مركز محمد بن راشد للابتكار الحكومي
MOHAMMED BIN RASHID CENTRE FOR GOVERNMENT INNOVATION

ابتكر
IBTEKR

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

2025

UAE'S CYBERSECURITY VISION

A BLUEPRINT FOR THE FUTURE

TABLE OF CONTENT

FORWARD BY H.E HUDA AL HASHIMI

DEPUTY MINISTER FOR CABINET
AFFAIRS FOR STRATEGIC AFFAIRS

Amid the growing digital challenges faced by governments around the world, the need for innovation in the public sector has become more urgent than ever. Cybersecurity is no longer just a technical function, it has become a fundamental pillar for enhancing national digital security, reinforcing public trust, and supporting economic progress.

The United Arab Emirates stands at the forefront of this transformation, not only through its investment in advanced technologies but also by developing practical, applicable models that other government entities can benefit from. This report highlights these pioneering experiences and showcases how the UAE turns ideas into tangible results through national initiatives, effective public-private partnerships, and an institutional culture rooted in experimentation and learning. It also presents leading international innovations and experiences in cybersecurity and public sector innovation, from cyber volunteer teams in the United States to national innovation challenges in Malaysia, and multi-sector cybersecurity hubs in France. These global models offer rich inspiration for experts and policymakers seeking practical and innovative solutions for the future of government work.

Through simulated cyberattack programs, national awareness campaigns, AI-powered defense solutions, and international exercises, the UAE continues to provide a leading model that demonstrates how governments can respond flexibly and effectively to evolving digital threats while fostering a culture of excellence and proactivity. These initiatives are not merely theoretical visions—they are practical models that offer valuable lessons for governments around the world.

We believe that sharing these experiences contributes to mutual learning and strengthens the collective security ecosystem. We hope this report opens the door to dialogue, stimulates creative thinking, and helps drive a broader global movement of governments striving to advance and stay at the forefront together.

FORWARD BY H.E DR. MOHAMED HAMAD AL KUWAITI

HEAD OF CYBERSECURITY | UAE GOVERNMENT

In an era where digital transformation drives every facet of economic and social progress, cybersecurity has become a pivotal pillar in strengthening national resilience. The United Arab Emirates (UAE) recognizes that trust in cyberspace is not merely a technical necessity—it is a strategic imperative that fosters innovation, prosperity, and international cooperation.

Since its establishment in 2020, the UAE Cybersecurity Council has been dedicated to positioning the nation as a global leader in digital trust and resilience. Guided by the ambitious vision of the National Cybersecurity Strategy 2025–2031, the Council has worked to develop frameworks, forge strategic partnerships, and build the capabilities required to protect critical infrastructure, enable the secure adoption of emerging technologies, and cultivate a culture of awareness and innovation across society. This vision reflects the UAE's firm belief that trust in cyberspace goes beyond technical need; it is a catalyst for innovation, prosperity, and international collaboration.

In recent years, we have witnessed a surge in cyber threats that have the potential to disrupt critical infrastructure and endanger national security. From ransomware attacks targeting healthcare systems to data breaches affecting government agencies and both public and private institutions, the impact of these cyber crises is profound. These threats jeopardize not only our digital assets but also public safety and trust.

This reality underscores the growing risks posed by cyber threats on a global scale and highlights the need for continuous vigilance and advanced security measures. The financial, healthcare, and energy sectors, in particular, bear the brunt of these threats. To combat them effectively, we must adopt a proactive approach focused on innovation and crisis anticipation. Predictive modeling capabilities now allow authorities to make swift, well-informed decisions—not just to respond to emergencies, but to foresee them. This marks a paradigm shift in how we address accelerating cyber threats.

Investing in cybersecurity innovation ensures the development of predictive analytics, real-time data assessments, and emergency scenario simulations. These tools provide valuable insights for preparedness and response by modeling different situations, enabling institutions and governments to prepare for diverse scenarios, refine emergency plans, and allocate resources more effectively based on real-time assessments.

Today, we face an urgent issue that affects us all: the increasing frequency and complexity of cyber crises in our interconnected world. Amid these challenges, it is essential to leverage advanced technologies to enhance national resilience through innovation, talent development, and the strengthening of expertise.

Our efforts have yielded unprecedented international recognition. The UAE has hosted global cyber exercises involving over 120 national entities from more than 133 countries—a milestone in strengthening international cooperation. These efforts culminated in 11 Guinness World Records achieved at GISEC 2025, a testament to our commitment to leadership and innovation.

Moreover, pioneering technology platforms such as the National Security Operations Center (NSOC), the "Pulse" Cyber Training Simulator, and the "Crystal Ball" Intelligence Information Exchange Platform are setting new global benchmarks for technical readiness, operational resilience, and strategic cooperation.

As we look to the future, the UAE will continue its leadership in promoting international collaboration, developing human capital, and securing digital innovation. Our unwavering commitment is to ensure that cyberspace remains a source of opportunity and trust for our citizens, a pillar of support for our economy, and a trusted partner to all our allies around the world..

EXECUTIVE SUMMARY

Cybersecurity has emerged as one of the most pressing global challenges of our time. The accelerated adoption of artificial intelligence, cloud services, IoT, and soon quantum computing has expanded the digital attack surface at unprecedented speed. Threat actors are growing in sophistication, as seen in the UAE's 2025 "blitz" campaigns involving 82.7 million exploitation attempts, 500 ransomware incidents, and 1.8 billion scanning events within just a few months.

At the same time, global ransomware ecosystems are diversifying — with a 58% increase in active groups in 2024 — while AI is enabling deepfake fraud, malware automation, and autonomous attack frameworks. Post-quantum cryptography has moved from theory to urgent necessity as adversaries adopt "harvest now, decrypt later" strategies.

Against this backdrop, the UAE has taken decisive steps to safeguard its digital future. The National Cybersecurity Strategy (2025–2031) provides a comprehensive roadmap with six goals: strengthening resilience, safeguarding society, building digital trust, enabling secure innovation, developing talent, and leading global partnerships. Its delivery pillars — Govern, Protect & Defend, Innovate, Build, Partner — align with the UAE's vision to be a trusted global digital hub.

This report highlights the UAE's progress and innovations, including:

Global Cyber Drill 2025: The world's largest cyber exercise, convening 124 authorities from 133+ countries, with scenarios led by ITU, UNCCT, INTERPOL, and FIRST.

Crystal Ball Platform: A secure environment for international intelligence collaboration, strengthened in 2025 through AI-powered analytics, onboarding improvements, and a government-to-government exchange program.

The Pulse Cyber Range: A flagship training platform driving workforce readiness and resilience across all sectors.

Guinness World Records: Eleven achievements at GISEC 2025, including the largest number of nationalities in a single cyber drill and the largest global awareness session.

Policy & Frameworks: Updated Information Assurance Standard, CIIP Policy, SOC Baseline, and new efforts on IoT, Cloud, and cross-border data flows.

Talent Development: Initiatives such as X-Labs, the GISEC Academy, and the Government Accelerators Dialogue to close the workforce gap and empower Emiratis in cybersecurity.

The UAE's approach reflects a simple truth: cybersecurity is not only about defense, but also about enabling innovation, economic growth, and social trust. By integrating policy, technology, talent, and partnerships, the UAE is shaping a secure digital future for its citizens and contributing to global resilience.

01

CURRENT STATE OF CYBERSECURITY IN THE UAE

The cybersecurity landscape in the UAE has continued to evolve rapidly, reflecting both the country's digital ambitions and the increasing sophistication of adversaries targeting its infrastructure.

The UAE currently hosts approximately

223,800

digital assets, and analysis shows that half of the top vulnerabilities are more than five years old. This outdated exposure continues to be exploited by adversaries, highlighting the importance of proactive patch management and coordinated national-scale vulnerability reduction. Addressing these long-standing weaknesses is critical to ensuring that the UAE's digital infrastructure remains resilient in the face of increasingly complex and sustained cyber campaigns.

The ransomware ecosystem in the UAE has also shifted significantly between 2023 and 2024, reflecting a diversification of threat actors and tactics. The number of active ransomware groups increased by 58%, underscoring the growing complexity of the threat environment. While LockBit3's share declined from 31% in 2023 to 16% in 2024, new players such as RansomHub (13%), DarkVault, Qilin, RansomEXX, and KillSec gained traction. Meanwhile, some groups, including Clop, disappeared entirely from UAE reporting, signaling both disruption and replacement within the ransomware ecosystem.

The financial impact of cyber incidents is equally significant. In 2024, the average global cost of a data breach reached

$4.88 million

driven by lost business, customer response costs, and incident containment. The Middle East, including the UAE, recorded the second-highest breach costs worldwide, underscoring both the region's economic importance and the financial pressure imposed by cyberattacks.

Distributed Denial of Service (DDoS) activity in the UAE saw a remarkable reduction. From the first half of 2023 to the first half of 2024, the country experienced a

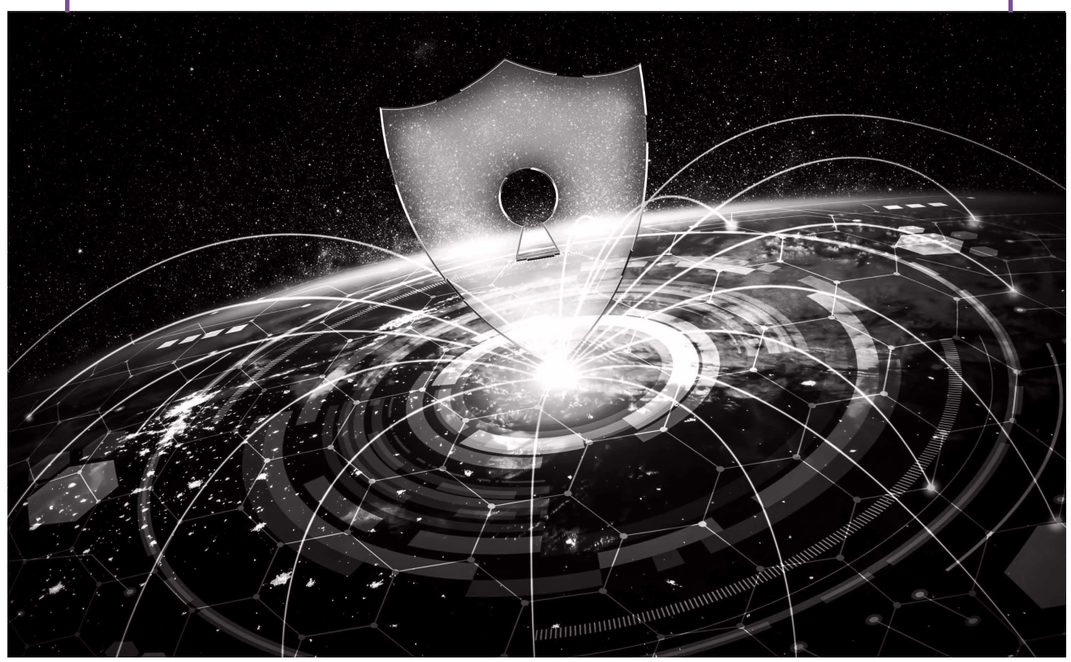
96% decrease

in DDoS attacks — **from 58,538 incidents to just 2,301.** The maximum recorded bandwidth **dropped from 266.9 Gbps to 85.92 Gbps,** while the average duration **fell to 18.53 minutes.** These improvements reflect greater resilience, even as global DDoS volumes increased and peak attack sizes rose to nearly 1 Tbps.

Meanwhile, infostealer malware has surged in prevalence. In 2024, **RedLine Stealer** accounted for

69.9%

of observed infections, followed by **META (13.1%)**, **Lumma (12.6%)**, and **Vidar (4.4%)**. These campaigns led to the leakage of more than 238,000 unique passwords. Notably, 77% of these compromised credentials already met NIST guidelines for password length, showing that even strong credentials are insufficient if devices and networks are infected with malware. This underscores the importance of layered defenses, endpoint monitoring, and multi-factor authentication.



According to CPX SOC analysis, the most frequent types of incidents in the UAE during 2024 were:

32% Misconfigurations

19% Improper Usage or Unlawful Activity

15% Scans & Probes

12% Phishing & Spoofing

9% Malicious Code

9% Unauthorized Access

4% Web Application Attacks

This breakdown emphasizes that governance weaknesses and configuration errors remain as impactful as technical exploits, reinforcing the need for both cultural and technical resilience.

Adversaries have also maintained a strong focus on high-value sectors. The most targeted industries in the UAE during 2024 were:

34.9% Government

21.3% Finance

14.1% Energy

11.6% Insurance

6.7% Healthcare

6.6% Defense

4.8% IT services

This concentration reflects adversaries' prioritization of national and economic infrastructure, with government systems remaining the primary focus of state-linked and eCrime groups alike.

Taken together, these trends illustrate a cybersecurity environment that is both highly dynamic and deeply challenging. The UAE faces adversaries with growing operational maturity — capable of launching intense blitz campaigns, exploiting outdated vulnerabilities, and rapidly evolving ransomware tactics — even as the nation strengthens its defenses and reduces exposure in critical areas such as DDoS resilience.

KEY CHALLENGES AND THREATS

The cyber threat landscape is evolving rapidly, with new tactics, techniques, and procedures (TTPs) emerging constantly. Threats now range from AI-generated malware and ransomware campaigns to deepfake-enabled social engineering and state-backed advanced persistent threats (APTs). Adversaries are increasingly exploiting cloud complexity, identity sprawl, and IoT devices, while also integrating artificial intelligence into their attack playbooks. In the UAE, the first half of 2025 saw adversaries conduct over 82.7 million exploitation attempts targeting the SMB protocol, followed by a "blitz" campaign involving 500 ransomware incidents, 28.7 million brute force attempts, and 2 million botnet recruitments. This combination of scale, speed, and automation makes it challenging for organizations to stay ahead and safeguard critical assets.

Some of the most concerning cyber threats on the horizon for 2025 include:

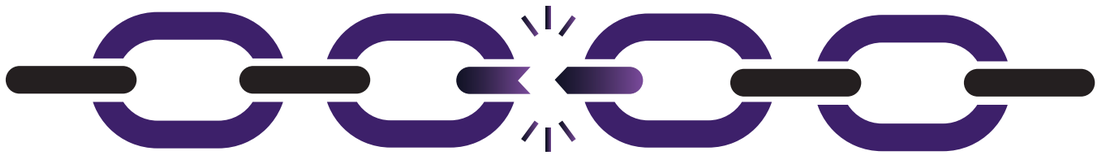
- AI-powered social engineering and deepfake-enabled fraud
- Software and open-source supply chain attacks
- Cybersecurity talent and skills shortage
- AI-driven malware and stealthy, malware-free attacks
- Post-quantum cryptography challenges
- Agentic AI and autonomous attack frameworks

AI-Powered Social Engineering and Deepfake Fraud

Social engineering scams are increasingly leveraging artificial intelligence (AI) and deepfake technology, creating highly convincing phishing emails, fraudulent calls, and video impersonations. In the UAE, AI-powered phishing campaigns targeting financial institutions and deepfake audio scams impersonating executives have already led to significant losses. Most strikingly, an Iranian-linked campaign hijacked UAE television broadcasts in 2024, using deepfake newsreaders to spread disinformation. These incidents underscore how generative AI tools have lowered the barrier for cybercrime, enabling even non-technical actors to craft targeted attacks that bypass traditional security controls.

