcement agencies to adopt more agile and responsive production and procurement methods.
- The development of affordable, AI-enabled, and electronic warfare-resistant drones poses new challenges for law enforcement in the context of potential criminal and terrorist abuse. The spill-over of warfare innovation into the internal security domain poses difficult challenges for law enforcement to address, particularly regarding counter-drone capabilities, as potentially lethal threats to the civilian population from crime and terrorism could take on a novel dimension.

The demonstrated operational effectiveness has pushed unmanned systems high up on the priority list of military forces and other security authorities. While significant investments from the military sector could lead to a greater variety of unmanned systems potentially available to LEAs, the stark contrast in operating procedures and mandate mean that they are often of limited interest and value in a policing context. As such, European law enforcement cannot rely on potentially beneficial trickle-down consequences in the adoption of innovative unmanned solutions.

Figure 10: Europol photo from Stockholm

Additionally, a growing societal adoption of robots can lead to wide-scale, more fundamental consequences. The rise of unmanned systems may impact employment and the nature of work, for instance, leading to major shifts in labour markets, displacing a potentially significant number of jobs leading to the need for new skills. These skills will initially be held by, and provide advantages for, the early adopters of this technology.

Law enforcement will be heavily impacted by this trend. This will include the need to investigate crimes carried out by, or directed towards, robots, managing potential direct and indirect consequences of labour market shifts – including increases in criminal activities as a result of growing unemployment – as well as managing its own work force in accordance with these changes.

The future operating environment

One key consequence that the aforementioned trends all have in common is that LEAs, in the future, will see an increasing number of unmanned systems, from autonomous cars to social companion robots. This is going to have a significant impact on the work of law enforcement, as these additional entities may require new ways of policing, both to use them effectively, as well as to prevent their abuse.

Unmanned systems as part of society

As more and more robots, drones and other unmanned systems are deployed to perform various functions in increasingly autonomous ways, they will become part of our lives and our public spaces. As it is the duty of law enforcement to police this space, LEAs will have to develop new ways to interact with these systems to separate the legal from illegal operations and ensure a safe space for everyone. This means being able to detect, monitor, stop, investigate or, ultimately, counter them with force. All of these will require exploration to identify novel operating procedures for law enforcement that are both safe and effective.

Different kinds of unmanned systems may require different approaches. A key factor in this regard relates to the different types of technology and standards involved. This includes the following:

- The design and development of unmanned systems might differ significantly based on their intended use. While the use of a law enforcement robots is likely to be heavily regulated, commercial or consumer-grade systems could have a much lower level of safety measures. The latter is also going to affect the forensic investigation of unmanned systems, as each encountered type might use different operating systems or data storage capacities.
- Unmanned systems may use different types of technology, including sensors and communications systems. While drones might rely on GPS, an autonomous ground vehicle might use LIDAR and computer vision. The response of law enforcement needs to take these differences into account, as different types of unmanned systems might require different types of approaches.
- The regulation of unmanned systems may vary per type. While drones might be subject to aviation laws, ground, surface and under water systems might be subject to entirely different regulation. Additionally, new regulation may emerge that seeks to cover all, as well as additional types. LEAs will need to understand these differences and how they will impact their operating environment and their capabilities.

Additionally, from a practical point of view, law enforcement will need to prepare for changing societal expectations: while today's discussions touch on points such as how to effectively stop a drone, the future operating environment might require LEAs to consider how to stop a humanoid robot.

INFO BOX – QUESTIONING A ROBOT

In some jurisdictions, law enforcement agencies are already beginning to encounter the challenges of policing unmanned systems, such as driverless cars. For instance, when a police officer stops a driverless car involved in a minor accident, they need to determine whether the car's actions were the result of a malfunction, a cyberattack, or a deliberate instruction from the car's owner. However, the car itself may not be able to provide a clear answer, and performing a full forensic analysis of the system in real-time may not be feasible.

