# Reima'GenAI'ng Command Centres of the Future

January 2024

pwc

# Contents

# Foreword

**Rajat Chowdhary**
**Partner, Technology Consulting**
**PwC Middle East**

Command Centres (CCs) stand as pillars of intelligence and collaboration in the fields of security and operational management. These centres have demonstrated exceptional proficiency in managing complex operations and delivering advanced services by leveraging data capabilities. Acknowledging the current state of CCs, we will examine the opportunities they can seize to navigate the challenges of today. This sets the stage for understanding the intricacies of CCs, laying the groundwork for envisioning the future.

The paper examines the evolution of CCs over time, showcasing their adaptive functionalities to meet evolving customer needs and address the emerging threat landscape. Leveraging GenAI, CCs will leapfrog towards delivering enhanced predictive capabilities, reduced response times, and generate a higher return on investment.

Join us on a journey of exploration, envisioning a future where CCs redefine operational excellence.

**Naoufal el Ouali**
**Co-Founder & CEO**
**Obvious Technologies (OODA World)**

To answer the question of best practices and pitfalls for a Command Centre (CC), various factors need to be considered, including priorities of leaders, investment capacities, global infrastructure, legacy systems, and the technological preferences of end-users at all levels. This paper presents an opportunity to envision the ideal state of CCs, encompassing control rooms, crisis rooms, and the evolving cognitive command centres, when their scope extends beyond security.

Despite the absence of universally established best practices and standards for CCs, this document aims to outline their trajectory. The evolution of CCs is influenced by the infusion of selected technologies that disrupt traditional approaches and solutions. Moreover, the rise of new threats, particularly in the last decade, necessitates a recalibration of these operational hubs. The goal is to stimulate collaborations, gather insights, and propose solutions, steering the transformative journey of CCs and positioning them at the forefront of emergency preparedness, response, and investigation.

# 1. Introduction

As technology rapidly advances, we have an ever-evolving landscape of threats and crimes due to cyber risks, the evolving nature of terrorism and changing geopolitical scenarios. The traditional Command Centres (CCs) that form the backbone of public safety are undergoing a transformative journey. The conventional image of CCs, characterised by static displays and manual decision-making, is giving way to a dynamic and intuitive environment. This shift is not merely a response to current challenges but an ambitious pursuit to improve the efficiency, responsiveness, and adaptability of these critical hubs.

Propelled by technological advancements, particularly the integration of GenAI and other emerging technologies such as Augmented and Virtual Realities (AR/VR), the capabilities of CCs is undergoing a profound evolution.

Latest AI and ML technologies, including GenAI, are having a tremendous impact on the private sector. GenAI can analyse text, images, signals, structured and unstructured data to answer questions, extract information, generate personalised content, and serve as a general aid in boosting worker productivity and self-service. In the public sector, this has the potential to transform how agencies engage with residents and conduct field operations.

The rise of GenAI marks a turning point in this ongoing narrative. It not only processes and analyses data but also contributes to decision-making by generating innovative solutions, scenarios, and responses. This paper aims to understand how technology can enhance traditional CC functions, address integration challenges such as interoperability and ethical considerations, showcase real-world use cases with tangible benefits, and envision a future where GenAI shapes the landscape of public safety and crisis management.
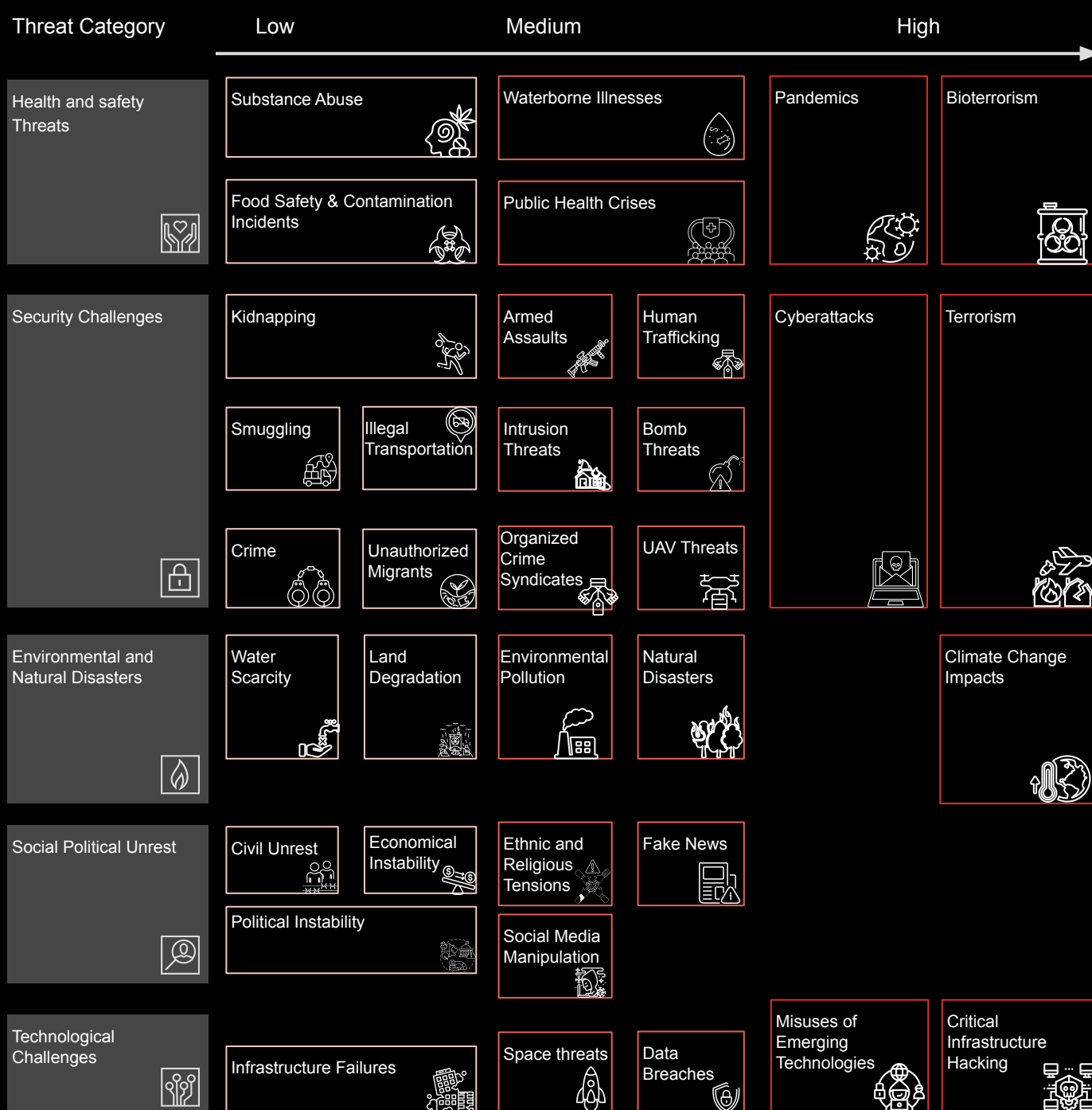
It also talks about how adoption of GenAI will enable public safety agencies more effectively address a real world scenario ensuring seamless and proactive response.

