Unlocking the future of border security

Borders of the future

Foreword

Sharang Gupta
Partner, Technology
PwC Middle East

We envision a future where digital borders are defined not by geography, but by intelligence, agility and resilience. As threats evolve and global interconnectivity deepens, traditional border infrastructures must give way to adaptive, technology-led ecosystems capable of real-time response and seamless interoperability.

By deploying AI, advanced analytics and integrated digital platforms, we can enable predictive risk management, autonomous decision-making and trusted data exchange across jurisdictions – creating smarter, faster and more secure border environments.

Our approach reimagines borders as strategic enablers of security and commerce. Together, we are setting new standards for border innovation – fusing technology, policy and collaboration to shape a future where borders are not barriers, but intelligent gateways in a rapidly shifting landscape.

Majdi Dodokh
Partner - Strategy & Operations
PwC Middle East

We envision a future that leverages non-kinetic warfare and moonshot technologies to counter emerging threats. Traditional methods fall short against today's challenges – prompting investment in advanced information, electronic and cyber warfare to safeguard borders.

By deploying AI, quantum computing and autonomous systems, we can achieve superior situational awareness and spectrum control – enabling decision-makers to act swiftly and effectively.

Our approach ensures comprehensive security while contributing to global stability. Together, we are setting new standards for integrated border security, anticipating and neutralising threats in an ever-evolving landscape.

Introduction

In the evolving landscape of global security, border protection is undergoing fundamental transformation. Traditionally reliant on physical barriers and personnel, today's challenges demand a new approach to counter digital, autonomous and sensor-driven threats. Modern adversaries deploy cyber tools, drones and spoofing devices, creating a real-time, nonlinear warfront that is both elusive and dynamic. This evolution renders conventional models inadequate against the speed and complexity of contemporary threats.

To respond effectively, the adoption of non-kinetic technologies is essential for the future of border security. These capabilities enhance detection and accelerate response, enabling layered defence strategies that expand surveillance, deepen situational awareness and compress decision timelines. Advanced sensors and AI-powered analytics optimise the OODA loop (observe, orient, decide, act), allowing faster decisions while complicating the adversary's own process.

PwC is a strategic partner in this transformation, combining deep industry expertise with technology-driven consulting to help tackle today's security challenges. We design and deliver future-fit solutions that harness emerging technologies and empower clients to navigate uncertainty, neutralise threats and secure their borders in a constantly shifting global environment.

