Advancing Regional Cybersecurity (ARC) KENYA

Roundtable and tabletop exercise report

4 May 2026

Authors: Elizabeth Eigner, Patricia Eke, Colonel (Dr) James Kimuyu, PhD, Markus Münzer

Contents

Executive summary 1

Roundtable discussion 2

- Session 1: Next 12 Months Plan 2
- Session 2: Ransomware & Information Sharing 5

Tabletop Exercise Format 8

Exercise Setting & Scenario Events 10

- Phase 1: DDoS Attacks and Subsea Energy Cable Cut 10
- Phase 2: 0-Day Vulnerabilities and Publications 12
- Phase 3: Banking Ransomware 13
- Phase 4: AI-Enabled Large-Scale Cyber Attacks 14

Executive summary

This document is meant to accompany the Advancing Regional Cybersecurity (ARC) Actionable Toolkit and serves to document and analyse the roundtable discussion and tabletop exercise, capturing key conversations, themes, and areas of consensus. For more information on how the tabletop exercise was executed, see the Tabletop Exercise Annex.

Roundtable discussion

This section summarizes the outcomes of the discussions from the roundtable.

Methodology

This traditional in-person roundtable operated in accordance with Chatham House Rule, ensuring that participants could speak freely without attribution. During the session, attendees were divided into two groups based on their roles and expertise: General Governance and Cybersecurity Governance. Each group received tailored questions relevant to their focus area.
At the conclusion of each section, the groups reconvened to share their insights and discuss key takeaways, facilitating collaborative dialogue and cross-pollination of ideas.

The participants of the roundtable included over 40 participants from 14 organisations including key stakeholders responsible for ensuring national level cybersecurity in Kenya. Participants were invited from areas of expertise such as Cybersecurity Governance, General Governance, Private Sector & Industry and Civil Society & Academia.

Session 1: Next 12 Months Plan

In Section 1 of the roundtable, participants were asked to **consider how they would strengthen Kenya's cybersecurity posture over the next 12 months.** Participants were tasked with triaging Kenya's cybersecurity challenges to determine two key aspects. First, which issues were most urgent and required immediate attention, and second, which challenges represented achievable or 'low hanging fruit' that could realistically be addressed within the next 12 months. This approach ensured that the group prioritised both critical needs and practical, actionable steps for strengthening the national cybersecurity posture in the year ahead. Below are priorities and activities that emerged in consensus from the roundtable.

Discussion

Addressing the most pressing challenges

Among the **most pressing challenges** identified by participants were the **urgent need to reduce fragmentation in Kenya's cybersecurity landscape, the lack of standardised incident management processes across organisations, and weaknesses in communication between sectoral Security Operations Centres (SOCs).** Stakeholders also highlighted the necessity for clear reporting obligations for both public and private entities, as well as the development of national playbooks for critical incident types such as DDoS, ransomware, and phishing. These issues were viewed as requiring immediate attention to ensure a more cohesive and effective national response to cyber threats.

To address these most pressing challenges, **participants called for a clearly defined 12-month programme to improve cyber readiness, reduce fragmentation, and standardise incident management across stakeholders.** This includes developing a national operating model that clarifies roles and decision rights, especially given the mix of public and private ownership in critical infrastructure.

Participants also urged for the Bolstering of Kenya's Incident Response Framework, and recommended Kenya adopt a National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 (CSF 2.0)-aligned, operational framework with clear minimum requirements for detection, reporting, coordination, and recovery. This framework should prioritize preparedness through policies, clear responsibilities, staff training, regular exercises, and baseline security tools. This framework should prioritise preparedness through

policies, clear responsibilities, staff training, regular exercises, and baseline security tools, particularly focusing on detection and reporting capabilities.

Participants converged on a set of priority playbooks to be standardised nationally. These would include Distributed Denial of Service (DDoS), ransomware, phishing, data breach including cloud service incidents. Playbooks should focus on detect, respond, and recover activities and be supported by baseline organisational requirements, particularly business continuity planning.

