The Future of Crime

Fighting Fire with Fire: Technology will Enable Law Enforcement Agencies to Prevent, Combat, and Investigate Tech-Driven Crime Effectively

WORLD
GOVERNMENTS
SUMMIT 2024

in collaboration with

pwc

To Inspire and Enable **The Next Generation of Governments**

The World Governments Summit is a global platform dedicated to shaping the future of governments worldwide. Each year, the Summit sets the agenda for the next generation of governments with a focus on how they can harness innovation and technology to solve universal challenges facing humanity.

The World Governments Summit is a knowledge exchange center at the intersection of government, futurism, technology, and innovation. It functions as a thought leadership platform and networking hub for policymakers, experts and pioneers in human development.

The Summit is a gateway to the future as it functions as the stage for analysis of future trends, concerns, and opportunities facing humanity. It is also an arena to showcase innovations, best practice, and smart solutions to inspire creativity to tackle these future challenges.

Table of Contents

Topics

Introduction

Technology is both a facilitator and a mitigator of crime in the 21st century. As advanced technologies have become part of everyday life, criminals have also integrated them into their methods and activities: encrypted messaging platforms are used for offenses including money laundering and migrant smuggling, increasing the perpetrators' global reach and with greater anonymity; biometrics are misused to impersonate victims and gain unauthorized access to sensitive information; drones, 3D printing, and blockchain facilitate the transportation of illegal items, including drugs, firearms, and currency; and there has been a surge in deepfake fraud using artificial intelligence (AI) to carry out identity theft, extortion, and espionage.

The UK Home Office categorizes cybercrimes in two ways: cyber-dependent crimes, which can only happen as a result of digital tools, including hacking and ransomware attacks; and cyber-enabled crimes, which are traditional crimes, including fraud, theft, or child exploitation, but "increased in their scale or reach" by the use of computers[1]. Both categories are set to define future criminal landscapes, offering higher rewards with lower risks.

As a result, it is crucial for law enforcement agencies (LEAs) to prioritize a tech-driven approach to preventing and combatting crime. Key use cases already implemented by LEAs include drones for surveillance, acoustic sensors for precise incident location and gunshot detection, and 3D imaging for reconstructing crime scenes. Similarly, use cases at the pilot stage in countries such as India include AI/machine learning (ML) for detecting suspicious behavior, blockchain for evidence storage, and autonomous vehicles for routine patrolling (e.g., as used by police forces in key Indian cities).

In this paper, we consider the success factors for increasing technology adoption by LEAs to realize their objectives by realigning their operational frameworks around three core pillars:

01 Using a tech-powered collaborative decision-making model to work closely with other government bodies, leveraging their deep understanding of crime trends and human behavior to shape policies and devise comprehensive programs.

02 Adapting to the evolving nature of crime by establishing tailored training programs to increase awareness of cybercrimes, enhance detection and prevention expertise, and ensure regulatory compliance.

03 Fostering a safer society through active engagement with communities, transparent communication, and forming partnerships for collective action.

Technology is the critical link between the three pillars, enabling LEAs to combat, prevent, and investigate crime efficiently. Moving forward, LEAs must integrate technology adeptly, ensuring its secure and optimal utilization. This includes ensuring data reliability and accuracy and the mitigation of technological biases while prioritizing data privacy; identifying the latest tech, mobilizing investments amidst complex regulations, and developing strategies to navigate these challenges; establishing an interoperable tech infrastructure, addressing vulnerabilities, and efficiently managing security with third-party providers; and recruiting skilled people, facilitating continuous training, and instituting standardized capacity-building programs.

LEAs will also need to focus on aligning technology investments with strategic goals, collaborating with industry experts to overcome obstacles, and investing in R&D in order to tackle head on the crimes of the future.

Section 1

The Role of Technology in The Evolution of Crime

Technological advancements have directly impacted criminal activities; digital tools mean that crime can now be carried out on a far larger scale, across international borders, and without criminals ever coming into direct contact with their victims. This has presented new challenges for policymakers and law-enforcement agencies, as criminals leverage technology to their advantage.

Figure 1 shows the changing growth rates of a range of crimes between 2014 and 2020, according to data from the United Nations Office on Drugs and Crime (UNODC). As can be seen, cyber-dependent and cyber-enabled crimes such as intercepting computer data increased at the fastest pace, while traditional offenses of theft and burglary, involving limited, if any, use of technology, declined.

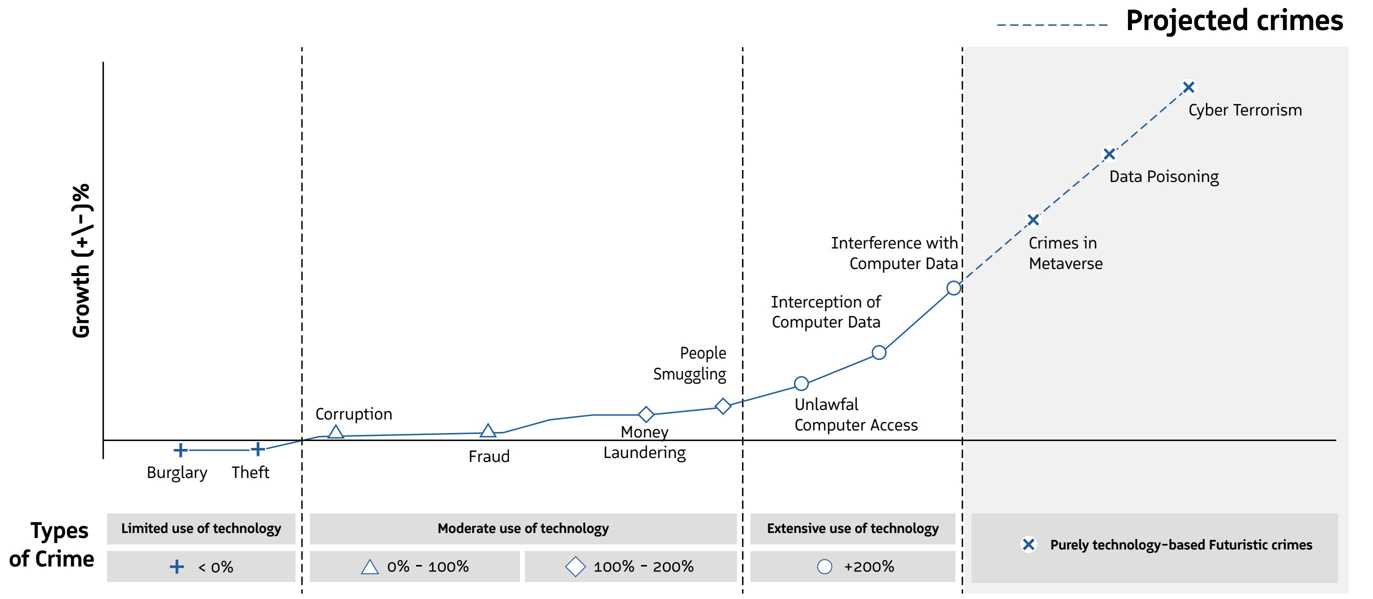
```
elif _operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
#one = bpy.context.selected_objects[0]
```

Section 1

The Role of Technology in the Evolution of Crime

Figure 1: Growth rates of crime types, 2014-20



Source: **Based on UN ODC Data: 2014-20**[2]

PwC analysis

Technological advancements have contributed to this change in two ways. While technology has improved surveillance and safety measures, leading to a significant decrease in conventional methods of theft, it has powered an upsurge in next-generation crimes. This has made clear how technology-driven methods can intensify criminal activities by making it easier to commit large-scale crimes from behind a phone or computer screen. For example, money laundering and people trafficking have notably surged, which may be partly due to the rise of encrypted messaging platforms that offer anonymity and global reach.

Computer and digital crimes, including data interception, interference, and unlawful access, are also on the rise. Criminals are leveraging digital channels more frequently, capitalizing on the low risk of detection, increased convenience, specialized skills, and greater gains for minimal effort.

Furthermore, unlawful activities that are purely dependent on technology are projected to shape the future crime landscape, according to the UNODC's data. Examples include breaches in the metaverse, injecting malicious data into databases to disrupt data-driven decisions, and attacking or damaging IT infrastructure.