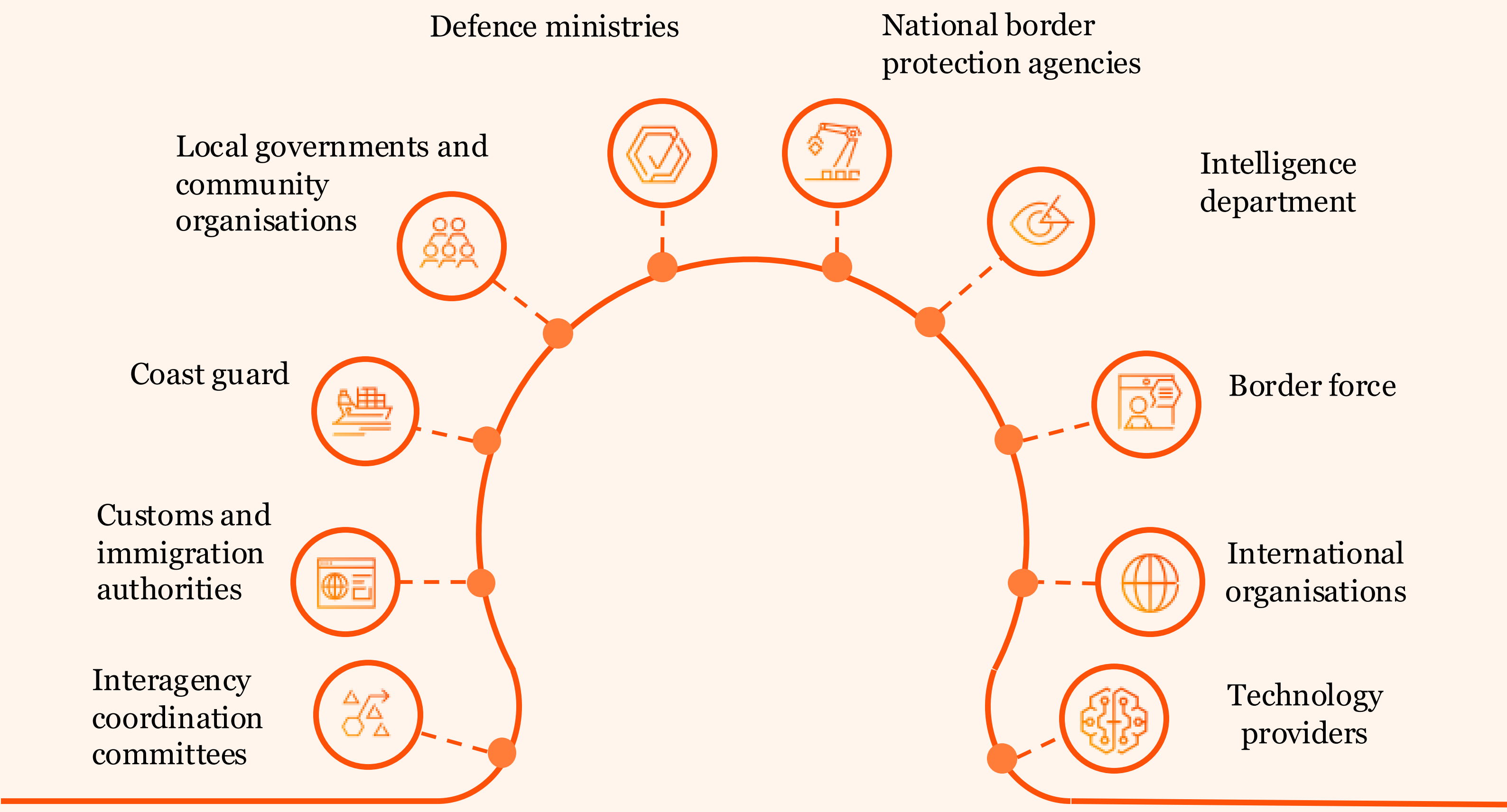
“

Borders are not just lines on a map, but the frontlines of a nation's sovereignty, security, and economic prosperity

Understanding the stakeholder ecosystem in border security

The stakeholder ecosystem is essential to border security as it enables a coordinated approach to protecting a nation's borders. Diverse stakeholders such as government agencies, international organisations and technology providers each bring distinct expertise and resources. This collaboration supports comprehensive coverage, efficient use of resources and seamless operational integration. By working together, these entities help prevent security gaps and respond promptly to evolving threats.

Moreover, the stakeholder ecosystem facilitates information sharing and adaptability in policy implementation. Alignment with national priorities and international standards strengthens cross-border cooperation. Involving a broad set of stakeholders helps ensure that border security strategies remain effective and proportionate, adapting to emerging challenges such as cyber threats and organised crime. Ultimately, this ecosystem contributes to safer and more efficient border management.


Defence ministries
National border protection agencies
Local governments and community organisations
Intelligence department
Coast guard
Border force
Customs and immigration authorities
International organisations
Interagency coordination committees
Technology providers

Key stakeholders in border security and their respective roles

National border protection agencies: Their role involves conducting inspections, preventing illegal smuggling and ensuring compliance with immigration and customs laws.

Coast guards: Coast guards collaborate with other agencies to maintain a secure maritime environment and often works with international counterparts to address transborder maritime threats.

Border forces: They play a pivotal role in controlling the flow of travellers and cargo, ensuring compliance with customs, immigration and trade laws. Border forces balance security with the facilitation of trade and travel, requiring the use of advanced technologies such as biometrics and surveillance systems to enhance operational efficiency and effectiveness.

Interagency coordination committees: They ensure seamless communication and interoperability across different systems, agencies and technologies. By coordinating efforts, these committees help develop unified strategies and responses to complex border security challenges, promoting efficient resource use and information sharing.

Defence ministries: This entity provides military support and resources, particularly in scenarios where heightened security is required. Their involvement is critical during emergencies or conflicts where national security may be compromised, ensuring responsive and rapid defence capabilities.

Intelligence department: The intelligence department plays a vital role in collecting, analysing and disseminating information on potential threats to national security. Their work involves collaboration with international intelligence agencies to share and acquire data necessary for safeguarding borders.

Local governments and community organisations: Entities near border regions work directly with national agencies to support security measures and promote community involvement. Local governments manage resources and implement local strategies to address region-specific border issues.

