UNIDIR

CONFERENCE SUMMARY REPORT

2025 Cyber Stability Conference

Crisis Averted: Cyber Resilience in Action

Acknowledgements

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. Work of the Security and Technology Programme is funded by the Governments of Czechia, Germany, Italy, the Netherlands, Norway and Switzerland and by Microsoft. In addition to this, International Cyber Security Workstream of the Security and Technology Programme is also supported by the Government of France. UNIDIR extends its sincere gratitude to all speakers, moderators, and audience for their insightful presentations, comments, and contributions, which form the foundation of this report. For detailed information on the speakers and moderators, refer to the conference agenda included in the annex.

About UNIDIR

UNIDIR is a voluntarily funded, autonomous institute within the United Nations. As one of the few policy institutes worldwide that focus on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, it assists the international community in developing the practical, innovative ideas needed to address critical security problems.

About the Security and Technology Programme

Contemporary developments in science and technology present both new opportunities and challenges to international security and disarmament. UNIDIR's Security and Technology Programme aims to build knowledge and awareness about the international security implications and risks associated with specific technological innovations. It also convenes stakeholders to explore ideas and develop new approaches to address these issues.

About the Author

This report was produced by **UNIDIR Security and Technology Programme**. This report was drafted by Aamna Rafiq, with contributions from Samuele Dominioni, Lenka Filipová, Andrea Gronke, Andraz Kastelic, Dominique Steinbrecher, and Pavel Mráz.

Note

The designations and presentation of material in this publication do not signify any opinion from the Secretariat of the United Nations regarding the legal status of any country, territory, city or area, or of its authorities, nor concerning the delimitation of its frontiers or boundaries. The views expressed in this publication are solely those emerging from the conference discussions and do not necessarily represent the views or opinions of the United Nations, UNIDIR, its staff members, or sponsors.

Contents

Executive Summary

On 12 May 2025, the United Nations Institute for Disarmament Research hosted its annual flagship event—**the Cyber Stability Conference**—at the Palais des Nations in Geneva, Switzerland. This year's conference, **Crisis Averted: Cyber Resilience in Action**, marked the opening of the inaugural Geneva Cyber Week and brought together diplomats, cybersecurity experts, and stakeholders from various sectors to address emerging challenges in cyberspace through a dynamic, scenario-based approach. Through expert discussions, the Conference aimed to enhance understanding of cyber threats, promote international cooperation, and strengthen resilience against information and communications technology (ICT) incidents. The following recommendations emerging from the conference build on the good practices shared in the discussions, including on the role that the framework for responsible State behaviour in the use of ICTs can play, if implemented, to strengthen cyber resilience.

- **Cyber resilience is a team sport.** Cyber resilience is a team sport that requires a comprehensive, multi-faceted and multi-stakeholder approach. This involves not only understanding relevant frameworks, but also effective coordination among relevant stakeholders to implement those frameworks. Effective implementation includes identifying internal vulnerabilities and external threats through regular assessments, investing in continuous capacity-building, and embedding cyber preparedness into institutional processes. Crucially, organizations should develop and routinely test adaptable response strategies to stay ahead of the rapidly evolving ICT threat landscape.
- **Cyber capacity-building is a strategic imperative.** Cyber capacity-building is not merely a technical exercise; it is a strategic imperative for achieving sustainable development in the digital age. Cyber capacity-building is a key enabler of economic growth and long-term social resilience. As such, capacity-building efforts should be universal, non-discriminatory, evidence-based, politically neutral, transparent, accountable, and results-oriented. Moreover, capacity-building activities should be inclusive, coherent, demand-driven, gender-sensitive, and crafted to reflect mutual respect for human rights, confidentiality, and national ownership.[1]
- **Inclusive participation of developing countries strengthens global ICT security.** Insights from developing countries bring valuable diversity and essential strategic perspectives, enriching multilateral discussions on ICTs. A diversity of insights is also important in shaping the multilateral discussions in the Global Mechanism on ICTs in the context of international security and ensuring equitable global cybersecurity cooperation.

1 Final Substantive Report of the Open-ended Working Group 2021–2025, para. 56.

- **Multilateral cyber diplomacy enhances collective cyber resilience.** Multilateral cyber diplomacy plays a vital role in deterring malicious actors and managing the risk of escalation. Sustained diplomatic engagement in the short, medium, and long term supports timely information-sharing, promotes good practices, and strengthens collective capabilities for coordinated response and rapid recovery from ICT incidents. Multilateral cyber diplomacy is also essential for the implementation of the framework for responsible State behaviour in response to evolving ICT activities involving critical infrastructure.
- **Mutual trust among stakeholders is essential for effective cyber cooperation.** Mutual trust among relevant stakeholders is essential for effective collaboration in the ICT environment. Trust is a valuable yet fragile asset that must be protected. Trust underpins relationships among Member States, private sector actors, academia, and civil society, enabling information-sharing, coordinated responses to ICT threats, and adherence to the framework for responsible State behaviour. Building and maintaining trust among relevant stakeholders requires transparency, accountability, respect for sovereignty, and the cultivation of strong technical, legal, diplomatic, policy, and operational networks at national, regional and global levels.

Credit: Pete © Adobe Stock

1. Introduction

The global cyber threat landscape is rapidly evolving, with increasing frequency, sophistication, and impact of malicious ICT activities. As essential sectors such as energy, transportation, healthcare, and water systems become more digitized and interconnected, they present attractive targets for malicious ICT activities. This growing threat complexity underscores the urgent need to strengthen ICT incident response capacities at the national, regional and global levels, recognizing that such incidents are no longer a question of if, but when, and preparedness is key.