Vendor onboarding to federal projects was identified as a gap, as was a lack of national guidance on minimum supplier security requirements. **The group recommended establishing a structured Security Operations Centre (SOC) coordination model** that connects organisational, sectoral, and national SOCs, with clear escalation pathways and defined thresholds for escalation. Sectoral SOCs in telecommunications and banking were highlighted as strong reference models, although the group acknowledged that communication between sectors remains a weakness. To address this, participants proposed developing a centralised incident reporting channel to ensure effective alignment and coordination during active incidents.

The group recommended that **incident reporting from critical infrastructure entities be undertaken regularly and proactively with clear obligations also defined for private sector stakeholders**. Participants believed a 12-month plan from Kenya's government to establish precise procedures for responding to reported incidents would be beneficial. This should encompass triage, coordination, technical assistance, information sharing, and the activation of national communication mechanisms to ensure an effective and unified response.

In addition to immediate priorities, participants **recognized that artificial intelligence (AI) presents both near-term and long-term challenges for Kenya's cybersecurity landscape.** They agreed that emerging risks associated with AI demand policy and legislative updates, Participants recommended that cyber laws—such as the Computer Misuse and Cybercrime Act (CMCA)—be reviewed to address AI-related threats. Separately, responsible state behaviour was also highlighted as a priority, underscoring the need for continual attention within the national cybersecurity agenda.

The group acknowledged that **achieving these outcomes relies heavily on the development of capacity and specialist skills across the sector.** Rather than concentrating on general awareness, the group concluded focus should be on building expertise in priority areas such as digital forensics, cloud security, ethical hacking, and incident response. Participants emphasised the importance of ongoing accreditation and practical development pathways for cyber forensics and identified the need for national-level investment in facilities, tools, and robust procedures to strengthen forensic capabilities for sophisticated cyber-attacks.

Other near-term opportunities

Participants also highlighted the need to harmonise cybersecurity and national security priorities by establishing clear values, ensuring accountability, and enforcing consistent standards. Despite recognising that the country has already put in place key legislative and strategic documents, such as the CMCA establishing offences, investigation powers, and national coordination mechanisms, the Data Protection Act, and the draft National Cyber Strategy to 2029, **participants observed ongoing gaps in organisational implementation and called for practical national guidance.** The integration of data protection and cybersecurity into a unified framework was proposed to minimise duplication and inconsistency.

Effective information sharing and classification were identified as critical for national coordination, with the lack of standardisation hindering cooperation. A national framework clarifying what information can be shared, with whom, and under which conditions, alongside practical classification guidance, is needed to support consistent incident reporting and sector collaboration.

Law enforcement representatives noted that **the justice system remains misaligned with the realities of cybercrime,** resulting in limited prosecution success even with robust evidence. They asserted that in the next 12 months Kenya should endeavor to strengthen the entire investigative and judicial process, including evidence handling and forensic capacity.

Collectively, these findings underscore the importance of clear governance, robust frameworks, cross-sector coordination, and transparent reporting protocols in strengthening Kenya's national cyber resilience.

Session 2: Ransomware & Information Sharing

The discussion explored how national coordination bodies could better integrate cyber information sharing, establish legal and policy frameworks that balance transparency and confidentiality, and strengthen information-sharing mechanisms within and between governments —particularly in the context of ransomware incidents. Participants were also asked to consider immediate steps to support ransomware detection, strengthen trust among ministries, and the design of a sustainable, long-term interagency information-sharing model for Kenya.

The Cybersecurity governance group explored **what types of cyber threat data—such as indicators of compromise or vulnerability alerts—should be prioritised for sharing across sectors.** Participants were asked to reflect on which institution should coordinate information flow (for example, a national Community Emergency Response Team (CERT) or sectoral Computer Security Incident Response Team (CSIRTs)), what capacity or technology gaps exist, and whether automation could play a role in operationalising the system.

Discussion

Participants identified the lack of actionable information sharing, insufficient trust and confidentiality mechanisms, and the absence of unified data classification standards as the greatest risks. Additional risks included gaps in detection, response, and technical capabilities, as well as weak cross-sector collaboration and unclear legal or policy obligations for reporting and handling ransomware incidents.