International organisations: They offer platforms for collaboration, dialogue, information sharing and the development of shared standards and practices.

Technology providers: Their role involves innovating and maintaining technologies that enable agencies to detect, respond to and prevent threats efficiently, while adapting to evolving security challenges.

Customs and immigration authorities: Customs and immigration authorities play a vital role in facilitating lawful international trade and travel while safeguarding against threats, fraud and violations of law.

Ensure optimum participation from all stakeholders to achieve maximum potential

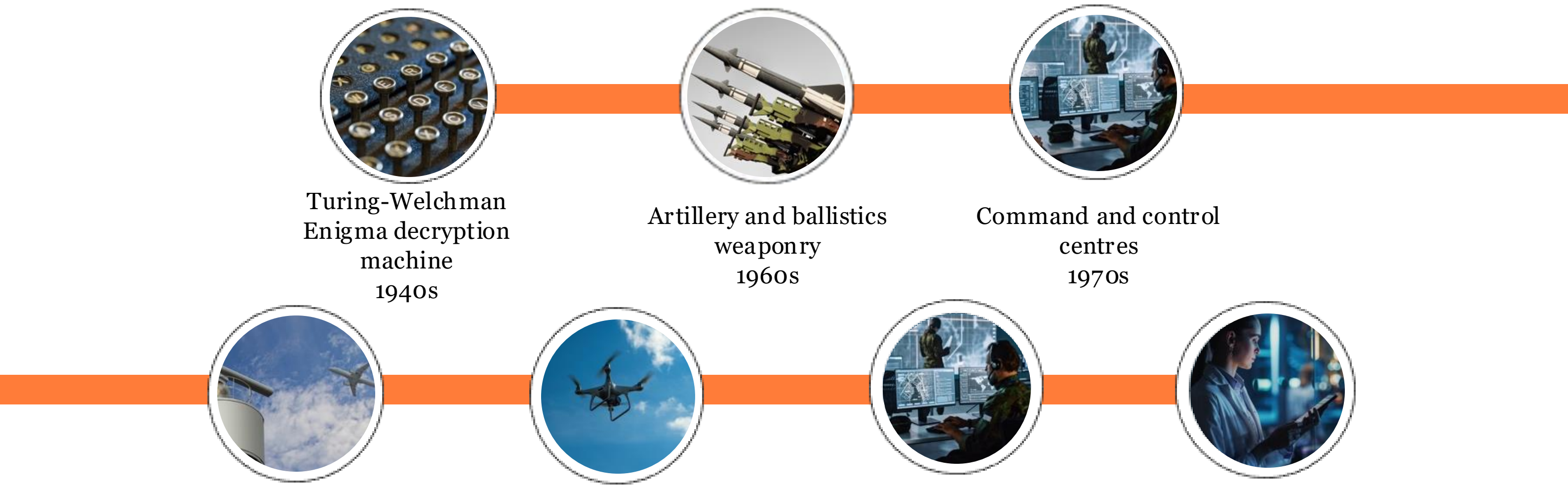
Enable clear roles and responsibilities for all stakeholders

Adopt emerging technologies and trends across the ecosystem

Evolution of border security from legacy kinetic systems to non-kinetic and AI supported systems

The constant evolution of modern warfare has significant implications for border security strategies. As threats continue to diversify, integrating border security solutions enables nations to protect sovereignty more effectively, respond decisively to emerging threats and optimise security expenditure and performance in the face of complex global challenges.

Modern warfare includes non-kinetic components such as cyber attacks, electronic jamming and signals intelligence (SIGINT). Non-kinetic warfare refers to strategic actions in military operations that do not rely on physical destruction through conventional munitions, but instead use logical, electromagnetic and behavioural methods. This approach is increasingly relevant in modern border security systems, where the emphasis has shifted towards new technologies such as drones for surveillance and sensors for detection, rather than traditional physical border controls.



Turing-Welchman Enigma decryption machine 1940s

Artillery and ballistics weaponry 1960s

Command and control centres 1970s

Electronic surveillance systems 1980s

Drones and unmanned aerial vehicles (UAVs) 2010s

AI and machine learning for data analysis 2020s

Quantum computing in encryption and security systems 2030s

The evolution of border security technology mirrors military advancements over several decades. Beginning with the Turing-Welchman Enigma machine in the 1940s, technology progressed through improved artillery accuracy in the 1960s to enhanced command, control and surveillance in the 1970s. These developments marked a shift from basic decryption to sophisticated communications, laying the groundwork for modern border security systems.