# 2. The rapidly evolving threats and crime landscape poses new and complex challenges

The world of public safety exists in a state of constant flux, driven by the intertwined forces of globalisation, technological advancements, socio-political interests, evolving health and safety concerns and changing demographics. Unlike the past, today's threats transcend borders, manifesting in diverse and ever-evolving forms. From the omnipresent threat of cyber attacks crippling essential infrastructure to the growing influence of transnational organised crime networks, contemporary challenges demand agile and adaptable responses. This section delves into the multifaceted threats to public safety, analyses the dynamic shifts in contemporary challenges faced by public safety entities, and highlights the impact on city resources.

| Threat Category | Low | | Medium | | High | |
|---|---|---|---|---|---|---|
| **Health and safety Threats** | Substance Abuse | | Waterborne Illnesses | | Pandemics | Bioterrorism |
| | Food Safety & Contamination Incidents | | Public Health Crises | | | |
| **Security Challenges** | Kidnapping | | Armed Assaults | Human Trafficking | Cyberattacks | Terrorism |
| | Smuggling | Illegal Transportation | Intrusion Threats | Bomb Threats | | |
| | Crime | Unauthorized Migrants | Organized Crime Syndicates | UAV Threats | | |
| **Environmental and Natural Disasters** | Water Scarcity | Land Degradation | Environmental Pollution | Natural Disasters | | Climate Change Impacts |
| **Social Political Unrest** | Civil Unrest | Economical Instability | Ethnic and Religious Tensions | Fake News | | |
| | Political Instability | | Social Media Manipulation | | | |
| **Technological Challenges** | Infrastructure Failures | | Space threats | Data Breaches | Misuses of Emerging Technologies | Critical Infrastructure Hacking |

# 2. Evolving threat and crime landscape

## The impact of evolving threats on society

The cumulative impact of these threats is significant. Public safety resources are stretched thin, communities face increased vulnerabilities, and trust in institutions can be eroded. Public safety officials require innovative and adaptable approaches to effectively navigate this complex environment. The evolving threat landscape also places a significant strain on societies:

| | | | |
|---|---|---|---|
| **Casualties and public safety:** Elevated threat levels may lead to higher casualties in the event of terrorist attacks, cyberattacks on critical infrastructure, or other security breaches.<br><br>01 | **Economic impact:** Decreased trade and investment may result from heightened security concerns, impacting economic growth and stability<br><br>02 | **Tourism decline:** The perception of a city as unsafe can lead to a decline in tourism, affecting local businesses, hospitality, and overall economic prosperity.<br><br>03 | **Reputation damage:** Persistent security issues can tarnish a city's reputation, potentially affecting its attractiveness for businesses, residents, and investors.<br><br>04 |
| **Infrastructure damage:** Direct attacks on critical infrastructure or secondary damage resulting from security incidents can lead to disruptions and financial costs associated with repairs.<br><br>05 | **Cybersecurity risks:** The reliance on digital infrastructure exposes cities to cybersecurity risks, including potential data breaches, service disruptions, and financial losses.<br><br>06 | **Political consequences:** Failure to effectively address emerging threats may have political consequences, affecting public trust in leadership and governance.<br><br>07 | **Strain on emergency services:** Increased threats can significantly burden on emergency services, potentially affecting their ability to respond promptly to various incidents.<br><br>08 |

## Among these evolving dynamics, the following key shifts stand out:

**The rise of AI-fueled information warfare:** Artificial intelligence (AI) plays a central role in modern hybrid warfare strategies. Deep Fakes and synthetic media, capable of replicating individuals with unsettling realism, are increasingly employed to manipulate information, orchestrate disinformation campaigns, and exploit social media platforms, destabilising governments and influencing public perception.

**The emergence of autonomous weapons:** Weaponised AI poses a profound threat due to the emergence of autonomous drones and AI-powered weapons. The development of autonomous drones and AI-powered weapons raises ethical concerns and blurs the lines between human control and machine autonomy. This technology poses a serious threat to public safety, potentially revolutionising warfare.

**AI-driven cyberattacks:** As nations continue to rely more on digital infrastructure for essential services, they become increasingly vulnerable to cyberattacks. The landscape of cybercrime has undergone a dramatic transformation, and cyberattacks are no longer solely aimed at financial gain. They have become more automated and sophisticated, fueled by AI, which enables complex and targeted attacks on critical infrastructure, economic systems, democratic processes, and public safety. Along with the rise of AI-powered cyber threats, ransomware attacks have also evolved, from being a mere nuisance for individual computer users to becoming sophisticated weapons with far-reaching consequences. These attacks now target entire organisations, including government agencies and critical infrastructure operators and involve encrypting vital data, accompanied by exorbitant ransom demands.

**Other emerging threats:**
- **Biological threats:** The potential for pandemics and the deliberate use of biological agents as weapons pose significant threats.
- **Critical infrastructure vulnerabilities:** The physical vulnerabilities of critical infrastructure, like power grids and transportation systems, present potential targets for adversaries seeking to disrupt essential services.
- **The impact of climate change and resource scarcity:** Climate change and resource scarcity exacerbate the threat landscape, potentially leading to conflict and displacement, adding another layer of complexity to the security landscape.

The devastating **NotPetya ransomware** attack, which **leveraged AI algorithms** to spread rapidly and cause billions in damage, stands as a stark example of this threat [6].

A **2022 ransomware attack** crippled a large critical infrastructure highlighting the potential for cybercriminals to target vital industries.

# 3. Opportunities and challenges of Command Centres

Recent technological advancements have enabled real-time data visualisation and analytics in the constantly changing landscape of Command Centres (CCs), providing decision-makers with greater agility. However, new security threats, increasing pressure on stakeholders to allocate resources effectively, and the proliferation of unstructured data sources present new challenges.

This evolving setting necessitates a nuanced perspective, wherein challenges are not merely viewed as obstacles but rather as opportunities to implement new technological solutions, leveraging the power of GenAI.

Balancing the need for more operational features with a more straightforward user experience, navigating the trade-off between increased mobility and heightened cybersecurity risk, and deciding between more extensive data collection and real-time performance are just a few dilemmas organisations encounter when formulating strategic goals for CC projects.