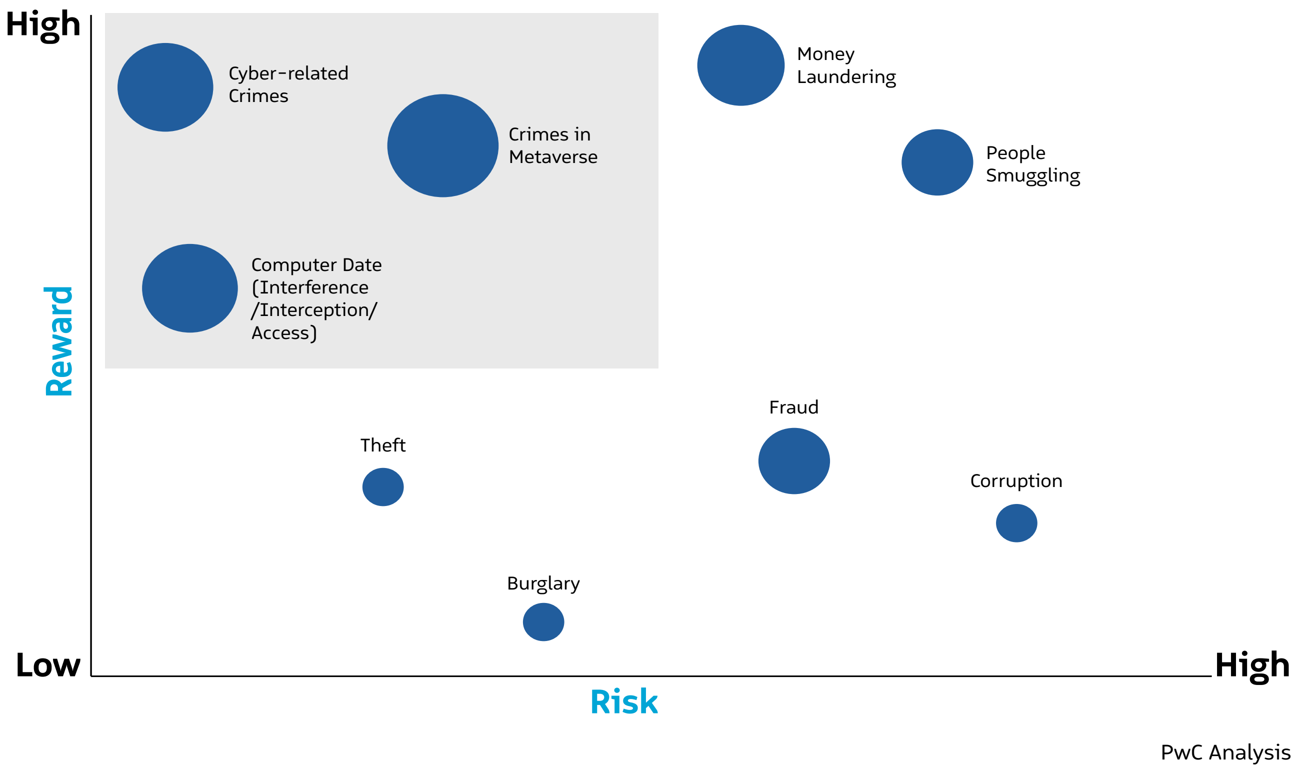
Note: The crime list shown in this chart is not exhaustive. While crimes such as gender-based violence and various forms of abuse within families have long been present, there is a rising trend in reporting and addressing them through legal measures. However, our focus in this paper is on technologically facilitated crimes.

Section 1

The Risk-Reward Matrix for Technology and Crime

The growth of technology-based crimes has altered the risk-reward balance of criminal activity. The risk is the chance of getting caught or facing hurdles during unlawful acts, while the rewards including money, possessions, or power. Figure 2 shows the degree of risk and reward in a range of crimes, where the degree of technology used is indicated by the size of the bubble. As can be seen, the most tech-enabled or dependent crimes, such as metaverse offenses, carry the highest reward for the lowest risk.

Figure 2: Mapping the risk, reward, and degree of technology used, by crime



PwC Analysis

Digital or online crimes such as data breaches, identity fraud, and money laundering are carried out discreetly using advanced technology, minimizing the chance of detection and maximizing rewards through access to valuable data and a global reach. Using technology allows for remote execution, concealed identities, and advanced methods that bypass traditional security measures. It also allows for access to a broader range of targets across borders, which makes law-enforcement actions more complex.

Moreover, technology streamlines criminals' efforts. For instance, automation widens the impact by exploiting vulnerabilities and enabling the simultaneous targeting of multiple applications. Limited victim awareness and inconsistent regulations further escalate such activities.

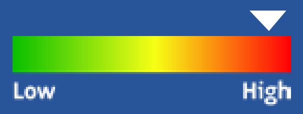
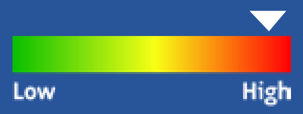
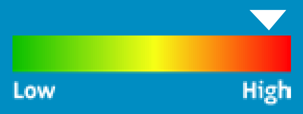
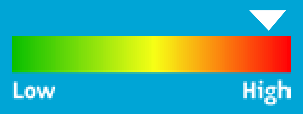
On the other hand, crimes that require minimal use of technology are generally less financially rewarding and come with a moderate level of risk. Theft, burglary, and fraud fall under this category, due to the additional physical effort required to effectively commit such crimes.

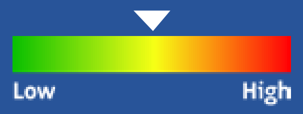
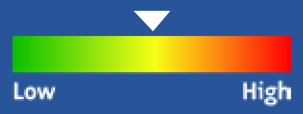
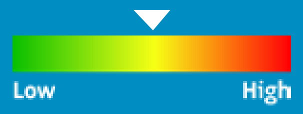
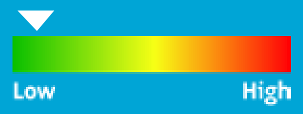
Section 1

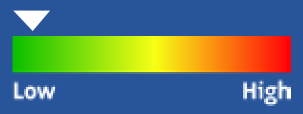
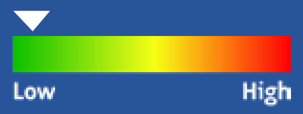
How Technologies are Being Used to Commit Crime

With technology acting as an enabler to commit higher-reward, lower-risk crimes, its role in criminal activity has become more critical than ever before. The world's growing dependency on digitally interconnected systems has also created opportunities to exploit the same technology to gain access to sensitive information, commit fraud, manufacture illegal consumables and guns, and launch sophisticated cyberattacks in exchange for ransoms. The anonymity of the digital era has opened up new avenues for criminal activities. Together, these changes present a formidable challenge to law enforcement and legal systems worldwide.

Below, we set out how a range of technologies are being used to commit crimes and disrupt public safety.

Technology	Description	Impacted crimes
Biometrics 	• Biometric data (fingerprints, iris scans, voice, and facial recognition) is being leveraged by criminals to impersonate victims for fraudulent activities and gain unauthorized access to sensitive information. • **Example:** In 2022, cybercriminals extorted around 150 citizens in India by cloning fingerprint data to commit identity theft and fraud.[3]	• Identity theft • Unlawful computer access • Fraud • Interception of computer data
Malware/ransomware 	• Malware and ransomware (a type of malware attack that restricts access to data or a system) have been repeatedly leveraged by criminals to compromise computer systems and networks with the intent to commit crimes and extort money from victims. • **Example:** Between October 2021 and April 2023, the criminals behind Qakbot (a botnet and type of malware spread through spam emails) extorted US$58 million in ransoms from victims.[4]	• Unlawful computer access • Interference with computer data • Interception of computer data • Financial crime • Ransom extortion
IoT 	• Criminals exploit vulnerabilities in IoT devices to compromise the security of victims by gaining access to private data and sensitive information. • **Example:** In 2021, Verkada, a US-based cloud surveillance service company, faced a security breach that exposed the private information of clients and live feeds from over 150,000 IoT-enabled surveillance cameras in various client locations.[5]	• Theft • Unlawful computer access • Identity theft • Interception of computer data
GPS 	• GPS technology is being used by criminals to track the whereabouts of victims and goods using location data in order to kidnap or steal them. • **Example:** Between April 2022 and October 2023, nearly 150 police reports were filed in the US alleging the use of AirTags by stalkers to track victims.[6]	• Theft • Burglary • Stalking and harassment • Kidnapping and extortion • Drug trafficking • Spying

Technology	Description	Impacted crimes
Drones  	• Drones or unmanned aircraft are being used by criminals and cartels for aerial surveillance, transporting illegal items such as weapons and drugs, and initiating attacks. • **Example:** In 2023, drones carrying explosives were used by insurgents to attack a military academy ceremony in a country in the Middle East, killing and injuring hundreds of people.[7]	• Burglary • Theft • Drug smuggling • Physical attacks • Aerial surveillance
3D Printing  	• Criminals are using 3D printing technology to create illegal consumables (drugs) and non-consumables (guns, keys and access cards, currency, and high-value products). • **Example:** In 2021, an illegal 3D-printed gun factory was raided in Spain from which several 3D printers, printed handgun frames, and other weapons parts were seized.[8]	• Fraud • Drugs and firearms manufacturing • Unauthorized replication of copyrighted objects
Blockchain/ cryptocurrency  	• Criminals leverage features such as anonymity at the point of creation, and rapid increases in exchange rates, to launder money and make transactions on the dark web using blockchain-based cryptocurrencies. • **Example:** In 2023, various blockchain networks were leveraged to launder illicit funds totaling US$7 billion through crypto wallets holding over 80 assets across 26 blockchains.[9]	• Money laundering • Fraud • Crypto-related crimes • Ransom attacks
Deepfakes (Image/video/audio)  	• In 2023, deepfake fraud attempts increased manifold, signifying its emerging status as one of the crimes of the future. Deepfakes leverage ML and deep learning (DL) models to create manipulated content, which is then exploited by criminals for fraudulent activities. • Example: In 2021, fraudsters in Dubai used deepfake AI technology to mimic the voice of a company director, executing US$35 million.[10]	• Unlawful computer access • Data and privacy breach • Identity theft • Fraud • Blackmail and extortion • Espionage • Deliberate mis- and disinformation