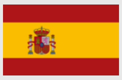
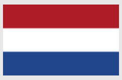
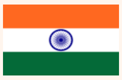
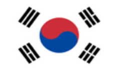
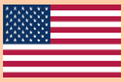
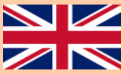
Legacy approach	→	Non-kinetic approach
Patrolling troops		Autonomous UGVs & UAV swarms with EO/IR payloads
Fortified walls		Smart fence and virtual perimeters with sensors

Transitioning of countries and borders from kinetic to non-kinetic solutions

Countries can be classified into three strategic tiers - Foundational, Integrated and Intelligent Border Security, based on the maturity of defence forces in adopting advanced technologies.

Maturity Level	Transition in border security					
	Level 1		Level 2		Level 3	
Battlefield	Land Air Sea		Land Air Sea Information		Land Air Sea Information Space	
Tech Focus High Medium Low	Kinetic	Non-Kinetic	Kinetic	Non-Kinetic	Kinetic	Non-Kinetic
	Platforms	NCW	Platforms	NCW	Platforms	NCW
	Weapon Systems	EW	Weapon Systems	Cyber	Weapon Systems	Cyber
				EW		EW
				Space Tech		Space Tech
	Unmanned Systems		Unmanned Systems		Unmanned Autonomous System	

Classification of technology maturity in border security

	Level 1	Level 2	Level 3
	Foundational Border Security	**Integrated Border Security**	**Intelligent Border Security**
Characteristics	• Heavy reliance on manpower (border patrols, physical checkpoints) • Use of physical barriers (fences, walls) • Conventional weaponry and deterrence • Limited use of smart surveillance and predictive systems in special regions	• Integration of kinetic defenses with electronic surveillance • Use of drones, sensors and early AI for surveillance • Data-assisted patrolling and resource deployment	• AI, ML and big data analytics for threat detection • Cyber defense integration with border security • Satellite and UAV-based monitoring • Focus on deterrence and disruption through electronic, legal and economic tools
	 	 	 

Note- NCW: Net Centric Warfare, EW: Electronic Warfare

Evolving border threats require enhanced surveillance, global cooperation and adaptive strategies

As borders evolve, they will face increasingly sophisticated threats driven by technological advancement, climate change and geopolitical tension. Cyber attacks, smuggling, biological threats and human trafficking will continue to exploit vulnerabilities in border areas and many actors are increasingly resorting to use of drone. Enhanced surveillance and international collaboration will be essential to maintaining security. A few critical threats at future borders include:

	Threat	Description	Drone usage
EVOLVING THREATS AT BORDERS	Terrorism	Includes border attacks with IEDs and hoaxes, creating panic, destabilising security and challenging defense systems.	✓
	Geopolitical and military	Conflicts in border areas which have spill-over consequences on the border security operations.	✓
	Cyber and information threat	Comprises cyberattacks on critical infrastructure and spreading misinformation to disrupt border operations and data integrity.	✕
	Criminal and illegal activities	Criminal activities, including drug and weapons smuggling, organized crime and explosives trafficking, destabilise societies and threaten public safety.	✓
	Unauthorised entry and migration	Comprises of human trafficking, illegal migration and mass migration which disrupt borders, posing severe sociopolitical and economic challenges.	✓
	Economic danger	Economic dangers such as infrastructure attacks via drones on critical assets and currency counterfeiting undermine financial stability, disrupt services and erode trust in systems.	✓

Transitioning from legacy systems to modern non-kinetic defence solutions

	Legacy approach	Non-kinetic approach
Terrorism	• Physical fortification of borders with fences and barriers	• AI- enabled UAVs for surveillance • Smart sensor-based fences
Geopolitical and military	• Diplomacy and political negotiations • Deployment of military forces	• Cyber intelligence operations • Strategic communication campaigns
Cyber and information threat	• Manual monitoring of network traffic • Periodic security audits	• AI-driven anomaly detection systems
Criminal and illegal activities	• Border patrols and checkpoints • Manual inspection of goods and vehicles	• Advanced non-invasive inspection systems • Behaviour analytics enabled cameras
Unauthoriaed entry and migration	• Physical barriers to control migration flows	• Surveillance technologies to monitor migration routes and patterns
Economic danger	• Traditional security systems • CCTV and physical checks	• Counter drone systems • Facial and behaviour recognition systems

Transforming border security with central command and control centre

The advantages of a central command and control centre (CCC) include faster response times and more informed data-based decision-making, all of which contribute to a more efficient and effective border security management system. This is achieved through a set of attributes.