Participants converged around **three overarching priorities for strengthening Kenya's ransomware response: improving the sharing of actionable threat intelligence, deepening understanding of adversary tactics, and strengthening recovery practices across sectors.** Underpinning all three priorities was the need to build greater trust between public and private sector actors so that information can be shared quickly, confidently, and at scale.

Prioritise the Sharing of Actionable Data

Participants emphasised that **ransomware information-sharing mechanisms must focus on operationally useful intelligence that allows organisations to detect and respond to threats quickly.** The group recommended prioritising the exchange of indicators of compromise (IOCs), including malicious IP addresses, domains, file hashes, and malware signatures, as well as vulnerability alerts and other technical indicators that can be immediately integrated into security monitoring systems.

However, participants noted that **Kenya currently faces several structural barriers to effective intelligence sharing.** These include limited trust between organisations, uncertainty about how sensitive information should be handled, and the absence of consistent reporting and data classification standards. Without clearer guidance on what can be shared and through which channels, organisations often default to withholding potentially valuable threat information. To address this challenge, **participants recommended developing a unified national data classification framework** with clear tiers—such as confidential, secret, and top secret—supported by "need-to-know" principles. A central coordinating body should define and disseminate these standards to ensure that organisations understand how to share sensitive cyber intelligence appropriately.

Participants also highlighted the **need for stronger institutional coordination to support the flow of actionable data.** A layered coordination model was recommended, in which sectoral CERTs or CSIRTs facilitate information sharing within their industries while consolidating sector-specific intelligence. At the national level, the Cybersecurity Authority—mandated under the Computer Misuse and Cybercrime (The Critical Information Infrastructure and Cybercrime Management)

Regulations (CMCA)—would coordinate cross-sector intelligence flows. CERT structures were seen as the operational backbone of this system and as the primary link between Kenyan incident responders and regional and international CERT communities.

Finally, participants stressed that **effective information sharing depends on adequate detection and monitoring capabilities.** Significant gaps remain in technical infrastructure, tooling, and cybersecurity skills across sectors. **Sustained investment in technologies such as** Security Information and Event Management **(SIEM),** Extended Detection and Response **(XDR), and** Managed Detection and Response **(MDR) platforms was recommended to strengthen monitoring and response capabilities**. While automation and AI-based tools could eventually enhance these systems, participants cautioned that such capabilities will only be effective once foundational processes, data quality, and operational maturity are in place.

Highlight Adversary Tactics

Beyond sharing technical indicators, participants underscored the **importance of exchanging intelligence about adversary tactics, techniques, and procedures (TTPs).** Understanding how ransomware actors operate—how they gain initial access, move laterally through networks, and target specific sectors—can help organisations anticipate threats and strengthen defensive measures before incidents escalate.

Participants recommended that **threat intelligence sharing should include analysis of sector-specific targeting patterns and emerging geographic trends in ransomware campaigns**. This type of contextual intelligence allows organisations to understand whether their sector is being actively targeted and to prepare accordingly.

Cross-sector collaboration was seen as essential for developing this broader threat awareness. Participants noted that while some industries—particularly telecommunications and banking—have relatively mature cybersecurity coordination structures, others lack similar mechanisms. Expanding cross-sector SOC collaboration and establishing joint training programs could help bridge these gaps.

Participants also emphasised that collaborative exercises, capacity-building initiatives, and national forums provide opportunities for organisations to exchange insights about adversary behavior and emerging threats. These interactions help build operational familiarity between institutions and enable more effective coordination during real incidents.

Emphasise Recovery Information

Participants highlighted that ransomware response strategies must extend beyond prevention and detection to include stronger mechanisms for recovery and resilience. In particular, the group noted the growing prevalence of double extortion tactics, in which attackers threaten to release stolen data even after systems have been decrypted or restored. To address this evolving threat, participants recommended **sharing practical recovery experiences across sectors.** Organisations that have faced ransomware incidents can provide valuable lessons about system restoration, data recovery, crisis communication, and strategies for handling repeat ransom demands. Disseminating these experiences would allow other organisations to learn from real incidents and reduce the operational and financial impact of future attacks.