Technology	Description	Impacted crimes
Dark Web/TOR Networks  	• The dark web is made up of encrypted online content that is not found by conventional search engines. Users need specific browsers, such as TOR, which allows anonymous browsing by hiding IP addresses, to access dark web content. Criminals use it for a range of covert purposes, including drug dealing and sharing exploitative content. • **Example:** UK prosecutors successfully convicted three men in 2023 for distributing counterfeit drugs, including counterfeit Xanax on the dark web, which customers paid for using cryptocurrencies.[11]	• Fraud • Crypto-related crimes • Money laundering
Metaverse  	• The 3D virtual world of the metaverse is still at an early stage of development, and some real-world crimes such as harassment are hard to police when they occur between anonymous avatars. However, police forces and public-safety agencies are looking into how crimes, including fraud, data theft, and counterfeiting, will be tackled in the metaverse environment. • Example: Violent offenses in the metaverse could be treated as criminal offenses in the real world, Graeme Biggar, the head of the UK's National Crime Agency, said in 2023, because people wearing haptic suits, which allow the wearer to feel actions carried out in VR, would be able to feel the violent actions.[12]	• Fraud • Identity theft • Data and privacy breach • Harassment • Violent crime

Adoption Meter 🟩 Low 🟨 Meduim 🟥 High

Section 1

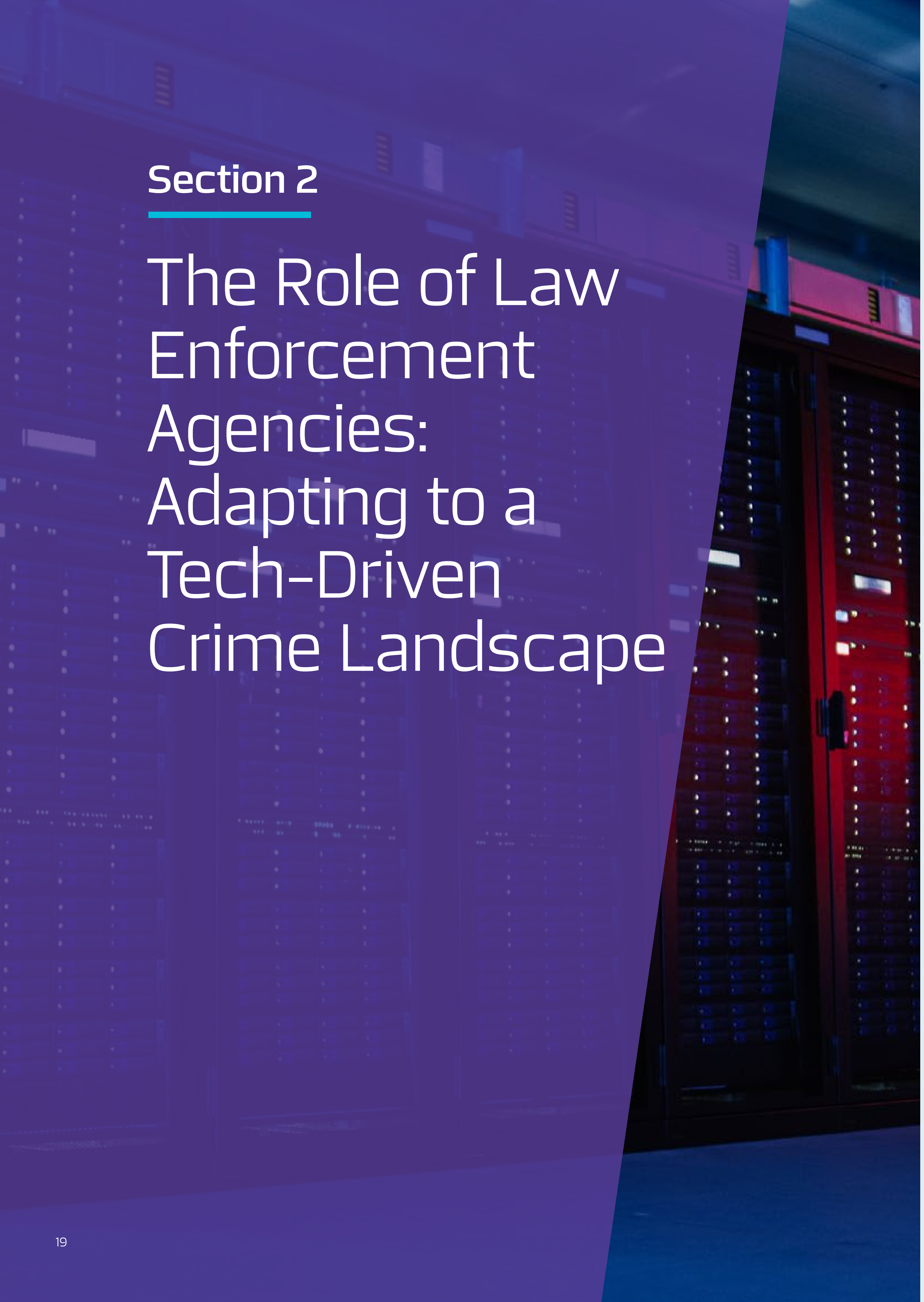
How Technology is Changing the Way Criminals Operate: What Does the Future Look Like?

Unlawful acts have always evolved along with society, and the integration of technology has only expedited the pace of change in recent years. Crimes such as identity fraud and drug trafficking have increasingly shifted online, leveraging social media, mobile applications (especially gaming applications where users are encouraged to share personal information), and end-to-end encrypted platforms, along with other advanced technologies.

Identity fraud, for example, has progressed from traditional methods of stealing people's personal information by trash diving or through phone scams to using networking platforms, biometric data, and advanced technologies such as deepfakes and the metaverse.

Identity fraud[13]	**Past**	**Present**	**Future**
	Data theft through telephone calls, using private information of either a deceased person or by theft of personal IDs, assuring false promises of monetary rewards	'Catfishing' (pretending to be someone else) via social media, mobile apps, emails and SMS, biometric data, and use of deepfakes, currently in the nascent stages	AI/ML-based deepfakes, biometric data theft, fraudulent activities in the metaverse with automated bots and targeted attacks, and the use of generative AI tools and large language models (LLMs)
Key technologies	Telephone and Letters	Biometrics and Deepfakes	Deepfakes, AI Voice Generators, Biometrics, and Metaverse

Drug trafficking[14]	**Past**	**Present**	**Future**
	Trafficking via consignments of goods or human carriers (voluntary or forced), online portals, prepaid disposable phones, and computers for carrying out transactions	Broadband radio frequencies, encrypted platforms, social media, communication via the dark web, and emerging use of drones	Transactions via cryptocurrency, synthetic (3D printed) drugs, and utilization of drones with advanced AI based video analytics
Key technologies	Digital Platforms, Websites, Social Media Chat Rooms, Online Multiplayer Gaming Applications	Social Media, Encrypted Platforms and Hardware, Drones	3D Printing, Blockchain, and Robotic Vehicles



Section 2

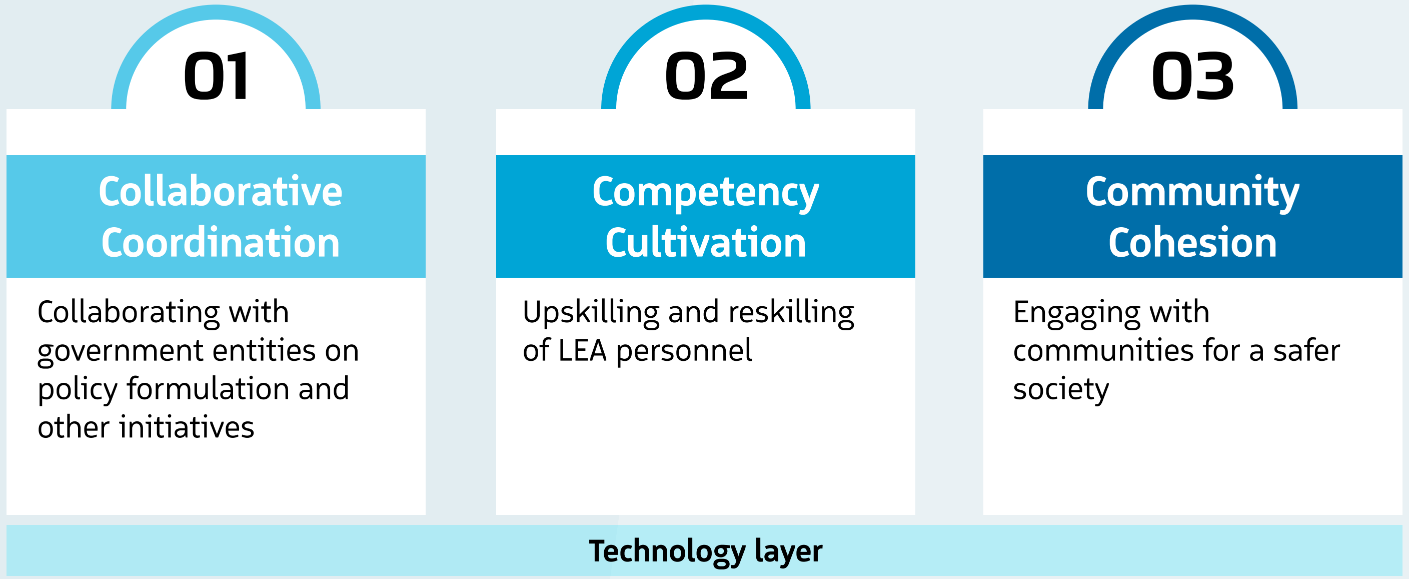
The Role of Law Enforcement Agencies: Adapting to a Tech-Driven Crime Landscape

As crime and complex criminal networks evolve and become increasingly international in the ways described above, LEAs face the challenge of keeping pace with the changes and upgrading their existing tools, processes, and procedures. They must swiftly grasp the way criminal networks are changing, to create effective crime-prevention strategies.