Member States have voiced growing concern over the rise in malicious ICT activities targeting critical infrastructure and the potential for widespread national, regional, and global repercussions.[2] Discussions within the Open-ended Working Group (OEWG) on security of and in the use of ICTs 2021–2025 have highlighted the value of practical, scenario-based methods to improve cooperation and coordination among Member States and non-State stakeholders, including civil society, industry, and academia.[3] The OEWG has stressed the importance of enhancing the protection of critical infrastructure by sharing good practices for detecting, defending against, responding to, and recovering from ICT incidents.[4] Furthermore, with the conclusion of the OEWG's mandate in July 2025, the permanent mechanism could provide an important opportunity to promote better discussion, engagement and cooperation with interested parties and stakeholders.[5]

---

2 Third Annual Progress Report of the Open-ended Working Group 2021–2025, para. 14.
3 First Annual Progress Report of the OEWG 2021–2025.
4 Third Annual Progress Report of the OEWG 2021–2025.
5 See Third Annual Progress Report of the OEWG 2021–2025, Annex C, para. 11.

The 2025 Cyber Stability Conference aimed to support such discussions by exploring concrete strategies for preventing, managing, and mitigating ICT incidents through strong cybersecurity measures and collaboration among governments, industry, and technical experts. The Conference used an innovative scenario-based approach to facilitate practical and forward-looking dialogue on real-world challenges. As one of UNIDIR's flagship annual events, the Conference brought together a diverse group of stakeholders to address pressing challenges in international ICT security and to support multilateral dialogue. The innovative scenario-based approach was strategically selected to advance objectives of the 2025 Cyber Stability Conference, which included:

- highlighting mechanisms for effective collaboration among States, technical experts, and the private sector to address cyber threats;
- analysing the practical implementation of the framework for responsible State behaviour in the context of an evolving ICT incident affecting critical infrastructure; and
- facilitating practical discussions on how cooperation can enhance cyber resilience at national, regional, and international levels.

The 2025 Cyber Stability Conference marked the opening of the inaugural Geneva Cyber Week. Geneva Cyber Week is a joint initiative of UNIDIR and the Government of Switzerland to bring together experts in cybersecurity, diplomacy, and technology to promote global cooperation. Taking advantage of Geneva as a centre for multilateral diplomacy and digital governance, Geneva Cyber Week serves as an international platform for dialogue, collaboration, and knowledge exchange. It aims to bring together policymakers, industry professionals, researchers, and civil society to tackle emerging cybersecurity challenges and to explore new opportunities.

Giacomo Persi Paoli, Head of Programme, Security and Technology, UNIDIR. Credit: © UNIDIR/Pierre Albouy

1.1 Content of the Conference

The 2025 Cyber Stability Conference was centred around a hypothetical malicious ICT operation against critical infrastructure in the **fictional region of 'Dystopia'**. The scenario, involving a cloud vulnerability and supply chain breach, illustrated how such incidents can ripple across interconnected services and States in a highly networked region. Designed to spotlight key decision-making points in ICT incident response, the simulation formed the basis for discussions. These sessions followed different layers of analysis as conceptualized in **UNIDIR's ICT Intrusion Pathway** framework.[6]

- **Outside the perimeter** (the 'external environment'). This layer of analysis encompasses the systems, networks, and data sources that exist beyond an organization's direct control in the external environments where perpetrators may gather intelligence on a target (in this case critical infrastructure) without interacting with its protected perimeter. In the scenario, this phase was where malicious cyber actors discovered the ICT vulnerability and exploited it to gain unauthorized access to the cloud environment.
- **On the perimeter** (the 'security barrier zone'). This layer represents the boundary between an organization's internal systems and the external environment where perpetrators attempt to breach perimeter defences by exploiting ICT vulnerabilities, and defenders are focused on maintaining robust defences through firewalls, intrusion detection systems, and authentication mechanisms. In the scenario, this second phase involved the perpetrators trying to breach the perimeter of a critical infrastructure operator by compromising the cloud environment through a software update embedded with malware.

6 Giacomo Persi Paoli, Samuele Dominioni. "Introducing a new framework to analyse ICT activities". UNIDIR, 2025.

- **Inside the perimeter** (the 'compromised network zone'). This layer encompasses the systems and subnetworks containing sensitive data and operational systems that are under an organization's direct control. In the scenario, this phase involved critical cybersecurity breakdowns and cascading impacts after malicious actors breached the perimeter of a critical infrastructure operator in the region.
- **Beyond the perimeter.** Beyond the three layers of an ICT incident as conceived under the ICT Intrusion Pathway are broader considerations regarding prevention, response, and recovery from a major ICT incident. These issues include both technical and legal attributions, diplomatic responses, international law considerations, capacity-building, critical infrastructure protection, and the future of multilateral discussions on cybersecurity. In the scenario, this phase illustrated how actors in the region positioned themselves to respond to the catastrophic ICT incident.

At the outset of the conference, the end-stage cascading impacts of the fictional ICT incident were presented. The scenario then rewound to a point before the perimeter defences were breached by malicious actors, and stepped through each phase of the evolution of the ICT incident. The scenario presented the perspectives of the cyber intruder, while the sessions retrospectively analyzed the perspectives of cyber defenders during each phase of the ICT incident, specifically focused on how the incident evolved and how different actors could have prevented, managed, and mitigated it though the implementation of the framework for responsible State behaviour.

After UNIDIR presented each phase of the scenario through a video, multi-stakeholder panels engaged in dialogue—both among themselves and with the audience. Details on panel composition and panelists profiles are available on the event's **official webpage**. Discussion focused on four key considerations:

1. What could defenders have done differently?
2. What good practices could have helped prevent the intrusions depicted in the scenario?
3. How could implementation of the framework for responsible State behaviour help to mitigate risks and build resilience?
4. What response options and de-escalation strategies were available when intrusions succeeded?

Credit: © Adobe Stock

1.2 Purpose of this Summary Report

The following report summarizes the substantive discussions on concrete strategies for preventing, managing, and mitigating ICT incidents through cybersecurity measures and collaboration among governments, industry, academia, civil society, and technical experts. The resulting recommendations are grounded in the good practices shared throughout the deliberations, including insights into the role that the framework for responsible State behaviour can play in strengthening cyber resilience.