Software and Open-Source Supply Chain Attacks

Supply chain compromises remain one of the most critical risks in 2025. Attackers increasingly exploit dependencies, build pipelines, and deployment mechanisms to infiltrate trusted environments. The UAE has also seen adversaries target widely used open-source components such as OpenSSH and Exim, with CVEs like CVE-2024-6387 (“regreSSHion”) affecting more than 16% of tested systems. These campaigns mirror the global wave of breaches through 2024, including attacks on widely used file-transfer and authentication platforms. To counter this, UAE organizations are adopting secure-by-design principles, NIAP posture testing, and zero-trust architectures, embedding resilience directly into their development and operations.



Cybersecurity Talent and Skills Shortage

The cybersecurity talent shortage remains a pressing issue in 2025, with estimates of over 4 million unfilled positions globally. This workforce gap poses significant risks as adversaries scale their operations using AI and automation. For the UAE, building local capacity has become a national priority. Initiatives such as X-Labs, the GISEC Academy, and the Government Accelerators Dialogue are developing skills pipelines, while public–private collaboration is expanding access to advanced training. Cultivating a robust cybersecurity workforce is essential to maintain resilience against increasingly sophisticated adversaries.

AI-Driven Malware and Stealthy Attacks

Advanced malware is becoming more adaptive and evasive in 2025. Adversaries are leveraging AI-driven tools to modify malware in real time, bypassing signature-based detection.

Ransomware-as-a-Service (RaaS) continues to dominate, with the UAE witnessing a

58% increase

in active ransomware groups in 2024.

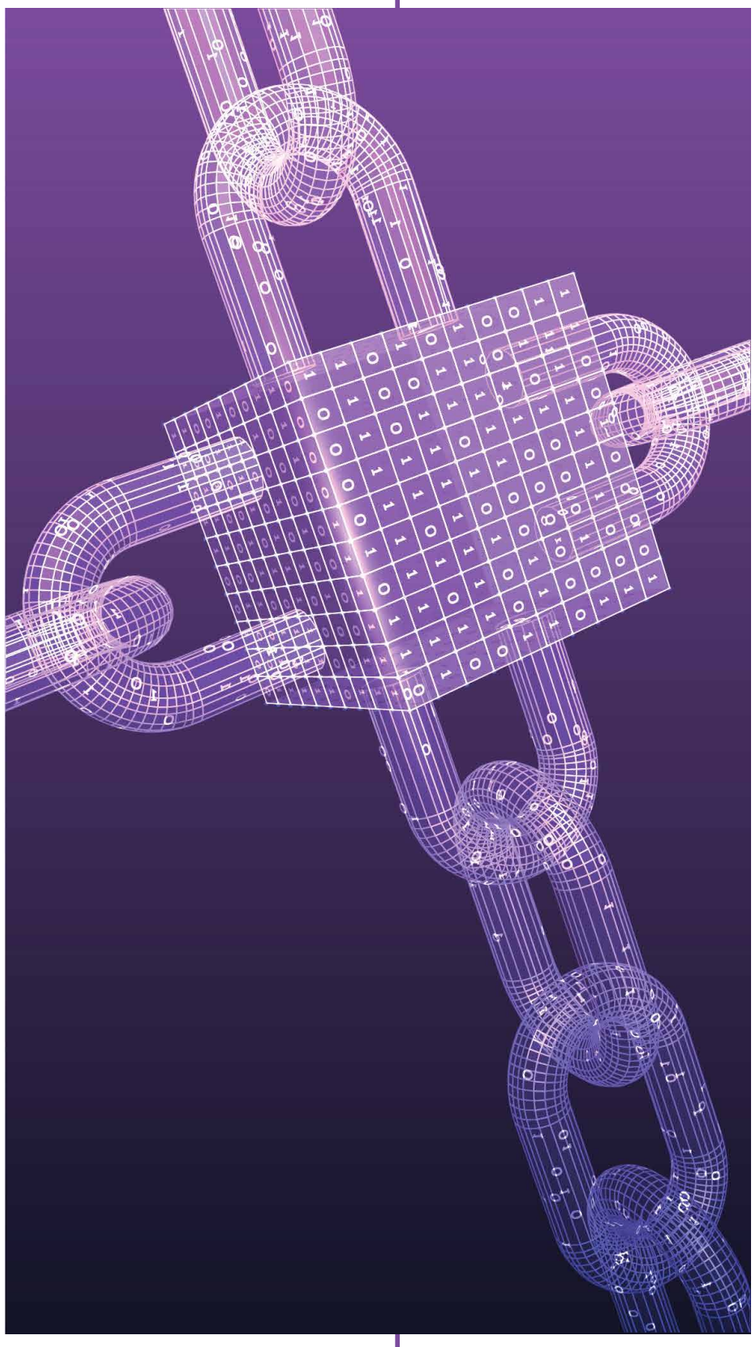
Attackers also exploit newly disclosed vulnerabilities (e.g., OpenSSH CVE-2024-6387) to execute code remotely. These developments underscore the need for proactive threat hunting, continuous monitoring, and rigorous patch management across all sectors.

Post-Quantum Cryptography Challenges

As adversaries adopt “harvest now, decrypt later” strategies, post-quantum cryptography (PQC) is gaining urgency. The UAE is aligning with global standardization efforts to implement lattice-based and code-based algorithms that resist quantum decryption. While PQC adoption faces challenges — including complexity, interoperability, and migration costs — early investment is critical for long-term security, especially in government, finance, and energy sectors, where the confidentiality of sensitive data must be preserved for decades.

Agentic AI and Autonomous Attack Frameworks

Agentic AI — autonomous AI systems capable of independently pursuing goals — is emerging as a frontier risk. Early signs suggest adversaries are experimenting with AI agents that can automate reconnaissance, vulnerability scanning, and even exploitation without human oversight. While still in its infancy, the weaponization of agentic AI poses a potential paradigm shift: from human-directed cybercrime to autonomous, machine-led attacks. The UAE and its partners are beginning to assess this horizon risk, prioritizing AI governance frameworks and safe AI adoption models.



KEY CHALLENGES AND THREATS

03

INNOVATION IN CYBERSECURITY

Definition of Innovation in Cybersecurity

Innovation in cybersecurity refers to the creation and implementation of new ideas, technologies, or processes that enhance resilience against evolving threats. This includes developing novel approaches to identify, prevent, detect, respond to, and recover from attacks.

In the UAE, innovation is embodied in platforms such as the National Security Operations Centre (NSOC), the Crystal Ball threat-intelligence exchange, the Pulse cyber range, and new programs such as X-Labs and the GISEC Academy, which together drive a culture of experimentation and leadership in global cybersecurity.

Importance of Innovation in Cybersecurity

The cybersecurity landscape is constantly evolving, with new threats emerging daily. Innovation is therefore critical for several reasons:

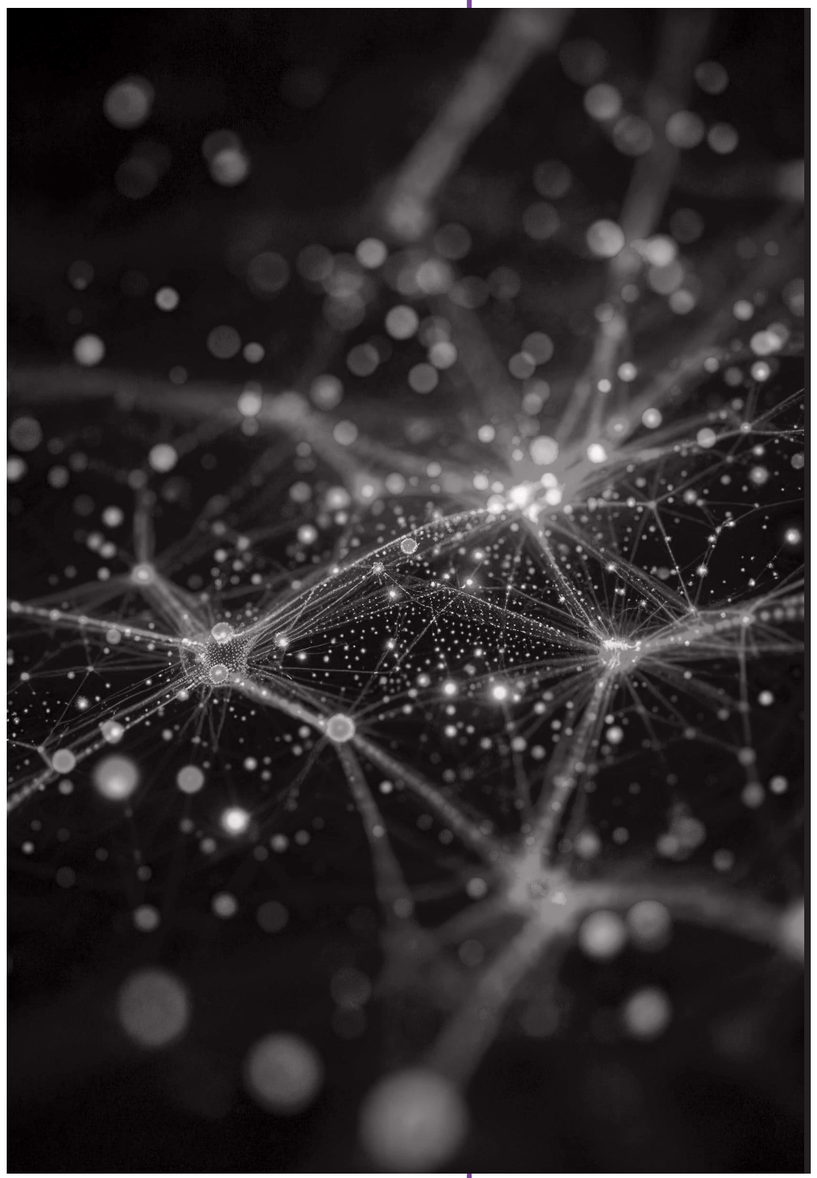
Staying ahead of threats: New threats require new countermeasures. Innovation helps organizations stay ahead of cybercriminals by developing advanced protection methods. In 2025 alone, UAE adversaries launched over 82.7 million exploitation attempts and a “blitz” campaign with 500 ransomware incidents and 1.8 billion scans.

Strengthening defenses: Innovative solutions can fortify existing security measures, creating a more robust defense against attacks. From 96% fewer DDoS attacks in 2024 to the 11 Guinness World Records won at GISEC 2025, the UAE has proven that innovation translates into measurable resilience.

Improving efficiency: Innovative technologies can streamline security operations, making them more efficient and cost-effective, such as Crystal Ball.

Protecting critical infrastructure: As reliance on digital systems grows and the UAE accelerates digital transformation across sectors including finance, energy, transport, and government, the protection of critical infrastructure becomes paramount to ensure that they remain secure.

Building trust: Demonstrating a commitment to cybersecurity innovation strengthens public confidence and reinforces the UAE’s reputation as a secure hub for global investment.



INNOVATION IN CYBERSECURITY

Global Benchmarks

Building Out a Cyber Civilian Corps

Michigan - USA

Most people are aware of the concept behind a volunteer fire department. When a fire disaster breaks out and there aren't enough full-time firefighters to combat the flames, a trained volunteer corps of firefighters can supplement the effort, and hopefully bring the fire to a halt with their help. Michigan is taking the concept of the volunteer fire department and applying it to another effort to protect citizens' safety: It has created and is rapidly expanding a volunteer civilian cyber corps.

The Michigan Cyber Civilian Corps (MiC3) is a group of trained cybersecurity experts who volunteer to provide expert assistance to enhance the state's ability to rapidly resolve cyber incidents when activated, and the group includes volunteers from government, education and business sectors. Michigan has made the expansion of this corps a priority since 2017, realizing that cybersecurity threats to the government are accelerating at an unforeseen pace.

The MiC3 began as a partnership among the state's Department of Technology, Management and Budget, the state's volunteer registry system, and the Merit Network. Volunteer recruitment initially depended on Merit and word of mouth. Interested volunteers completed an online assessment to verify their cybersecurity expertise, and Merit sent qualified applicants to the state's volunteer registry. Volunteers who passed a subsequent background joined the MiC3.

Membership today to the volunteer corps is open to information security professionals who are residents of the state of Michigan. Applicants are also required to have two years of direct involvement with information security, preferably security operations, incident response and/or digital or network forensics. Since 2018, the organization has onboarded around 200 members. New members apply through the State Government's website, and have to demonstrate their cybersecurity skills as well as commit to two weeks per year of dedicated training to be admitted.

Originally, members were grouped to handle cyber issues based on geographic proximity, but due to the proliferation of remote work over the last couple of years, they are considering shifting to groups focused on different sectors, such as finance, healthcare, and so forth.

What is also inspiring about the program is Michigan's dedication to making sure it gets replicated in other states across the country. The Deputy Chief Security Officer for the state of Michigan noted they had interest from about 15 other states in how to start similar programs.

INNOVATION IN CYBERSECURITY

The New American, a public policy think tank, even called for a 25,000-member national version modeled after Michigan's program (as of 2022 this does not yet exist, but the idea has been repeatedly brought up and is gaining some national traction).

The impact of this group of cyber volunteers is only set to grow since Michigan's Governor signed legislation to make it easier to call on and deploy the corps and expand its reach so it doesn't just help Michigan-level government, but so it can help local governments, nonprofits and businesses across the state in the case of a breach or cyberattack. Previously, the corps could only be activated if the governor declared a "cyber state of emergency" – which had never happened before.

Lastly, the volunteer corps doesn't benefit just the government, but the entire cybersecurity community across Michigan. Michigan now has cybersecurity experts who are out in loosely knit communities who really don't have any way to know each other unless they happen to attend the same event or have the same employer. So, members started monthly conference calls to chat about what's going on, what's coming in their programs, and general networking and team-building and questions and answers. All of these features are great for the cybersecurity ecosystem in Michigan.

Cybersecurity Innovation Network
Canada

In February 2022, to address the cybersecurity challenges in terms of research and development, innovation, and training, and to help institutions and businesses across the country manage cyber threats, the Government of Canada announced $76.4 million in funding over four years to the National Cybersecurity Consortium (NCC).

The NCC, as a lead recipient, is establishing the Cyber Security Innovation Network (CSIN), a vital platform for the advancement of cybersecurity in Canada. The CSIN is a pan-Canadian network of post-secondary institutions, large and small private-sector firms, provincial/territorial and municipal governments, and not-for-profit organizations. The members are linked into a collaborative and engaged network that delivers strategically selected highly innovative projects in research and development, commercialization and training.

The NCC and the CSIN network are co-led by five Canadian universities: University of New Brunswick, University of Calgary, Ryerson University, Concordia University, and University of Waterloo.

The network will enhance research and development, increase commercialization, and develop skilled cybersecurity talent across Canada. It will fund high-impact projects that will be realized in collaborations between universities and colleges, private-sector firms of all sizes and public-sector and not-for-profit organizations from all regions of Canada.