In the future, this problem is likely to become even more complex. Humanoid robots, in particular, may pose unique challenges, as they could be designed to interact with humans in a more sophisticated way, potentially making it more difficult to distinguish between intentional and accidental behaviour. Assessing the intention of such a system may be quite different from that of a natural person. While stopping a person allows for the questioning of a suspect carrying out an action, an unmanned system might be less cooperative about its instructions and intentions, maybe even incapable of explaining it. Current efforts aimed at making artificial intelligence systems more interpretable, explainable, as well as aligned[83], will become critical when these systems move autonomously and physically. These developments will also impact how law enforcement will have to adapt and may have to result in new approaches to policing.

Law enforcement, too, may increasingly integrate different types of unmanned systems into its operational activities. Further integration of machine learning, deep learning, and computer vision will allow these robots to recognise and respond to potential threats in real-time. As such, human-robot collaboration is expected to become a crucial aspect of law enforcement operations, with officers and robots working side by side to respond to emergencies, conduct searches, and gather evidence together, building on each other's advantages.

Internet of everything

More widespread, low latency, high speed data networks, such as 5/6G and satellite communication, ensure connectivity everywhere. This will make ground for the use of Internet of Things (IoT) devises anywhere from underground areas to cities, rural areas and even oceans.

With more and more unmanned systems in circulation, an emerging concern relates to how these systems report on their activities to their owners, as well as how they will communicate with their environment and each other. This is likely to mean a vast increase in the amount of communication as well as dynamic changes in the nature of this communication. Device-to-device communication will likely not be the same as communication between humans or even human-to-device This means developing new capabilities for legal wiretaps of communications of individual, as well as between such systems, and having the technical capability of interpreting this communication.

Digital becomes physical

As unmanned systems become increasingly autonomous, equipped with AI and task-based controls, they are gaining agency to act on their own. This newfound autonomy raises concerns about undesirable and criminal behaviour, as their actions can have real-world consequences. Furthermore, their connected nature allows them to be controlled and instructed from anywhere, making it difficult to identify the intentions and responsible parties behind their actions, exacerbating the jump of cybercrime from the digital to the physical world.

Another aspect for law enforcement is the right to, and process for, seizing objects in criminal investigations. Robots will be seized as other objects but they pose a new risk since they, unlike other objects, can perform actions inside law enforcement facilities, such as record, steal, destroy or escape. With increasingly autonomous unmanned systems in circulation, law enforcement agencies will need to implement adequate processes for the seizure and storage of such technologies.

The convergence of unmanned systems and cybercrime enables new forms of crime to emerge in the physical world. As such, these systems can be used as a means for cybercrime to interact with the physical environment and cybercrime may have more impact in the physical environment. To address this challenge, it will become increasingly critical to develop methods for monitoring, querying, and investigating these systems, as well as their instructors. Effective and acceptable ways of making them comply with the law or stopping them will be vital for law enforcement to remain relevant.

INFO BOX – JAILBRAKING A ROBOT

Already today, we are facing the challenge on how to prevent AI from engaging in harmful behaviour. LLMs have repeatedly been jailbroken, either due to a lack of safeguards, or because of a wide variety of prompt engineering methods 'trick the system' into outputting content it does not understand is harmful. This is mainly because of the complexity and ambiguity of natural language used for prompting combined with the limitations of (current) AI systems in only predicting output based on training data, rather than actually understanding the content. As a result, guardrails are often external add-ons, added to the model after it has been trained.

Safeguards need to balance usefulness and safety – restricting an AI system too much can make it unusable, leading to a trade-off.

These attempts – trying to break current AI systems – will pave the way for doing the same with AI-driven unmanned systems. As unmanned systems increasingly rely on more and more capable AI for autonomous behaviour, the challenge on how to prevent safeguards from being bypassed for malicious activities is going to become increasingly important. Unless addressed, unmanned systems could be coerced into unintended behaviour. This might include the hijacking of autonomous vehicles or drones, the leaking of data from cameras and microphones, as well as the infliction of harm by unmanned systems on potential victims.

Social robots

Social robots are specifically designed to interact with others on a more human level. While still in early stages, applications of social robots already exist, including those helping the elderly[84] and children with autism[85], as well as social robots acting as romantic partners[86]. Powered by AI, these robots are getting more and more convincing in their empathy, as well as better at anticipating human needs.