Key attributes of central CCC

Human-centric: Strengthening connections among border security staff and stakeholders, with an emphasis on service quality and accessibility to improve traveller experience and safety.

Adaptable threat response: Developing scalable systems that can rapidly adjust to evolving security threats, with agile protocols ensuring effective and timely incident responses at border crossings.

360° holistic decision intelligence: Leveraging cross-domain data fusion to generate comprehensive insights into border activities, enabling proactive management and mitigation of potential risks and threats.

Omnipresence: Maintaining constant vigilance along borders through continuous remote monitoring technologies, enhancing situational awareness and enabling timely intervention.

User-friendly workflows: Implementing intuitive and engaging interfaces for border security operations to improve efficiency and accuracy through enhanced visualisations and streamlined processes.

Interoperability and unified communications: Facilitating coordinated action among border security agencies through integrated communication systems, improving response speed and effectiveness in addressing security challenges.

Streamlined coordination across agencies

Improved efficiency and response times

Enhanced security and situational awareness

Levers enabling border security evolution and resilience against emerging threats

In an era of rapidly evolving and complex security threats, achieving dominance in border security requires the use of advanced technologies and strategic frameworks. Traditional methods alone cannot address the range of challenges posed by modern adversaries equipped with sophisticated tools and tactics.

Effective border defence today demands a holistic approach – integrating innovation in surveillance, detection and decision-making to ensure comprehensive protection. The parameters outlined below, supported by emerging technologies, offer a path towards achieving operational superiority in border security.

Increasing probability of detection 01

- Utilize advanced sensors and AI analytics for precise threat identification
- Implement real-time monitoring systems

Layered defence 02

- Integrate multiple security measures such as cybersecurity, surveillance, and physical barriers
- Develop resilience through redundancy and multifaceted strategies

Reduction of OODA (observe, Orient, decide, act) loop 03

- Utilize advanced sensors and AI analytics for precise threat identification
- Implement real-time monitoring systems

Increasing OODA loop for adversaries 04

- Introduce complexity in gathering data for enemy through stealth technologies and jammers
- Employ deceptive tactics and misinformation

Increasing surveillance range 05

- Deploy drones and satellites for extensive area coverage
- Use of long-range sensors for enhanced situational awareness

Key tenets for unlocking next-gen border security

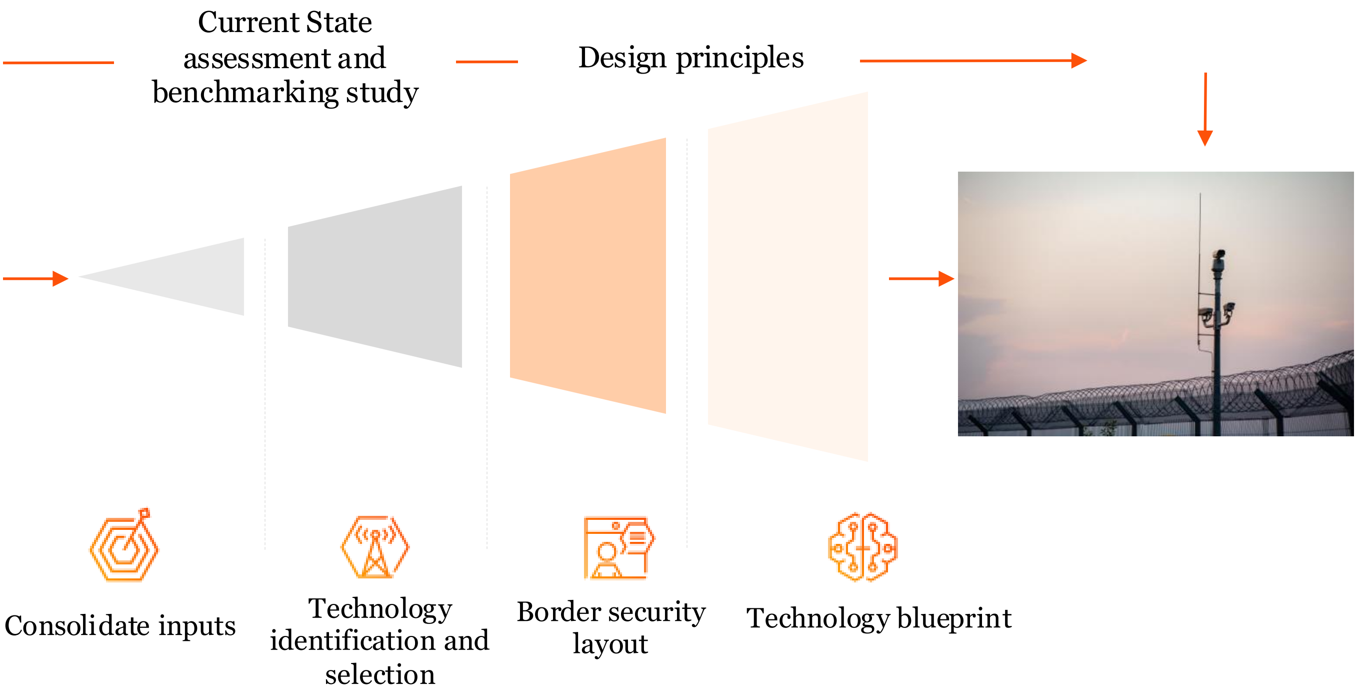
Designing future border security involves several key tenets that address evolving threats and enhance resilience.