To address these challenges, it is crucial to conduct a preliminary analysis of critical pain points, such as digital technology adoption, risk assessment, and change management. The analysis should focus on three key areas:

**A** Interagency collaboration

**B** Actionable data visualisation

**C** The power of solutions and use cases

This is designed to address the challenges posed by these dilemmas, providing organisations with a roadmap for successful CC project implementation.

# 3. Opportunities and challenges of Command Centres

## A. Interagency collaboration: The data governance and leadership dilemma

In the dynamic landscape of modern CCs, the significance of interagency collaboration cannot be overstated. As security threats become increasingly interconnected and complex, a collaborative approach that transcends organisational boundaries is essential. Recognising the transformative potential of GenAI, our strategic emphasis must be on nurturing collaboration among diverse agencies within the CC ecosystem.

An evolving landscape necessitate a collective response, and interagency collaboration emerges as a crucial component. Through the integration of GenAI, PSA's can elevate communication, promote seamless information sharing, and facilitate coordinated decision-making processes across agencies. This not only enhances the effectiveness of addressing security threats, but also optimises resource allocation by tapping into collective intelligence.

**01 Fostering strategic decision-making**
- Effective leadership in command centres relies on well-informed, strategic decisions
- Data governance ensures decision-making is accurate, reliable, and aligned with organisational goals.

**02 Establishing data ownership**
- Leadership designates responsibility for data ownership, ensuring accountability and streamlined processes.
- Individuals or teams are identified for data collection, maintenance, and security within the command centre

**03 Aligning data strategies with organisational goals**
- Understanding how data enhances efficiency contributes to improved response times and overall mission success.

**04 Promoting a data-driven culture**
- Leadership fosters a culture of data literacy, encouraging analytics tool use.
- Data is viewed as a valuable resource that enhances decision-making and operational capabilities.

**05 Overcoming data silos**
- Leaders address challenges related to data silos, emphasising integrated data management.
- Collaboration ensures relevant information is shared across command centre teams and the various departments

**06 Enforcing data security and privacy**
- Leadership safeguards sensitive information by prioritising compliance with data protection regulations.
- Robust security measures and a culture of responsible data handling maintain public trust & organisational integrity.

**07 Continuous improvement through data analysis**
- Leaders encourage the use of data analytics tools for insights, enhancing operational strategies based on empirical evidence.

**08 Ensuring resilience in the face of data challenges**
- Robust data governance practices enable leaders to navigate challenges effectively.
- Quick recovery is ensured, minimising the impact on command centre operations.

**B. Actionable data visualisation:** A success factor when overcoming access to 3D data mapping source and achieving simplified user experience

Data visualisation solutions that offer actionable insights are becoming increasingly important in modern Command Centres. With simplified access to 3D data mapping sources, these solutions are providing a paradigm shift from traditional video wall management, which is mostly based on multiple live video streaming with no context. The significance of these advanced technologies lies in their ability to improve situational awareness, response times, decision-making, and overall operational efficiency. Here is a comparative breakdown of their significance:
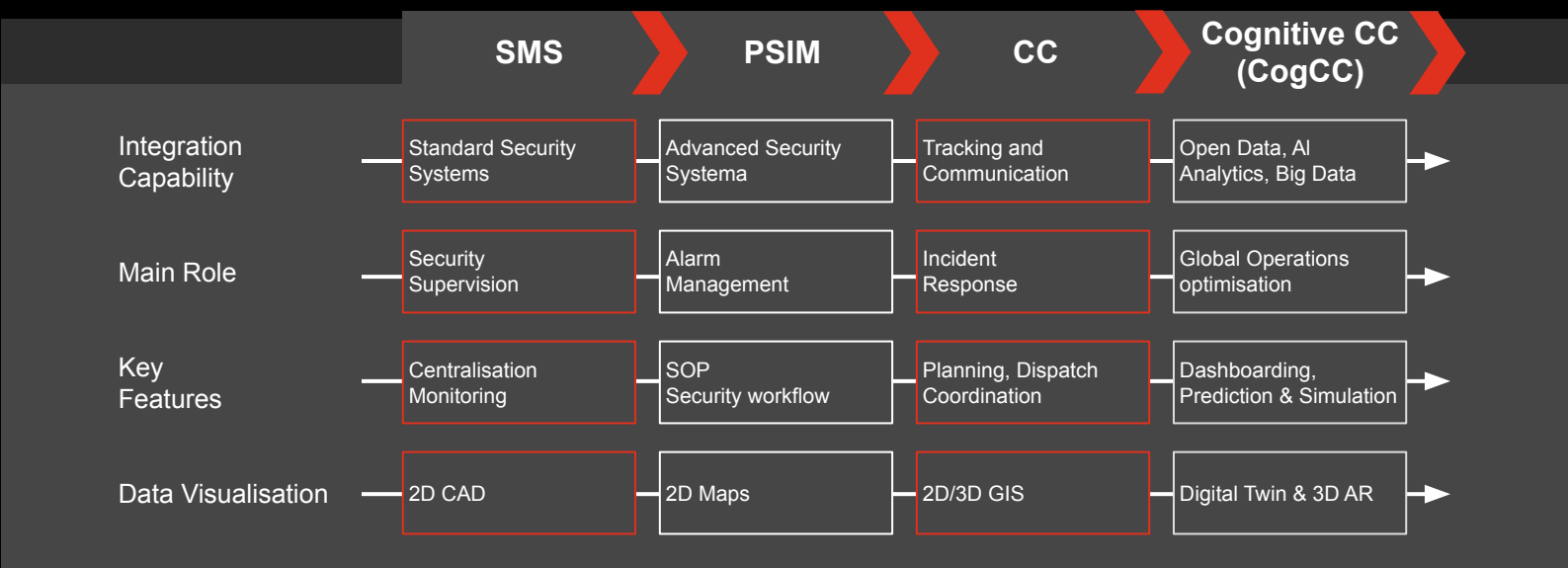
| Features / Capabilities | Traditional Video Wall Management | Advanced Solutions With 3D Visualisation |
|---|---|---|
| Comprehensive insights | Limited to 2D representations | Introduce immersive and realistic spatial representation of events and incidents |
| Real time analysis | Limited to displaying live camera feeds | Incorporation of real-time analytics and effective alerting on abnormal events or incidents |
| Interconnected data | Primarily integrates with video management with minimal or partial integration with other data sources | Data visualisation platforms connect various data streams including IoT sensors, social media and external databases |
| User-friendly interfaces | Often relies on basic or complex manual controls for video feeds | Simplifies interactions, facilitates navigation, and interpretation of data and provides guidance |
| Scenario modelling and predictive analysis | Limited capability to simulate different scenarios | Often include scenario preparation and offer proactive plan response |
| Adaptability to dynamic events | Reactive responses to unfolding events without a proactive approach | Provides real-time insights into dynamic events to manage evolving situations effectively and adjust plans instantaneously |
| Efficient collaboration | Minimal collaboration features – sharing a screen view between control room operators | Incorporates collaborative tools enabling all team members (strategic-operational and tactical) to share, annotate and communicate real-time |
| Scalability | Limited in the accommodation of diverse data types and integration | Designed to scale, accommodating an increased volume of data sources and types |

**C. The power of solutions and use cases:** From purely technical requirements to tailor-made operational usages

Command Centre (CC) solutions have transformed from providing technical hardware and software products to offering comprehensive operational solutions customised for specific use cases. This shift is characterised by a more holistic approach that combines advanced functionalities with workflow automation, thereby directly contributing to the success of CC implementation projects.