One such model is a tech-driven three-pronged approach, which we have set out here. It involves close collaboration with lawmakers to formulate adaptive regulations that address evolving safety needs; focusing on continuous training and upskilling of staff and leveraging cutting-edge technologies such as 5G-enabled mission-critical communications, AI, VR/AR, the metaverse, robotics, and other advancements; and establishing robust connections with the community to address local safety concerns, both through online and in-person engagement.

A Three-Pronged Model Based on a Tech-Driven Approach

Aligning operating models to reduce the impact of tech-driven crime:



01

Collaborative Coordination

Collaborating with government entities on policy formulation and other initiatives

02

Competency Cultivation

Upskilling and reskilling of LEA personnel

03

Community Cohesion

Engaging with communities for a safer society

Technology layer

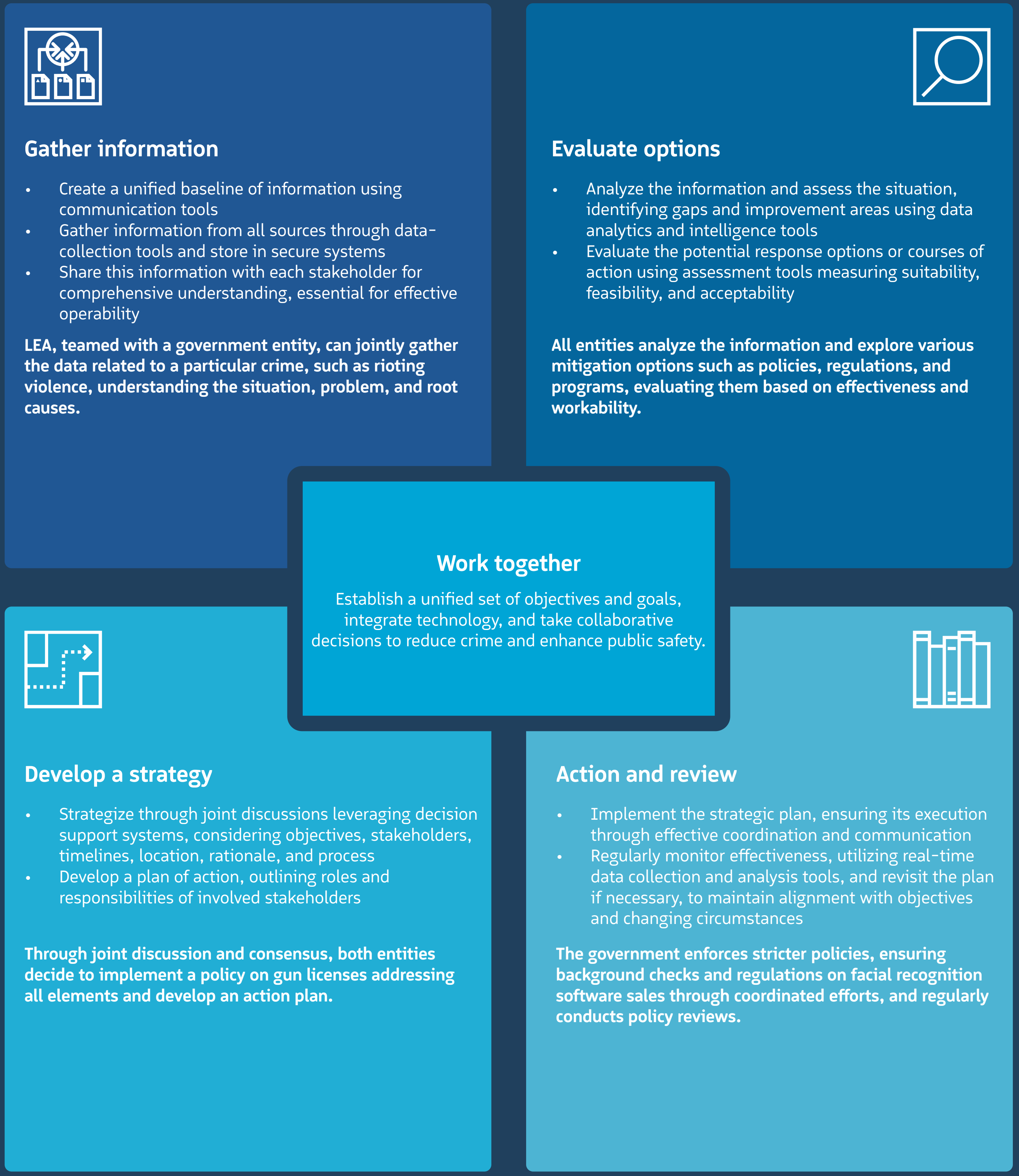
These endeavors enable LEAs to navigate the evolving crime landscape, diminishing the societal impact of crime and fostering a safer, more resilient society.

Pillar 1: Collaborating with Other Government Entities[15]

Around the world, LEAs often collaborate with other public entities to develop effective policies, regulations, and frameworks to reduce crime and enhance safety. In many cases, they use Collaborative Decision Models—a structured approach in which the various stakeholders work together to reach a consensus and formulate and execute informed decisions. As part of these collaborations, technology can be used to strengthen the different frameworks and models used by LEAs.

Advanced tools facilitate efficient data collection, communication, and assessment, streamlining operations. Modern data storage systems ensure secure accessibility, while data analytics aids informed decision-making by identifying patterns of crime and predicting potential threats. Utilizing data aggregation, high-risk areas or individuals are identified, enabling pre-emptive, multi-agency interventions to prevent crime. An example is Risk Terrain Modeling (RTM), a geospatial technology used by several law-enforcement agencies such as Merseyside Police, headquartered in Liverpool, northwest England. The RTM tool analyzes geographic areas and landmarks to identify places where the risk of crime is highest, allowing LEAs to assess crime trends, allocate resources efficiently, and proactively guide decision-making. The software's analytics aid in pinpointing problem areas and fostering tailored responses with partners.

A technology-powered collaborative decision model becomes pivotal for building streamlined operations, facilitating seamless teamwork and well-informed decisions by enhancing coordination among the agencies involved.



Gather information

- Create a unified baseline of information using communication tools
- Gather information from all sources through data-collection tools and store in secure systems
- Share this information with each stakeholder for comprehensive understanding, essential for effective operability

LEA, teamed with a government entity, can jointly gather the data related to a particular crime, such as rioting violence, understanding the situation, problem, and root causes.

Evaluate options

- Analyze the information and assess the situation, identifying gaps and improvement areas using data analytics and intelligence tools
- Evaluate the potential response options or courses of action using assessment tools measuring suitability, feasibility, and acceptability

All entities analyze the information and explore various mitigation options such as policies, regulations, and programs, evaluating them based on effectiveness and workability.

Work together

Establish a unified set of objectives and goals, integrate technology, and take collaborative decisions to reduce crime and enhance public safety.

Develop a strategy

- Strategize through joint discussions leveraging decision support systems, considering objectives, stakeholders, timelines, location, rationale, and process
- Develop a plan of action, outlining roles and responsibilities of involved stakeholders

Through joint discussion and consensus, both entities decide to implement a policy on gun licenses addressing all elements and develop an action plan.

Action and review

- Implement the strategic plan, ensuring its execution through effective coordination and communication
- Regularly monitor effectiveness, utilizing real-time data collection and analysis tools, and revisit the plan if necessary, to maintain alignment with objectives and changing circumstances

The government enforces stricter policies, ensuring background checks and regulations on facial recognition software sales through coordinated efforts, and regularly conducts policy reviews.

As LEAs navigate the multifaceted nature of their mission, adopting collaborative models and advanced technologies becomes a strategic imperative, providing a comprehensive and nuanced framework for addressing the challenges in ensuring public safety.

By leveraging technology, LEAs create an interconnected system where information flows seamlessly, enabling swift decision-making and coordinated efforts to address the complex challenges associated with crime reduction and community wellbeing. However, the decision-making framework and knowledge-sharing with other government agencies are as important as the technology itself; collaborative decision models help in the rounded assessment of situations, the formulation of strategic plans, and the execution of effective actions.

Using these ways of working, LEAs can harness collective insights, optimize resource allocation, and foster a proactive and unified approach to safeguarding communities.