Threat and current tech assessment	Evaluates existing technologies against identified threats to pinpoint vulnerabilities and inadequacies, laying the groundwork for necessary enhancements and adaptive strategies in border security.
Technology selection as per evolving threats	Focuses on choosing technologies that dynamically respond to newly emerging threats, ensuring proactive and future-ready border security measures.
Threat domain classification	Organises threats into distinct categories such as land, air and sea, enabling targeted technology applications and specialised strategies for effective threat management across diverse border security challenges.
Technology functions criteria	Establishes specific requirements and capabilities needed from technologies to address diverse threat scenarios, guiding informed selections that enhance efficiency and response effectiveness.
Technology maturity classification	Assesses how developed and proven technologies are in real-world applications, ensuring chosen solutions are reliable, resilient and ready for immediate implementation in border contexts.
Alignment with strategic pillars	Integrates chosen technologies with overarching strategic goals, ensuring cohesive efforts that bolster security, operational efficiency and resource optimisation at borders.
Asset mapping	Details technological assets with locations and resource deployment, providing a comprehensive overview that supports strategic planning, optimised utilisation and enhanced situational awareness across border security domains.
Quantification of Systems	Determines the quantity and types of systems required for comprehensive border security, including supporting infrastructure such as wiring and provides approximate costing to support effective resource planning.
Technology blueprint	This constructs a comprehensive framework for border security technology deployment, consisting of several integrated layers to ensure cohesive operations.

Unlocking next-gen border security: A strategic approach for transformation and safety

Highlighted below is a strategic approach aimed at transforming border security and strengthening borders against future threats. The framework encompasses key steps including consolidating inputs, technology identification and selection, border security layout and technology blueprints.

By adopting this framework, border agencies can enable next-generation advancements and achieve greater safety.



Current State assessment and benchmarking study

Design principles

Consolidate inputs

Technology identification and selection

Border security layout

Technology blueprint

Total operating model including technology blueprint

Consolidate inputs	• Inputs • Leading practices (Process, technology, infrastructure)	• Regulations and guidelines (global) • Key risks applicable
Technology identification and selection	• Technology benchmarking • Define design principles • Mapping technologies to threats	• Evaluate technology mitigation capability • Determine technology maturity
Border security layout	• Detailed asset mapping layout • Location and quantity rationale for technology deployment	• Determine new BS infrastructure locations
Technology blueprint	• Develop technology blueprint guiding principles • Determine CCC requirements	• Detailed technology and software specifications

How can PwC help you?