The empathetic capabilities of social robots might, in the future, be abused by criminal and terrorist actors for a variety of malicious activities. Particularly activities containing an element of convincing people, from disinformation to grooming, could see the advantage in the abuse of social robots for these purposes, making it a new modality of criminal social engineering. As chatbots are already being employed to deceive victims[87], social robots may bring this trend to the physical realm and, potentially, cause even greater harm. These malicious efforts aimed at manipulating and deceiving their victims may be reinforced with increasing amounts of intimate data collected by social robots. As they become increasingly important parts of people's lives and move around in their private sphere, they will increasingly know their owners more intimately – and possess highly sensitive information about them[88].

Additionally, as social robots continue to connect with humans, we can expect shifts in how society feels about them and, consequently, how law enforcement should interact with them. While it may currently be acceptable for the police to take down a drone, interventions of unmanned systems evoking a more emphatic response might require more consideration. For instance, in 2015, a video showing people kicking a dog-shaped robot to demonstrate its balancing capabilities, sparked a debate about the ethics of kicking such a 'dog'[89]. As robots become more human-like, in behaviour, appearance or both, it may be increasingly difficult for LEAs to apply existing legislation to respond to situations involving unmanned systems. Would hitting a "human" robot constitute physical abuse as others may perceive it? And at which point do people identify enough with a robot to consider negative behaviour towards it an offense? It will be critical to have anticipatory public debates and legislative efforts in order to provide a relevant and clear legal context.

No more privacy

Satellites, artificial intelligence, open-source intelligence, and real-time surveillance have transformed modern conflict zones into what is now being called the transparent battlefield[90], and maybe this expression is equally relevant for society in general, the transparent society.

Unmanned systems, navigating our world and interacting with us and each other will be observing the world around them, with us in it. When these become ubiquitous in society, this will mean that there is the possibility to be observed almost everywhere, anytime. With household assistant systems, this extends to people's privacy spaces. Depending on the implementation and applicable data protection standards, the observations made by these systems could be used to gather data on people without their knowledge or explicit consent. While this has already been a business model widely applied in smartphones and a vast number of IoT devices, including household robots, an increase in capability and autonomy of unmanned systems are likely to exacerbate this threat to individual privacy. As these systems rely on sensors like cameras to navigate our world, questions relating to how to effectively regulate their use and deployment without stifling innovation will become increasingly important. While some general privacy related legislative aspects are already in place, a failure to regulate and implement may lead to a situation where people are subject to significant threat to their personal privacy when these potentially vast amounts of data are leveraged by companies and, potentially, criminals. Current crimes relying on the exploitation of data leaks and unsecured personal devices could become even more invasive when capable unmanned systems are found everywhere – in public, as well as at home.

Law enforcement operations may be tactically limited by these omnipresent observers. Already, the widespread introduction of home security camera systems and smart cars has limited the possibility for law enforcement officers to investigate criminals covertly. Mobile robotics systems on the lookout for police, equipped with facial recognition to decide who is friend or not, may make it even more difficult for police to conduct their investigations and police certain areas effectively.

Less accountability

The increasing autonomy of unmanned systems raises complex questions about liability and accountability. Unlike directly controlled systems, where the controller is clearly responsible for the system's actions, autonomous systems blur the lines of responsibility. When an autonomous system breaks the law, it is unclear whether the owner, producer, coder, or system itself should be held liable. The current legal framework is inadequate to address these questions, and new concepts and regulations will be necessary to resolve them. The fact that the owner, producer, or system may not be within the same jurisdiction as the crime adds an additional layer of complexity, as is currently the case in the area of cybercrime, highlighting the need for a comprehensive approach to addressing these challenges.

Effective regulation will be essential for law enforcement, too, in this context. A lack of relevant regulation may lead to limited uptake of these systems in law enforcement as well as a lack of public trust in the use by law enforcement of these systems. While unmanned systems provide unique opportunities to more effectively fight organised crime and terrorism, further precision of the general regulation of such systems to the context of law enforcement work will be key to enabling police organisations to develop needed capabilities to maintain relevance in a more unmanned future.

To address the emerging challenges posed by autonomous unmanned systems, it is essential to establish a new framework that clarifies liability, accountability, and regulation. This framework must consider the complex relationships between the system, its instructors, and the physical environment, as well as the potential consequences of their actions.