Below is a graphical representation of the progression of CC software solutions, based on the emergence of new technologies and the increasing maturity of operational use within organisations.

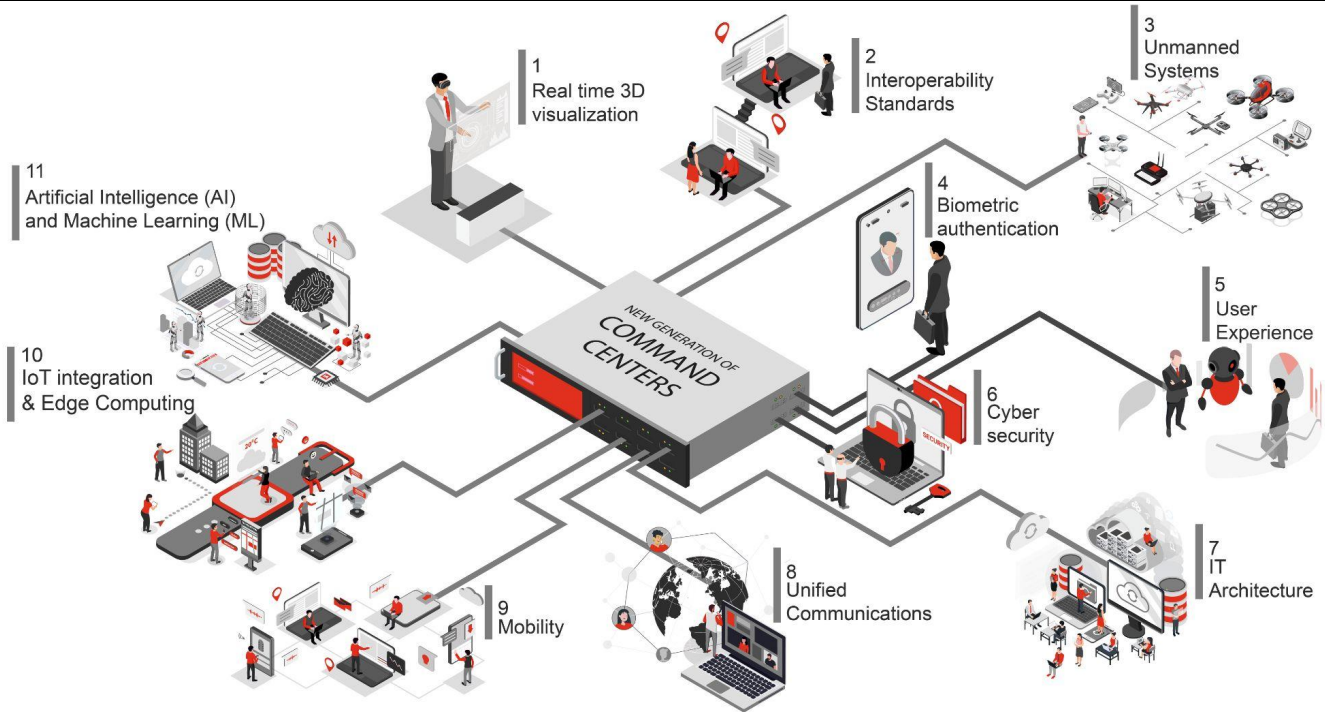| | SMS | PSIM | CC | Cognitive CC (CogCC) |
|---|---|---|---|---|
| Integration Capability | Standard Security Systems | Advanced Security Systema | Tracking and Communication | Open Data, AI Analytics, Big Data |
| Main Role | Security Supervision | Alarm Management | Incident Response | Global Operations optimisation |
| Key Features | Centralisation Monitoring | SOP Security workflow | Planning, Dispatch Coordination | Dashboarding, Prediction & Simulation |
| Data Visualisation | 2D CAD | 2D Maps | 2D/3D GIS | Digital Twin & 3D AR |

This paradigm shift underscores the recognition that successful CC solutions are those that not only meet technical requirements but also have the agility and scalability to adapt to the organisations' customers' technical infrastructure, business ecosystem, human organisation and operational processes.

Last but certainly not least, the initial training, operational rehearsal, and drill phases - often neglected or deferred until the project's conclusion - are not just crucial determinants of success. They also serve as potential catalysts for groundbreaking GenAI technologies, fundamentally reshaping the implementation and long-term optimisation of CCs.

# 4. Evolution journey of CCs in addressing emerging challenges

Command Centres have undergone a significant evolution in their approach to managing emerging challenges. Initially designed as centres for direct command and control, these facilities have gradually shifted towards becoming hubs of information processing and strategic decision-making.



**11 Points to consider for a Modern & efficient command center:**

| | | |
|---|---|---|
| **Real time 3D Visualization** 01 : GIS, Digital Twin, Virtual Reality/ Augmented Reality | **Interoperability standards** 02 API integration, Data organization, Data processing | **Unmanned Systems** 03 Autonomous drones, IAV, Robots |
| **Biometric Authentication** 04 Face Voice, Iris | **User Experience** 05 Situational Awareness, Information presentation, Responsiveness | **Cyber Security** 06 Data privacy, Communication protection, Threat monitoring |
| **IT Architecture** 07 Microservices, Cloud compatibility, Redundancy | **Unified Communications** 08 Voice, Video, Instantaneous Chat | **Mobility** 09 Mobile Command, Smart Patrol, Field Intervention |
| **IoT Integration & Edge Computing** 10 Environment condition , Social Media , Smart Traffic | **AI & Machine Learning** 11 Computer Vision, Predictive Analysis, Automated Decision support | |

This evolution has been driven by the need to adapt to an increasingly complex and data-intensive operational landscape, where the ability to process and act on large volumes of information quickly is crucial. CC has seen only incremental changes, primarily in the form of flatter, larger or more interactive screens.

The core challenge remains unchanged: Processing an ever-increasing volume of data with few personnel. The next section explores the potential of GenAI's impact across the lifecycle of the CC operations i.e. Predict, Pre-empt and Prescribe.

