Leveraging digital intelligence to foster the management of convergent national security, public safety and cyber security

The most compelling answers to national safety and security challenges lie not with technology alone but in how both government organisations and critical infrastructure providers structure and manage their operating models and technology deployments at the national level.

pwc.com/me

Table of **Content**

In a digitally connected age, convergent national security is a prime concern for governments everywhere. The growth of the data economy, interconnected worlds of individual actors, state and private organisations, smart cities and global communication through digital devices have created immense opportunities for value creation. But at the same time, they have introduced new threats to security that governments have to address.

No single technology solution can ensure safety and security. Governments can, however, integrate a range of technologies into a powerful platform that can identify threats to convergent national security, whether it's public safety or potential attacks from internal or external malign actors.

This paper discusses how to design and implement a solution that allows law enforcement and national intelligence authorities to use automation to identify and track potential threats to safety and security more effectively than ever before. The solution uses rule-based pattern matching, artificial intelligence (AI), personal and public and private organisational data to meet the needs of state security and public safety while preserving citizens' privacy.

01

Smart cities and convergent national security

The “smart city” is emerging as the template of the urban future. According to the World Bank, more than half of the world’s population lives in cities. By 2050, that figure to reach around 70%1, and by that time, many of the world’s largest cities will have become “smart cities.”

They will have environments where digital connectivity will generate vast amounts of data on everything in the urban space. For convergent national security, this will be of profound importance. Managing the data for public safety and privacy will become a primary responsibility for any organisation concerned about security.

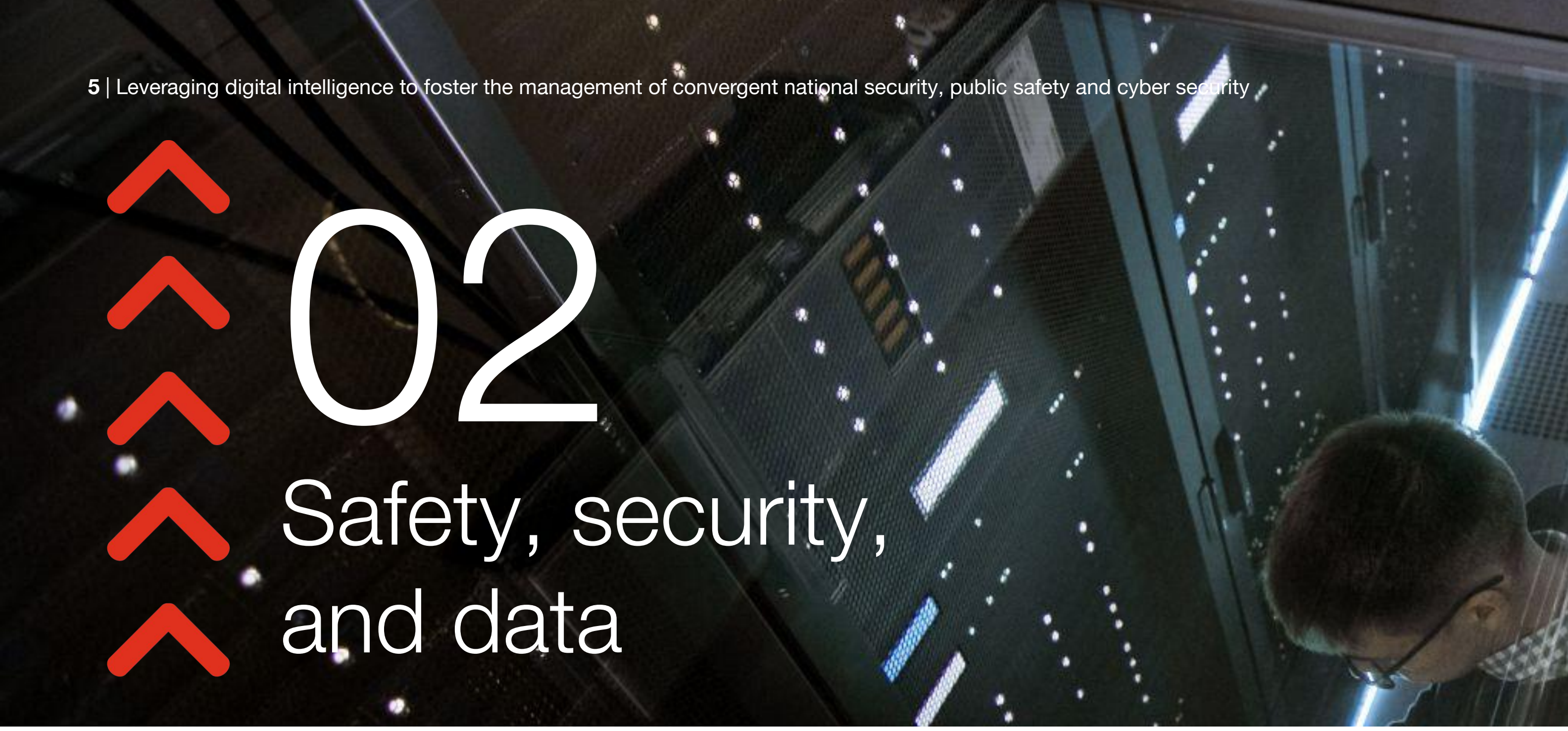
Policymakers should be aware of the rapid development of smart city communication and surveillance technologies, which now allow reactive and predictive approaches to safety and security. These will provide a rich data source for which convergent national security organisations must have the analytical capacity and appropriate privacy controls to ensure acceptability.