Participants also recommended **developing a national ransomware playbook that provides clear guidance for incident response, recovery coordination, and communication among government agencies, regulators, and affected organisations.** Such a framework could serve as a common reference point during major incidents. Roundtable Moderators recommended leveraging the Ransomware Task Force's (RTF) cornerstone report offering 48 recommendations primarily directed at governments and industry to better combat ransomware (for more details, refer to Actionable Recommendations section of this Toolkit).

More broadly, participants stressed that **recovery planning should be embedded within**

a long-term national resilience strategy. Participants recommended that over the next five to ten years, Kenya should expand cybersecurity capabilities across all critical sectors—not only telecommunications and banking, but also healthcare, agriculture, and education, which is classified as critical infrastructure. Achieving this level of resilience will require stronger funding models, workforce development programs for both cybersecurity professionals and general users, and measurable maturity targets to track progress across sectors.

Building Trust Between Public and Private Sectors

Across all three priorities, participants repeatedly emphasised that **effective ransomware defence depends on stronger trust between government institutions and private sector organisations. Fear of reputational harm, regulatory consequences, or loss of customer confidence continues to discourage companies from reporting ransomware incidents or sharing threat intelligence.**

To address these concerns, participants recommended **establishing legal protections for organisations that share information in good faith,** alongside confidentiality guarantees and anonymised reporting mechanisms. These measures could help create a safer environment for incident reporting and encourage more consistent information exchange. At the same time, participants stressed that **trust cannot be built solely through legal frameworks. It must also be reinforced through sustained collaboration and relationship-building.** Joint training programs, cross-sector exercises, SOC cooperation, and regular national and sectoral workshops were all identified as practical mechanisms for building trust and working-level relationships before crises occur.

Together, these steps would help create a more collaborative ransomware defence ecosystem in Kenya—one in which actionable intelligence, insights into adversary tactics, and practical recovery knowledge can flow more freely between government and industry, enabling faster detection, more coordinated response, and stronger national resilience.

Tabletop Exercise

Objectives

The primary goal of the exercise was to raise preparedness of Kenya in cybersecurity in dealing with and responding to cyber threats both in the short-term and long-term perspectives. The exercise set focus to the National Cyber Incident Response Framework, National Critical Information Infrastructure Protection and Cyber Resilience Framework as well as National Cyber Crisis Communication Framework.

Tabletop Exercise Format

Setup

The tabletop exercise was held in person, with participants divided into groups according to their roles and backgrounds. The participants of the exercise were key stakeholders responsible for ensuring national level cybersecurity in Kenya. **Participants were invited from areas of expertise such as Cybersecurity Governance, General Governance, Private Sector & Industry and Civil Society & Academia.** A total of 34 participants attended the exercise from 14 different organisations.