Assessment	Current state assessment	Current state assessment (assessment of the existing border security) in three aspects i.e. • People • Process • Technology • Leading practice study for alignment and best practice
Design and Analysis	Threat mitigation technology assessment	• Define department vision and mandate • Identify existing and futuristic threats and existing technology infrastructure • Benchmarking technology and selection of technology • Develop framework for technology and threat mapping
	Technology selection and asset mapping	• Technology benchmarking and selection basis functionality • Develop design principles for asset mapping aligned to strategic goals • Devise strategic roadmap and detailed asset mapping layouts • Creating technology deployment plan with the planned physical infrastructure assets and terrain analysis • Design conceptual use cases and journey maps
	System performance analytics	• Defining layers of technology blueprint • Develop guiding principles for technology blueprint • Selecting network technologies and software for different layers • Prepare layer wise technology details and quantity breakup
Planning	RFP and supplier evaluation	• RFP preparation including pre-qualification, technical evaluation, scope of work, technical/functional specifications • Define service-level agreement parameters for different components • Support on pre-bid meeting and clarification response • Vendor response analysis (technical and commercial)
Implementation	Project management and implementation support	• Project management activities including risk mitigation and daily project coordination to meet project milestones • Supply installation testing (use case testing) and go live monitoring • Service level agreement monitoring for the edge devices, applications and IT infrastructure • Evaluation of change requests across project life cycle

Conclusion

Border security is crucial for Middle Eastern countries, as it plays a vital role in protecting national security, and ensuring regional stability. Strengthening the operational capabilities of border forces, improving surveillance and enhancing coordination between countries are essential to addressing many evolving threats. These measures are crucial for ensuring the security of both national borders and the broader geopolitical landscape.

Implementing intelligent systems, AI-powered analytics and state-of-the-art surveillance techniques will deliver new levels of security while facilitating trade and travel. This forward-looking approach ensures that borders are not only secure but also adaptive to the rapid changes of our digital age.

All stakeholders in the border security ecosystem must collaborate closely to adopt and optimise these next-generation solutions. By harnessing emerging technologies, we can build smarter, more resilient and people-centric border systems. The collective efforts of industry leaders, governments and technology providers will be critical to bringing this vision to life.

The journey towards next-generation border security has only just begun. PwC is committed to guiding you through every step of this transformation – ensuring our borders are better equipped to meet tomorrow's challenges while improving the experience for all who cross them.

References

- https://www.wto.org/english/res_e/booksp_e/wcotech22_e.pdf
- https://www.elibrary.imf.org/display/book/9798400200120/9798400200120.xml?code=imf.org
- https://www.wto.org/english/res_e/booksp_e/wco_wto_annex_the_case_studies.pdf
- https://www.apec.org/docs/default-source/groups/sccp/compendiumofsmartcustomspracticesforapececonomies_0424.pdf?sfvrsn=acc161e1_2
- https://mag.wcoomd.org/magazine/wco-news-104-issue-2-2024/automating-image-analysis- china-customs-implements-new-model-for-the-development-and-deployment-of-algorithms
- https://www.krit.re.kr/krit/bbs/reportsEng_pdf.do?bbsId=reportsEng&article_category=&nttId=4436&page=1&searchCnd=&searchWrd=&startd=&endd=&menu_no=05010000

PwC Middle East

Rajat Chowdhary

Partner, Technology

Mobile: +971504293733
Email: rajat.c.chowdhary@pwc.com

Majdi Dodokh

Partner - Strategy & Operations

Mobile: +971 56 682 0626
Email: majdi.dodokh@pwc.com

Sharang Gupta

Partner, Technology

Mobile: +971 504326559
Email: sharang.g.gupta@pwc.com

Dipesh Guwalani

Senior Manager, Technology

Mobile: +971 565205132
Email: dipesh.g.guwalani@pwc.com

PwC India

Vishal Kanwar

Partner, Aerospace and Defence

Mobile: +91 91677 45719
Email: vishal.kanwar@pwc.com

Sandeep PM

Associate Director, Aerospace and Defence

Mobile: +91 98735 53013
Email: sandeep.pm@pwc.com

Contributors

Ashutosh Phalke

Associate, Aerospace & Defence

Mobile: +91 82378 23672
Email: ashutosh.phalke@pwc.com

Saurabh Doke

Associate, Aerospace & Defence

Mobile: +91 98602 19748
Email: saurabh.doke@pwc.com

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 370,000 people in 149 countries. Across audit and assurance, tax and legal, deals and consulting we help build, accelerate and sustain momentum. Find out more at www.pwc.com.

With over 12,000 people across 12 countries in 30 offices, PwC Middle East combines deep regional insight with global expertise to help clients solve complex problems, drive transformation, and achieve sustained outcomes. Learn more at www.pwc.com/me.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.