Section 2 of this report outlines the main themes and insights from the Conference, following the structure of the event across six subsections. Section 2.1 summarizes the opening remarks and keynote address; 2.2 provides foundational context by examining the broad range of factors beyond the defender's direct control, with particular emphasis on ICT vulnerabilities and supply chain security; 2.3 addresses how cybersecurity measures could strengthen perimeter defences against unwelcome intrusions, using the scenario as a point of departure; 2.4 explores the ways in which defenders could contain and mitigate disruptions once a perimeter is compromised; 2.5 explores what measures can be used to assess, respond to, and recover from a major ICT incident beyond the three key phases; 2.6 unpacks a wide range of diplomatic measures to advance collective cyber resilience. Section 3 summarizes the closing of the Conference. Section 4 concludes with a list of suggestions, based on the discussions at the 2025 Cyber Stability Conference, for strengthening cyber resilience in future.

This report is not meant to provide a comprehensive account of the conference proceedings. Rather, it serves as an accessible reference point. For those interested in the detailed discussions that took place during the event, the full conference recording is available on UNIDIR's official **YouTube** channel. An overview of the Conference is available on **UNIDIR's website**.

Credit: © UNIDIR/Pierre Albouy

Robin Geiss, Director of UNIDIR, opening the 2025 Cyber Stability Conference. Credit: © UNIDIR/Pierre Albouy

2. Summary of the Conference Discussions

2.1 Conference Opening

In the opening address, **Robin Geiss**, Director of UNIDIR, emphasized that the Dystopia scenario is not a prediction but a tool to stimulate realistic thinking about the growing threat of ICT incidents. This fictional scenario traced how a seemingly minor incident could escalate into a national, regional or global disruption. Geiss emphasized the urgent need for collective action across policy, technical, diplomatic, business, civil society, and academic domains. The scenario-based approach aimed to encourage discussion on how such incidents unfold, analyse failures, and identify opportunities for resilience and prevention. This approach supports calls from the OEWG and aligns with the Secretary-General's New Agenda for Peace, which stresses protecting critical infrastructure and essential public services. The 2025 Cyber Stability Conference marked the launch of Geneva Cyber Week, highlighting UNIDIR's commitment to advancing international cooperation, supporting evidence-based cyber diplomacy, and informing the types of multilateral discussions on the future of ICT security in the context of international peace and security towards a more secure and stable ICT environment for all.

The opening address was followed by a keynote by **Will Smart**, Director, CareTech Partners Ltd., and former National Chief Information Officer of the UK National Health Service. Smart detailed the profound impact that the 2017 WannaCry ransomware incident [7] had on the National Health Service and how it became a catalyst for change. The WannaCry ransomware affected more than 230,000 computer systems across 150 countries within hours. In less than two days, it had affected services in 80 out of 236 hospitals and 595 general practices across the United Kingdom, resulting in over 6,900 cancelled appointments. Remarkably, no patient data was stolen, and no deaths were officially attributed to the incident. The financial impact was estimated at GBP 92 million, yet the true cost extended beyond monetary losses to include the erosion of patient trust, and the emotional and psychological toll on healthcare staff and patients. The incident became a catalyst for change, motivating the National Health Service to overhaul its cybersecurity strategy. This included a cultural shift towards recognizing that cybersecurity is critical to patient safety, and not just a technical issue. The Service embarked on a digital infrastructure modernization programme, replacing vulnerable systems and outdated technology while implementing stronger security measures. However, ICT incidents like the 2017 WannaCry ransomware incident show that cyber resilience is an ongoing effort. Smart detailed five critical lessons that emerged from this crisis:

- **Governance matters.** Cybersecurity is not just a technical issue. It requires a governance mechanism with mandatory compliance with the cybersecurity safeguard mechanism.
- **Basic cyber hygiene saves lives.** Patching known ICT vulnerabilities is crucial to patient welfare, just like basic medical infection control.
- **Infrastructure age matters.** The National Health Service had been using outdated technology that needed modernization to refresh the most vulnerable devices.
- **Preparation is key.** A specific ICT incident recovery and response plan and regular drills are essential for building preparedness and emergency response capacity.
- **Contingency planning is essential.** Medical systems should have redundancies and back-ups in place to ensure that medical care can continue even when digital systems fail.

7 WannaCry was a ransomware used for financial extortion, known for its simple yet effective design. It spread rapidly via Eternal Blue, an exploit targeting a vulnerability in the Server Message Block (SMB) protocol in Microsoft Windows, which facilitates network communication between machines. The malware had four main components: a dropper to extract embedded tools, an encryption/decryption application, a file with encryption keys, and a Tor client for anonymous command and control. Once activated, WannaCry encrypted data on the infected system and demanded ransom for decryption—unless it successfully contacted a built-in 'kill switch' URL, which would halt execution. Despite its first major outbreak in May 2017, WannaCry continues to pose a threat today.