A 3D society needs 3D policing

The future operating environment for law enforcement will likely see a shift from monitoring two dimensional surfaces to three dimensional volumes. As criminal activities migrate across air, sea, and underground domains simultaneously, traditional perimeter-based policing becomes obsolete. **This multi-dimensional criminality will require a multi-dimensional law enforcement response.**

The majority of transport and logistics today moves on pre-determined streets and paths. Unmanned systems might challenge this arrangement, as drones, submersibles, and ground-based robots may not take the same paths as humans (and human-operated systems). With an increase in unmanned systems, under water and in the air, the planes in which humans operate will be become increasingly multi-dimensional. For law enforcement, unmanned systems not moving along the paths that are currently being policed will bring new challenges in terms of monitoring and enforcement.

For instance, smuggling operations may choose remote or inaccessible routes to cross borders while avoiding detection, as drones enable them to fly through previously impossible to navigate domains. An increase in autonomy might make these criminal use cases more attractive, as the distance (and, subsequently, deniability) between smuggler and recipient can be greatly increased. Particularly remote areas, such as vast forests, may be extremely difficult to monitor effectively, given technical and resource constraints. If traffic in such remote areas increases, it will be increasingly important to find ways to have the means to respond to potential criminal abuse quickly and effectively. Furthermore, maritime smuggling can be decentralized effectively, using unmanned systems trafficking a variety of small harbours or coastal locations to avoid security in large, commercial harbours.

Cities will also see a major impact. As drone swarms replace individual drones, patrolling the skies will become a core law enforcement task, creating aerial highways that are increasingly dense with autonomous traffic. Criminal organisations will seek to exploit this density, blending in their own drones while carrying illicit goods through urban landscapes. The challenge will not be limited to detecting individual threats, but distinguishing malicious intent within clouds of legitimate aerial activity moving at significant speed. These emerging, multi-dimensional developments may mean that criminal activity goes undetected, also preventing statistical analysis and, thus, limiting prioritisation of this crime unless new monitoring techniques and modes of mitigation are identified and implemented.

The emergence of swarms will effectively create a volume problem for law enforcement. Criminal and terrorist networks, as a result, think in volumes rather than routes, treating air, land, and sea as a single operational space. Consequently, the law enforcement response will require volumetric jurisdiction—the authority and capability to pursue threats seamlessly across vertical boundaries. Officers will need to understand how criminal activities flow through the three-dimensional spaces above, around, and beneath traditional patrol areas.

Unmanned systems themselves might provide part of the law enforcement response. Patrol drones and high-altitude pseudo-satellites (HAPS) equipped with high-resolution cameras and thermal imaging, for instance, could cover vast urban areas and provide real-time data to command centres. This capability would enable rapid response to incidents, improve detection of illicit system activity, and enhance overall policing effectiveness in the more unmanned future. Furthermore, law enforcement agencies could deploy fleets of drones in collaborative swarm formations to quickly assess and respond to large-scale emergencies, such as natural disasters or public safety threats, providing a coordinated response that maximises resource efficiency. On the borders, unmanned systems might patrol vast and otherwise inaccessible areas, using advanced sensors to detect illegal activities, while relaying crucial intelligence to human operators for swift intervention.

These examples illustrate a future where technology not only enhances the capabilities of law enforcement but also transforms the way officers interact with their communities, environments, as well as robots and unmanned systems. The potential for collaborative swarms of drones to quickly respond to emergencies or for collaborative robots to enhance community policing and engagement could offer new and valuable capabilities in intelligence gathering, surveillance, and emergency response. At the same time, it would free up cognitive ability for human officers to focus on what humans do better, generating a double win.

Recommendations

To address the emerging challenges and opportunities posed by unmanned systems, we recommend a joint approach on building law enforcement capability with and against unmanned systems, at both national and European levels. The recommendations are centred around four key capability components: *operations management, competence, system and structure.*

Operations management

- Develop a strategic intent that outlines how LEAs want to respond to the development, use, and potential misuse of unmanned systems, as well as their impact on society.
- Establish a "physical sandbox" environment that enables LEAs to test, learn, and adapt unmanned systems in a real-world setting, outside of a laboratory, and facilitate international cooperation and collaboration on development, testing, and procurement. This will also provide fact-based input to policy makers.
- Develop a comprehensive strategy to support the creation of EU-based regulation, standards and certification for safety, security, lawful use, and interoperability.