With the federal investment, the consortium will have a starting budget of over $160-million in cash and in-kind contributions from supporting organizations. The consortium's focus is to help expand the commercial cybersecurity sector in Canada while contributing to the country's cybersecurity health.

In applying to lead the network, the consortium worked collaboratively with more than 140 researchers from 35 postsecondary institutions across Canada, 46 companies of all sizes, 26 not-for-profit organizations as well as provincial governments and governmental organizations.

The network will be required to provide a 1:1 cost-matching of the federal contribution, for an additional $80 million over four years, to be provided in the form of a combination of cash and/or in-kind contributions.

The matching contributions will be expected to come from a combination of non-federal government partners (e.g., private sector, provincial/territorial/municipal governments, and others, such as not-for-profit organizations and Canadian post-secondary institutions).

According to Statistics Canada, the Canadian cybersecurity industry contributed over $2.3 billion in GDP and 22,500 jobs to the Canadian economy in 2018. Meanwhile, Canadian businesses reported spending $7 billion in 2019 to prevent, detect and recover from cyber security incidents. CSIN will lead training projects that make equity, diversity and inclusion a priority. In addition to the research and training, the network will connect scholars, entrepreneurs, cybersecurity professionals and learners through many channels such as working groups, conferences, workshops and research challenges.

Active Cyber Defence Program
United Kingdom

In the UK, over four in 10 businesses and one-fifth of charities were subject to a cybersecurity breach or attack in 2020-2021. Official figures suggest that a UK resident is more likely to be a victim of cybercrime or fraud than any other offense. Moreover, perhaps on account of the UK's relative wealth, its population is more than twice as likely to be targeted by cybercriminals compared to the global average, and each crime is more than twice as lucrative as the global average. One estimate suggests that £4.6 billion was stolen from 17 million UK internet users in 2017.

The government-funded Active Cyber Defence (ACD) program was first deployed in 2018. Its principal goal was to prevent cybercriminals from leveraging government networks and brands to defraud and deceive users of government services. Fortunately, most cyber criminality is relatively unsophisticated and careful use of available technologies can do much to reduce its volume and effect. Deployed and tested initially across the public sector, ACD tools and techniques are now being promoted for use beyond government networks to improve cybersecurity across the private sector and civil society. This raises questions about government intervention in the private sector and elsewhere, particularly as ACD was set up and is overseen by part of the UK's signals intelligence agency.

The overall aim of the ACD program is to ensure that UK networks, data and systems in the public, commercial and private spheres are resilient to and protected from cyber-attack. This approach correctly recognizes that it is impossible to deter every malicious cyber actor, whether state, criminal, terrorist, or any other committed group or individual. The requirement therefore arises to improve cyber defenses such that they 'will significantly reduce our exposure to cyber incidents, protect our most precious assets, and allow us all to operate successfully and prosperously in cyberspace.'

Its unique contribution is in taking a proactive approach to improving cybersecurity outcomes, using relatively automated processes that scale well in a timely and efficient fashion to protect UK networks, users and interests. The ACD program has prevented thousands of attacks and reduced the average time a phishing site is online from 27 hours to 1 hour.

Its unique contribution is in taking a proactive approach to improving cybersecurity outcomes, using relatively automated processes that scale well in a timely and efficient fashion to protect UK networks, users and interests.

The ACD program has prevented thousands of attacks and reduced the average time a phishing site is online from 27 hours to 1 hour.

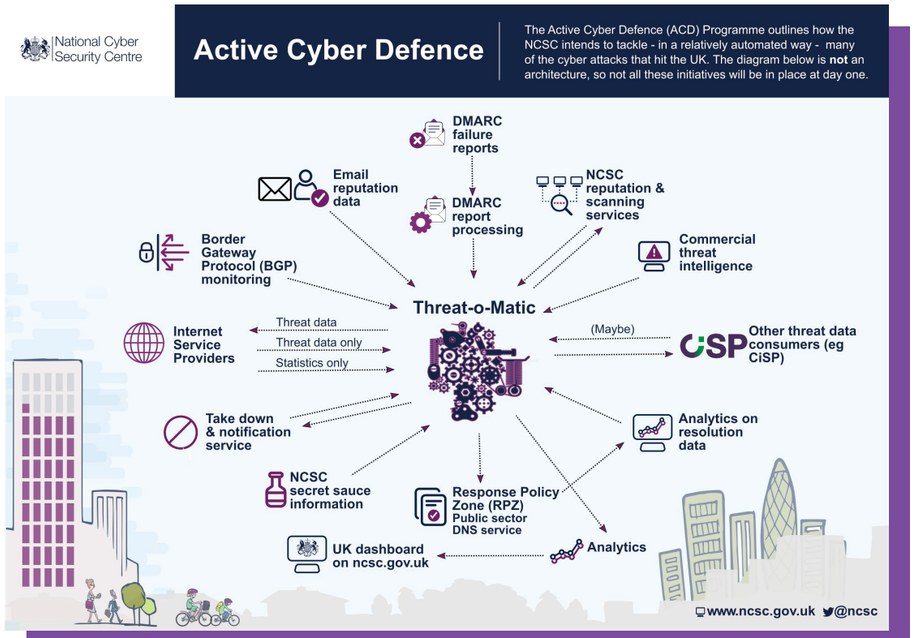


Figure 1

ACD tackles the problem of 'commodity attacks', understood as the high volume of relatively unsophisticated malicious software (malware) that afflicts networks, systems and users on a daily basis, as well as multiple forms of credential theft, account hijacking, and so on. It is not set up to deal with 'high-end' actors, political or criminal, that develop and deploy much more sophisticated and targeted operations against UK assets. This responsibility lies elsewhere, which works with its intelligence, military and policing partners on tailored operations to counter these high-level threats.

ACD automates responses to many different types of commodity attacks, including phishing, but the ACD 'ecosystem' also includes a range of other operations (see Figure 1). The following provides a snapshot of its four main activities, all of which have initially been deployed across the public sector only:

Takedown Service:
Asks hosting providers to remove websites and content impersonating the UK government and others.

Mail Check:
Makes it harder for criminals to distribute emails that look like they come from a trusted source, such as a government agency.

Web Check:
Helps government website owners check for common security issues.

Protective Domain Name System (DNS):
Blocks government users' access to bad websites, such as those known to distribute malware.

ACD includes a range of other initiatives, including protocol monitoring. This component aims to improve how internet and telecommunications protocols handle internet traffic, so as to make it more difficult to hijack UK assets and use them in, for example, distributed denial-of-service attacks. This applies across the public and private sectors by dint of the common protocols used.

In its first annual report on ACD, published in February 2018, it was reported that people in the UK are objectively safer in cyberspace because of the ACD program. In October 2018, further figures were released to bolster these claims. For example, the Takedown Service more than halved the UK's share of global phishing attacks to 2.4 per cent, with nearly 140,000 UK-hosted phishing sites being removed, plus more than 14,000 impersonating the UK government. Protective DNS blocked an average of nearly 11,000 malicious domains every month, making these unavailable to government web users. Web Check identified over 2,300 urgent issues across the government's digital estate, allowing them to be fixed. The figures also showed that uptake of these services across the government had increased significantly.

Five interlocking principles underpin the ACD approach to UK cybersecurity:

The first is that ACD in its initial iteration has only been used to protect the public sector. NCSC has described this as an 'eat your own dog food' attitude, using the government as a guinea pig. The presumption here is that the government will not ask anyone to implement cybersecurity solutions that it has not tested on itself.

The second principle is automation. NCSC and its partners are working towards automating as much of the day-to-day operation of ACD components as possible. This applies to the forms of technical monitoring and filtering required of ACD but also to the generation of threat intelligence and reporting mechanisms to government and other partners.

Third, ACD emphasizes that cybersecurity cannot be left to the market alone and serves to remind businesses that the UK government is not averse to taking decisive action if the market cannot deliver adequate cybersecurity solutions.

The fourth principle concerns transparency in reporting. ACD publishes an annual report, to drive up awareness and quality of cybersecurity.

A fifth identifiable principle is that of partnership. Many of the ACD elements have been developed and implemented with organizations outside the public sector.

National Innovation Challenge Program
(Cyber100) - Malaysia

In order to meet the ever-growing demand of cybersecurity solutions, the Malaysia Digital Economy Corporation (MDEC), in collaboration with the National Cyber Security Agency (NACSA), initiated the National Cybersecurity Innovation Challenge Program (Cyber100). A collaboration between NACSA and MDEC helps to create a conducive domestic environment for innovation and R&D. The Cyber100 initiative hosts numerous cybersecurity challenges on a national scale. Its goal is to seek solutions for industry-specific problems while promoting the creation of local innovative technologies. This further strengthens Malaysia's information security community and position as a digital hub.

Cyber100 is Malaysia's First Cybersecurity Innovation Challenge Program. The initiative includes various awareness and innovation platforms and services that help develop and enhance national cybersecurity capacities and capabilities.

The Cyber100 Challenge was launched in November 2019 in the hopes of building a better connected and more secure nation. The Cyber100 Challenge began with entry submissions from various existing companies, of which only six were shortlisted. Unlike many other tech competitions in other countries, participants here need not be startups. The shortlisted firms then participated in an orientation program, whereupon the companies updated committee members of their progress. In return, the committee members guided and advised these participants accordingly.

After the orientation period, the six companies were required to present and demonstrate their challenges and proposed solutions. The demonstration gave them the opportunity to receive feedback and comments on their respective solutions. By the end of the Cyber100 Program, there was an opportunity for the solutions that the six companies presented to undergo pilot testing and be adopted by other agencies with help from the supporting ecosystem partners.

INNOVATION IN CYBERSECURITY

Challenges and solutions from the first cohort of shortlisted companies included:

Securemetric (a leading cybersecurity company in Southeast Asia with strong in-house R&D capabilities in Digital Signature, Time Stamping and Authentication Solutions utilizing Public Key Infrastructure technologies). Problems: security digital identity, transactions, and applications. Solutions: using AI to prevent unauthorized access, new password criteria, and new password-free authentication standards.

Nexagate (one of Malaysia's Leading IT Security Consulting and Service Providers). Problem: facing significant challenges in mitigating cyber risks which include increasing compliance requirements, costly security solutions to deploy and maintain, and shortage of cybersecurity talents. Solution: a unified management system that shows relevant information to various levels of stakeholders. The platform presents 3 key areas in monitoring the cybersecurity posture of the organization, which includes Compliance, Threat, and Protection Management.

Compliance Management	Threat Management	Protection Management
ISMS Dashboar	Asset and Threat Dashboard	Protection Dashboard
Document Management	Asset Discovery	Web Security
Implementation Tracking	Vulnerability Scanning	DDOS Protection
Incident and Change Management	Vulnerability Report	Endpoint Protection

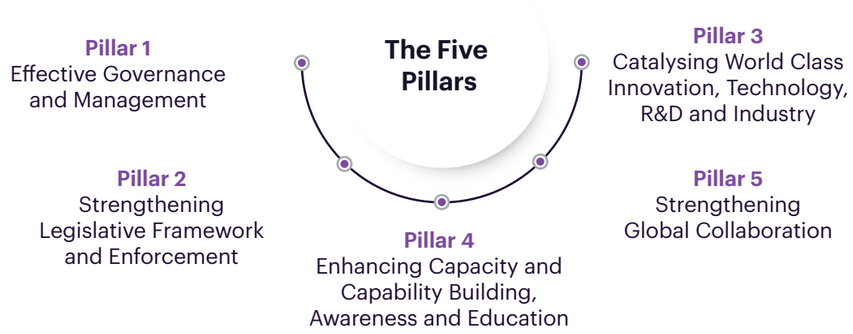
DNSVault ITP (a DNS based domain filtering solution, hosted and managed by a shared cloud environment). Problem: Cyberattacks against big companies are well-publicized by the news media, while attacks against small firms generate little attention; This can give small businesses a false sense of security, yet, small firms are generally more vulnerable than large ones because they have fewer resources to devote to security. Solution: scalable cloud security systems reduce IT overhead costs.

Tecforte (an award-winning company that specializes in Cybersecurity Information and Threats Management). Problem: there are too many new devices and new cyber threats to manage and monitor; due to lack of resources and tools, many fail to process security events and attacks in real-time. threat intelligence platforms that make cybersecurity operations more secure and sustainable by combining everything needed to manage cybersecurity effectively in one place.

SecureKi (specializes in securing and managing credentials which helps many customers to stop targeted attacks, mitigate insider threats, achieve compliance, improve operations and secure the hybrid enterprise). Problem: need for compliance risk reduction and improving operational efficiency by enabling privileged access defense. Solution: next generation automated privileged password management, with visual recording, fine-grained access control, multi-factor authentication, and Infrastructure Single-Sign-On capabilities.

e-Lock (premier IT security company that provides enterprises with solutions against identity thefts, advanced cyber-attacks and threats to corporate data integrity). Problem: the sophistication and ingenuity of the ransomware strikes have made it difficult for standard anti-viruses and firewalls to be effective against strikes. Solution: two-step protection against ransomware; the first layer is a Zero-day Attack Solution which creates a wall of trusted applications to provide a fence of protection for hardware and devices against unknown attacks, and the second layer protects the data while providing seamless real-time encrypted data backup.

Malaysia Cyber Security Strategy 2020-2024



National Cybersecurity Talent and Innovation Base
China

Each year the demand for cybersecurity professionals in China dwarfs the supply. In fact, only 5% of open positions are filled annually. Despite a deficit of 1.4 million cybersecurity professionals, China is already a near-peer cyber power to the United States, and now China wants to be a “cyber powerhouse”.

At the heart of that mission is the sprawling 40 square kilometer campus of the National **Cybersecurity Center (NCC).** Formally called the National Cybersecurity Talent and Innovation Base, the NCC is being built in Wuhan. The campus, which China began constructing in 2019 and is still building, includes seven centers for research, talent cultivation, and entrepreneurship; two government-focused laboratories; and a National Cybersecurity School.

The NCC is a major component of China’s response to its cybersecurity problems. The NCC will improve China’s cyber capabilities by focusing on two goals: cultivating talent and spurring innovation. The “base” is more of a sprawling industrial park than a gated military installation. Although there are four smaller cybersecurity parks and industrial bases in Chengdu, Shanghai, Shanxi, and Tianjin, none are on par with the NCC. The other four combined are less than a quarter of the NCC’s size, and many orders of magnitude smaller by investment. The breadth of the initiative is indicative of its importance. China’s policymakers argue that the NCC is the only “base” to merge government, industry, academia, research, and application of technology.

The NCC's impact will soon be felt—the National Cybersecurity School opened to students in August 2020. Its first class of graduates will graduate in June 2022. From there, they will go on to join the ranks of China’s cyber operators, whether in the public or private sphere. No matter where they go, government leaders will have continued access to NCC’s graduates and innovations. Rather than teaching basic content, the school aims to ensure that the best and brightest of academia and the private sector are teaching promising students under government direction, with particular focus on practical skills, innovation, and entrepreneurship. To that end, the school counts training programs, competitions, published papers, inventions and patents obtained, and professional certificates towards degree credits. The school pays special attention to its doctoral program, providing a strategic scientific mentor and an innovative entrepreneurship mentor to help doctoral candidates conduct and monetize applied research. Although its first graduating class includes only 1,300 students, policymakers hope to increase that number to 2,500 each year.