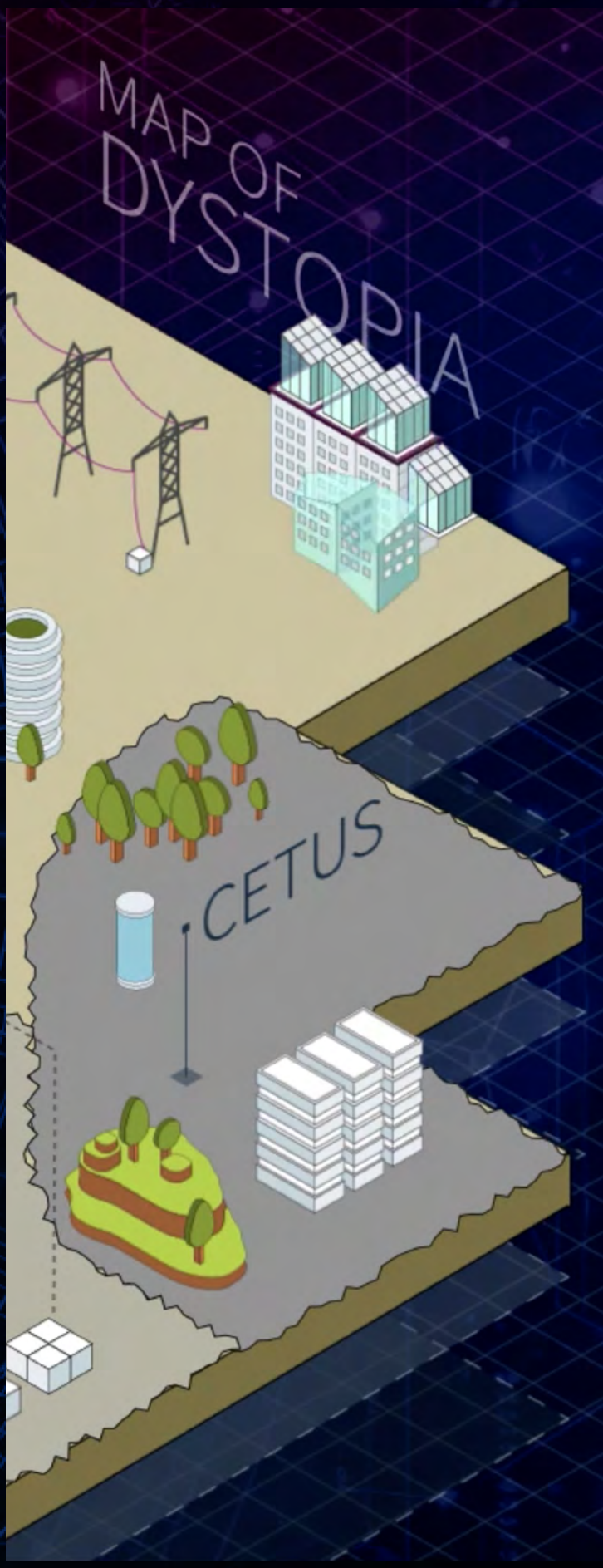
Welcome to Dystopia

The region of Dystopia was characterized by the digital ambitions of six States, namely URSA, VIRGO, MALIN, CETUS, COSMOS, and CENTAURUS.

Over the past decade, Dystopia has undergone rapid transformation. Societies, infrastructure and services have become increasingly digitalized, automated, and integrated. Much of this progress is powered by cloud services. Across the region, most institutions and public services rely on a small number of cloud service providers, making digital operations efficient, but highly interlinked at the same time. The region shares more than just ICT tools—it is interconnected by a common infrastructure, such as cross-border energy grids, regional water systems, and shared natural resources. All six States of the region belong to the United Nations and are party to relevant international treaties. National, regional and global cooperation frameworks are in place, and diplomatic and technical channels are active.

A major ICT incident disrupted critical infrastructure across Dystopia, starting with delayed flights and power outages and escalating to a catastrophic mid-air collision, grounding air travel and stranding thousands.

On the ground, self-driving vehicles and automated transport systems failed, causing widespread gridlock, while power outages crippled hospitals and communication networks. Environmental damage raised health concerns and affected agriculture. Panic buying started amid paralyzed supply chains. In this chaos, URSA—a less developed State of the region—faced additional vulnerabilities due to the recent migration of critical national systems to cloud-based systems and stalled cybersecurity legislation. URSA shares key waterways with neighbouring States, adding cross-border environmental and political complexity to the crisis.



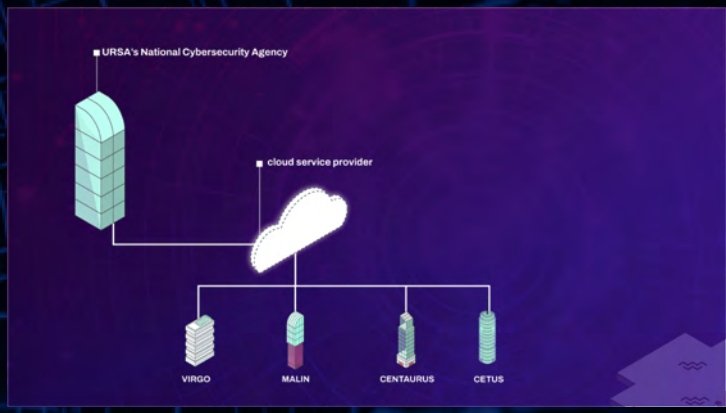
Panel 1 speakers. Credit: © UNIDIR/Pierre Albouy

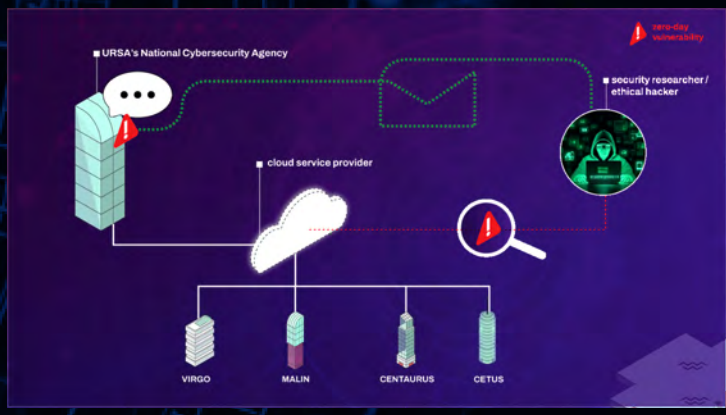
2.2 Session 1. Outside the Perimeter: Strengthening Digital Supply Chains

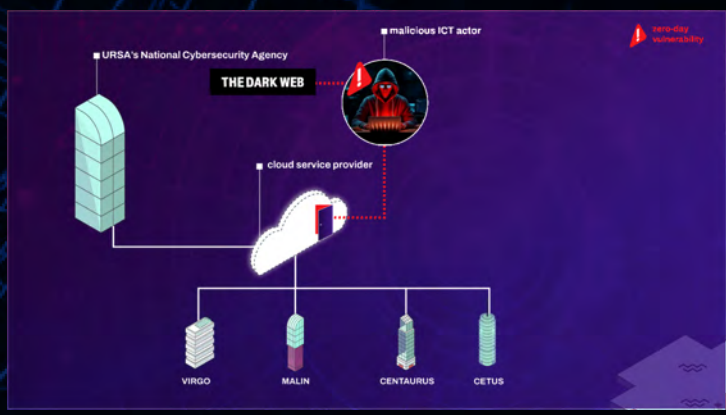
The first session examined the origin and evolution of cyber threats and vulnerabilities in ICT environments. Discussions explored risks posed by unreported ICT vulnerabilities, software supply chain dependencies, and software update tampering. In this context, the panel considered some missed opportunities in Dystopia for threat detection, early prevention, and multi-stakeholder cooperation. The session touched upon the role of the framework for responsible State behaviour, emerging good practices, current initiatives, and innovative approaches that could mitigate ICT threats well before a breach.