Competence

- Establish a competence hub that connects internal teams to a centralised repository of knowledge, expertise, and best practices. This hub should be linked and coordinated at European level, facilitating the gathering and dissemination of relevant insights about unmanned systems across borders. When appropriate, the hub could give guidance on technological standards.
- Invest in comprehensive training programs for personnel that cover a range of topics, including regulations, use, countermeasures, investigation, forensics and protection related to unmanned systems.
- Build trust and transparency with society by establishing outreach, consultation, and co-creation programs to actively involve citizens.

System

- Integrate unmanned systems into existing information systems. This includes information access, information management, and decision-making flows to enhance operational effectiveness.
- Develop a structured information flow regarding the criminal use of unmanned systems in Europe. Include in this flow forensic data to support counter-technologies.
- Establish a centralised standardisation and procurement process for technologies that benefit from coordinated and standardised purchases. Ensure that this process prioritises interoperability, technological independence and fosters the creation of law enforcement-centric solutions.

Structure

- Adapt the command structure of law enforcement agencies to accommodate the capabilities of unmanned systems and AI. Agencies should transition to Command, Control, Collaboration, and Autonomy (C3A) frameworks, which enables interoperability, collaboration, flexibility, and adaptability. C3A frameworks recognise that unmanned systems and AI can operate more autonomously, making decisions and taking actions in real-time, and that human operators must be able to collaborate with these systems to achieve shared goals within necessary timeframes.

Conclusions

The integration of more capable unmanned systems into society is expected to have a significant impact. Driven by the convergence of emerging technologies such as AI, sensors, robotics, and next-generation communications systems, the rapid progress in the field will likely lead to the widespread adoption of unmanned systems in various domains, including everyday life and law enforcement operations.

Law enforcement agencies will have to police a wider physical space, than they traditionally have. As unmanned systems become more prevalent, they will continue to challenge traditional policing practices and raise new concerns. The technology will also bring a more transparent operating environment where few things stay hidden.

Law enforcement agencies will face significant challenges in preparing for this shift towards an even more "phygital" society in the more unmanned future. The increasing capabilities and numbers of unmanned systems will introduce new threats, and criminals and terrorists will likely exploit these technologies for malicious purposes. Recent conflicts have shown that threat actors are often early adopters of new technologies, and law enforcement must be prepared to counter these emerging threats.

However, unmanned systems also offer tremendous benefits to law enforcement operations, with the potential to enhance capabilities and improve public safety. To realise these benefits, a solid regulatory foundation and investments in public trust are essential. The public must trust law enforcement to use these technologies effectively and accountably.

Furthermore, the development of unmanned systems is largely driven by non-EU companies, which poses a risk of critical dependence on foreign suppliers for Europe. To maintain technological autonomy and uphold European values, significant investments and joint innovation procurement processes are necessary.

The future of unmanned systems is uncertain, and various trends could unfold in different directions. The purpose of exploring these trends is not to predict the future but to identify desirable and undesirable outcomes and take proactive steps to increase the chances developments will lead to an acceptable outcome. Further law enforcement and policing oriented research is needed to delve deeper into the topics discussed in this report.

This report aims to raise awareness about the potential impact of unmanned systems on law enforcement and encourage preparedness and deliberate action for the challenges and opportunities that lie ahead. It is possible to prevent harm caused by unmanned systems and harness their potential to make Europe safer, but our decision making must adapt to the tempo of this development.