INNOVATION IN CYBERSECURITY

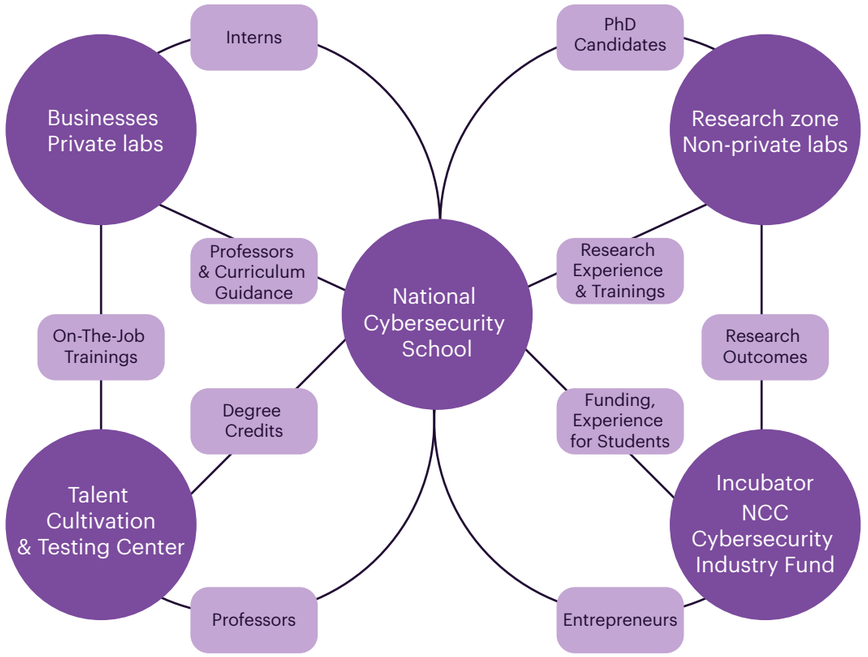
The Talent Cultivation and Testing Center, the second talent-focused component, offers courses and certifications for early- and mid-career cybersecurity professionals. The Talent Cultivation and Testing Center has the capacity to teach six thousand trainees each month, which is more than seventy thousand in a year at full capacity. Combined, both components of the NCC could train more than five hundred thousand professionals in a decade.

Attracting China's top cybersecurity professionals to work at the NCC is crucial to its success. CCP policymakers' vision for luring the country's top cyber talent with housing and employment opportunities is something akin to the cybersecurity version of an old U.S. "company town," but with greater investment in compensation packages.

Wuhan Municipal Cyberspace Administration and the National Cybersecurity School will use research subsidies and talent awards to attract talent to the NCC. The Wuhan Party Committee and municipal government will offer a one-time sum of RMB 2 million (approximately $309,000) to attract highly-qualified cybersecurity professionals to teach at the school. 34 This represents between 10- and 20-years' worth of the median annual salary in the cybersecurity field—a staggering sum that falls on the more generous side of China's talent programs. A separate program targets teams of researchers whose work is deemed critical to cybersecurity. The Wuhan municipal government will provide up to RMB 100 million to support their move to the NCC. These two policies act in tandem to attract the best practitioners without disrupting ongoing innovation.

Though the NCC is still under construction, businesses are lining up to claim a slice of land. As of September 2020, 114 companies had agreed to establish a presence in the NCC, promising more than $71.5 billion in investment.

Concept map for components of the NCC



Technology Authentication Center	Technology Evaluation Center	Supercomputing & Big Data Center	Talent Programs	Exhibition Center	Commercial Center

Driving maritime innovation, cybersecurity resilience
Singapore

Singapore has unveiled plans to drive innovation and beef up cybersecurity resilience in its maritime industry through new initiatives that include a roadmap to guide organizations in the sector to trial additive manufacturing practices. Maritime and Port Authority of Singapore (MPA) said it would look to develop maritime cybersecurity capabilities, so the industry had the resilience and infrastructure to manage disruptions. The country has said it aspires to be the “Silicon Valley for maritime technology”, focusing on digitalisation, innovation, and partnerships.

Specifically, it introduced a report that aimed to provide a roadmap to help organizations trial new practices in additive manufacturing. The new report outlined maritime additive manufacturing capabilities in Singapore as well as learning points from previous trials and adoption processes.

To further drive digital transformation in the sector, MPA said the Sea Transport Industry Digital Plan had been expanded to allow some 3,000 small and midsize businesses (SMBs) in all sea transport market segments to apply for co-funding assistance. This would include SMBs in subsectors such as ship brokers, marine surveyors, and ship operators, which can now apply to receive funding support for the adoption of pre-approved digital tools. They also inked an agreement with seven industry players, including Eastport Maritime, Ocean Network Express, and Orient Maritime Agencies, to boost the local sector's cybersecurity capabilities.

The collaboration would see the establishment of a maritime cybersecurity roundtable, during which participants would recommend initiatives aimed at improving maritime cybersecurity partnership. These would include data sharing, boosting local maritime cyber skillsets, and driving greater awareness as well as access to digital maritime tools and skills. This roundtable was slated to kick off its first meeting later in 2022. The event will look at initiatives over the next three years to boost Singapore's cybersecurity defense and maritime cybersecurity skills.

Government leaders noted the need for maritime cyber risk management to be incorporated into the safety management systems of companies operating Singapore-flagged vessels.

The Maritime Cluster Fund will also provide co-funding support for cybersecurity training courses to ensure workers are aware of risks and have the knowledge and skills to protect themselves from cyberattacks. In addition, the MPA had been working with its peers through the Port Authorities Chief Information Officer Cybersecurity Network to share data and best practices.

Launching a dedicated 'Cyber City'
France

In early 2022, the French government unveiled a cyber city, designed to bring together public and private sectors to collaboratively tackle cyber attacks. This comes on the back of a record year for ransomware attacks and more recently as governments worldwide, but especially those in Europe, prepare themselves for possible cyberattacks from Moscow in retaliation for Ukraine sanctions.

Dubbed the **"Cyber Campus"**, and located near Paris' La Defense business district, this new cyber city arrives a year after the launch of France's cybersecurity strategy. The strategy is a €1 billion initiative designed to both improve the country's resilience and build its cyber industry, as the government looks to triple the revenue in the cybersecurity sector to €25 billion in the coming years, double the number of jobs to 75,000 and produce new French cybersecurity 'unicorns'.

It is in the just-opened, 13-storey Cyber Campus that the French government's cyber strategy will be achieved – as it brings together private companies, both large corporations and startups, public bodies, the military, government departments, cyber researchers and students to pool resources and collaborate. A short term expansion nearby in Versailles is possible, according to the government, and regional versions of Campuses are additionally planned for the coming years.

The Cyber Campus **building** consists of:

12,000 square
meters of private
or shared workspaces.

3,000 square
meters of project and
innovation platforms.

2000 square
meters devoted
to training.

Common areas
with an auditorium, a
showroom, and a TV studio.

(Cyber Campus building in La Defense)

Taking a multi-disciplinary approach, the Cyber Campus not only encourages collaboration between private and public sectors to tackle the growing threat of cyberattacks but brings together the best minds in the industry to ensure France becomes a hotspot for cyber innovation. It will also provide a place for professional skills development and for developing awareness publicly. The Campus is based on Israel's success with the CyberSpark venture in Beer Sheva, which began as a cybersecurity research facility and later successfully morphed into a hub for startups and innovation. The Cyber Campus project will provide a platform for multi-stakeholder collaboration, particularly around incident response.

Campus Cyber can currently host 1,800 people across its 26,000 square meter building, but initially launched with only 700 experts. It is run by a new joint-stock company that is 44% owned and funded by the French state, with the rest of the capital divided among about 90 organizations, including France's leading companies in the field.

French corporations such as Orange, Capgemini, Thales and Atos have signed up as both investors and participants, along with numerous cyber-related startups, research organizations, and government departments including the cyber defense department. To date, more than 160 players from a variety of business sectors have confirmed their commitment to the Digital Campus. The French Ministry of the Interior, the Ministry of the Armed Forces, the National Information Systems Security Agency (ANSSI), and the National Institute for Research in Digital Sciences and Technologies (INRIA), will also set up on the site, using approximately 21% of the building.

Cyber Campus was originally announced in summer 2019, when, against a backdrop of heightened risk, French President Emmanuel Macron announced its creation to promote synergy within the sector and develop leading-edge cyber solutions. French leadership has declared they do not want to depend on foreigners in regards to advanced technology.

Best Practices

Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) is a security model that assumes no one or nothing is inherently trustworthy, regardless of location (inside or outside the network). It's built on the principle of "never trust, always verify."

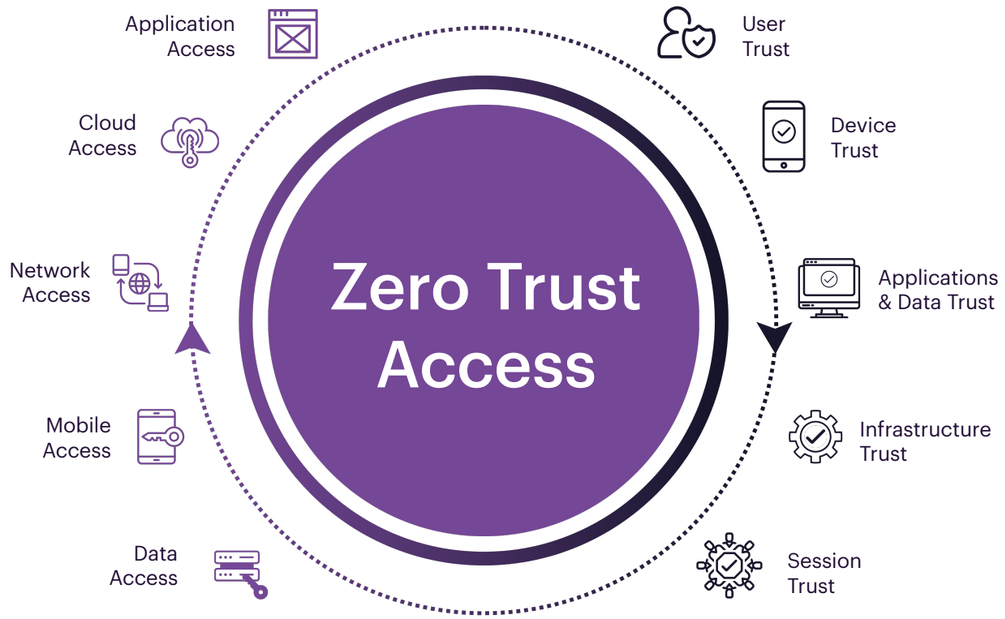
ZTA is a security architecture based on this model. It focuses on:

- Strong authentication: Every user and device must be verified before access is granted.
- Least privilege access: Users only have access to the data and resources they need to do their job.
- Continuous verification: User and device security is constantly monitored and assessed.
- Microsegmentation: Networks are divided into small segments to limit the impact of a breach.

Benefits of ZTA:

- Enhanced security by reducing the attack surface
- Improved protection against data breaches
- Better visibility into network activities
- Faster incident response

Essentially, ZTA shifts the focus from protecting a network perimeter to protecting data and resources, no matter where they are located.



Cloud-native security

Cloud-native security is a holistic approach to protecting cloud environments, integrating security into the development lifecycle from the start. It focuses on securing applications, platforms, containers, and infrastructure, while addressing the unique challenges of cloud environments.

Key Components and Strategies

DevSecOps: Incorporating security into the development process (shift-left) to identify and address vulnerabilities early.

Cloud Native Application Protection Platform (CNAPP): A unified platform providing comprehensive protection for cloud-native applications throughout their lifecycle.

Zero Trust Architecture: A security model based on the principle of "never trust, always verify," limiting access to resources and data.

Identity and Access Management (IAM): Controlling access to cloud resources through robust authentication and authorization mechanisms.

Infrastructure as Code (IaC) Security: Securing cloud infrastructure defined and managed through code.

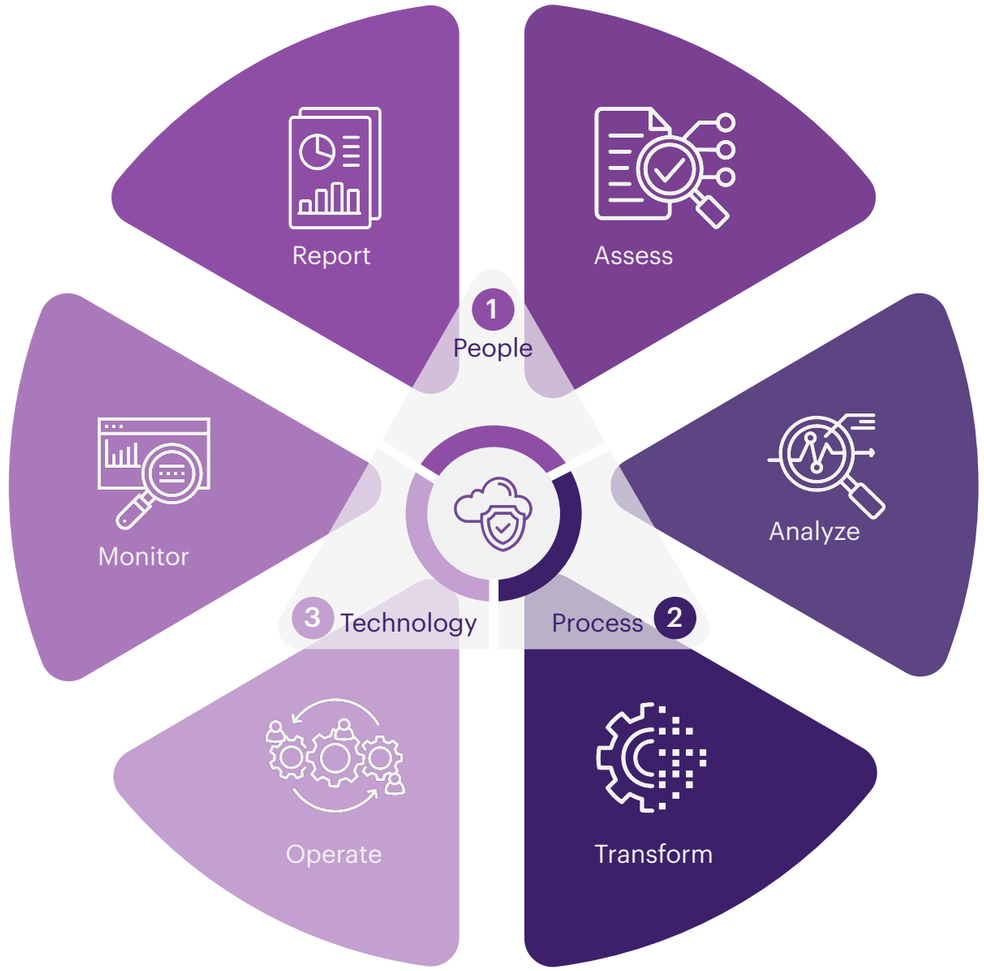
Container Security: Protecting containerized applications and their runtime environments.