Sixty Days to Catastrophe: The Breach That No One Claimed

Sixty days before the cascading network failure across Dystopia, URSA's National Cybersecurity Agency was alerted by a security researcher to a previously unknown vulnerability in a major regional private cloud provider based in MALIN.
Due to the lack of a national vulnerability management policy and institutional disagreements, URSA delayed disclosing the issue to the provider and to other States of the region. The vulnerability was eventually leaked, being sold on the dark web and turned into an exploit to gain covert administrative access to the cloud service provider's internal networks, installing a persistent backdoor and moving laterally within the system.







Key Insights from the Session

- **Cybersecurity is an investment.** Speakers stressed the need to reframe cybersecurity not as a cost but as a strategic investment with long-term benefits. Cybersecurity should be treated as a critical national security, economic, and societal priority. To be effective, cybersecurity should be integrated early into national strategies, policies and legislation to support safe and sustainable digital transformation. Long-term resilience and success require sustained investment in people, skills, knowledge and processes.
- **Approaches for ICT vulnerability disclosures.** Speakers emphasized the vital role that cybersecurity researchers play in detecting and disclosing ICT vulnerabilities. To support the responsible disclosure of vulnerabilities, some speakers underscored the importance of providing legal protections and limiting liability for cybersecurity researchers acting in good faith. Some speakers identified reporting directly to manufacturers as a preferred approach, for faster remediation. However, some speakers highlighted that in cases where researchers face challenges to report vulnerabilities directly to manufacturers, intermediaries such as Computer Emergency Response Teams (CERTs) can serve as an alternative. Speakers also highlighted the specific risks associated with vulnerabilities in government ICT systems, such as delayed patching due to vulnerability stockpiling, reinforcing the need for transparent and well-defined disclosure policies. 'Bug bounty' programmes were mentioned as a useful tool for fostering trust and technical collaboration on vulnerability disclosure. Positive examples of vulnerability disclosure practices noted by speakers included legal protection for researchers and patches issued prior to public disclosure.
- **Vulnerability disclosure is a multi-stakeholder process.** According to the speakers, disclosure often requires a collective approach, especially when multiple stakeholders are involved. While governments can play a supportive role, they should not dominate the process. International cooperation on vulnerability disclosure may face challenges due to mistrust, fear of reputational harm, and geopolitical tensions. Trust among technical communities—built through shared professional cultures, conferences, and collaboration—is crucial for effective coordination of disclosure but remains delicate and easily disrupted. Having established points of contact before emergencies arise greatly improves preparedness for and mitigation of ICT incidents.
- **Mapping supply chain dependencies.** Several speakers highlighted the importance of mapping supply chain dependencies to better understand vulnerabilities across both critical and non-critical systems. Supply chain dependencies may pose distinct challenges due to their complexity, reliance on a range of digital products and services supplied from multiple jurisdictions, and varying analytical capabilities of relevant actors to scan for vulnerabilities. Mapping these dependencies proactively was proposed as one facet of effective crisis response.

- **Policy principles for supply chain resilience.** Speakers emphasized the need for strategic approaches to supply chain security that strengthen cohesion across the complex interconnections of digital supply chains to reduce the risk of malicious cyber actors exploiting weak links to gain access to downstream users. Reducing global fragmentation through the adoption of consistent baselines and standards for supply chain security was highlighted as an essential policy principle for improving supply chain resilience. Furthermore, policies should prioritize system availability alongside integrity and confidentiality to ensure continuity of critical operations and essential services during disruption.
- **Framework of responsible State behaviour for supply chain security.** The framework should be viewed as a practical guide and not just a theoretical approach to supply chain resilience. In the context of the Dystopia scenario, speakers agreed that two voluntary norms in the framework deserved particular attention: norm 13(i) on ensuring the integrity and security of supply chains and digital products, and norm 13(j) on promoting responsible vulnerability reporting and information-sharing. Given that vulnerabilities in any part of the supply chain can have wide-ranging and even global consequences, attention should be given to negotiating diplomatic and legal measures for multi-stakeholder capacity-building at the national, regional and international levels to fully operationalize the framework within the permanent mechanism.

Lessons Learned

Timely action on ICT vulnerability disclosure could possibly have prevented the regional ICT incident that unfolded in the scenario. A delay in reporting a previously unknown vulnerability by URSA's National Cybersecurity Agency—due to a policy gap and a lack of institutionalized agreements for vulnerability disclosure—turned a simple patch window into a potential attack window. The compromise of a regional cloud service provider through exploitation of the unreported vulnerability ultimately led to a compromise of cloud-infrastructure operators, triggering cascading effects across multiple States.

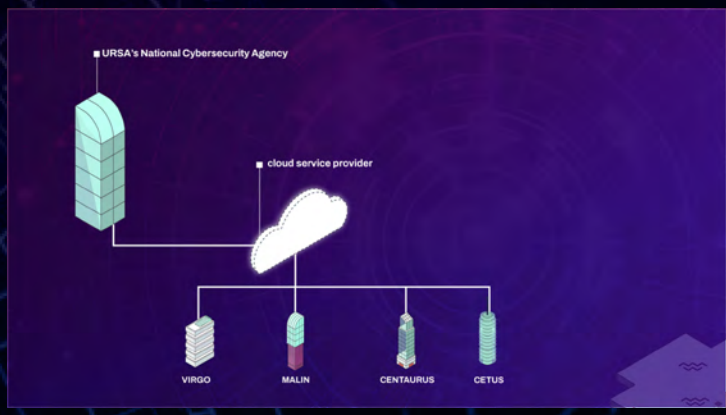
Panel 2 speakers. Credit: © UNIDIR/Pierre Albouy