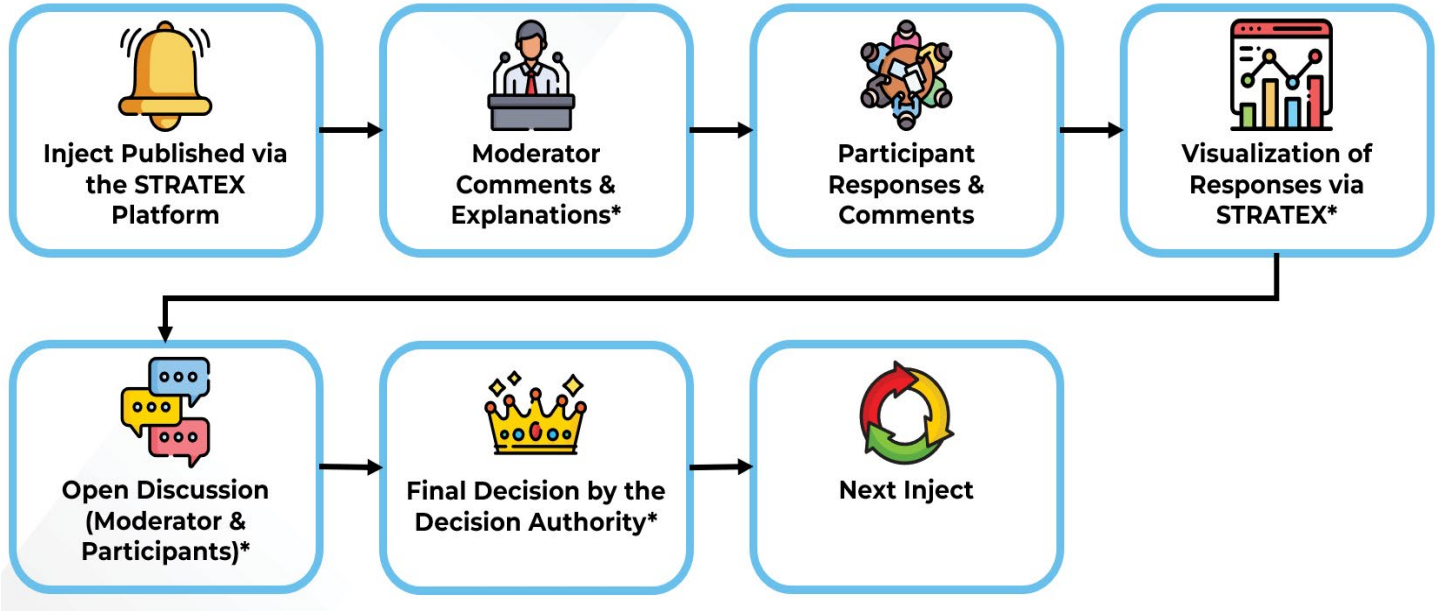
The format was designed to encourage open dialogue, enabling participants to share information, express their views, and highlight differences in opinion in a collaborative setting.

For many participants, this exercise marked their first experience engaging in a multi-agency simulation, and for some, it was even their initial exposure to a tabletop exercise. This provided a valuable opportunity to familiarise themselves with collaborative crisis response in a controlled, collaborative environment.

Format

The exercise had four phases featuring a simulated cyber incident. Participants received 29 injects—pieces of information in formats such as text, images, videos, or questions—to respond to key topics and track the scenario's progression. Injects provided context, requested input, or served both purposes, guiding the scenario's development. The STRATEX Platform (Exercise Platform) was used to provide an anonymous voting and benchmarking interface of the participant submissions which served as the baseline discussion starters.

The exercise took place according to the following inject flow:



1.1 The exercise did not include scoring of strategy or decisions. Rather, the goal of the exercise was to facilitate discussions, highlight differences in opinion, capture consensus where it existed, and identify opportunities for growth within the exercise objectives.

Exercise Setting & Scenario Events

The exercise scenario referred to fictitious countries, organisations and operations. These actors mentioned in the scenario do not represent any existing country, operation or organisation and are included for the purposes of building the scenario narrative.

The exercise scenario was based on the 4 following cyber incidents:

- DDoS Attacks and Subsea Energy Cable Cut
- 0-Day Vulnerabilities and Publications
- Banking Ransomware
- AI-Enabled Large-Scale Cyber Attacks

Scenario Phases

Phase 1: DDoS Attacks and Subsea Energy Cable Cut

Scenario 1 Summary

The first scenario outlined a coordinated cyber-physical incident in which undersea energy cables supplying the home state were cut, allegedly by a research vessel linked to a rival energy powerhouse, resulting in widespread disruptions to the regional power grid. At the same time, several key energy infrastructure organisations in both the impacted home country and its major energy supplier face a wave of distributed denial-of-service (DDoS) attacks, causing outages and operational difficulties. The event sparks accusations, denials, and demands for multinational investigations, intensifying regional tensions and contributing to instability in energy markets.

Key Themes

- The vulnerability of critical infrastructure to hybrid and cyber attacks, especially in interconnected regional energy networks.
- State attribution and the potential for escalation.
- The interplay of technical failures, malicious actions, and information operations in modern crisis scenarios.
- The role of alliances, international organisations, and collective defence mechanisms in addressing cross-border cyber threats and energy security challenges.
- The impact of such incidents on public trust, political discourse, and regional stability.