Data Protection: Safeguarding sensitive data through encryption, access controls, and data loss prevention.

Continuous Monitoring and Response: Proactively identifying and responding to threats through real-time monitoring and automated incident response.

Benefits of Cloud-Native Security

- Improved security posture
- Faster time-to-market
- Reduced risk of data breaches
- Enhanced compliance
- Increased agility and scalability



Identity Management Powered by Blockchain

Blockchain-based identity management is a revolutionary approach to managing and verifying digital identities. Unlike traditional systems reliant on centralized authorities, blockchain offers a decentralized, secure, and transparent platform.

Key Features:

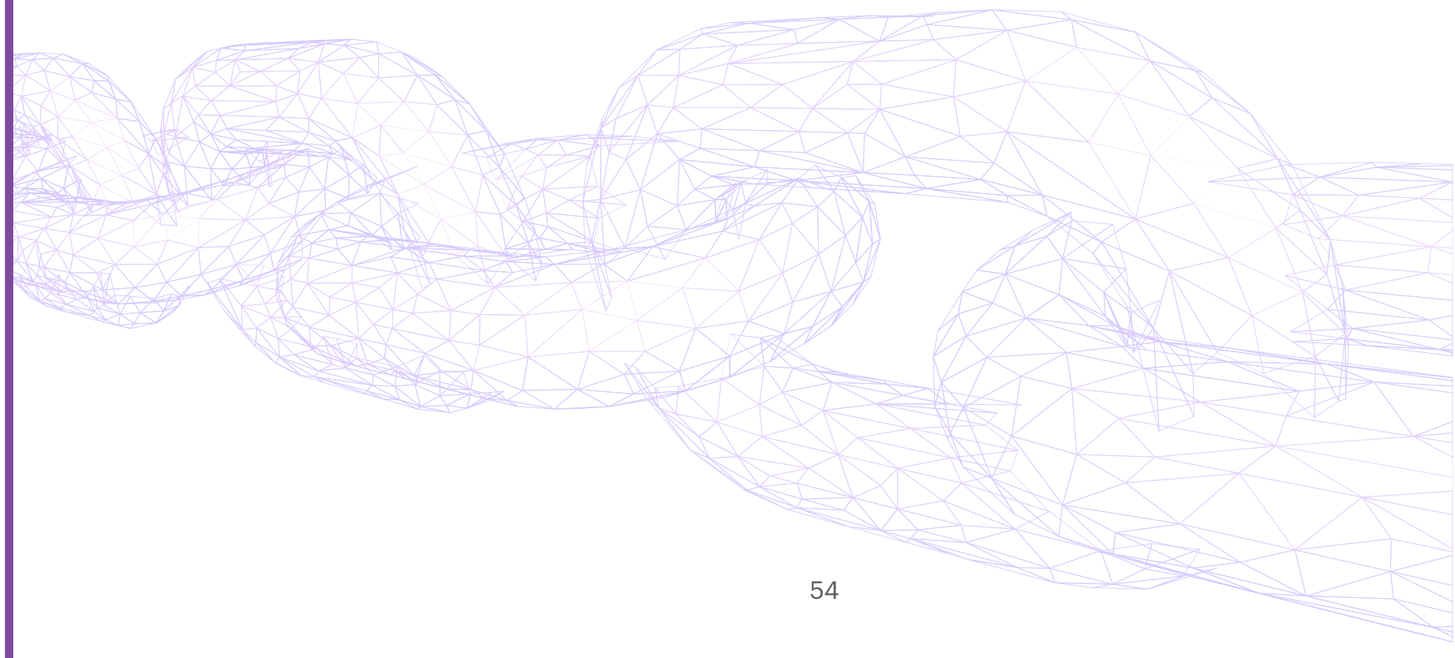
- Decentralization: Identity data is stored across multiple nodes, reducing the risk of data breaches and single points of failure.
- Security: Blockchain's cryptographic mechanisms ensure data integrity and protect against tampering.
- Privacy: Users have control over their data, deciding what information to share and with whom.
- Efficiency: Streamlined identity verification processes reduce costs and time.
- Interoperability: Different systems can easily share and verify identity information.

How it Works:

- Identity Creation: Users create a digital identity, often using a self-sovereign identity (SSI) approach, where they control their data.
- Data Storage: Identity information is stored on the blockchain as a series of encrypted blocks.
- Verification: When identity verification is needed, users can selectively share specific attributes with verifiers.
- Consent Management: Users have granular control over their data, determining who can access it and for what purposes.

Benefits:

- Enhanced security and privacy
- Reduced identity fraud
- Improved efficiency in identity verification
- Increased trust and transparency
- Empowers individuals with control over their data



Automated Incident Response and Information Sharing Platform

An Automated Incident Response and Information Sharing Platform (AIRISP) is a technology solution designed to streamline and enhance the process of responding to cybersecurity incidents. It combines automation, collaboration, and intelligence to improve efficiency and effectiveness in incident management.

Key functionalities of an AIRISP typically include:

Incident Detection and Alerting: Automatically identifies potential security incidents based on various data sources and triggers alerts.

Incident Orchestration: Automates routine tasks, such as creating incident tickets, assigning responders, and initiating response playbooks.

Threat Intelligence Integration: Incorporates threat intelligence data to enrich incident analysis and inform response actions.

Collaboration and Communication: Facilitates collaboration among security teams and other stakeholders through integrated communication tools.

Automation of Response Actions: Executes pre defined response actions based on incident severity and type, reducing manual intervention.

Information Sharing: Enables secure sharing of incident data and intelligence with external partners to improve collective defense.

Benefits of using an AIRISP:

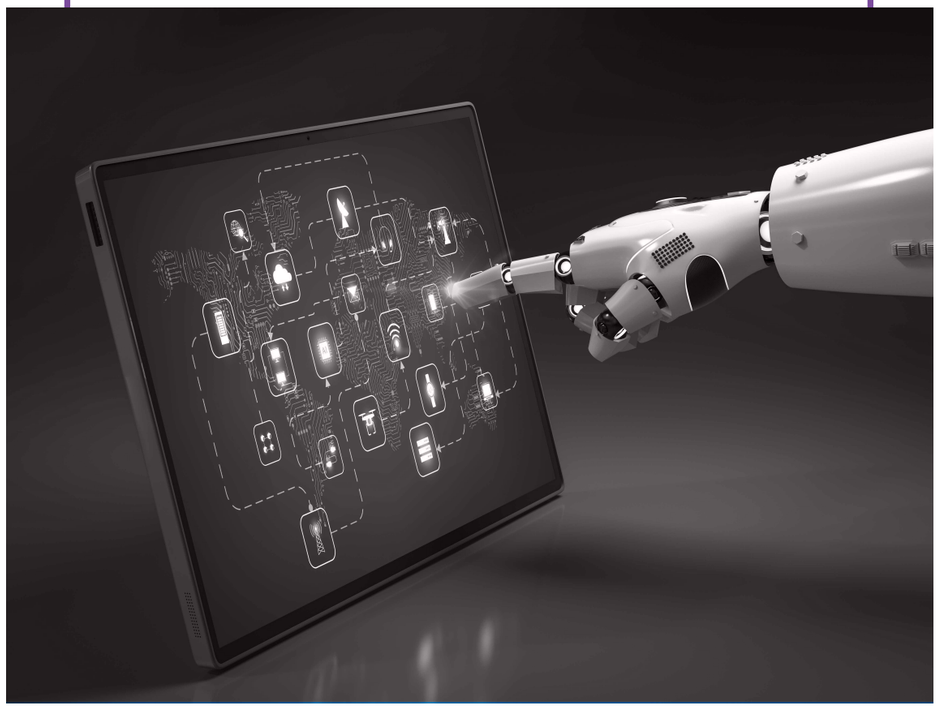
Faster incident response times: Automation speeds up the initial stages of incident handling.

Improved incident management: Streamlined processes and clear workflows enhance overall efficiency.

Enhanced threat visibility: Integration of threat intelligence provides better understanding of the threat landscape.

Stronger collaboration: Effective communication and information sharing among teams.

Reduced incident impact: Faster containment and recovery through automated response actions.



Gamification and Cyber Ranges

Gamification involves incorporating game-like elements into non-game contexts, such as learning or work. It aims to increase engagement, motivation, and enjoyment by leveraging elements like points, badges, leaderboards, and challenges.

Cyber Ranges

Cyber ranges are simulated environments where individuals or teams can practice cybersecurity skills in a safe and controlled setting. They replicate real-world cyberattacks and defense scenarios, allowing users to learn from their mistakes without real-world consequences.

Combining gamification with cyber ranges enhances the learning experience by making it more engaging and competitive. It can involve:

- Scoring systems: Assigning points for completing tasks or defending against attacks.
- Leaderboards: Ranking users based on performance to foster competition.
- Badges and achievements: Recognizing accomplishments to provide a sense of progression.
- Challenges and quests: Creating structured learning paths with clear goals.
- Storytelling: Incorporating narratives to make the learning process more immersive

INNOVATION IN CYBERSECURITY

INNOVATION IN CYBERSECURITY

UAE NATIONAL CYBERSECURITY STRATEGY

2025 TO 2031

The UAE Cybersecurity Council & National Strategy

The UAE Cybersecurity Council (CSC), established in 2020 and chaired by His Excellency Dr. Mohammed Hamad Al Kuwaiti, is the national authority responsible for safeguarding the country's digital future. The Council drives the UAE's ambition to be a global leader in cyber resilience and digital trust, working with government, critical infrastructure operators, private sector partners, academia, and international organizations. Its mandate spans from developing policies and standards, to building national capabilities, to leading international collaboration.

The UAE has unveiled an ambitious National Cybersecurity Strategy (2025–2031)

The UAE has unveiled an ambitious National Cybersecurity Strategy (2025–2031) to cement its position as a global leader in cyber resilience and digital trust. Building on earlier foundations, the new strategy aligns cybersecurity directly with the UAE's digital transformation, economic diversification, and national security priorities. It aims to enable the UAE's vision of being a trusted digital hub, driving innovation and safely embracing emerging technologies such as artificial intelligence, quantum computing, 5G/6G, and the Internet of Things (IoT).

Strategic Goals

The strategy is structured around six overarching goals:

- **Strengthening national cyber resilience** across critical infrastructure, government, and private sector.
- **Safeguarding citizens and society** by embedding cyber awareness and culture at all levels.
- **Driving trust in the digital economy** by ensuring security of data, transactions, and emerging technologies.
- **Enabling innovation and future technologies** through secure-by-design adoption of AI, cloud, blockchain, and quantum-ready systems.
- **Developing national talent and capabilities** to close the cybersecurity skills gap and foster Emirati expertise.
- **Leading global cyber diplomacy and partnerships**, reinforcing the UAE's role as a convener of international collaboration.

Implementation

Delivery of the strategy is organized into five pillars of action:

Govern: Establishing updated laws, standards, and regulatory frameworks to safeguard digital infrastructure.

Protect & Defend: Enhancing detection and response capabilities through advanced SOCs, incident response frameworks, and sector-level readiness.

Innovate: Positioning the UAE as a testbed for cybersecurity innovation, piloting new technologies and creating ecosystems that attract R&D and startups.

Build: Developing national capacity and resilience through workforce development, research programs, and cyber-awareness campaigns.

Partner: Expanding collaboration with global bodies such as ITU, INTERPOL, UNCCT, FIRST, and CRI, as well as fostering public–private partnerships.

CSC Mission

Raising national resilience by embedding cybersecurity as a foundation of digital life — from protecting critical sectors and services, to strengthening the awareness of all members of society. The CSC promotes a culture of cybersecurity, equips citizens and organizations with the tools to respond to evolving threats, and ensures trust in the UAE's digital ecosystem.

CSC Vision

To build a safe, secure, and resilient cyberspace that empowers innovation and protects the UAE's society, economy, and future governments from cybercrime and digital risks — in line with the UAE's Centennial 2071 and We the UAE 2031 vision.

UAE NATIONAL CYBERSECURITY STRATEGY 2025 TO 2031

CSC Mandate

Aligned with the UAE National Cybersecurity Strategy (2025–2031), the Council is mandated to:

- Develop, modernize, and oversee the National Cybersecurity Strategy, submitting it to the Cabinet and monitoring implementation in coordination with all relevant stakeholders.
- Propose and prepare legislation, policies, and standards to enhance cybersecurity across critical national infrastructures, government systems, and emerging technologies such as AI and quantum computing.
- Design and execute a national cyber defense and response framework, conducting periodic drills, crisis simulations, and large-scale readiness exercises.
- Establish national platforms for information exchange and governance, strengthening trust across public, private, and international partners.
- Ensure compliance and maturity of cybersecurity across government entities and CIIs, supported by frameworks such as the UAE Information Assurance Standard and the National Cyber Accreditation Program.
- Build and accredit national cybersecurity operations centers (NSOCs) and enhance national situational awareness through monitoring, detection, and coordinated response.
- Develop policies for the secure import, export, and use of critical technologies with cybersecurity implications.
- Lead capacity building and talent development, expanding Emirati representation in cybersecurity fields, and fostering inclusion across youth, women, and people of determination.
- Drive research, innovation, and global partnerships in cybersecurity, reinforcing the UAE's position as a trusted global leader in cyber diplomacy and collaboration.

Current Cybersecurity Policies & Frameworks

The Cyber Security Council's goal is to propose policies and legislation to improve cybersecurity in the country for all targeted sectors and bring them to the Cabinet for adoption and implementation in collaboration with the relevant authorities.

The Council of the UAE has developed a set of priority cybersecurity documents with a vision of enhancing cybersecurity within the country:

National Cyber Security Accreditation Program

The National Cyber Security Accreditation Program (NCAP) is an initiative that aims to cultivate trust in the UAE cyber ecosystem through raising its security maturity in a transparent way. Based on international best practice, the program balances security and efficiency in this national level assurance effort.

Critical Information Infrastructure Protection (CIIP) Policy

The CIIP Policy is established to ensure a baseline measure of security and cyber resilience of its Critical Information Infrastructure (CII), aligned with the UAE's national priority to be a global leader in cyber security; and to implement measures towards a resilient and secure cyberspace for its critical information infrastructure.

Cyber Incident Response Plan

The CIRP is developed to support the implementation of the National Cybersecurity Strategy by establishing a national incident management capability and defining how the UAE will prepare for, protect against, detect, respond to, recover, and continuously learn from significant cyber incidents.

Security Operations Centre (SOC) Baseline Capabilities

This baseline is established to outline minimum requirements for CII Security Operations Centers and define maturity targets to enhance national cyber resilience. This initiative builds upon the UAE's position as a global leader in cyber security, and further enhances the security posture of organizations and individuals within the UAE.

National IoT Security Policy

National IoT Security Policy is established to protect the use, adoption and implementation of IoT, aligned with the UAE's national priority to be a global leader in cyber security; and enhance the security posture of organizations and individuals within the UAE using IoT products and solutions.

Cyber Security Information Sharing Framework

This framework is developed to establish a National Cybersecurity Information Sharing Framework to promote and institutionalize cybersecurity information sharing and collaboration across multiple stakeholders. It is aligned with the UAE's national priority to be a global leader in cyber security and will enhance the security posture of organizations across the UAE.