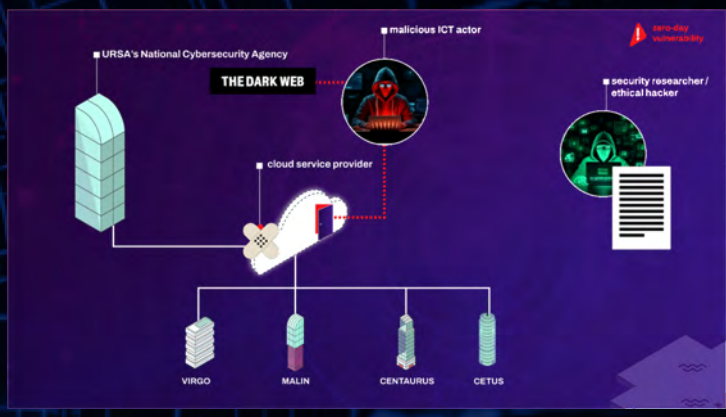
2.3 Session 2. On the Perimeter: Enhancing Endpoint Security and Protecting Critical Systems

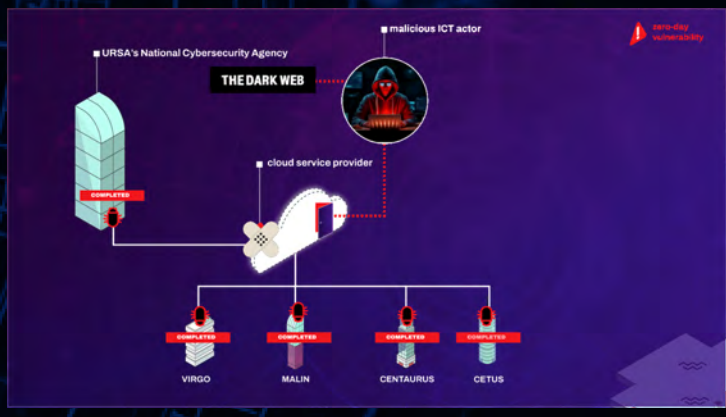
Continuing with the Dystopia scenario, the second session addressed how cybersecurity measures, including at the technical, organizational and policy levels, may help to protect the perimeter from unwelcome intrusion. The discussion focused on how to deter and prevent intrusion attempts from breaching perimeter defences of critical infrastructure, including the role of the framework for responsible State behaviour. Speakers also explored the role of stakeholder cooperation, policies, practices and endpoint solutions to prevent intrusion.

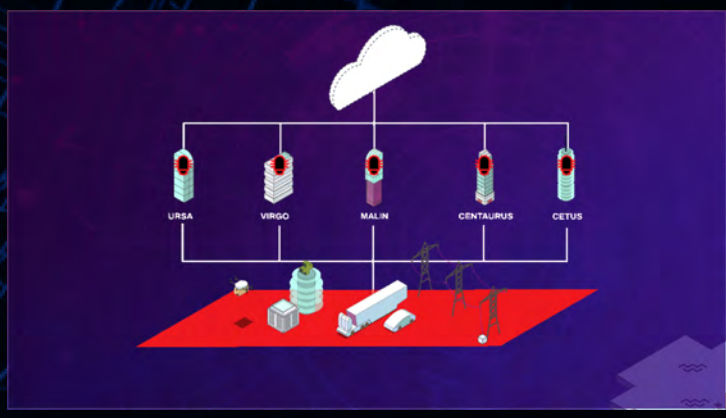
Malware in the Supply Chain: A Crisis Delivered

After URSA failed to act on a reported vulnerability, a security researcher disclosed it to the private cloud provider, which issued a patch. The researcher later published technical details publicly. Prior to patch being issued, however, a malicious actor exploited the vulnerability by disguising malware as a software update. As concerned users installed the update, the malware spread widely, including to critical infrastructure. A private cloud provider unknowingly distributed this malware, which infiltrated individual devices as well as business and government systems. URSA was especially affected due to lacking supply chain security, allowing the attacker to install rootkits and remain undetected.









Key Insights from the Session

- **Early preventive measures are key.** Speakers were of the view that States can strengthen early prevention by improving early detection systems, enabling real-time threat intelligence sharing and vulnerability disclosure, enhancing transparency with cloud service providers, and conducting regular integrity verifications and audits of supply chain security practices. Additional early preventive measures discussed included enacting robust national data protection laws, developing technical certification frameworks, and ensuring compliance with stakeholder-specific guidelines.
- **Prioritize the development of people, skills, and technology.** Speakers advocated for incorporating a security-by-design approach for both software and hardware components into national frameworks. National policies should identify critical infrastructures and define the roles and responsibilities of all key stakeholders. Speakers emphasized the importance of developing cybersecurity awareness among the general public to promote cyber hygiene, and of developing skilled cybersecurity teams. In particular, speakers underscored the value of public–private partnerships, especially in less developed countries, as a means of strengthening national cybersecurity capacities.
- **Cloud service providers have greater responsibility.** Speakers highlighted that defining clear parameters is a first step to understanding the trust boundary between users and cloud service providers. The focus should be on threat exposure and the attack surface across users, infrastructure and applications. Providers are primarily responsible for enhancing network security, protecting physical assets, maintaining rigorous supply chain integrity practices, ensuring timely and trusted communication with clients, and developing early threat detection and ICT incident response capabilities. To effectively manage risks and maintain trust with users, providers should adopt a 'zero trust' strategy across five aspects: i) user identity, ii) device security, iii) access privileges, iv) intra-organizational transactions, and v) overall user cybersecurity experience.