Notable Global Approaches to Ecosystem Collaboration

Platform approach[17]

- Provide a secure and accessible platform for a ransomware grievance mechanism and resources to aid prevention
- Singapore Police Force (SPF) and the Cyber Security Agency of Singapore (CSA) were the primary entities engaged to develop a platform
- The organizations were responsible for providing aid to ransomware victims seeking recovery support
- Developed and deployed a one-stop solution platform that aligned with a policy initiative to strengthen the country's crime-prevention ecosystem and boost its capabilities

Framework approach[18]

- Created a joint alliance to analyze and outline countrywide guidelines on violence reduction
- Canadian Association of Chiefs of Police leading the initiative, with think tanks, policy experts, and police personnel assuming the active advisory roles
- Think tanks and experts provided necessary inputs based on empirical research to formulate a holistic framework that addresses the multiple dimensions of violent crime
- Developed a national-level framework that supports community safety, health, and wellbeing; knowledge transfer; and support for victims and families

Shared expertise approach[19]

- Created an innovative and inclusive space for prisoners to enhance cultural and social support
- A joint initiative between Ras Al Khaimah Police and the Sheikh Saud bin Saqr Al Qasimi Foundation for Public Policy Research
- Both parties synergized their expertise by outlining the preferences of the inmates as well as preparing the events organized on campus
- Launched a social club hosting a variety of events, social, cultural, and other activities, along with an electronic public library, computers, and classrooms

Pillar 2: Role of LEAs: Upskilling and Reskilling LEA Personnel

Worldwide, LEAs are adapting to the changing landscape of crime by leveraging upskilling and reskilling training programs. To develop this second pillar of the tech-driven approach, LEAs will create effective frameworks for training programs that update personnel with modern crime-response skills, including awareness of online crimes and increasing proficiency, especially with the help of immersive virtual reality (VR) based training sessions. Taking a structured approach fosters continuous learning and skill advancement through assessment, tailored planning, technology-integrated learning, and outcome evaluation.

Framework for Competency Cultivation

Assessment

Identifying emerging/required capabilities

Formulation

Creating a program in collaboration with an external party or in-house training team

Implementation

Imparting new skills and learnings using tech-enabled modes of delivery

Impact

Define and monitor the expected outcomes of the training courses

Notable Global Approaches to Competency Cultivation

Infusion of Advanced Technology

Dallas Police[20]

Assessment: Established a drone team to provide tactical support for fugitive searches and real-time monitoring of crime scenes using thermal imaging

Formulation: Developed dedicated training programs with Texas A&M University and DJI (a drone technology company)

Implementation: Launched an in-person training course at the university, along with other programs conducted by DJI on hardware and interface

Impact: Enhanced surveillance, effective use of drone and thermal monitoring equipment; and swift response

Crime-Specific Training

Kyrgyz Republic[21]

Assessment: Organized a training program to empower the relevant authorities in dealing with online/tech-enabled methods of drug trafficking

Formulation: Designed a dedicated program in coordination with the United Nations Office on Drugs and Crime and the Russian Federation

Implementation: Organized a five-day training workshop to educate LEA teams on the illegal documentation and financial technologies leveraged for drug-related crimes

Impact: Holistic knowledge of the evolving modus operandi of criminals; attained multi-faceted view on anti-drug trafficking operations

Enhancing Proficiency

South Wales Police[22]

Assessment: Established a Digital Forensics Unit to support other police units with computer and cellphone data recovery, vehicle telematics, and more

Formulation: Formed training modules and sessions both internally and in coordination with private entities (such as Cellebrite, a forensic technology company)

Implementation: Established South Wales Police training programs on digital forensics practices and co-led training sessions on effective utilization of the forensics tools and devices

Impact: Effective response, consistent enhancement in digital capabilities, and providing necessary support to police units

Pillar 3: The Role of LEAs: Engaging with Communities for a Safer Society

The third pillar of the approach recognizes that LEAs foster a safer society by actively interacting with communities, empowering residents through training programs and partnering for collective efforts. These multifaceted approaches contribute to a resilient and well-informed community, ultimately working toward the shared goal of creating a safer and more secure environment for all. Technology has a vital role to play, enabling real-time communication and information gathering from community groups, but in-person engagement remains an essential element of effective LEA work.

Three Elements of Effective Community Engagement

1

Communication

Engage with communities through direct interaction, fostering transparent communication, providing information during incidents, and gathering community feedback

2

Cohesion

Involve communities in collaborative efforts, address concerns through joint problem solving and strong partnerships to enhance safety, and build trust among citizens

3

Capacity Building

Empower communities by enhancing their capacity through training programs and workshops focused on safety measures and emergency preparedness

Notable Global Approaches to Community Cohesion

1

Communication

- **Tokyo Metropolitan Police Department** uses the Digi Police app, which keeps citizens updated on crimes in their local areas and provides crime-prevention tips[23]
- **Dubai Police's Smart Police Station** is an AI-driven smart channel available to the public to obtain policing services through video calls with officers, who speak seven languages[24]
- **Victoria Police** in Australia are proactively working with the community to seek feedback on how they can improve, through surveys, workshops, and town halls[25]

2

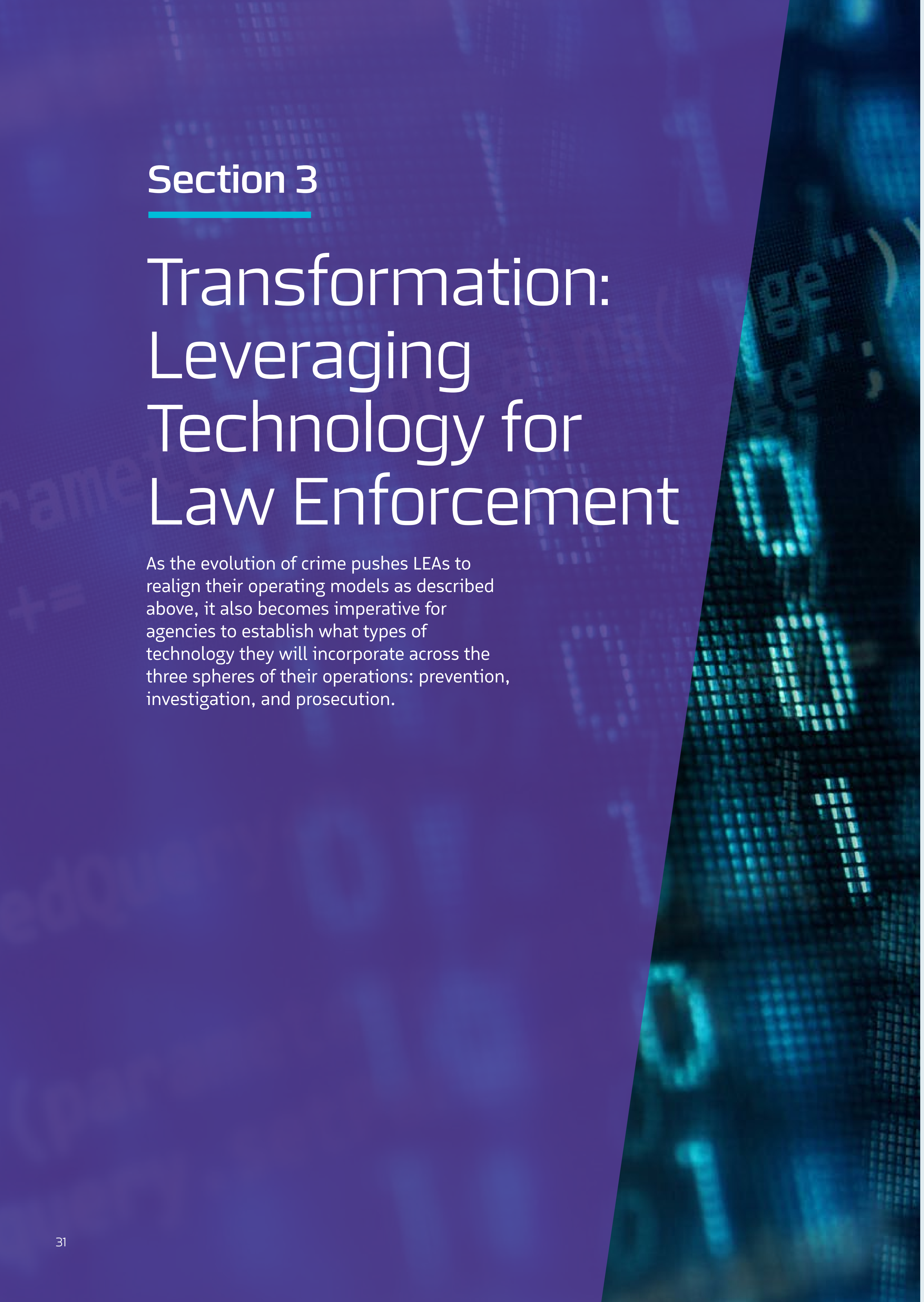
Cohesion

- **Chicago Police** monitors public sentiment by means of an online dashboard that features citywide data updated through surveys reflecting residents' perception of safety and trust in the police[26]
- **Vancouver Police Department** collaborates with the community through policing centers equipped with real-time data from citizen mobile applications, fostering strong partnerships to develop programs and initiatives that address local crime and safety concerns[27]
- **Mohalla Committees in India** are made up of a cross-section of society in local districts and act as the eyes and ears on the ground using body-worn cameras with video analytics generating behavioral alerts, becoming an integral part of community policing by assisting officers to prevent crime in their districts[28]

3

Capacity Building

- **Singapore Police Force** works closely with schools, organizing talks and exhibitions using gamification-based simulations to educate young people on crime prevention and safety measures[29]
- **The Victim Services and Crime Prevention Division** of Canada's Ministry of Public Safety develops and funds community programs, offering advice, training, and expertise to address specific local safety issues[30]



Section 3

Transformation: Leveraging Technology for Law Enforcement

As the evolution of crime pushes LEAs to realign their operating models as described above, it also becomes imperative for agencies to establish what types of technology they will incorporate across the three spheres of their operations: prevention, investigation, and prosecution.