Smart City technology will be one of the defining features of Egypt's New Administrative Capital (NAC), currently under construction to the east of Cairo. The NAC, which is a central plank of Egypt's Vision 2030 sustainable development plan, will include technologies such as a wide area network of smart public safety monitoring cameras, sensors and solutions, AI-powered water and waste management systems, and other applications that will draw on recent Smart City developments around the world.

These technologies include the creation of real-time AR (Augmented Reality)-based virtual command centres capable of monitoring, controlling and managing incidents; deployment of self-learning AI bots as command centre operators that emulate human intelligence to perform sensor monitoring, anomaly detection, alarms processing, correlation and incident management; drone-based predictive crowd management using correlations between real-time and historical data, processed by machine learning; multi-sensor detectors including automated audio analytics that can detect sounds from red-flag events like breaking glass or gunshots, and determine whether conversations are predictive of imminent conflict, and smell analysis that detects gas leaks or hidden explosives and narcotics. Smart cities will also feature autonomous mobile units equipped with IoT sensors, able to move in complex environments and communicate in real-time.

These technologies are evolving rapidly to supplement the more familiar urban data sources, such as traffic monitoring and management and usage patterns of power and other utilities. With applications in convergent national security and public safety, smart city data will demand responses from security organisations and policymakers.

[1] https://www.worldbank.org/en/topic/urbandevelopment/overview#:~:text=Today%2C%20some%2056%25%20of%20the,people%20will%20live%20in%20cities



02 Safety, security, and data

National policymakers and security agencies have traditionally considered public safety and domestic state security as different spheres.

Public safety issues typically include the safe operation of national physical infrastructure, power generation and grids, telecommunications services, transport infrastructure and operation management, and utilities such as water, drainage and urban management services. State security comprises defences against malign actors, spying, and other manifestations of inter-state conflict, carried out through cyber channels.

In recent years, these two realms have begun to overlap. As organisations and physical infrastructure become increasingly digitalised and connected, they have become vulnerable to attack and capable of risk mitigation through digital channels. And thus national security has become a convergent issue, encompassing both the physical and virtual (or digital) domains.

Furthermore, today a malign actor may be more likely to exploit a cyber-vulnerability in critical infrastructure to set a physical bomb, as the first is usually faster, most effective and can be executed from a remote location; at the same time, a public safety incident such as a power station failure or a destructive natural event may be predictable and manageable through digitally-assisted monitoring and anticipation.

Security and safety have become digital data issues and can be managed through digital techniques. The two may have different state responses, but common technology tool sets can bear on both. Yet ultimately, the answer to growing safety and security risk must be primarily organisational: digital technology may provide the tools for effective security policy, but effective organisations must deliver the solution.

03

Cybersecurity and ‘critical infrastructure’

The definition of ‘critical infrastructure’ must include all core public services needed to run a modern state, where the failure or disruption of anyone could seriously impact a nation’s health, economy or even political stability. At a minimum, this must include energy and utilities such as power, water supply, transportation infrastructure including road, rail, air and port facilities, healthcare and the increasingly digitalised realm of health records and service delivery, telecommunications including cable, wireless and satellite networks and hubs, and financial services and the communication networks that support them.

Critical infrastructure cyber attacks are increasing and will benefit from the current breakthroughs in AI. In recent years, there have been numerous high-profile examples, such as the ‘Triton’ malware attack that began in industrial control systems in petrochemical plants in Saudi Arabia, several attacks on Israeli water utility systems in 2020, attacks on the Ukrainian power grid in 2016, and the Colonial Oil Pipeline attack of 2021, which temporarily shut down almost half of the gasoline, diesel and jet fuel supply of the eastern United States.2

The first line of defence against critical infrastructure attacks is effective prevention. PwC’s most recent Global Digital Trust survey shows that technology is not the primary defence against cyber-attack. Instead, it is a combination of engaged leadership, streamlined decision-making, a culture of data trust and secure digital ecosystems (including digital supplier and stakeholder relationships) that combine to protect private and public organizations from attack and costly disruption.

[2] Analysis of top 11 cyber attacks on critical infrastructure, First Point, June 2, 2021

04

A multi-layered security strategy

An effective security response in a digital and connected era must have several key features. In particular, it must be able to gather data from various sources, including smart city data feeds, telecommunications records, financial transactions and social media information.

The data set must also be readily extendable to include additional input channels and provide flexibility. It must use rule-based matching and AI/ML data analysis, and the latter must be complemented by reinforced learning based on the actions of expert personnel. It must be capable of automated searching for security threats, requiring human intervention only after large data sets have been scanned, thereby providing scalability.

Finally, it must guarantee a publicly acceptable level of citizen privacy by limiting access to personally identifiable data and securing private data through strong authentication rules.