Outcome

Several key themes and takeaways emerged from participants during Phase 1. First, there was widespread recognition within the home country of the vulnerability of critical energy infrastructure to hybrid and cyber attacks, especially given the interconnected nature of regional energy networks. Participants expressed concern about limited control over supply and the ease with which targeted attacks could disrupt national and regional power grids. Participants believed that swift, coordinated action across both public and private sectors was essential in the scenario. They called for immediate geo-blocking of suspicious IP addresses, prioritisation of critical services, and national energy reduction measures to stabilize the situation.

Another major theme was the challenge of attribution and escalation. Participants discussed how leadership might respond to incidents with ambiguous or unclear origins, and the risk that misattribution or rapid escalation could further destabilize the region. Participants viewed the interplay of technical failures, potential malicious

actions, and information operations as complicating crisis management and response strategies—and emphasised the need for caution and deliberation when addressing attribution and escalation. They discussed the importance of transparent investigations before making public accusations, as well as the risks of misattribution leading to unintended escalation. There was consensus that leadership should prioritise fact-finding, consult with international partners, and communicate carefully to avoid inflaming tensions while preparing for possible defensive or diplomatic responses.

Participants also highlighted the importance of coordinated action across sectors, including the need for collective defence mechanisms and international cooperation. Participants emphasised the role of alliances and regional organisations in addressing cross-border cyber threats and ensuring energy security. Finally, the impact of such incidents on public trust, political discourse, and regional stability was a recurring concern, underscoring the necessity for transparent communication and swift, effective responses to maintain confidence and order. There was consensus on the need for transparent communication, active international cooperation—especially through alliances and regional organisations—and academic collaboration to share expertise and enhance response capabilities. These steps were viewed as vital to mitigate disruption, restore public trust, and reinforce regional stability.

Phase 2: 0-Day Vulnerabilities and Publications

Scenario 2 Summary

During Phase 2, following coordinated DDoS attacks on energy infrastructure in the home country and a neighboring state, a security review uncovered that the national oil company's database had been compromised, with chat logs altered through a sophisticated 0-day vulnerability in software. This vulnerability allowed attackers to gain extensive access and manipulate sensitive data, raising concerns about the integrity of critical infrastructure systems. The discovery led to urgent patching efforts and highlighted the global risks posed by such undisclosed software flaws. Independent experts emphasised the necessity for enhanced vigilance and robust cybersecurity measures in the sector.

Key Questions/Themes

- The vulnerability of critical infrastructure to hybrid and cyber-attacks in interconnected regional energy networks.
- State attribution and the potential for escalation.
- The challenges of identifying perpetrators and the importance of international cooperation in resolving cyber incidents.
- Handling of 0-day incidents: Rapid detection, coordinated disclosure, and swift patching for mitigating risks from unknown vulnerabilities.

Outcome

Phase 2 highlighted the immense risks posed to essential infrastructure and the urgency of coordinated response measures. Key themes included the diversity and inconsistencies in company notification obligations, ranging from immediate to 24-hour reporting, as well as varying approaches to the classification and disclosure of vulnerabilities—some favouring public transparency, others opting for strict confidentiality.

The group largely agreed on Company notification obligations regarding vulnerability reporting—with slight variations in opinions on how the Computer Misuse Act obligations would impact an organisation. However, opinions on implementation of information security policies for classifying 0-Day vulnerabilities were highly diverse, ranging from mandatory public disclosure to strict classification.

International collaboration emerged in Phase 2 as both a necessity and a challenge, with most participants supporting open information sharing among trusted partners, but notable outliers advocating limited or universal sharing.

The phase also emphasised the importance of robust cybersecurity practices, proactive threat hunting, and the critical role of independent experts in maintaining the security of critical infrastructure. Ultimately, Phase 2 revealed gaps and complexities in reporting timelines, vulnerability disclosure policies, and cross-national cooperation, highlighting the ongoing need for unified standards and resilient cyber defences to address evolving threats.

Phase 3: Banking Ransomware

Scenario 3 Summary

A major bank in the home country suffers a severe ransomware attack that disrupts key operational systems and results in the theft of sensitive data. The incident forces the bank to halt essential services like online banking and ATM withdrawals as a precautionary measure. An internationally known cybercriminal group is behind the attack, demanding a large ransom and threatening to leak stolen data if not paid. The central bank responds by coordinating with cybersecurity and financial stakeholders to contain the threat and maintain the stability of the national payment infrastructure. Despite efforts, the bank is unable to restore data from backups, highlighting the challenges of responding to sophisticated ransomware incidents.