Technology and the Three Key Spheres of LEA Operations

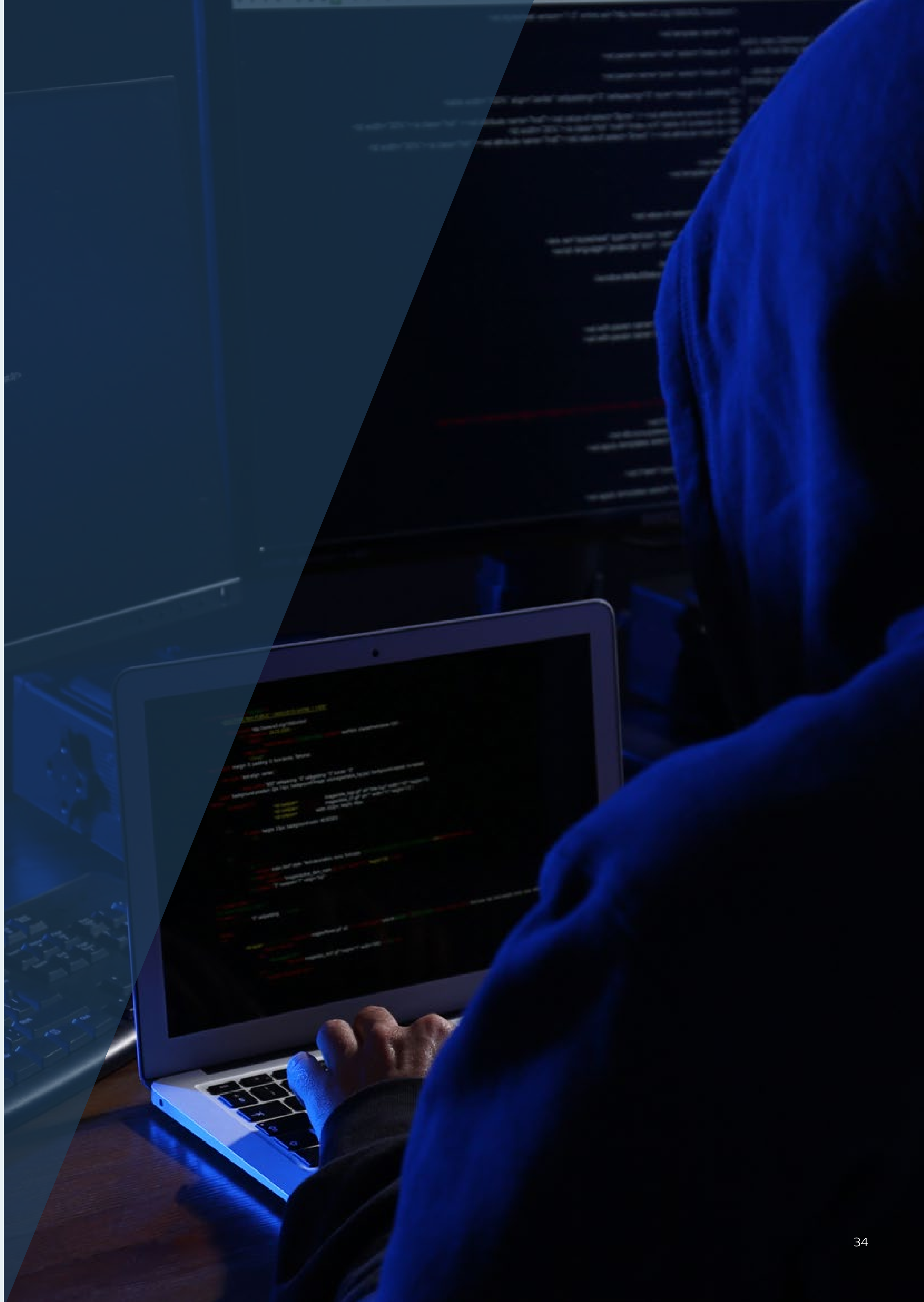
Definition	Key use cases	Technologies deployed
Prevention		
Any activity by an individual or group, public or private, that aims to reduce the probability of crime occurring.	Patrolling and surveillance, suspicious behavior detection, and criminal activity detection.	Robots, AI/ML, and autonomous vehicles
Investigation		
Assimilating supporting evidence to prove/disprove the occurrence of crime, identify the perpetrator of a crime or intended crime, and motives.	Evidence preservation, real-time gunshot detection, and crime-scene recreation.	Generative AI, acoustic sensors, and 3D imaging
Prosecution		
Initiating proceedings (in coordination with the judicial body), filing criminal charges, and holding a trial of a suspect after collecting sufficient supporting evidence.	Crime-scene recreation, evidence database systems, and identity verification.	AR/VR, blockchain, and AI/ML

Ranging from sophisticated surveillance systems and predictive analytics to facial recognition and biometric identification, technology enhances LEAs' overall effectiveness and adaptability and equips them with a formidable array of tools to counteract crime and uphold public safety. Globally, public-safety agencies and researchers are using and trialing the following technologies:

Use case	Application and technology integration	Notable examples
Prevention		
Surveillance 🟢🟢🟢	**Unmanned aerial vehicles or drones** are being deployed to monitor large areas, aiding surveillance.	During FIFA 2022, Qatar deployed autonomous interceptor drones to capture and disable potentially dangerous drones, ensuring public safety.[31]
Suspicious behavior detection 🟢🟢⚫	Advance **surveillance cameras** equipped with **AI and facial recognition** are being leveraged to detect potentially dangerous activities.	The National Police Academy in Japan will begin testing AI-equipped cameras with 'behavior and object detection' technology to spot guns and suspicious behavior in crowds. However, the use of facial recognition has raised concerns about citizens' privacy in countries including the UK.[32]
Public safety awareness 🟢🟢🟢	**Metaverse** platforms with **virtual venues** are being adopted for public-safety education and awareness against online scams.	Hong Kong Police launched a metaverse platform, CyberDefender, to educate the public on cybercrime challenges and prevention strategies.[33]
Autonomous patrolling 🟢🟢⚫	**Autonomous vehicles** equipped with **AI, facial recognition, and cameras** are being adopted for **patrolling**, ensuring safer communities.	Dubai Police plans to leverage AI-based self-driving vehicles for patrolling residential areas and monitoring criminal activities.[34]

Use case	Application and technology integration	Notable examples
Investigation		
Real-time gunshot detection 🟢🟢🟢	**Acoustic sensor-based gunshot detection systems** are being deployed across public spaces to identify the location of gunshot incidents.	Cleveland Police, USA, deployed acoustic sensor-based gunshot detection technology to accurately identify an incident's location and number of shots fired.[35]
Crime-scene recreation 🟢🟢🟢	**3D imaging devices** equipped with **laser and high-resolution cameras** are being used for **forensic evaluation** of crime spots in 3D.	Delhi Police, India, leveraged a 3D scanning device for crime-scene recreation and to boost forensic evaluation efficiency.[36]
Marine inspection 🟢🟢⚪	**Deterrence drones** equipped with **GPS, scanners, and high-resolution cameras** are widely leveraged for inspecting cargo.	Dubai Police introduced deterrence drones to conduct inspections on traditional wooden dhow ships, targeting smuggled items in bulkheads or hidden compartments.
Suspect sketches 🟢⚪⚪	**Generative AI**'s ability to generate content based on user prompts and inputs is being explored by researchers for **generating suspect sketches and response to FAQs.**	Portuguese computer scientists are exploring the use of generative AI for generating suspect sketches using the Dall-E 2 deep learning model.[37]
Drug detection 🟢⚪⚪	**Portable drug detection kits** can detect the presence of a **variety of drugs** as part of efforts to uncover and stop drug crimes.	NPA (South Korea) in collaboration with the National Forensic Service is developing a portable drug kit that can immediately detect 10 types of illegal drugs to prevent people having their drinks spiked.[38]
Prosecution		
Witness visualization 🟢🟢🟢	Real-time VR systems are being adopted to virtually explore the crime and present high-quality evidence.	Beijing First Intermediate People's Court in China incorporated the 'VR Witness Visualization System' for trials, enabling witnesses to recreate crime scenes with VR headsets.[39]
Evidence storage and sharing 🟢🟢⚪	**Blockchain** is being adopted for **evidence storage and secure sharing** across departments.	His Majesty's Courts and Tribunal Services in the UK has started a pilot program testing blockchain to streamline court processes such as handling digital evidence.[40]
Rehabilitation		
Upskilling 🟢🟢🟢	**Augmented reality-based simulation** is being incorporated as part of **skill development** among prisoners.	Langi Kal Kal prison, Australia, introduced AR-based training in welding as a part of the skill development program for inmates[41], aimed at increasing their chances of employment upon release.
Real-life scenario simulation 🟢🟢⚪	**Virtual-reality** platforms equipped with sensors are being adopted to simulate real-life scenarios for prisoners, to help with **positive behavioral responses** upon release.	Rikosseuraamuslaitos (Finnish Criminal Sanctions Agency) launched a VR program to create the kind of real-life situations that prisoners are expected to encounter post-release.[42]

🟢🟢🟢 Implemented 🟢🟢⚪ Pilot/Trial phase 🟢🟢⚪ R&D phase



Section 4

A Framework for Adopting Tech-Enabled Operating Models for Law Enforcement

In their commitment to keeping communities safe as technology changes the nature of crime, LEAs are turning to new and emerging technologies to improve their capabilities. While these tools bring exciting possibilities, it is important to consider the technology itself within the context of its alignment with the agency's broader strategy, the existing infrastructure, and the people who work there. The seamless integration of these elements is pivotal: successful technology adoption goes beyond simply bringing in new tools; it is about ensuring that these elements work harmoniously within the operational framework of LEAs and address the evolving needs of the communities they protect.