# 5. GenAI's impact on Command Centre operations

GenAI is poised to bring unprecedented advancements to Command Centres. It introduces new opportunities, including creative content generation, seamless human-machine collaboration through natural language generation, sophisticated chatbots and virtual assistants, pattern analysis or enhanced simulation capabilities for predicting complex scenarios.

GenAI contributes to facial and emotional recognition, fosters transparency, and plays a pivotal role in developing defenses against adversarial attacks in machine learning systems. These advancements position GenAI as a key enabler to help prepare against new threats and offer heightened efficiency and responsiveness in command-and-control operations.

To illustrate the effectiveness of **CC operations powered by GenAI,** we consider a case where civic riots have occurred within a city.

| Predict | Pre-empt | Prescribe |
|---|---|---|
| **Automatically generate predictive models** | **Intervening before threats or incidents fully materialise** | **Deploying effective actionable intervention strategies during crisis improved by continuous learning** |
| **01**. CC analysed **historical riot patterns**, public interactions, and posts from social media feeds about the riots. CCs were able to generate a list of high-risk roads and different areas within the city (hotspots). **02. Utilising the prediction model output**, Command Centres operators were able to generate simulated synthetic scenarios about the riots, anticipating future development and the extent of riots. **03. AI-generated heat maps -** Visualising riots escalation and traffic congestion. | **01. VR crisis response training -** By generating synthetic riot scenarios that imitate real-world scenarios. CC personnel are enabled to have a full immersive virtual reality training against riots. **02. Strategic resourcing** Based on recommendations generated by the model about possible hotspots, police personnel, fire brigades and ambulances were strategically allocated, allowing for immediate response. **03. Optimal routes recommendations -** By identifying congested routes and road closures, the system produces GIS images that indicate the best alternative route for public safety agencies (police, fire brigades, ambulance, etc). **04. Drone based unified reporting** Deploying drones equipped with high-resolution cameras and GenAI modules to identify risk prone areas based on past trends | **01. Unified reporting** Produce a unified reporting for CC by analysing live video feeds from surveillance cameras and drones, studying actions taken and continuously improving intervention strategies. **02. Automated voice assistance** Using speech generation to establish communication with affected individuals. This allows for delivering emergency information and instructions, answering FAQs in multiple languages and ensuring insights are fed into unified reporting and process improvement. **03 - Automated alerting and prioritisation system** By analysing data from different sources and applying predefined rules, incidents are automatically prioritised and alerted based on their severity, urgency, and potential impact. **04 - Automated Key Performance Indicators (KPIs)** Assessing the efficiency of prevention measures by automatically generating KPIs based on relevant factors derived from the model. |

# 6. Case studies: Practical applications inspired by video gaming technology

This section presents real-world applications of technologies such as machine learning, predictive analytics, computer vision, and smart resource allocation in Command Centre, drawing parallels with their use in interactive gaming:

## Emergency management

Incorporating gaming technology in emergency management revolutionises **real-time strategy and response efforts**. Interactive simulations offer **immersive training for emergency responders**, enhancing decision-making and situational awareness.

Inspired by gaming Human Machine Interface (HMI), r**eal-time data integration and visualisation** provide a dynamic view of emergencies, enabling swift and informed decisions. **GenAI-driven resource management**, mirroring video game strategies, ensures efficient allocation of resources. Communication tools, akin to multiplayer configurations, facilitate effective coordination among responders. For example, in fire scenarios, these technologies simulate fire propagation, **guide navigation through AR** in smoke-filled environments, and assist in strategic resource deployment, significantly improving emergency response effectiveness.

## Safe cities

The **integration of AI and augmented reality (AR) mirrors** the dynamic environments of video games, offering advanced surveillance and threat detection for safe cities. AI algorithms analyse surveillance feeds for anomalies, enabling real-time threat identification and predictive policing.

AR enhances this system by providing interactive, real-time data overlays. For instance, AR headsets display **virtual layouts of buildings and potential hazard locations** to officers on the ground, while CCs use AR for 3D mapping of the city, showing live data and AI alerts.

This combination creates a responsive, interactive urban security network reminiscent of strategic control in video games but applied to real-world safe cities.

## Natural disaster response

In disaster management, **3D visualisation technologies** play a pivotal role in enhancing response efforts. Detailed 3D models created from satellite imagery, drone footage, and ground-level sensors provide responders with a dynamic view of disaster-affected areas.

Continuously updated with real-time data, these models reveal damage extent, potential hazards, and accessible routes, aiding in planning and rescue operations. They enable rescue teams to identify safe and quick paths for aid delivery, assist CCs in resource allocation, and facilitate collaboration among agencies.

Making these models accessible to the public informs and guides community evacuation and relief efforts. **In earthquake response, 3D models guide search and rescue operations** and infrastructure assessment, significantly improving overall efficiency and effectiveness in disaster response.

# Conclusion: Window of opportunity in the Middle East

## Transformation of Middle East

The Middle East today is on the cusp of a grand vision-led transformation. Particularly in the Gulf Cooperation Council (GCC1), countries have set ambitious targets to grow their non-oil economies.