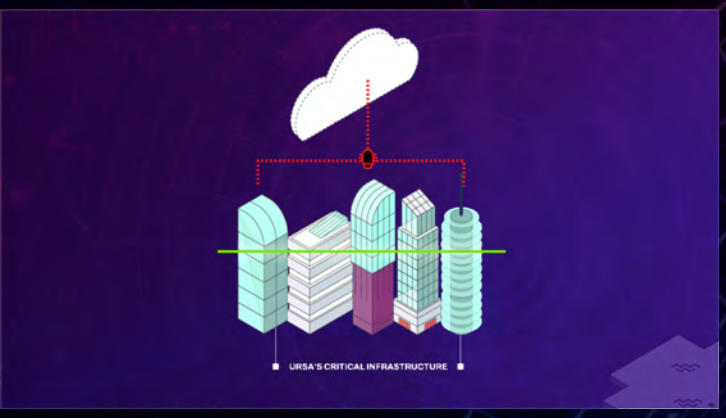
Lessons Learned

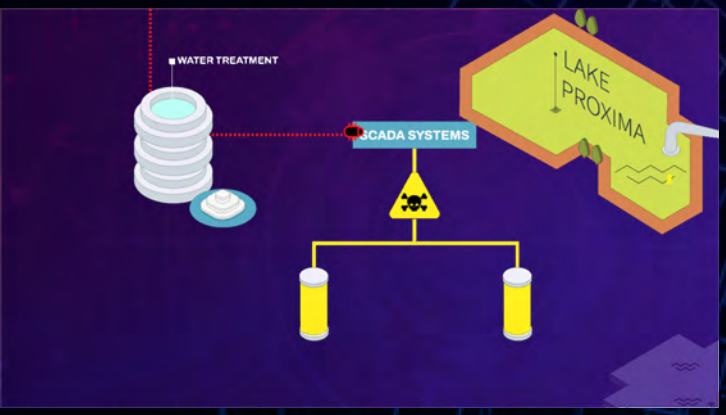
Timely action on ICT vulnerability disclosure could possibly have prevented the regional ICT incident that unfolded in the scenario. A delay in reporting a previously unknown vulnerability by URSA's National Cybersecurity Agency—due to a policy gap and a lack of institutionalized agreements for vulnerability disclosure—turned a simple patch window into a potential attack window. The compromise of a regional cloud service provider through exploitation of the unreported vulnerability ultimately led to a compromise of cloud-infrastructure operators, triggering cascading effects across multiple States.

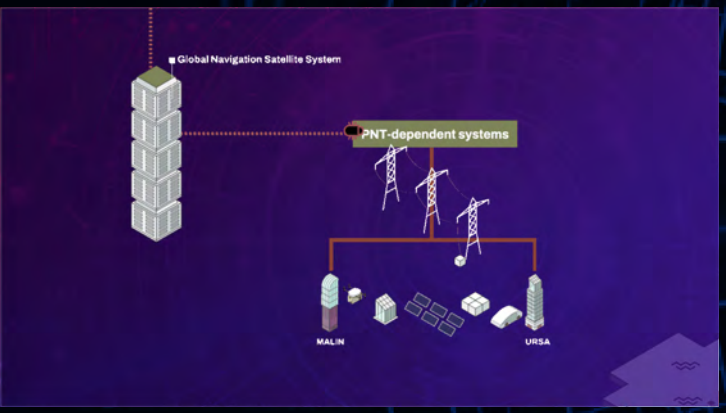
Panel 3 speakers. Credit: © UNIDIR/Pierre Albouy

2.4 Session 3. Inside the Perimeter: Preventing Cascading Effects Across Essential Services

The third session explored cybersecurity failures and cascading impacts following the breach of critical infrastructure in the Dystopia scenario. The session examined how weak cybersecurity enabled widespread disruption and discussed technical and organizational practices to reduce vulnerabilities and improve ICT incident response. It also focused on strengthening internal defences, enhancing ICT incident management, and promoting collaboration among States, the private sector, and technical experts. The discussion highlighted the role of the framework for responsible State behaviour, and of sharing emerging good practices, innovative approaches and existing initiatives to improve cybersecurity and resilience.







Inside the Heart of the System: A Silent Takeover

The perpetrators gained administrative access to URSA's critical infrastructure, embedding malware into industrial control systems by exploiting weak network segmentation and outdated monitoring. The malware targeted Supervisory Control and Data Acquisition (SCADA) systems in water treatment, altering chemical dosing and causing unsafe chlorine levels in drinking water. Wastewater systems were also targeted, resulting in a release of untreated waste into Lake Proxima, shared among URSA, VIRGO and CENTAURUS. Simultaneously, satellite navigation systems receivers were compromised, disrupting the positioning, navigation, and timing data critical to multiple sectors. The energy grid, lacking fail-safes, became destabilized, triggering cascading failures and widespread blackouts in URSA and neighbouring MALIN. Operators, deprived of real-time data, struggled to regain control.

Key Insights from the Session

- **Segmentation as a delay and detection mechanism.** Segmentation was highlighted as a critical mechanism to prevent lateral movement within the network and to extend the window for response. Speakers emphasized dividing systems into microsegments—ideally air-gapped with distinct firewalls, identity gateways, authentication protocols, and endpoint detection tools. Zero trust architecture and just-in-time privilege escalation were noted as best practices to contain intrusions and allow time for response in the event of an intrusion.
- **Rebuilding digital trust after ICT incidents.** Rebuilding trust after ICT incidents requires transparent, timely, and well-coordinated communication among affected entities, relevant stakeholders and the public. Speakers underscored the importance of pre-established crisis communication plans that enable organizations to share accurate information through trusted, official channels, helping to prevent misinformation and speculation. Legal and regulatory frameworks should guide post-incident data handling to safeguard privacy.
- **Public–private partnership for effective ICT incident response.** The risk of ad hoc and uncoordinated responses to ICT incidents was highlighted by speakers as a serious threat. To mitigate uncoordinated responses, speakers emphasized the need for close collaboration between the private and public sectors in developing domestic legal frameworks and coordinated CERT deployment plans. Such plans should clearly define the roles and responsibilities of each stakeholder, outline activation procedures, and establish coordination mechanisms for ICT incident response. Speakers also highlighted the importance of regular and large-scale joint exercises to test these plans, improve operational readiness, and ensure a unified and effective response.
- **Early coordination for multi-sector ICT incidents.** Speakers cautioned against stagnation in the early stages of planning multi-sector cooperation for ICT incident response. Contributing factors leading to stagnation include unclear objectives, limited data-sharing, inadequate stakeholder engagement, conflicts of interest, resource constraints, and bureaucratic delays. To address these kinds of challenges, speakers recommended sustained cross-sector engagement, mandatory testing of contingency protocols, annual audits of sector-specific cybersecurity standards, regular evaluations of contingency mechanisms, scenario-based stress testing, and training in rapid switching systems.[8] Ongoing planning efforts should aim to build on these recommendations to ensure continuous improvement and adaptability.