The **four core considerations** are workforce, infrastructure, strategy, and technology (WIST). To effectively integrate technology into LEAs' core functions, the WIST framework serves as a guiding principle for constructing and reshaping LEAs' operational models to meet evolving demands.

WIST Framework: Key Considerations[43]

Workforce

- **Hiring people with relevant technical skills:** Recognizing the need for skilled resources in line with the evolving technology landscape and enhancing the integration of new technologies with a skilled workforce
- **Continuous capacity-building programs:** Developing training programs and effective mechanisms to measure training outcomes to ensure employees have the up-to-date skills they need

Infrastructure

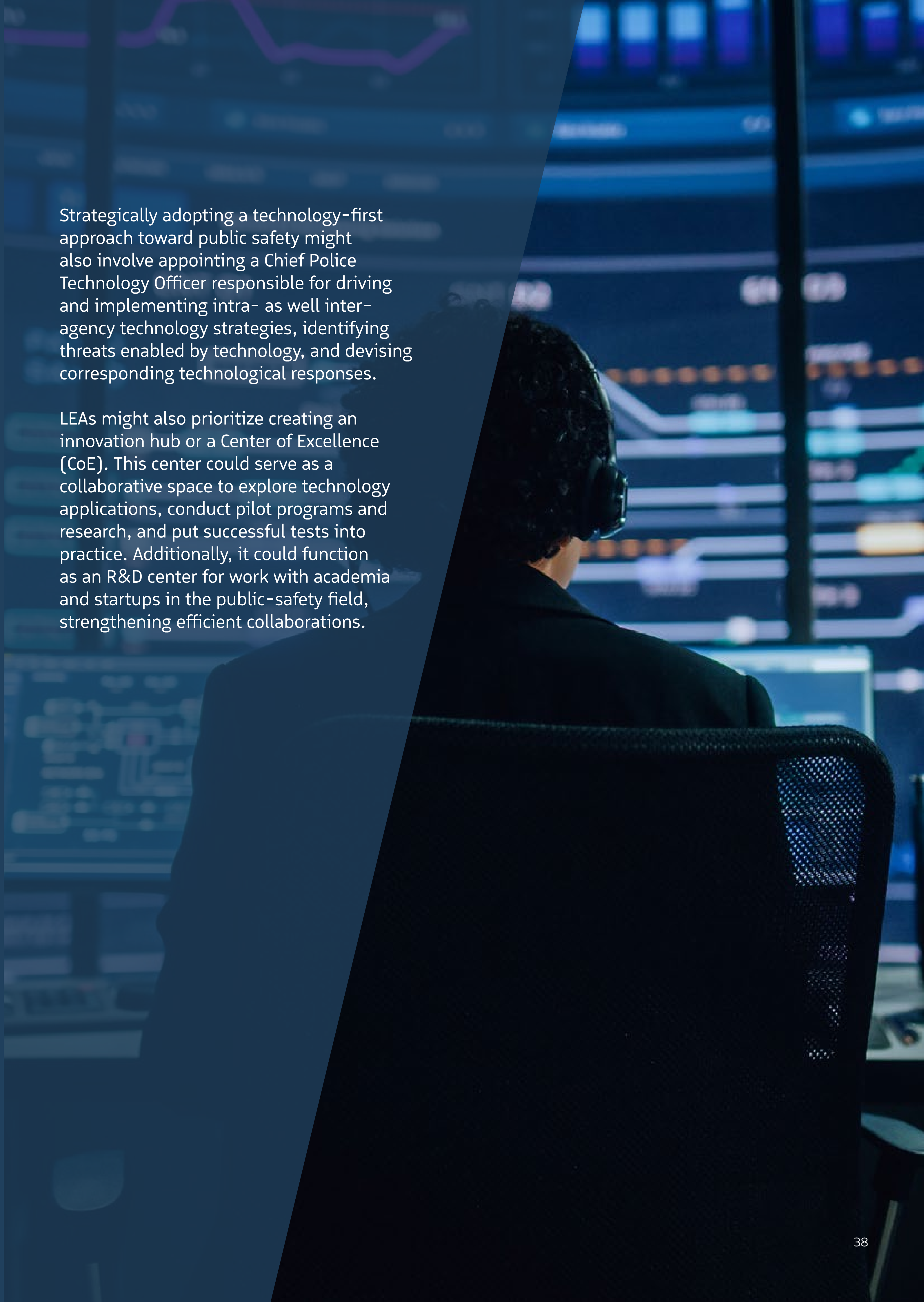
- **Ensuring system interoperability:** Enforcing standard protocols and integration of disparate systems can help ensure interoperability. This promotes seamless collaboration and data sharing, expediting decision-making processes
- **Addressing vulnerabilities for operational safety:** Robust cybersecurity policies and safety measures must be in place to ensure smooth operations and safeguard critical data from cyberattacks and breaches
- **Handling security concerns with third-party service providers:** Minimizing dependency on external entities and ensuring strict adherence to service level agreements (SLAs) is essential to maintain control over critical systems and mitigate the risk of attacks and breaches

Strategy

- **Identifying the latest technologies:** Phasing out outdated systems by regular assessments of existing technology infrastructure, maintaining existing systems, and scouting new technologies that can further enhance operational efficiency
- **Prioritizing investment decisions:** Conducting thorough analysis to identify key areas needing technology investment, aiding budget management, and addressing modern challenges efficiently
- **Navigating complex regulatory landscapes:** Ensuring technology adoption complies with laws and staying updated on legal advancements for specific technology use

Technology

- **Ensuring reliability and accuracy:** Implementing human oversight in automated processes and data quality assurance is a crucial consideration to maintain reliability. This prevents errors that could compromise decision-making in public-safety operations
- **Overcoming tech-inherent biases:** Pre-emptive testing for biases becomes necessary to avoid discriminatory outcomes in widely used applications such as facial recognition
- **Safeguarding data privacy:** Addressing concerns about personal information use maintains public trust. Ensuring data privacy through technology-based safeguards, compliance measures, and techniques such as masking is vital



Strategically adopting a technology-first approach toward public safety might also involve appointing a Chief Police Technology Officer responsible for driving and implementing intra- as well inter-agency technology strategies, identifying threats enabled by technology, and devising corresponding technological responses.

LEAs might also prioritize creating an innovation hub or a Center of Excellence (CoE). This center could serve as a collaborative space to explore technology applications, conduct pilot programs and research, and put successful tests into practice. Additionally, it could function as an R&D center for work with academia and startups in the public-safety field, strengthening efficient collaborations.

Conclusion

Amid the changing crime landscape, technology is double edged—fueling illicit activities and empowering law-enforcement efforts. The surge in tech-enabled and dependent crimes, such as hacking and data breaches, underscores the impact of technology in reshaping criminal tactics. As bad actors work with increasingly advanced technologies such as deepfakes, AI voice generators, and the metaverse, LEAs are confronted with a transformative mandate. Worldwide, agencies are recalibrating their strategies through upskilling initiatives and adding new tech capabilities. However, despite advancements, obstacles remain, including technology-specific limitations, cybersecurity vulnerabilities, and how to link strategy and use of technology. To navigate this terrain, LEAs must adopt an adaptive approach, aligning technology investments, collaborating with industry experts, and fostering continuous skills development.

The future of crime prevention and public safety will rely heavily on the use of emerging technologies. LEAs' commitment to fostering safer societies involves harnessing technology judiciously, leveraging expertise, and fortifying partnerships for collective resilience against the evolving face of crime.

About PwC

At PwC, our purpose is to build trust and solve the most important challenges facing government, businesses and communities. We are on a mission, bringing our community of solvers together to deliver human-led, tech-powered solutions from strategy through to execution, developing talent and scaling exponential opportunities that deliver sustained outcomes for our clients for future generations. We're a network of firms in 151 countries with nearly 364,000 people who are committed to delivering quality in assurance, advisory and tax services.