National Visions introduced across the GCC recognise the critical role that digital and emerging technologies play in achieving sustained economic growth, together with other enablers propelling the region's GDP from USD 1.7 tn in 2021 to a target of USD 3.2 tn in 2030 – an 83% growth rate.
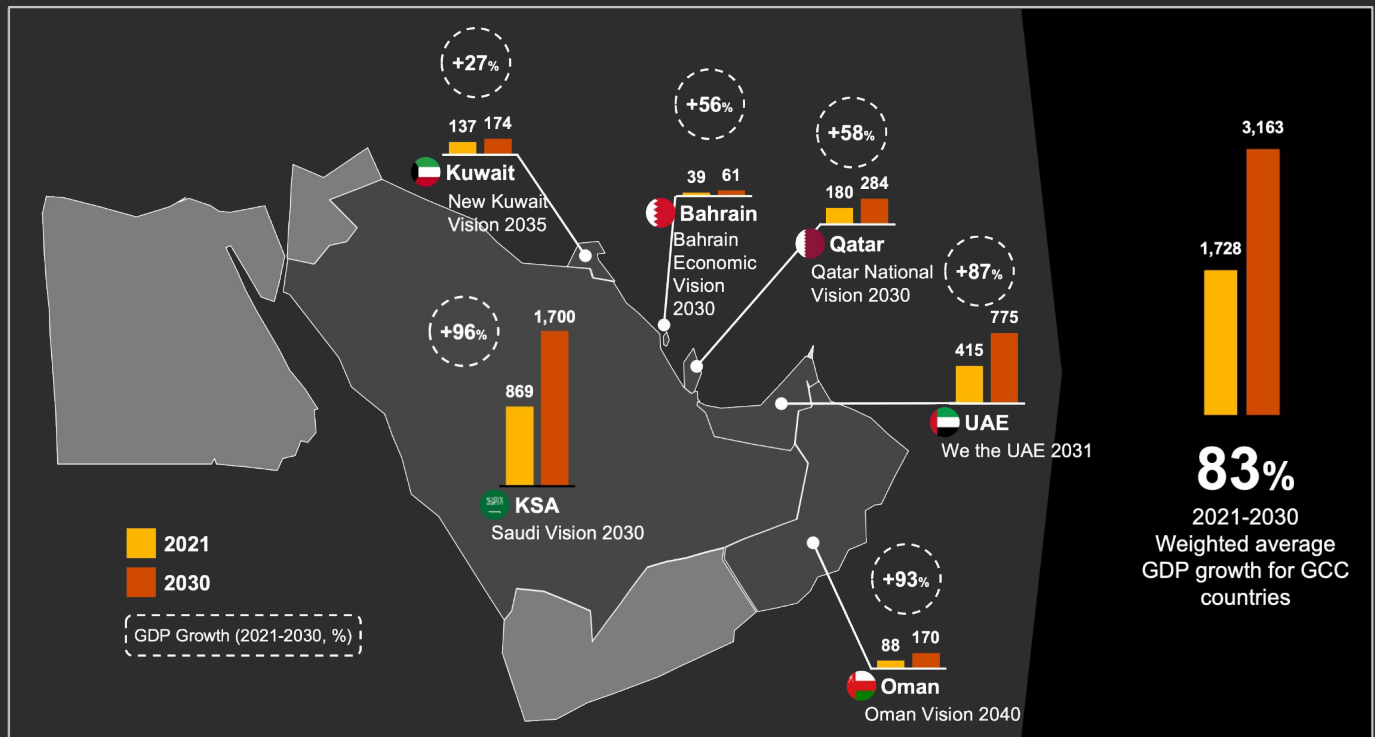


**Figure : GCC Economic Growth by Country (GDP in USD bn, 2021 – 2030)**

## Inception of giga projects

In line with their National Visions and diversification strategies, GCC countries have launched plans to build new mega cities – many of which are set in entirely new geographies with no existing infrastructure. These large-scale projects are technology-driven, aiming to improve quality of life while driving economic growth and promoting sustainable development.

- The largest of the mega cities, NEOM in KSA, is set out to create a futuristic cognitive city, providing high quality of life for its residents, utilising state-of-the art technology and digital infrastructure, and fostering disruptive solutions through cutting-edge innovations (e.g., 5G hyperconnectivity, AI and advanced robotics, augmented, mixed and virtual reality, etc.).

- Part of the Dubai 2040 Urban Master Plan, Expo City is set to become a global business hub with an ecosystem combining global talents, technology, and digital advances. It features one of the largest cutting-edge cloud technology platforms enabling smart metering, augmented reality, big data, IoT, AI, and NLP applications.

- The Red Sea in KSA project is spearheading a new model of development, leveraging innovative concepts and smart technologies to enhance visitor experience and the wellbeing of its communities and environment.

- AlUla in KSA aims to become a global tourist destination in KSA, augmenting its rich natural heritage with robust digital infrastructure and advanced digital services.

1. Includes KSA, UAE, Qatar, Kuwait, Oman, and Bahrain

# Safety and Security at the core

In many of their plans, GCC countries have prioritised safety and security as a key component of their national agendas – with ambitions for creating stable and prosperous societies and improving the overall quality of life for their citizens.

### Saudi Vision 2030
**KSA**

Improve livability in Saudi cities and protect vital resources of the nation
"

### We the UAE 2031
**UAE**

Place of the UAE globally as first in the "safety" index
"

### Qatar National Vision 2030
**Qatar**

Establish secure and stable society operating on the principles of justice, equality and the rule of law
"

### New Kuwait Vision 2035
**Kuwait**

Develop and modernise the national infrastructure for the purpose of improving the quality of life for all
"

### Oman Vision 2040
**Oman**

Develop smart, sustainable and vibrant cities and a vital countryside with a viable architecture that ensures high quality of life, work and leisure
"

### Bahrain Economic 2030
**Bahrain**

Install a safe and secure environment, adopting the latest technologies, and modernisation of police services and community policing programs
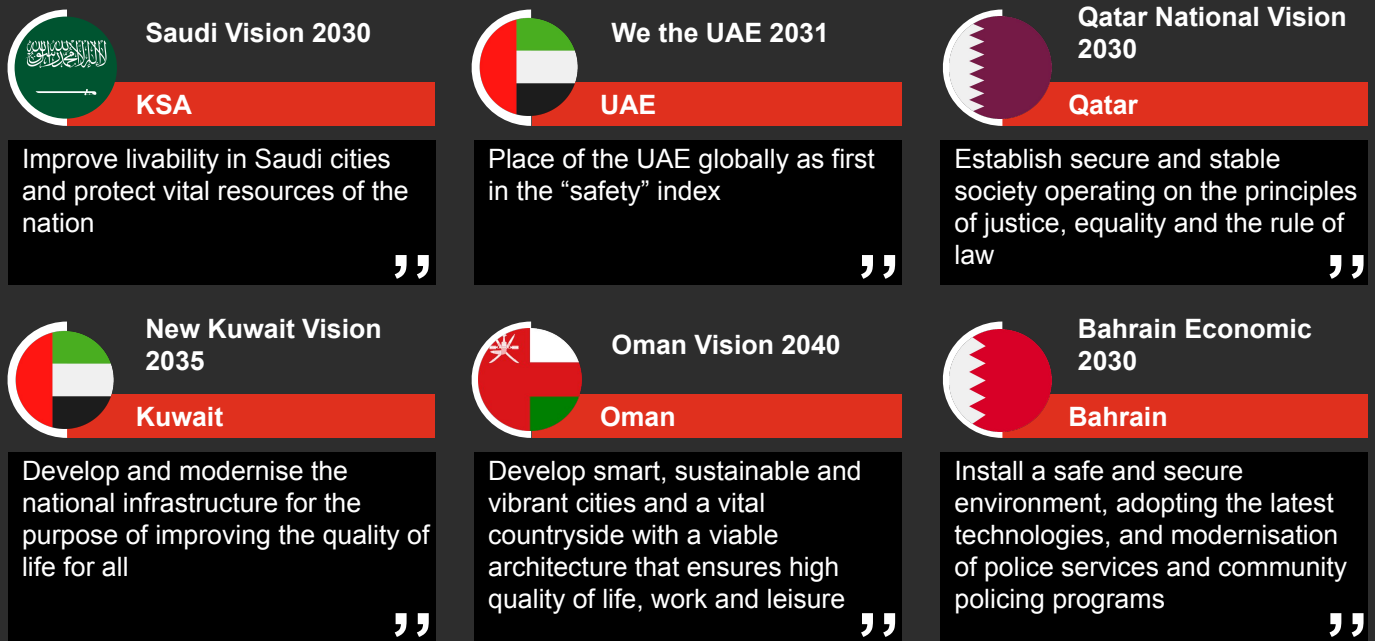"