Endnotes

1. Europol intelligence notification, November 2025
2. International Federation of Robotics, January 22, 2025, https://ifr.org/ifr-press-releases/news/top-5-global-robotics-trends-2025#:~:text=1%20%E2%80%93%20Artificial%20Intelligence%20%E2%80%93,Physical%2C%20Analytical%2C%20Generative
3. Amazon.com, 10 December 2024, https://www.aboutamazon.com/news/operations/amazon-robotics-robots-fulfillment-center
4. CNBC, 15 October 2025, https://www.cnbc.com/2025/10/15/waymo-p.html
5. New York Post, 12 July, 2024, https://nypost.com/2024/07/12/us-news/angry-birds-are-attacking-nyc-beach-drones-flown-to-track-sharks-and-save-drowning-swimmers/
6. The Guardian, 24 July, 2022, https://www.theguardian.com/sport/2022/jul/24/chess-robot-grabs-and-breaks-finger-of-seven-year-old-opponent-moscow
7. Police1, 8 July 2024, https://www.police1.com/body-camera/bwc-ariz-officer-stops-self-driving-car-after-it-entered-oncoming-traffic-lanes-to-avoid-construction
8. Under water, surface, ground and air.
9. Forbes, 21 December, 2024, https://www.forbes.com/sites/davidaxe/2024/12/21/ukraines-first-all-robot-assault-force-just-won-its-first-battle/
10. Catalan News, 24 October 2022, https://www.catalannews.com/society-science/item/3-year-sentence-for-plotting-drone-terror-attack-in-camp-nou-during-barca-v-real-madrid-game
11. BBC, 10 October 2025, https://www.bbc.com/news/articles/cd721zdzr4xo
12. The Diplomat, 29 November 2024, https://thediplomatinspain.com/en/2024/11/29/national-police-dismantle-narco-drone-network-operating-between-spain-and-morocco/?noamp=mobile
13. BBC, 22 August 2025, https://www.bbc.com/news/articles/cwypw0xvdk5o
14. LiDAR (Light Detection and Ranging) – Light Radar
15. Member state input
16. Member state input
17. Member state input
18. Member state input
19. Member state input
20. Member state input, France (ECA Group, Shark robotics), Spain (Aunav), Germany (United Robotics Group, Telerob), Ireland (ICP), UK (NIC Instruments), Canada (Allen Vanguard, ICOR), Israel (Goldfec), USA (RE2 Robotics, FLIR/Teledyne) among others
21. Member state input
22. Robot Operating System 2, ScienceRobotics, 11 May 2022, https://www.science.org/doi/10.1126/scirobotics.abm6074
23. The Hague Centre for Strategic Studies, October 2024, https://hcss.nl/wp-content/uploads/2024/10/Looming-Lethal-HCSS-2024.pdf
24. Cohen and Felson (1979), ScienceDirect, https://www.sciencedirect.com/topics/social-sciences/routine-activity-theory
25. The New York Times, https://www.nytimes.com/2025/01/04/world/europe/nato-attacks-drones-exploding-parcels-hybrid.html
26. CNN, 26 September 2025, https://edition.cnn.com/2025/09/25/world/drones-denmark-hybrid-attack-wwk-intl
27. CNN, 4 October 2025, https://edition.cnn.com/2025/10/02/europe/munich-airport-closed-drone-sighting-intl-hnk
28. Grey Dynamics, 26 October 2024, https://greydynamics.com/narco-drones-the-use-of-drones-by-drug-cartels/
29. Policía Nacional, https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=12781#
30. Bulletin of the Atomic Scientists, 1 November 2023, https://thebulletin.org/2023/11/how-hamas-innovated-with-drones-to-operate-like-an-army/
31. Europol intelligence notification, November 2025
32. The Hague Centre of Strategic Studies, October 2024, https://hcss.nl/wp-content/uploads/2024/10/Looming-Lethal-HCSS-2024.pdf
33. Europol 2025, The changing DNA of serious and organised crime - EU Serious and Organised Crime Threat Assessment 2025 (EU-SOCTA), https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime
34. Input from a European national agency
35. El País, 28 November 2024, https://elpais.com/espana/2024-11-28/cae-una-banda-que-usaba-narcodrones-ucranios-para-transportar-hachis-por-el-estrecho.html
36. The Hague Centre of Strategic Studies, October 2024, https://hcss.nl/report/looming-and-lethal/
37. Centre for Strategic & International Studies, 6 March, 2025, https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare

38. Global Initiative Against Transnational Organized Crime, 30 October 2025, https://globalinitiative.net/analysis/crime-by-drone-a-new-paradigm-for-organized-crime/

39. Member state input

40. Primary Surveillance Radar (PSR), https://skybrary.aero/articles/primary-surveillance-radar-psr

41. Flight tracking like “Flightradar24”

42. Member state input

43. Protection against unmanned aircraft systems, European Union, 2023, https://op.europa.eu/en/publication-detail/-/publication/e05f89e1-6bc9-11ee-9220-01aa75ed71a1/language-en