We see the optimal organisational approach to digital public safety and convergent national security management as having four main layers:

Acquisition layer

This layer standardises, parses and homogenises different data sources to simplify processing and maximise the data quality. It is designed to acquire data from various platforms and feed it to the analysis layer to maximize data quality and the possibility of matching rules and profiles. Data is transferred into a single specific format for each category (such as video, text, pictures, and sound) using minimal loss formats. The acquisition layer also includes a correlation engine to identify whether a single person or group uses multiple devices or accounts.

Analysis layer

This layer uses different technologies and solutions to identify persons of concern or emerging public safety events. It uses rule-based pattern matching, based on an operator-defined set of rules modelled on post-mortem investigations of previous security incidents and additional parameters such as personal histories and locations. The analysis layer can use cognitive technology and machine learning to increase the effectiveness in identifying, for example, the stress in captured conversations or red-flag sounds and other data from sensors in the public sphere.

Monitoring and investigation layer

This layer allows human operators to manage cases, perform queries and retrieve further information about the high-risk events identified by the solution.

Visualisation and decision support layer

This layer allows senior government executives to understand trends and make decisions to manage emerging or established trends.

05

Predictive security: automation, rule matching and AI

The connected world contains a wealth of data about people and things. In the recent past, applying sophisticated AI approaches to this data means that both adverse events and adverse actions by individuals and groups can be anticipated and mitigated with increasing accuracy and effectiveness.

The wide range of motivations, ideologies and socio-economic backgrounds of attacker individuals and groups has always made advanced identification of threats challenging. However, automated rule matching and AI-assisted recognition of patterns in individual behaviours and large-scale events, are beginning to meet this challenge. In the case of convergent national security issues, intelligent automation is helping security agencies overcome the difficulty of identifying malign actors.

In the case of public safety issues, AI and machine learning can extract patterns from large datasets that combine information from transportation monitoring, weather reports, utilities usage, human traffic in urban areas, and telecommunications flows to anticipate events such as crowding, floods and fire. Correlations that may be undetectable by human monitors can be extracted and stored for future use and learning.

Individuals and groups who may compromise public safety or convergent national security can also be subject to automated identification techniques. Rule-based pattern matching can help here, based on an operator-defined set of rules modelled on post-mortem investigations of previous incidents and the agents involved, or may be identified by artificially intelligent agents trained on datasets based on prior criminal behavior. Rule-based matching can include many parameters, including location, recent contacts, possession of weapons and more, to enhance the validity of the matching processes.

One example of rule-matching is when a person transfers all their funds to a relative or another contact; this may have an innocent explanation or indicate preparation to perform an extreme act.

Profiling may also use AI algorithms, including cognitive and machine learning technologies, creating profiles of individuals and groups of concern and then scanning general population datasets to match the profile with actual cases, verifying if real cases demand scrutiny or intervention, and learning to refine this matching process according to real-world results. Such AI-assisted identification of security concerns can unearth patterns that would not be apparent to human observers.

These approaches to security issues must be relevant to safety and security events as AI and machine learning do not discriminate between the two, and both are equally treatable subjects for data analysis based on pattern recognition.

Service layer

Within this security function, operators receive notifications about potential matches whenever a public safety or convergent national security rule or profile is matched and perform manual analyses of the collected data. In any case, every event is assigned to one operator at any given moment, and the whole chain of operators dealing with a specific case is stored for audit purposes. Finally, multiple key performance indicators are collected for operators to ensure they act quickly and effectively upon notification and for the team to learn from previous successes or mistakes. Whenever a new attacker is identified, the team flags it and sends it back to the solution to enhance its profiling database.

Management layer

Although this solution is highly automated in the acquisition and analysis layers, it still requires skill and judgment to deploy it and account for false positives and negatives effectively. The management layer is designed to manage the solution rather than individual cases. For example, new rules can be added based on experience acquired in the field, or existing rules can be amended or enhanced. New connectors can also be added for acquiring and parsing data from unknown sources.

In an age of data proliferation and universal connectivity, the challenges of managing safety and security can be tackled head-on. National governments can create solutions based on collecting massive amounts of data and analysing it effectively in a way impossible a few years ago. Technology tools that security agencies need are readily available. Now, governments must take steps to integrate these tools into an organisational model that is accurate, effective and mindful of the legitimate privacy concerns of the general public.

These technology challenges are particularly relevant to Egypt and the execution of its Vision 2030 plans. They include the use of digital technology to link together a massive array of urban developments in the New Administrative Capital currently under construction,as well as to improve the country's planning and response to natural hazards and disasters, and to improve national cyber-security and combat terrorism and organized crime.

Contact us

Maged EzzEldeen
Egypt Country Senior Partner
and Deals Leader
PwC Middle East
maged.ezzeldeen@pwc.com

Walid El Sayed
Partner and Egypt Consulting
Leader
PwC Middle East
walid.el.sayed@pwc.com

Simone Vernacchia
Partner | Digital & Technology
Consulting
PwC Middle East
simone.vernacchia@pwc.com

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 327,000 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.