Figure : Safety and Security in National Aspirations

In fact, many GCC countries have already made headlines for the high-level of safety and security they offer their citizens, residents, and visitors – vouched for by global indices. For instance, the UAE tops the Women, Peace, and Security (WPS) Index 2021 for women's safety, while Qatar has ranked as the safest country in the world on the Numbeo Crime Index since 2019.
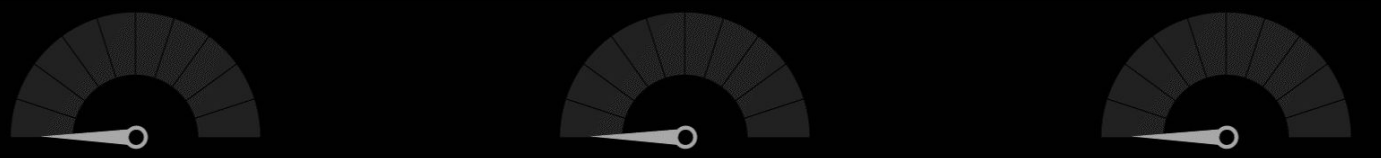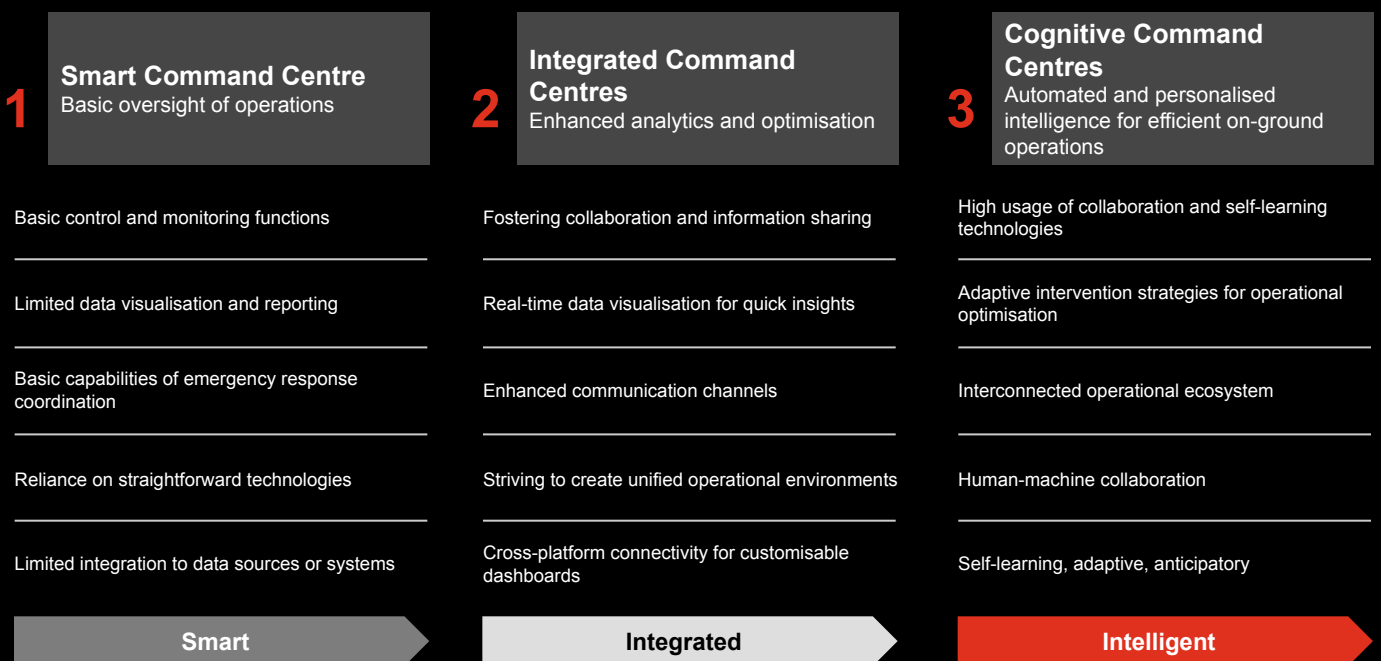
# Cognitive Command centres