National Cloud Security Policy

This policy is established to enhance cloud security, aligned with the UAE's national priority to be a global leader in cyber security; and enhance the security posture of organizations and individuals within the UAE using cloud services.

Cyber Incident Response Framework

This framework is developed to establish a national incident management capability and defining how the UAE will prepare for, protect against, detect, respond to, recover from significant cyber incidents; aligned with the UAE's national priority to be a global leader in cyber security, and enhance the security posture of organizations and individuals within the UAE.

UAE Information Assurance Update

The UAE Information Assurance Regulation has been set to define the required level of protection of information assets and supporting systems across the UAE critical information infrastructure and has been mandated to be the minimum protection required across the UAE banking sector.

The UAE Information Assurance Standard is being updated to reflect the significant changes in the technical and cyber security landscape that have occurred since this standard was last updated.

CSC conducted workshops with Policy Committee members, national entities, Emirate leads, sector regulators and key UAE entities. Currently, the UAE IA Framework is being updated based on a survey and the envision workshop feedback received.

Upcoming Strategies, Policies, and Frameworks

Building upon the strong foundation established by the National Cybersecurity Strategy, the UAE is actively developing a new wave of initiatives to further enhance its cybersecurity posture. These upcoming strategies, policies, and frameworks aim to address emerging challenges, capitalize on technological advancements, and solidify the UAE's position as a global cybersecurity leader.

National Encryption Policy: The National Encryption Policy is established to enhance data security, aligned with the UAE's national priority to be a global leader in cyber security; and enhance the security posture of organizations and individuals within the UAE dealing with critical and personal data.

National Third-Party Security Policy: The National Third-Party Security Policy is established to enhance third party security, aligned with the UAE's national priority to be a global leader in cyber security; and enhance the security posture of organizations and individuals within the UAE dealing with third party providers.

Data Exchange Security Policy: The Data Exchange Security Policy is established to enhance data exchange security, aligned with the UAE's national priority to be a global leader in cyber security; and enhance the security posture of organizations and individuals within the UAE sharing business critical and personal data.

Blockchain Security Policy: This policy is established to ensure secure implementation and operation of blockchain-based systems, aligned with the UAE's national priority to be a global leader in cyber security; and enhance the security posture of organizations adopting blockchain.

National Secure Remote Work Policy: National Secure Remote Work Policy is established to enhance remote work security, aligned with the UAE's national priority to be a global leader in cyber security; and enhance the security posture of organizations and individuals within the UAE utilizing remote work arrangements.

National AI Security Policy: This policy is established to enhance artificial intelligence security, aligned with the UAE's national priority to be a global leader in cyber security; and enhance the security posture of organizations and individuals within the UAE using artificial intelligence.

05

UAE'S PIONEERING PROGRAMS AND GLOBAL INITIATIVES

CSC's Initiatives and Programs

Cyber Pulse

Cyber Pulse is an initiative launched by the UAE Cyber Security Council with the aim of enhancing cybersecurity awareness and readiness in the country. The Cyber Pulse initiative is a comprehensive program that includes multiple projects focused on different aspects of cybersecurity. These initiatives aim to raise awareness, develop future leaders, conduct cyber drills, and enhance the capabilities of cybersecurity professionals through various targeted efforts.

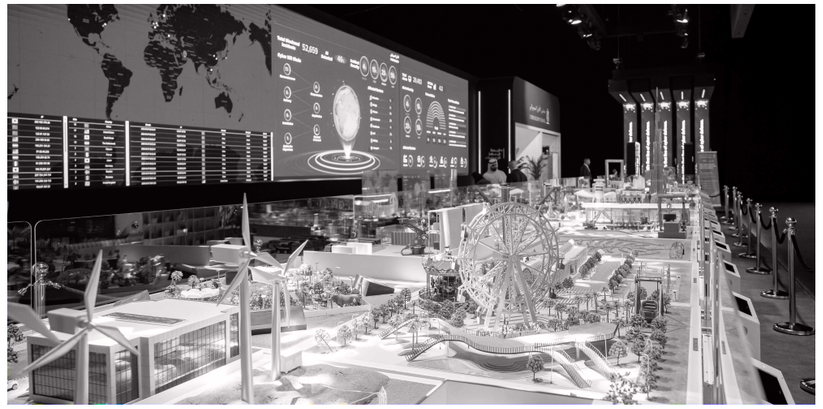
Cyber Pulse organizes and conducts "Cyber Drills" across various sectors, including food, healthcare, financial services, digital infrastructure, and more. These drills are designed to improve the readiness and response capabilities of organizations against cyber threats. They include exercises like incident response simulations and readiness drills.

The "Future Leaders" component focuses on developing the next generation of cybersecurity professionals. This includes selecting university students from across the UAE and providing them with specialized training through a dedicated academy. The program targets young professionals, government executives, and new graduates, offering them opportunities to engage in cybersecurity through workshops, conferences, and other educational activities.

The initiative places a strong emphasis on "Cyber awareness Campaigns" through tailored campaigns targeting different demographic groups, including young families, youth, entrepreneurs, and senior citizens. These campaigns cover critical topics like online shopping security, digital entertainment, work and learning in the digital world, and protecting children online. Awareness is raised through regular, quarterly campaigns addressing specific cybersecurity threats and best practices.

The Cybersecurity Center (CSC) has set its sights on achieving various accolades, such as the prestigious Lifetime Achievement and Cybersecurity Thought Leadership of the Year awards. These sought-after accolades are intended to enhance the organization's global reputation and recognition within the cybersecurity industry.

Moreover, the CSC has actively cultivated an extensive and robust network of partnerships, encompassing both local and global alliances. This strategic approach aims to magnify the impact of the CSC's initiatives and solidify its position as a key player in the cybersecurity domain.



UAE'S PIONEERING PROGRAMS AND GLOBAL INITIATIVES

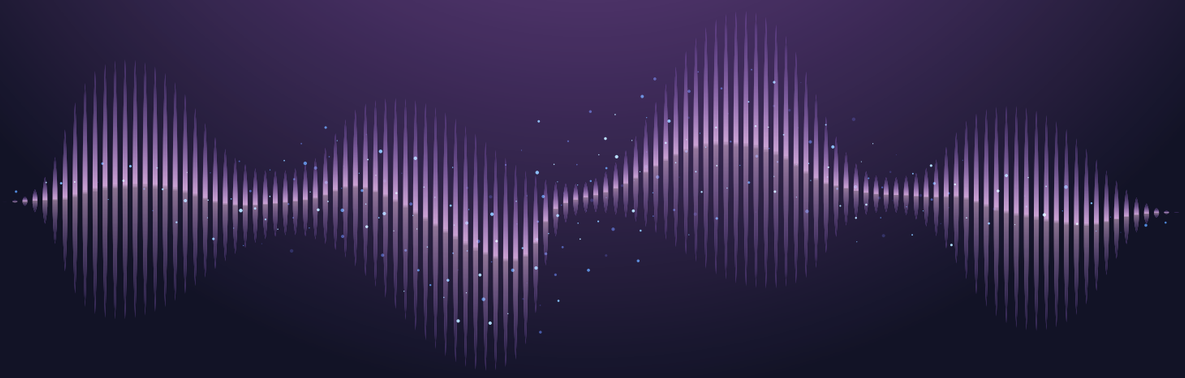
The Pulse

Project Brief: The Pulse is a cutting-edge UAE Cyber Range Lab, a predictive model for multistage cyber-attack simulation. The state-of-the-art scaled model serves as a real-time representation of the UAE's life-like places of Interest, providing a platform to simulate, analyze, and evaluate cyber threats in a controlled environment across UAE critical sectors.

Holder of three Guinness World Records, The Pulse is one of the world's largest and most advanced cyber range labs—in terms of scale, number of devices, and number of available scenarios. It has pioneered a novel approach in simulating and understanding cyber threats to provide unique experiences for training cybersecurity professionals, testing defense strategies, improving incident response capabilities, and upskilling the UAE in IoT/SCADA and industrial security.

Project Goals: The Pulse aims to offer a highly rewarding, engaging, and motivating experience based on life-like UAE points of interest. It brings unparalleled realism to cybersecurity training and crisis simulation and a breakthrough in preparing for and responding to cyber threats.

This novel approach aligns with the UAE's vision to become a hub for technology and digital innovation, creating a secure environment for organizations to operate.



The Global Cyber Drill at GISEC 2025

The Global Cyber Drill 2025, hosted by the Cyber Security Council (CSC), was one of the largest international cyber exercises to date, designed to advance global resilience against emerging digital threats. It brought together 124 national cybersecurity authorities/CERT/CIRT/CSIRT teams from over 133 countries, with more than 260 participants and 15 international partners, all competing and collaborating on the CYBER RANGES platform. The 2025 edition featured four advanced scenarios delivered with leading global custodians: the International Telecommunication Union (ITU), the United Nations Counter-Terrorism Centre (UNCCT), INTERPOL, and the Forum of Incident Response and Security Teams (FIRST).

The drill focused on strengthening collective defense by unifying international teams to refine incident response strategies, foster collaboration, and share expertise in confronting sophisticated cyberattacks.

The exercise had several key objectives, including:

- Providing practical, hands-on experience in detecting, investigating, and mitigating cyber incidents.
- Deepening participants' exposure to complex cyber tactics, techniques, and procedures (TTPs).
- Building competencies in areas such as threat hunting, log and traffic analysis, and dark web intelligence gathering.
- Reinforcing collaboration between national cybersecurity agencies, law enforcement, and multilateral partners.

Participants engaged in realistic scenarios such as APT compromise investigations, dark web analysis of terrorist cyber-activity, phishing campaign disruption in the financial sector (Operation Black Ledger), and ransomware decryption challenges. These scenarios tested both technical expertise and international cooperation.

At GISEC 2025, the Cyber Security Council (CSC) entered the Guinness World Records with an unprecedented 11 achievements, marking a milestone in global recognition for the UAE's leadership in cybersecurity. These records celebrated the scale, inclusivity, and innovation of the Global Cyber Drill and surrounding activities.

The records reflected both the size of participation and the uniqueness of the collaborative exercises.

Key Accomplishments Included:

- Most nationalities participating in a cybersecurity capture-the-flag (CTF) competition.
- Largest cybersecurity awareness session held globally.
- Largest number of national authorities engaged in a single international drill.
- Fastest response time recorded in a coordinated cyber incident scenario.
- Widest participation of international partners in a cyber exercise, among other achievements.

These accolades not only reinforced the UAE's role as a convener of global cyber collaboration, but also showcased how innovation in training and preparedness can set new international benchmarks. The recognition further elevated the standing of the UAE on the world stage, affirming its commitment to advancing collective cybersecurity resilience.

Crystal Ball Platform at GISEC 2025

Crystal Ball is an international Threat Intelligence Collaboration Platform designed to strengthen trust, transparency, and collective defense, aligned with the objectives of the Counter Ransomware Initiative (CRI). At GISEC 2025, a Closed-Door Crystal Ball Session was convened, featuring opening remarks from H.E. Dr. Mohamed Al Kuwaiti, alongside senior industry leaders. The session reaffirmed the platform's role in enabling secure, real-time intelligence exchange between governments and trusted partners, ensuring faster and more coordinated responses to evolving cyber threats.

Objectives & Principles (2025 focus):

- Reinforce attribution of incidents and attacks through multinational intelligence sharing.
- Support deterrence by enabling proactive, joint responses that reduce the impact of global ransomware and cybercrime campaigns.
- Promote a culture of trust and transparency, embedding information-sharing practices into the international cyber ecosystem.
- Enhance capacity-building by onboarding more national authorities and enabling structured government-to-government exchanges.

Capabilities and Functionalities:

In 2025, Crystal Ball expanded its collaborative features, strengthening its position as a cornerstone of global threat intelligence efforts:

- AI-powered analytics and reporting to assist threat intelligence analysts in rapidly identifying patterns and anomalies.
- Secure, closed network for incident information sharing, aligned with standardized global protocols.
- Integrated collaboration tools to support multi-party investigations across borders.
- Government-to-government exchange program piloted at GISEC 2025, enabling structured, trusted intelligence flows.
- User onboarding enhancements, addressing lessons from international drills to improve access for first-time participants.
- 24/7 expert support and intelligence briefings to ensure continuity of operations.
- Event creation and intelligence exchange, allowing members to launch collaborative investigations at bilateral or multilateral levels.

Through these enhancements, the platform continues to evolve into a trusted global hub for cyber threat collaboration, positioning the UAE and its partners at the forefront of international cyber resilience.

Program Expansion at GISEC 2025

Building on the success of earlier editions, GISEC 2025 introduced an expanded program of side events and specialized forums to enhance knowledge sharing, skills development, and multi-stakeholder collaboration. These initiatives provided participants with unique opportunities to engage in advanced training, explore cutting-edge technologies, and connect directly with peers from across the globe.

Objectives:

- **Provide a diverse platform for hands-on technical training and policy dialogue.**
- **Strengthen the cybersecurity ecosystem by linking government authorities, industry experts, and academia.**
- **Highlight global best practices in cyber defense, resilience, and leadership.**
- **Foster the next generation of cyber professionals through dedicated learning tracks.**

Key Program Elements:

GCD Stage

- Introduced as a dedicated track focusing on industrial control systems (ICS) security and national cyber resilience.
- Hosted Sessions 7–10 with 350+ participants, including government agencies, industry leaders, and international organizations.
- Facilitated knowledge exchange on critical infrastructure protection, AI in security, and emerging threat landscapes.

Government Accelerator Program

The Government Accelerator Program at GISEC was designed to bring together key public sector stakeholders, industry leaders, and technology partners to fast-track the development and adoption of innovative cybersecurity initiatives in the UAE.

A total of 76 participants were divided into 6 groups to address key topics: Quantum computing, Citizen-Centric Cybersecurity, Cyber Diplomacy, Digital Frontier, Transformative Education, Sustainable Development.

GISEC Academy

- Delivered six specialized training sessions, targeting both early-career professionals and experienced practitioners.
- Focused on skill-building in digital forensics, malware analysis, and threat intelligence techniques.
- Expanded the talent pipeline by engaging students, researchers, and junior professionals.

X-Labs

- A collaborative workshop series designed to address national-level initiatives and posture assessments.
- Sessions included National Institute for the Assessment of Posture (NIAP) workshops and national readiness evaluations.
- Provided practical, scenario-based exercises to test strategic and technical preparedness.

CISO Roundtables

- Exclusive closed-door discussions tailored for Chief Information Security Officers and senior executives.
- Sessions featured AWS on “Leading Resilient Security Organizations in the AI Era” and Microsoft on “The Future of Security in the Age of AI.”
- Facilitated peer-to-peer dialogue on governance, resilience, and leadership challenges.

Through these expanded programs, GISEC 2025 reinforced its position as a global convening point for cybersecurity excellence, combining technical mastery with strategic leadership dialogue to advance collective resilience.