44. Reuters, 14 March 2024, https://www.reuters.com/sports/anti-drone-units-new-tool-keep-paris-2024-safe-2024-03-14/

45. Unmanned Airspace, 15 October 2021, https://www.unmannedairspace.info/counter-uas-systems-and-policies/belgian-police-develop-operational-capability-to-manage-hostile-drones/

46. MDPI Review, December 2023, https://www.mdpi.com/1424-8220/24/1/125

47. ScienceDirect, July 2025, https://www.sciencedirect.com/science/article/pii/S1874548225000058

48. Frontiers, 17 October 2024, https://www.frontiersin.org/journals/communications-and-networks/articles/10.3389/frcmn.2024.1440727/full

49. Netline, 4 January 2024, https://netlinetech.com/how-drones-are-being-controlled-and-the-way-to-neutralise-them/

50. AirSight, accessed November 2025, https://www.airsight.com/knowledge-hub/counter-drone-technology/air-to-air

51. DECENT, accessed November 2025, https://decentcybersecurity.eu/counter-uav-technologies-securing-airspace-in-the-drone-age/

52. The Guardian, 26 April 2023, https://www.theguardian.com/technology/2023/apr/26/robot-dogs-new-york-building-collapse-surveillance

53. Axios, 1 May 2021, https://www.axios.com/2021/05/01/new-york-police-retire-robotic-police-dog?

54. The New Yorker, 10 December 2022, https://www.newyorker.com/news/daily-comment/should-local-police-departments-deploy-lethal-robots?

55. NBC News, 4 October 2019, https://www.nbcnews.com/tech/tech-news/robocop-park-fight-how-expectations-about-robots-are-clashing-reality-n1059671

56. Cornell University, 8 August 2024, https://arxiv.org/abs/2408.04684?

57. Europol, 20 February 2025, Assessing Technologies in Law Enforcement: A Method for Ethical Decision-Making, https://www.europol.europa.eu/media-press/newsroom/news/europol-publishes-framework-for-ethical-technology-in-law-enforcement

58. The Machinery Directive, European union 2023, https://single-market-economy.ec.europa.eu/sectors/mechanical-engineering/machinery_en

59. The Machinery regulation does not explicitly target robots. Rather, the term ‘robots’ is understood to be comprised as a subset of – and, thus, cover by – the larger category of ‘machinery’.

60. Scandinavian University Press, 31 October 2024, https://www.scup.com/doi/10.18261/olr.11.1.5?

61. The AI Act, European union 2024, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

62. The Cybersecurity Act, European union 2019, https://eur-lex.europa.eu/eli/reg/2019/881/oj

63. The regulatory requirements for direct remote identification of unmanned aircraft are established in Commission Delegated Regulation (EU) 2019/945 of 12 March 2019, supplementing Regulation (EU) 2018/1139, particularly Annex Part 6, which specifies the technical and operational requirements for Remote ID systems. https://eur-lex.europa.eu/eli/reg_del/2019/945/oj

64. International Federation of Robotics, January 2025, https://ifr.org/ifr-press-releases/news/top-5-global-robotics-trends-2025#:~:text=1%20%E2%80%93%20Artificial%20Intelligence%20%E2%80%93,Physical%2C%20Analytical%2C%20Generative

65. Defense and security monitor, 21 January 2025, https://dsm.forecastinternational.com/2025/01/21/drone-wars-developments-in-drone-swarm-technology/

66. Encord, 27 March 2025, https://encord.com/blog/ai-and-robotics/

67. Cornell University, 13 November 2023, https://arxiv.org/abs/2311.07226

68. Social Robots, accessed September 2025, https://socialrobots.ca/

69. NVIDIA, ‘Isaac Platform for AI-Powered Robots’, 2023, accessed 27 Sept. 2024, https://developer.nvidia.com/isaac/ros

70. VTKR, 11 June, 2024, https://www.vktr.com/ai-market/10-top-ai-robotics-companies/

71. Google DeepMind, accessed November 2025, https://deepmind.google/models/gemini-robotics/

72. Tesla, accessed November 2025, https://www.tesla.com/AI

73. Boston Dynamics, 18 March 2025, https://bostondynamics.com/news/boston-dynamics-expands-collaboration-with-nvidia/

74. BBC, 2 June 2025, https://www.bbc.com/news/articles/cq69qnvj6nlo

75. The Kyiv Independent, 28 December 2024, https://kyivindependent.com/ukrainian-drones-made-up-over-96-of-uavs-military-used-in-2024-defense-minister-says/