Key Questions/Themes

- The growing threat and sophistication of ransomware attacks targeting the financial sector and their impact on national and regional payment infrastructure.
- Operational challenges and incident response.
- The role of internationally known cybercriminal groups, their motivations, and extortion tactics.
- Challenges related to ransomware payments.
- Challenges in restoring compromised data, the limitations of backup systems, and the broader ramifications for business continuity.
- The importance of transparent communication, official information channels, and cross-sector collaboration in maintaining public trust.

Outcome

Following the banking ransomware scenario, the discussion centered on the escalating sophistication of ransomware targeting financial institutions and the profound impact such attacks have on both national and regional payment infrastructure. Key outcomes included a recognition of operational challenges faced during incident response, such as the immediate suspension of services like online banking and ATM withdrawals to protect customers and contain the threat.

Participants debated the issue of ransomware payment, with opinions divided: some argued that payment should only be considered if human life is at risk, while others were completely opposed to paying under any circumstances. The decision-making framework for whether to pay ransom was similarly varied, but generally emphasised a brief deliberation period of just a few days, use of classified transparency for sensitive information, cooperation at the national level, and requiring at least company executive-level authority for the final decision.

The scenario's inability to restore data from backups underscored serious limitations in current backup systems and posed significant challenges for business continuity to the participants. Participants agreed on the necessity of prioritising resilience through robust backup systems. They emphasised that enhancing backup strategies is essential for improving recovery capabilities and ensuring continuity in the face of sophisticated ransomware attacks.

The importance of transparent communication and reliance on official information channels was emphasised to maintain public trust and financial stability during the crisis. Additionally, the scenario reinforced previous scenario findings for the need for cross-sector collaboration and coordinated action among financial regulators, cybersecurity authorities, and other stakeholders to effectively manage and mitigate the risks associated with sophisticated ransomware incidents.

Phase 4: AI-Enabled Large-Scale Cyber Attacks

Scenario 4 Summary

A widespread cyber crisis triggered by an exploit targeting critical systems across multiple neighboring countries. AI-driven attacks have disrupted essential services, including healthcare, border control, and financial trading, causing operational chaos and forcing authorities to prioritise which sectors receive immediate protection. Kaldonia, the home country, faces significant challenges as its utilities, healthcare, finance, telecommunications, public administration, transport, and emergency services are all affected, requiring coordinated response efforts to mitigate the risk and restore stability.

- Prioritise and protect critical sectors during a widespread AI-driven cyber crisis.
- Coordinated response strategies are effective across countries and sectors when resources are limited.
- Balancing immediate mitigation with intelligence gathering amid ongoing cyberattacks.
- Lasting impacts of AI-enabled attacks on public trust and infrastructure resilience.

Outcome

During Phase 4, participants discussed the ensuing operational chaos caused by large-scale attacks targeting essential services—such as healthcare, finance, utilities, telecommunications, transport, public administration, and emergency response—emphasising the challenge of prioritising protection when resources are limited and the necessity for rapid, coordinated action between national and regional authorities.

The conversation addressed the challenge of balancing rapid risk mitigation with ongoing intelligence-gathering, acknowledging the difficulties that arise when some sectors must be temporarily left exposed due to limited resources. Participants agreed on the importance of prioritising vital sectors for societal resilience and urgently identified Energy, Healthcare, Water Supply, and Food Production as the most critical sectors to protect. There was near-unanimous agreement on the need to set minimum cybersecurity standards for operators of critical information infrastructure, reflecting strong support for standardised requirements across stakeholders. Participants were united in the need for a robust National Cyber Strategy for a multi-pronged crisis such as this.

The exercise also underscored the impact that AI-driven attacks can have on public trust and the resilience of critical infrastructure, reinforcing the need for a shared regional framework for prioritisation and resource allocation during cyber crises.

Microsoft