Cyber Next 50

The United Arab Emirates Cyber Security Council collaborated with KPMG to explore the future of cyber security over the next 50 years. The research focused on the myriad issues arising from the adoption of information technology and highlights the current trends that are expected to impact our lives in the upcoming decades. The report presents valuable insight on potential policy decisions the UAE can consider maximizing its cyber resilience over the next 50 years. This includes a progressive legal framework underpinned by new laws.

National Cyber Bug Bounty

The UAE's National Bug Bounty Program is a significant cybersecurity initiative launched by the Cyber Security Council (CSC). This program, initiated in collaboration with major telecom providers like Etisalat and du, aims to enhance the nation's digital security. It focuses on safeguarding critical national infrastructure, including sectors such as energy, telecommunications, and defense.

The program enlists ethical hackers and security researchers from around the world to identify and report vulnerabilities in UAE's digital systems through an incentive-based model. This proactive approach allows the country to strengthen its cybersecurity posture by leveraging global expertise in penetration testing and vulnerability assessment.

Objectives

- Leverages Crowd, Security researchers to identify "bugs", vulnerabilities, and insecurities.
- Incentive Based System, To reward the discovery and disclosure of bugs and vulnerabilities.
- Result Oriented Capacity, Focused on the quality and severity of bugs and vulnerabilities

Cyber Sniper Programs

The Cyber Sniper program is aimed at improving the skills of government IT personnel, especially those at the federal level. The program is intended to develop specialized expertise in areas such as ethical hacking, advanced threat analysis, and penetration testing.

The main participants are federal employees and cybersecurity professionals responsible for safeguarding critical national infrastructure and dealing with national cybersecurity threats.

Objectives

Developing High-Level Cyber Expertise: Cyber Sniper aims to equip participants with advanced knowledge in handling sophisticated cyber threats, including nation-state-level attacks.

Practical Training: The program emphasizes hands-on experience through simulations, penetration testing, and red/blue team exercises, which are designed to mirror real-world cyber attack scenarios.

National Defense Readiness: By focusing on national security, Cyber Sniper ensures that participants are prepared to defend the UAE's digital infrastructure at both national and international levels.

DDoS Protection Initiative

Cyber Security Council (CSC) and etisalat by e& have joined hands to strengthen the UAE's critical infrastructure by improving organisations' security posture and enhancing the country's leading position in global competitiveness indicators.

The DDoS Protection initiatives are designed to enhance the security posture of organizations against cyber threats, with a focus on bolstering the country's critical infrastructure. These initiatives aim to protect both government and private enterprises from malicious cyberattacks using Cloud DDoS Mitigation Solutions. The services include real-time threat detection, multi-layered protection, and expert support from a Security Operations Centre (SOC). By offering visibility, control, and scalability to handle high-volume DDoS attacks efficiently, these initiatives ensure uninterrupted business operations and provide peace of mind for customers

URL Check-up Program

URL Checker, also known as “Stay Safe,” is a digital safety initiative launched by the UAE Cyber Security Council. This free online tool, accessible at staysafe.csc.gov.ae, helps users verify the legitimacy of websites. It assesses if a site may be involved in phishing, malware, or other online scams, providing a reliability score based on a color-coded system. Users can simply input a website URL to see if it’s safe or potentially a threat.

This tool was created in collaboration with Etisalat and the Global Anti-Scam Alliance, helping to stay safe while browsing online and protecting themselves from cyber fraud.

AI “Hemaya” security solution Initiative

The AI "Hemaya" security solution is an advanced initiative aimed at enhancing national cybersecurity by integrating artificial intelligence (AI) to address modern cyber threats. "Hemaya," is designed to utilize AI-driven technologies to safeguard critical national infrastructures such as energy, telecommunications, defense, and finance.

Objectives

AI-powered Defense: The initiative aims to use AI to better detect, analyze, and counter cyber threats, including mitigating ransomware and AI-enabled attacks, to ensure the security of the country's digital infrastructure.

Proactive Cybersecurity Measures: Hemaya aims to use AI to proactively stay ahead of cybercriminals. This initiative positions the UAE to better protect public and private sector entities by making AI a key part of its defense strategy, as cybercriminals are increasingly using AI to breach systems.

Collaboration and Innovation: The program emphasizes cross-sector collaboration to strengthen cybersecurity, focusing on continuous innovation and adaptation to emerging threats.

OIC Call to Action

The United Arab Emirates (UAE) has positioned itself as a key supporter of cybersecurity development, both in Arab countries and worldwide. This includes sponsoring the largest annual cybersecurity event, which took place in the UAE capital, Abu Dhabi, with the theme “Cybersecurity Innovation and Industry Development”.

The UAE Cyber Security Council has established a united front with ITU – the United Nations Agency for Information and Communication Technologies, and the Organization of the Islamic Conference (OIC).

Participating countries issued the joint Call to Action Abu Dhabi 2023, underlining their commitment to advancing the cause of cybersecurity in the ever-changing digital landscape.

Commitment: Pledging dedication to fostering confidence and security in the use of Information and Communication Technologies (ICTs).

Embrace Cyber Resilience: Urging industries to adopt frameworks that repel threats and ensure uninterrupted operations during cyberattacks.

Sharing: Actively sharing experiences and best practices related to cyber threats and cybersecurity.

Harmonization: Actively pursuing harmonization and integration with other relevant organizations to benefit from their experiences and prevent duplication of efforts.

Research & Development: Encouraging governments, academia, and the private sector to increase investment in cybersecurity Research & Development (R&D).

Strengthen Cyber Strategies: Collaborating with relevant stakeholders to establish and update cyber strategies that strategically approach cybersecurity development, implementing policies to enhance preparedness and resilience.

Cyber Inclusion: Advocating for the introduction of cybersecurity education at foundational levels and its continuation through higher education and ongoing professional development.

Ethical AI Adoption: Promoting ethical AI adoption by encouraging businesses and organizations to prioritize ethical considerations in AI development and deployment.

CyberE71

The CyberE71 program is a global initiative aimed at accelerating and supporting cybersecurity startups, launched by the UAE Cybersecurity Council to enhance the global innovation ecosystem by uniting cybersecurity startups under a single umbrella. This program seeks to promote the exchange of knowledge, collaboration, and support, contributing to the development of global and regional cybersecurity capabilities. It is based on a comprehensive benchmarking analysis of startup support and creation programs worldwide, ensuring the integration of best practices and effective strategies.

In partnership with entities such as Area2071, Hub71, and Dubai Silicon Oasis, CyberE71 creates a comprehensive environment to support cybersecurity startups. The program offers a structured acceleration framework that includes intensive training sessions, events, and strategic meetings, providing more than 900 hours of mentoring and access to 36 industry-leading instructors. The program emphasizes simplicity and scalability, featuring a streamlined registration process and a user-friendly online portal.

CyberE71 equips startups with the tools, knowledge, and connections needed to succeed, positioning itself as a leader in global cybersecurity innovation. The program aligns with the UAE's strategic objectives, strengthening global cybersecurity resilience and contributing to economic diversification. By fostering talent and driving innovation, CyberE71 supports the UAE Vision 2071, addressing cybersecurity challenges and advancing a knowledge-based economy.

UAE'S PIONEERING PROGRAMS AND GLOBAL INITIATIVES

National Cyber Operations Center (NSOC)

The United Arab Emirates (UAE) has established the National Security Operations Center (NSOC) to fulfill the country's leadership vision of safeguarding the nation against cyber-attacks and enhancing its national cyber security. The UAE acknowledges the increasing number and complexity of cyber incidents and their detrimental impact on the nation and its economy.

The NSOC aims to provide a comprehensive and practical solution to protect the nation against cyber-attacks. It has been built using a scalable, best-of-breed solution that incorporates Fundamental Methodologies, Field-Proven Technologies, Human Operability, and Capability Buildup to defend against cyber attacks.

The NSOC operation relies on well-defined and successfully implemented methodologies to monitor the nation’s status, detect national adversaries, correlate and disseminate cyber intelligence, and assess the country's resilience to cyber-attacks. With the establishment of NSOC, the UAE will have national-level visibility and coordination ability to combat cyber attacks, leveraging the power of AI and extensive automation to address challenges in various cyber fields worldwide.

NSOC Goals

One-glance cyber posture: Provides a way to glance through the nation’s threat landscape through sector & nation wide collaboration.

One-glance cyber posture: Provides a way to glance through the nation’s threat landscape through sector & nation wide collaboration.

One-glance cyber posture: Provides a way to glance through the nation’s threat landscape through sector & nation wide collaboration.

One-glance cyber posture: Provides a way to glance through the nation’s threat landscape through sector & nation wide collaboration.

The UAE Cyber Security Council's Cyber Defense Day (Train-the-nation)

Cyber Defense Day is an innovative educational initiative launched by the Cybersecurity Council with the goal of enhancing students' awareness of cybersecurity and educating them on how to build secure systems to prevent cyberattacks. This initiative was the result of collaboration with several strategic partners in the country, including the Education and Human Resources Council, the Ministry of Education, the Emirates Schools Establishment, the Department of Education and Knowledge, and the Sharjah Private Education Authority. Additionally, private schools in Dubai actively participated in this initiative, showing a collective effort to equip students with essential cybersecurity knowledge and skills.

Objectives

- Enhance students' awareness of cybersecurity and its risks.
- Focus on the importance of digital privacy and the need to adhere to ethical behavior.
- Enhance the quality of students' digital lives.
- Combat emerging risks and threats in the field of cybersecurity.

Women In Cybersecurity

The UAE's Women in Cyber initiative, also known as the Cyber Pulse Initiative for Women and Families, was launched in collaboration with the General Women's Union (GWU) and Cyber Security Council (CSC). This initiative aims to empower women in the field of cybersecurity and enhance their digital skills.

The Women in Cybersecurity program is dedicated to fostering greater representation of women in the cybersecurity industry. The initiative offers comprehensive training, access to valuable resources, and various opportunities designed to empower women and help them advance their skills and careers in the field of cybersecurity.

National Youth Cyber Awareness Program

The UAE National Youth Cyber Awareness Program is part of the UAE's broader efforts to educate and empower young people in cybersecurity. This initiative is spearheaded by the UAE Cyber Security Council, with the aim of transforming the younger generation into defenders against cyber threats.

Key components of the program include:

Workshops and Training Sessions
mitigating cyber threats such as phishing, malware, and hacking. These sessions focus on real-world scenarios to make young participants more adept at identifying and responding to cyber incidents

Interactive Campaigns and Drills
The program incorporates interactive elements like cybersecurity drills and competitions to engage youth. These activities are designed to build cybersecurity skills in a fun and competitive environment, often involving simulations that reflect actual cyber-attack situations

Awareness Campaigns
The initiative also promotes cyber awareness through campaigns that teach safe online behavior, digital ethics, and the importance of securing personal data. These campaigns often feature social media outreach and seminars tailored to young audiences

Collaborations and Partnerships
The program is often carried out in collaboration with educational institutions and private-sector partners, ensuring that students gain exposure to the latest developments in cybersecurity. Partnerships with organizations like Core42 and KPMG further enrich the program with industry insights

UAE'S PIONEERING PROGRAMS AND GLOBAL INITIATIVES

Cybersecurity Awareness Campaigns

52 Weeks of Cybersecurity Awareness

The 52 Weeks of Cybersecurity Awareness is a comprehensive initiative launched in the United Arab Emirates (UAE) by the Cyber Security Council (CSC) to promote a culture of cybersecurity among its citizens and residents. This campaign aims to educate and empower individuals to protect themselves and their organizations from cyber threats.

The 52 Weeks of Cybersecurity Awareness campaign has made a substantial impact in elevating cybersecurity awareness within the UAE and internationally. Through the dissemination of accessible information and resources, including to international public and private organizations, it has empowered both individuals and institutions to adopt proactive measures against cyber threats. Additionally, the campaign has strengthened the sense of community and collaboration among stakeholders in the global cybersecurity sector.

Objectives

Raise awareness: Increase public understanding of cybersecurity risks and best practices.

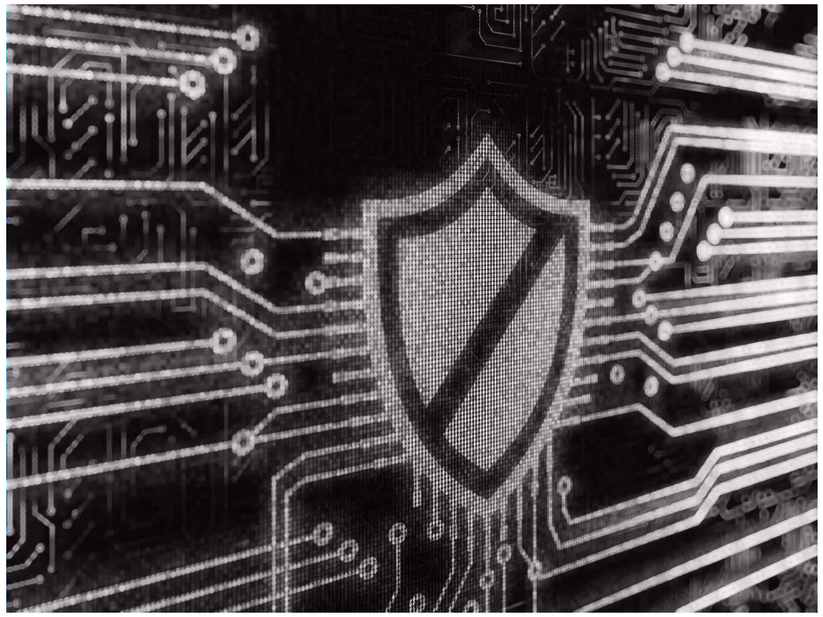
Promote education: Provide educational resources and training to enhance cybersecurity skills.

Foster collaboration: Encourage collaboration between government, private sector, and academia to address cybersecurity challenges.

Protect critical infrastructure: Safeguard the UAE's critical infrastructure from cyberattacks.

Campaign Highlights

- Weekly themes: Focus on different cybersecurity topics each week, such as phishing, malware, social engineering, and data privacy.
- Educational content: Ranking users based on performance foster competition.
- Online resources: Provide access to online courses, webinars, and workshops.
- Community engagement: Organize events and activities to involve the public in cybersecurity discussions.
- Partnerships: Collaborate with schools, universities, and businesses to promote cybersecurity education.



Jahiz Platform

Jahiz, launched by the UAE's Federal Authority for Government Human Resources (FAHR) in late 2022, is the country's largest digital upskilling platform designed to prepare government employees for future challenges through interactive and personalized learning. In a short time, it has reached over 53,000 learners with 90 programs covering 4 core future-skills groups, 27 subskills, and 163 modules, totaling more than 1.2 million learning hours. Supported by over 25 strategic partners, including the UAE Cybersecurity Council, the platform integrates specialized cybersecurity content to strengthen digital resilience and equip government professionals with the skills needed to protect against evolving cyber threats.

CSC's Public-Private Partnerships

Collaborations between the CSC and private sector entities to strengthen cybersecurity

Partner with the Private Sector

Etisalat

The Cyber Security Council and Etisalat have formed a strategic partnership to enhance the UAE's cybersecurity landscape. In this regard, the council has entered into a strategic collaboration with Etisalat, one of the world's leading telecom groups in emerging markets, and Help AG, the cybersecurity arm of Etisalat Digital, as part of its continuous efforts to strengthen the UAE's critical infrastructure, improve its security posture and enhance the country's leading position in global competitiveness indicators.