76. Forbes, 12 March 2025, https://www.forbes.com/sites/davidaxe/2025/03/12/45-million-drones-is-a-lot-of-drones-its-ukraines-new-production-target-for-2025/

77. Wired, 2 May 2024, https://www.wired.com/story/ukraine-drone-startups-russia/

78. New York Post, 29 September 2024, https://nypost.com/2024/09/29/world-news/ai-is-reshaping-drone-warfare-in-russian-and-ukraine/

79. Centre for Strategic & International Studies, 6 March 2025, https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare

80. Atlantic Council, 2 January 2025, https://www.atlanticcouncil.org/blogs/ukrainealert/missiles-ai-and-drone-swarms-ukraines-2025-defense-tech-priorities/

81. New York Post, 26 February 2025, https://nypost.com/2025/02/26/world-news/how-ukraines-drone-army-has-changed-the-battlefield-forever/

82. Forbes, 7 March 2024, https://www.forbes.com/sites/davidhambling/2024/03/07/how-ukraine-is-building-a-drone-army-at-its-kitchen-tables/

83. AI Alignment refers to the process of making AI systems behave in line with pre-determined values and intentions, such as those shared by humans. Solving the 'AI alignment problem' is considered one of the most critical challenges in the development of both, more powerful as well as safe AI systems.

84. MIT Media Lab, 'Designing social robots for older adults', 13 March 2019, accessed 10 April 2025, https://www.media.mit.edu/articles/designing-social-robots-for-older-adults/

85. NeuroLaunch, 'Autism Robots: Revolutionizing Support for Children on the Spectrum', 11 August 2024, accessed 10 April 2025.

86. Interesting Engineering, 'Photos: Humanoid robot girlfriend Aria created for companionship, costs $175K', 25 January 2025, accessed 10 April 2025, https://interestingengineering.com/photo-story/meet-aria-humanoid-robot-girlfriend

87. European Technologies, 'How South-East Asia's pig butchering scammers are using artificial intelligence technology', 16 May 2024, accessed 10 April 2025, https://europeantech.news/how-south-east-asias-pig-butchering-scammers-are-using-artificial-intelligence-technology/

88. We already see this trend with various IoT devices, such as vacuum robots, collecting sensitive data and being, at the same time, vulnerable to intrusion attempts. See https://www.abc.net.au/news/2024-10-11/robot-vacuum-yells-racial-slurs-at-family-after-being-hacked/104445408 or https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/ for reference.

89. CNN, 'Is it cruel to kick a robot dog?', 13 February 2015, accessed 10 April 2025, https://edition.cnn.com/2015/02/13/tech/spot-robot-dog-google/index.html

90. Ideon, 'Nothing Is Hidden Anymore. 'Welcome' to the Transparent Battlefield', 01 July 2025, accessed 05 December 2025, https://ideon.se/ideonscienceparknews/welcome-to-the-transparent-battlefield/

About the Europol Innovation Lab

Technology has a major impact on the nature of crime. Criminals quickly integrate new technologies into their modus operandi, or build brand-new business models around them. At the same time, emerging technologies create opportunities for law enforcement to counter these new criminal threats. Thanks to technological innovation, law enforcement authorities can now access an increased number of suitable tools to fight crime. When exploring these new tools, respect for fundamental rights must remain a key consideration.

In October 2019, the Ministers of the Justice and Home Affairs Council called for the creation of an Innovation Lab within Europol, which would develop a centralised capability for strategic foresight on disruptive technologies to inform EU policing strategies.

Strategic foresight and scenario methods offer a way to understand and prepare for the potential impact of new technologies on law enforcement. The Europol Innovation Lab's Observatory function monitors technological developments that are relevant for law enforcement and reports on the risks, threats and opportunities of these emerging technologies.

www.europol.europa.eu