The transformation potential of Command centres (CCs) is not limited to improving their existing capabilities, but it also represents a significant change in operational strategy. By embracing advanced technologies, such as Artificial Intelligence (AI), Augmented Reality (AR), and 3D visualisation, these centres can move beyond their traditional, isolated command hubs to become what is known as a Cognitive Command Centre (CogCC)
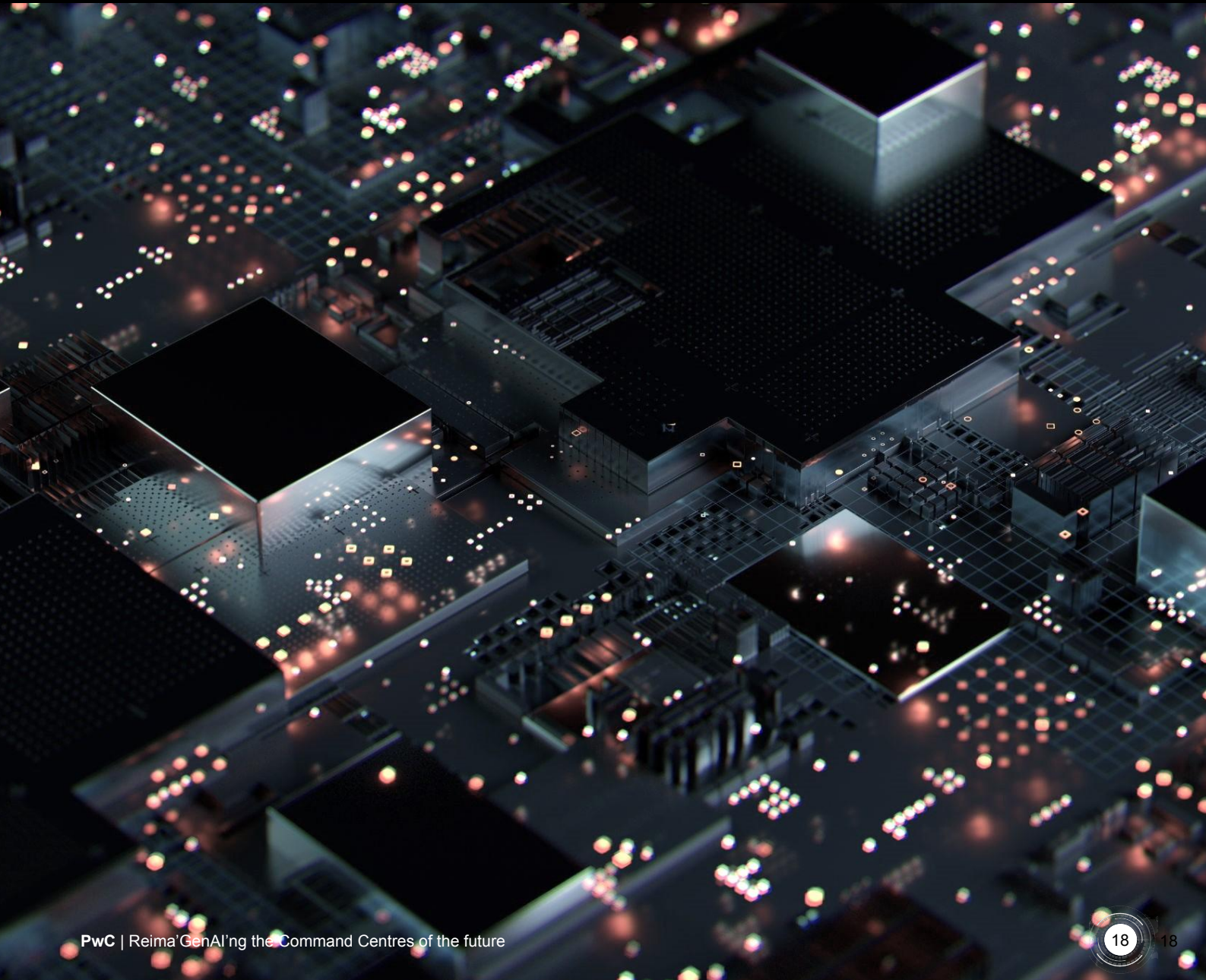
This evolution represents a shift towards a more integrated and intelligence-driven approach. It enables faster and more efficient decision-making while also being more holistic and informed. CogCCs enable the synthesis of data from diverse sources in real-time, providing a comprehensive operational picture. The immersive and interactive technologies, along with the power of GenAI, will help operators visualise complex scenarios in unprecedented detail. This will facilitate strategic planning and effective crisis management.
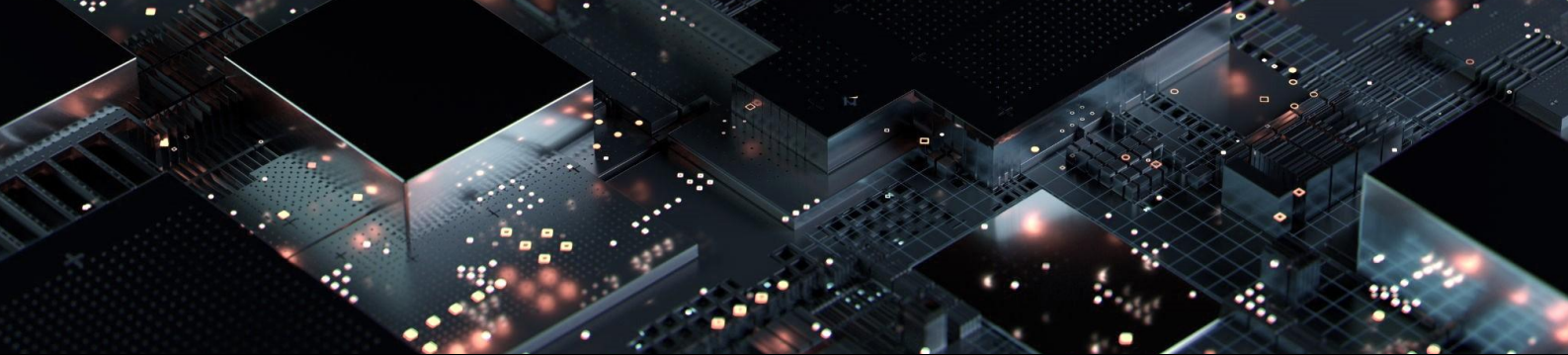
These centres would serve as the nerve centres of decision-making, capable of coordinating vast arrays of information and resources across various domains. They go beyond responding to immediate threats or challenges and anticipate future risks, ensuring a proactive stance in managing security, emergencies, and operational planning. This shift towards CogCC marks a significant advancement in the field of command and control, setting a new standard for operational excellence driving towards substantial financial gains and redefining the landscape of public safety and security management.

**1** **Smart Command Centre**
Basic oversight of operations

**2** **Integrated Command Centres**
Enhanced analytics and optimisation

**3** **Cognitive Command Centres**
Automated and personalised intelligence for efficient on-ground operations

| | | |
|---|---|---|
| Basic control and monitoring functions | Fostering collaboration and information sharing | High usage of collaboration and self-learning technologies |
| Limited data visualisation and reporting | Real-time data visualisation for quick insights | Adaptive intervention strategies for operational optimisation |
| Basic capabilities of emergency response coordination | Enhanced communication channels | Interconnected operational ecosystem |
| Reliance on straightforward technologies | Striving to create unified operational environments | Human-machine collaboration |
| Limited integration to data sources or systems | Cross-platform connectivity for customisable dashboards | Self-learning, adaptive, anticipatory |

**Smart** | **Integrated** | **Intelligent**

# References

1. https://www.arabianbusiness.com/politics-economics/uae-retains-position-as-one-of-worlds-safest-countries
2. https://www.vision2030.gov.sa/en/vision-2030/vrp/quality-of-life-program/
3. http://dubai2040.ae/en/
4. https://www.vision2030.gov.sa/en/projects/
5. https://www.oman2040.om/pillars?lang=en
6. https://www.newkuwait.gov.kw/plan.aspx
7. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/transport-and-infrastructure/dubai-2040-urban-master-plan#:~:text=The%20key%20objectives%20of%20Dubai,provide%20sustainable%20and%20flexible%20means
8. https://www.securityweek.com/saudi-aramco-facing-50m-cyber-extortion-over-leaked-data
9. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

# Contact us

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

**Sharang Gupta**
**Director, Technology Consulting**
**PwC Middle East**
sharang.g.gupta@pwc.com

**Vishesh Kalia**
**Director, Technology Consulting**
**PwC Middle East**
vishesh.k.kalia@pwc.com

# Contributors

**Naoufal El Ouali**
**Co-founder, CEO**
**Obvious Technologies**
**(OODA World)**

**Meline Soulie**
**VP Public Safety & Strategic Partners**
**Obvious Technologies**
**(OODA World)**

**Mohammed Sami Alomar**
**Manager, Technology**
**PwC Middle East**

**Riddhima Dutta Jajodia**
**Manager, Technology**
**PwC Middle East**
riddhima.jajodia@pwc.com

# Thank you