CSC has also partnered with Etisalat to start the Cyber Sniper Training for Levels 1, 2 & 3 in collaboration with Etisalat Academy for government official or a national cadre.

Partner with the Academic Sector

Abu Dhabi polytechnic

CyberPulse Innovation Centre: The UAE also established the CyberPulse Innovation Centre at Abu Dhabi Polytechnic. This center aims to address the cybersecurity skills gap by training the next generation of cyber professionals. It serves as a hub for collaboration between academia and industry, helping students gain real-world experience in emerging cyber threats and technologies

The CyberPulse Innovation Center and Abu Dhabi Polytechnic work together to ensure that academic programs at AD Poly align with the latest trends and technologies in cyber security.

Joint research projects and initiatives help advance knowledge and develop practical solutions to current and future cyber security challenges.

The partnership aids in creating a skilled workforce capable of addressing complex cyber security issues, supporting both national and industry-specific needs.

The Center of Excellence at Abu Dhabi Polytechnic, developed in collaboration with the UAE Cyber Security Council (CSC), represents a significant initiative aimed at enhancing cybersecurity education and workforce development in the UAE. It is part of broader efforts to position the UAE as a global leader in digital security and combat the growing cyber threats in the region.

The COE, established at Abu Dhabi Polytechnic, serves as a hub for training future cybersecurity professionals. The collaboration with corporate partners like Huawei ensures that students are not only exposed to the theoretical aspects of cybersecurity but also gain hands-on experience dealing with real-time cyber threats. This practical approach enables graduates to transition seamlessly into professional roles where their skills are in high demand.

UAE'S PIONEERING PROGRAMS AND GLOBAL INITIATIVES

Khalifa University

The UAE Cyber Security Council and Khalifa University have a collaborative relationship focused on advancing cyber security research and education.

The UAE Cyber Security Council is responsible for shaping national cyber security policies, strategies, and regulations. Its role includes developing frameworks to protect the country's digital infrastructure and addressing emerging cyber threats.

Khalifa University, a leading institution in the UAE, is known for its strong focus on research and innovation in various fields, including cyber security. The university collaborates with government entities and industry partners to advance knowledge and solutions in cyber security. Their research often contributes to national initiatives and helps in shaping effective cyber security strategies.

Khalifa University has established a significant partnership with the UAE Cyber Security Council (CSC) through the creation of the National Cybersecurity Center of Excellence (NCCoE).

Key highlights of this initiative include:

- **Cybersecurity Academy**
- **Research & Innovation**
- **Talent Development**
- **Cybersecurity Infrastructure**

Lockheed Martin

At IDEX 2025, the Tawazun Council, UAE Cyber Security Council, and Lockheed Martin signed an LoI to establish a Cybersecurity Centre of Excellence. This initiative marks a strategic milestone for the UAE, reinforcing its ambition to become a global powerhouse in cybersecurity. By integrating advanced technology, enhancing human capital, and fostering international cooperation, the Cybersecurity Centre of Excellence aims to strengthen national resilience and drive sustainable digital growth.

Key Goals

Strengthen national cyber resilience through advanced research, training, and Security Operations Centre (SOC) services.

Create "Cyber Valleys" across the UAE to support innovation and startups.

Foster collaboration between government, industry, and academia.

Impact

The centre will enhance digital security, build local talent, promote economic diversification, and position the UAE as a global hub for cybersecurity innovation.

Google Cloud

The UAE, in partnership with Google Cloud and Mandiant, launched the region's first Cybersecurity Centre of Excellence in Abu Dhabi during IDEX 2025. The Centre will strengthen national resilience through advanced training, cyber simulation ranges, and knowledge sharing with academia, government, and industry.

A core focus is on workforce development and job creation. By 2030, the Centre is projected to create over 20,000 new jobs across multiple domains:

- **Cyber Defense & Incident Response**
- **Cyber Policy & Governance**
- **Secure Digital Transformation Roles**
- **Education & Awareness**

Complementing this, the startup accelerator program will support 25 high-potential startups with mentorship and up to $300,000 in Google Cloud credits, fostering entrepreneurship and specialized cyber roles in innovation, product development, and cybersecurity R&D.

Economically, the initiative is expected to prevent $6.8B in cybercrime losses by 2030 and attract $1.4B in foreign investment, positioning the UAE as a global leader in cybersecurity innovation and talent development.

CSC’s Collaboration with International Bodies

The UAE Cybersecurity Council strengthens international cooperation by working with key local government partners including the Government Experience Exchange Office and the UAE Government Accelerators to co-design initiatives with partner governments. Through accelerator cohorts and experience-exchange programs with countries, UAE enables best-practice sharing, joint pilots and exercises, and capacity-building to advance interoperable standards, rapid incident response, and collective cyber resilience.

Cooperative efforts between the CSC and international organizations to enhance cybersecurity.

International Telecommunication Union (ITU)

Launched in collaboration with the International Telecommunication Union (ITU), CyberPulse focuses on safeguarding the UAE's cyberspace by increasing public awareness and fostering a sense of national loyalty towards cyber defense. The initiative includes workshops, training sessions, and other activities designed to improve digital literacy and resilience across various sectors of society, including government, businesses, and the general public.

The initiative has gained international recognition, winning prestigious awards at events such as the World Summit on the Information Society (WSIS) Prizes. This acknowledgment underscores the UAE's leadership in leveraging advanced technology for sustainable development and its commitment to creating a secure digital environment.

Additionally, CyberPulse plays a key role in global cybersecurity efforts, as seen in the ITU Global CyberDrills, where it helps strengthen the cybersecurity capabilities of other nations through knowledge sharing and collaborative exercises. This alignment with ITU's global agenda reinforces the UAE's position as a pivotal player in international cybersecurity cooperation

The UAE Cyber Security Council participates in and supports global cyber drills organized by the ITU and other international bodies. This participation helps in aligning the UAE’s cyber security practices with global standards and improving its readiness for cyber threats.

UAE'S PIONEERING PROGRAMS AND GLOBAL INITIATIVES

The Whitehouse

The UAE recently participated in the International Counter Ransomware Initiative (CRI) meeting in San Francisco. This event, organized by the White House, brought together 60 global partners to discuss strategies for combating ransomware. During the meeting, the focus was on enhancing trust, information exchange, and collective defense measures among nations. A significant topic of discussion was the "Crystal Ball Platform," an AI-driven threat-sharing system designed to improve cybersecurity cooperation. The UAE's involvement in this initiative highlights its commitment to global cybersecurity efforts.

Organization of Islamic Cooperation (OIC)

The UAE Cyber Security Council has been actively involved with the Organisation of Islamic Cooperation (OIC) in enhancing cybersecurity measures across member states. Recently, the UAE was elected as Vice President of the OIC's Computer Emergency Response Team (CERT) during the 10th Regional Cybersecurity Week for Arab Countries and OIC Member States. This position underscores the UAE's leadership in the global cybersecurity landscape and its commitment to safeguarding digital infrastructures across the Islamic world.

Additionally, the UAE participated in a high-level cybersecurity roundtable hosted by OIC-CERT at the MWC 2024. The event focused on instilling digital trust and resilience among OIC members, discussing critical areas such as 5G security, cloud security, and the potential formation of a new working group dedicated to AI and supply chain security.

These efforts demonstrate the UAE's proactive stance in collaborating with international partners to address evolving cyber threats and promote digital security across OIC member states. The UAE's engagement in these initiatives reflects its commitment to leading regional efforts in cybersecurity, fostering collaboration, and ensuring that OIC member states are well-prepared to address emerging cyber threats.

06

CYBERSECURITY OUTLOOK

Future Trends in Cybersecurity

What might the next 50 years of cyber security bring? The megatrends shaping our world include:

Demographics

The world population is projected to reach 9.7 billion by 2050. Changing demographics bring challenges, ranging from ageing populations, declining fertility rates and increased debt/taxation burdens in some economies, to infrastructure and educational challenges in the rapidly growing and urbanizing populations in sub-Saharan Africa and South Asia. The UAE's population is predicted to grow to 10.9 million in the next 20 years, with Dubai's population doubling, following a post-pandemic immigration wave. Factors such as economic diversification and attraction of foreign workers will largely contribute to the population increase.

Climate change

Currently implemented policies are predicted to result in further global warming of 2.8 degrees over the period leading up to 2100, with a diminishing window for global action which might limit that warming to 1.5-2 degrees. Changes in climate are predicted to lead to food security issues, population displacement and ecosystem degradation – as well as creating potential flash points for conflict. The UAE is taking measures to tackle the growing threat of extreme temperature and drought caused by climate change. It has outlined multiple initiatives to balance the short-term gains from fossil fuels with the existential imperative arising from climate change.

CYBERSECURITY OUTLOOK

Health challenges

- Growing antimicrobial resistance linked to increased risk of cross-infection of human populations with animal pathogens associated with increasing population density and mobility, lead to increased pandemic risk. Longer life expectancies lead to growing pressures on healthcare systems associated with diabetes, cardiovascular disease, cancer and chronic respiratory diseases.

- The Centennial 2071 project aims to place the UAE as the best country in the world by 2071, with superlative healthcare. The country's 2071 healthcare agenda focuses on medical tourism, telemedicine, Al and cloud technology in healthcare and regulation for the use of e-health.

Technology Trends

- Artificial intelligence: The advent of artificial general intelligence following the rapid development of AI and the extension of domain specific applications over the next decade.

- Hyper connectivity: Development of network infrastructure enabling greater bandwidth and massive interconnection of devices supporting further development of the internet of things, ubiquitous sensors, and effectors.

- Bio engineering: Developments in medical devices and implants (including neural links and advanced prosthetics), in the sequencing and manipulation of the genome for good and for bad, and in the synthesis of tailored therapeutics.

- Quantum computing: The development of quantum computing disrupting the current digital computing model and providing massive increases in computing power, linked to developments in quantum secure communication.

- Space technology: The race for space continues with increased access and reduced launch costs, establishment of interplanetary presence for humankind, more sophisticated autonomous space missions; but also risks from space debris fields and counter-space operations.

- Robotics: A broad set of advances in which robots become more sophisticated and ubiquitous in all spheres of life from high risk industrial and military applications, through advanced swarming drones, to anthropomorphized robots for personal care and miniaturized surgical robotic devices.

- Smart manufacturing: The continuing development of 3D printing technologies and the ability to provide highly tailored and personalized manufacturing systems, linked to just in time delivery models.

- Nuclear fusion: The growing availability of nuclear fusion including micro reactor developments resulting, along with growth in renewables, in fundamental changes in the dependence on oil and gas based energy sources.

- Augmented reality: The creation of high fidelity non-intrusive augmented reality systems and highly immersive virtual reality environments, linked to the potential developments in neural implants and neural stimulation technologies.

Securing the UAE's vision

The UAE has outlined the principles upon which it will build leading up to its centennial year in 2071. These principles chart the strategic roadmap for the UAE's new era of economic, political and social growth from strengthening the union and institutions to placing digital, technical and scientific development at the heart of its economic development.

The UAE Vision 2031 initiative aims to advance healthcare, education, sustainability, and infrastructure, positioning the UAE as a significant economic center and global partner. It seeks to boost societal well-being, drive economic growth, bolster global presence, and improve government performance using advanced technologies.

They will act as guidelines for all institutions in the UAE as the country approaches a new phase of development over the next five decades. They are part of the 'Projects of the 50' campaign, and are as follows.

- Strengthening the union - The key national focus shall remain the strengthening of the union, its institutions, legislature, capabilities and finances.
- The best economy - We will strive over the upcoming period to build the best and most dynamic economy in the world.
- A robust foreign policy - The Emirates' foreign policy is a tool that aims to serve our higher national goals, the most important of which is the Emirates' economic interests.
- Human capital - The main future driver for growth is human capital: developing the educational system, recruiting talent, retaining specialists and continuously building skills.
- Neighborly ties - Good neighborliness is the basis of stability. The geographical, social and cultural position of the country in its region is the first line of defence for its security, safety and its future development.
- A hub of excellence - Consolidating the reputation of the Emirates globally is a national mission for all institutions. The Emirates is one destination for business, tourism, industry, investment.

- Embracing innovation - The digital, technical and scientific excellence of the Emirates will define its development and economic frontiers.
- A defined set of values - The core value system in the Emirates shall remain based on openness and tolerance, the preservation of rights, the rule of justice and the law.
- Humanitarian aid - The Emirates' foreign humanitarian aid is an essential part of its vision and moral duty towards less fortunate peoples.

07

CONCLUSION & CALL TO ACTION

In today's increasingly digital world, the evolution of cybersecurity threats presents both challenges and opportunities on a global scale. This report emphasizes the urgent need to address these risks through coordinated efforts, advanced technologies, and strategic policy frameworks. Globally, cyberattacks are becoming more sophisticated due to emerging technologies such as AI, quantum computing, and the Internet of Things (IoT). As businesses, governments, and individuals rely more heavily on digital infrastructures, the frequency and impact of these attacks are escalating.

The UAE has shown strong leadership in cybersecurity, positioning itself as a regional and global hub for innovation in this critical area. The country has established the UAE Cybersecurity Council and continues to drive initiatives to safeguard its digital assets and secure critical infrastructures. The case studies in this report illustrate various cyber threats, such as ransomware attacks and supply chain vulnerabilities, emphasizing the importance of ongoing vigilance and innovation.

In the coming years, cybersecurity will rely on a multi-faceted approach that combines technological progress, policy enforcement, and collaboration between public and private sectors. The UAE serves as a strong example by promoting digital resilience, implementing advanced security protocols, and strengthening international partnerships. However, keeping up with rapid technological advancements, especially with the introduction of quantum computing and AI, presents a significant challenge for the cybersecurity landscape.

The crucial takeaways from this report indicate that taking proactive, adaptable strategies will be essential in mitigating future threats. This involves investing in cybersecurity talent, promoting innovation through research and development, and fostering a culture of cybersecurity awareness across all sectors of society. As the UAE continues to enhance its cyber defense capabilities, it is well-positioned to lead global efforts in shaping a secure digital future, paving the way for sustained economic growth and societal well-being in an interconnected world.

CONCLUSION & CALL TO ACTION

In response to these challenges, the report emphasizes a collective effort by governments, industries, and academic institutions to bolster cybersecurity infrastructure. This includes:

Call to Action

Enhance Cybersecurity Measures

Implement AI-driven detection and response systems, with a focus on Zero Trust Architecture. Invest in workforce development to close the talent gap and bolster defense readiness.

Encourage Public-Private Collaboration

Strengthen innovation by fostering partnerships between the public and private sectors, particularly in emerging technologies like blockchain and AI.

Focus on Cybersecurity Awareness and Education

Launch national awareness campaigns and mandatory training programs to arm individuals with the knowledge needed to combat modern threats.

Invest in Secure Technologies

Increase investment in cutting-edge technologies, such as post-quantum cryptography, to safeguard sensitive data and infrastructure.

Strengthen Incident Response Frameworks

Continuously refine incident response frameworks and promote proactive measures, such as bug bounty programs, to identify vulnerabilities before they are exploited.