Find out more and tell us what matters to you by visiting us at [www.pwc.com.](http://www.pwc.com)

Contacts

Rajat Chowdhary
Partner, Technology Consulting, PwC Middle East
rajat.c.chowdhary@pwc.com

Sharang Gupta
Director, Public Safety Technology, PwC Middle East
sharang.g.gupta@pwc.com

Vishesh Kalia
Director, Public Safety Technology, PwC Middle East
Vishesh.k.kalia@pwc.com

Andrew Morley
Director, Policing and Public Safety, PwC Middle East
andrew.morley@pwc.com

Endnotes

1. “Cyber crime: A review of the evidence,” UK Home Office, October 7, 2013, https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence
2. “Corruption and economic crime,” United Nations Office on Drugs and Crime, https://dataunodc.un.org/dp-crime-corruption-offences
3. Naveen Kumar, “Cyber fraud, cloned fingerprints: 7 arrested for fraudulent withdrawal of Rs 14L,” Deccan Chronicle, June 16, 2022, https://www.deccanchronicle.com/nation/crime/160622/cyber-fraud-cloned-fingerprints-7-arrested-for-fraudulent-withdrawal.html
4. Alexander Culafi, “FBI, Justice Department dismantle Qakbot malware,” TechTarget, August 30, 2023, https://www.techtarget.com/searchsecurity/news/366550298/FBI-Justice-Department-dismantle-Qakbot-malware
5. Chaim Gartenberg, “Security startup Verkada hack exposes 150,000 security cameras in Tesla factories, jails, and more,” The Verge, March 8, 2021, https://www.theverge.com/2021/3/9/22322122/verkada-hack-150000-security-cameras-tesla-factory-cloudflare-jails-hospitals
6. Brandon Vigliarolo, “Three dozen plaintiffs join Apple AirTag tracking lawsuit in amended complaint,” The Register, October 13, 2023, https://www.theregister.com/2023/10/13/three_dozen_plaintiffs_join_apple_airtag_suit/
7. David Gritten, “Syria war: Dozens killed in drone attack on graduation ceremony,” BBC, October 6, 2023, https://www.bbc.com/news/world-middle-east-67017010
8. “Spain dismantles workshop making 3D-printed weapons,” BBC, April 19, 2021, https://www.bbc.co.uk/news/world-europe-56798743
9. “$7 billion in illicit funds laundered across multiple blockchains in 2023: Report,” The Hindu, October 6, 2023, https://www.thehindu.com/sci-tech/technology/7-billion-illicit-funds-laundered-across-multiple-blockchains-2023-report/article67387419.ece
10. Thomas Brewster, “Fraudsters cloned company director’s voice in $35 million heist, police find,” Forbes, October 14, 2012, https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=798262c7755
11. “Three imprisoned in one of Britain’s largest dark web drugs cases,” Crown Prosecution Service, March 31, 2023, https://www.cps.gov.uk/wessex/news/three-imprisoned-one-britains-largest-dark-web-drugs-cases
12. Martin Bentham, “Rapes and murders in the metaverse could be treated as criminal offences, says National Crime agency boss,” The Standard, December 29, 2023, https://www.standard.co.uk/news/crime/rapes-murders-criminal-offences-virtual-reality-metaverse-nca-b1128084.html
13. facia.ai/blog/history-of-identity-fraud-and-identity-theft-measure/
14. https://www.unodc.org/southasia/frontpage/2012/october/drug-mules -swallowed-by-the-illicit-drug-trade.html https://www.itssverona.it/by-water-or-air-how-drones-are-changing-the-face-of-drug-trafficking https://sundayguardianlive.com/news/new-technology-making-drug-traffickers-efficient https://webz.io/dwp/drug-trafficking-in-the-dark-web-in-2023/
15. “The Joint Decision Model,” JESIP, https://www.jesip.org.uk/joint-doctrine/the-joint-decision-model-jdm/
16. “Merseyside Police adopts geospatial technology to support crime prevention,” Merseyside Police, September 22, 2023, https://www.merseyside.police.uk/news/merseyside/news/2023/september/merseyside-police-adopts-geospatial-technology-to-support-crime-prevention/?_cf_chl_tk=3d99I015flp2hpOSLIZeMBdsKj3GYQd-5mK1hNBkLUQg-1702889139-0-gaNycGzNGLs
17. “Launch of the ransomware portal – a one-stop access to ransomware related resources,” Singapore Police Force, Octiober 17, 2023, https://www.police.gov.sg/media-room/news/20231017_launch_of_the_ransomware_portal_a_one_stop_access_to_ransomware_related_resources
18. “National framework for collaborative police action on intimate partner violence,” University of New Brunswick and the Canadian Association of Chiefs of Police, March 2016, https://cacp.ca/index.html?asst_id=1200
19. “Police launch social club for prison inmates with library, classrooms, computers,” Khaleej Times, September 27, 2022, https://www.khaleejtimes.com/uae/uae-police-launch-social-club-for-prison-inmates-with-library-classrooms-computers
20. Jim McGill, “Dallas PD done unit launhces, following years of study,” Drone Life, March 8, 2022, https://dronelife.com/2022/03/08/dallas-pd-drone-unit-after-years-of-research-department-takes-flight/ and “sUAS for public safety personnel,” Texas A&M Engineering TEEX, https://teex.org/class/sap151/

21. “UNODC and Russian Federation enhance capacity of law enforcement of Kyrgyzstan in countering illegal drug trafficking via Internet,” United Nations Office on Drugs and Crime, https://www.unodc.org/centralasia/en/news/unodc-and-russian-federation-enhance-capacity-of-law-enforcement-of-kyrgyzstan-in-countering-illegal-drug-trafficking-via-internet.html
22. Adam Jaffe, “How South Wales Police manage the rapid pace of digital transformation to keep citizens safe,” Cellebrite, June 29, 2021, https://cellebrite.com/en/how-south-wales-police-manage-the-rapid-pace-of-digital-transformation-to-keep-citizens-safe/
23. The Associated Press, “Mobile app to warn gropers, get help, proves popular in Japan,” The Asahi Shimbun, May 23, 2019, https://www.asahi.com/ajw/articles/13063922
24. “Dubai police take personal security to a whole new level,” City Security, September 12, 2022, https://citysecuritymagazine.com/editors-choice/dubai-police-take-personal-security-to-a-whole-new-level/
25. “Service delivery consultation,” Victoria Police, https://www.police.vic.gov.au/service-delivery-consultation
26. “Chicago Police setiment dashboard,” Chicago Police Department, https://home.chicagopolice.org/statistics-data/data-dashboards/sentiment-dashboard/
27. https://vpd.ca/policies-strategies/strategic-planning/
28. “Mohalla Committees,” Solapur Police, https://solapurpolice.gov.in/Mohalla-Committees
29. “Police Pal,” Singapore Police Force, https://www.police.gov.sg/Community/Community-Programmes/Police-Pal#:~:text=SPF%20%7C%20Police%20Pal,Community%20Programmes&text=The%20programme%20was%20developed%20from,through%20interesting%20and%20interactive%20activities
30. “About the Victim Services and Crime Prevention Division,” British Columbia, https://www2.gov.bc.ca/gov/content/safety/crime-prevention/community-crime-prevention/about-us#:~:text=The%20Victim%20Services%20and%20Crime%20Prevention%20Division%20of%20the%20Ministry,expertise%20on%20community%20safety%20issues
31. Chris Vallance, “World Cup to use drones to help protect stadiums,” BBC, July 23, 2022, https://www.bbc.com/news/technology-62243427
32. Matthew Phelan, “Japan to deploy eerie ‘behavior detection’ technology to snare criminals before they commit crime – similar to that in Minority Report,” Daily Mail, July 20, 2023, https://www.dailymail.co.uk/sciencetech/article-12320413/Japan-deploy-eerie-behavior-detection-technology-snare-criminals-commit-crime-similar-Minority-Report.html
33. “About CyberDefender,” Hong Kong Police Force, https://cyberdefender.hk/en-us/about-us/
34. “Dubai Police unveils driverless, AI-powered patrol cars,” AsiaOne, October 25, 2023, https://asiaone.co.in/dubai-police-unveils-driverless-ai-powered-patrol-cars/
35. “City of Cleveland expands ShotSpotter technology to all five neighborhood police districts,” Office of the Mayor, City of Cleveland, May 23, 2023, https://mayor.clevelandohio.gov/news/city-cleveland-expands-shotspotter-technology-all-five-neighborhood-police-districts
36. Abhay Singh, “3D equipment to let Delhi cops analyse crime scene better,” The Times of India, April 2, 2023, https://timesofindia.indiatimes.com/city/delhi/3d-equipment-to-let-delhi-cops-analyse-crime-scene-better/articleshow/99180315.cms
37. Michelle Taylor, “AI software can create suspect sketches,” Forensic, February 8, 2023, https://www.forensicmag.com/594323-AI-Software-Can-Create-Suspect-Sketches/
38. “Police unveil newly developed drug detection kit,” The Korea Times, May 3, 2023, https://www.koreatimes.co.kr/www/nation/2024/01/113_350309.html
39. Liang Chenyu, “VR technology called to the stand in Beijing court,” Sixth Tone, March 2, 2018, https://www.sixthtone.com/news/1001846
40. David Hundeyin, “UK government pilots storage of digital evidence on a blockchain,” CCN, March 4, 2021, https://www.ccn.com/uk-government-pilots-storage-of-digital-evidence-on-a-blockchain/
41. Nick Baker and Belinda Sommer, “The training program that’s both helping prisoners and tackling Australia’s skills shortage,” ABC, December 13, 2022, https://www.abc.net.au/news/2022-12-14/welding-prisoners-australia-skills-shortage/101765704
42. “Rikosseuraamuslaitos intoruces vitual-reality assisted rehabilitation for prisoners to practice everyday situations,” Helsinki Times, May 22, 2023, https://www.helsinkitimes.fi/themes/themes/science-and-technology/23613-rikosseuraamuslaitos-introduces-virtual-reality-assisted-rehabilitation-for-prisoners-to-practice-everyday-situations.html#:~:text=The%20company%27s%20programs%20allow%20for,receiving%20feedback%2C%20and%20job%20interviews
43. https://assets.college.police.uk/s3fs-public/2020-08/Future-Operating-Environment-2040-Part3-Challenges.pdf

WORLD
GOVERNMENTS
SUMMIT

JOIN THE CONVERSATION

@WorldGovSummit

www.worldgovernmentssummit.org