Lessons Learned

The Dystopia scenario represented a systemic failure resulting from unidentified intervention lines, hidden enablers, shared credentials, and overlooked dependencies among organizations and supply chains. The absence of timely mapping of both internal and external dependencies—combined with a lack of infrastructure redundancy, failover strategies and coordinated multi-sector incident planning—hindered effective response to the crisis.

---

8 Rapid switching systems enable fast transfer of services and data to a safe and secure backup in the wake of a disruption or system failure.

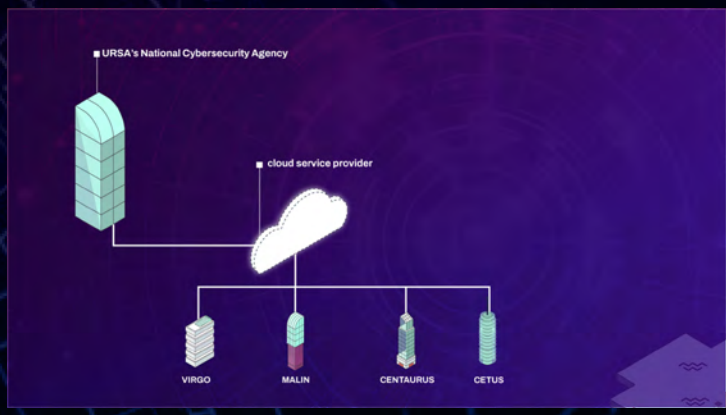
Panel 4 speakers. Credit: © UNIDIR/Pierre Albouy

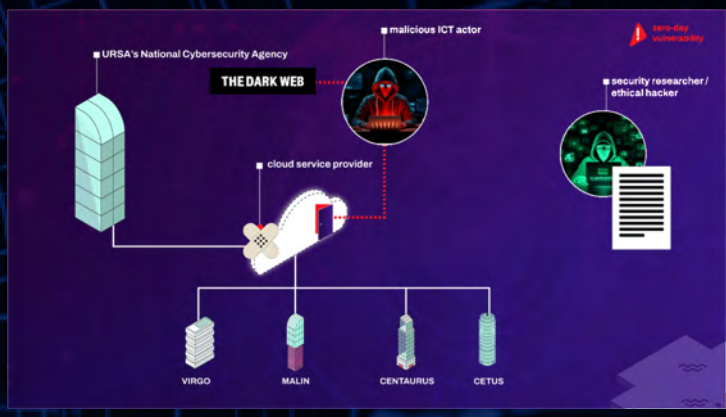
2.5 Session 4. Beyond the Perimeter: From National Crisis to Regional Response

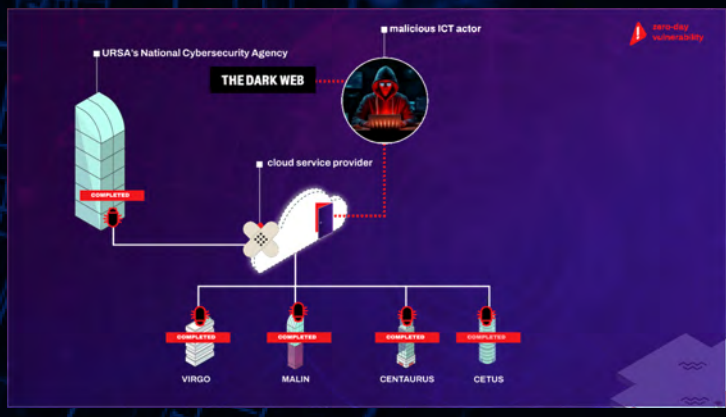
The fourth session focused on broader issues in ICT incident response and recovery. Using the scenario as a point of departure, speakers discussed how to characterize ICT incidents (including technical and legal attribution), relevant legal and policy frameworks, and the role of diplomacy, regional cooperation, and capacity-building. The session explored how ICT incidents like that in the scenario can be analysed under existing international norms and legal standards, what measures can be adopted to assess and respond to them, and what could improve preparedness and recovery for critical infrastructure. The discussion was grounded in the framework for responsible State behaviour that includes the 11 voluntary norms, international law, capacity-building, and confidence-building measures.

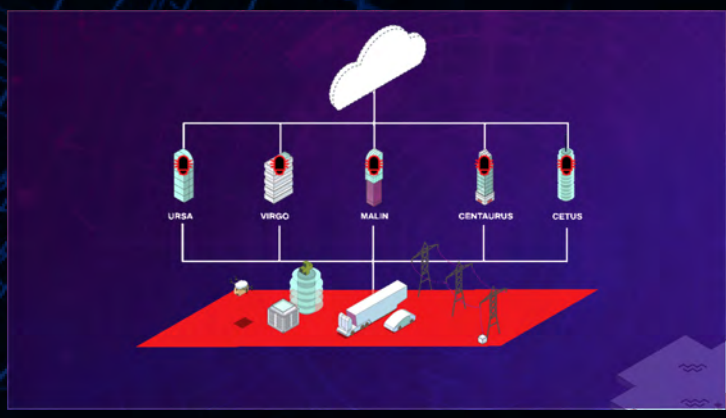
From Fragmented Response to Regional Resolve

URSA, lacking institutional coordination mechanisms, convened an ad hoc crisis management task force involving key government agencies to respond to the ICT incident. As its CERT worked on containment and recovery, a cybersecurity firm reported links between the malware used in the cyber operation and a malicious cyber group connected to COSMOS. Through international cooperation, URSA and partner States in the region traced the operation's origin to COSMOS territory. URSA initiated discussions on possible legal and diplomatic steps and convened a regional meeting to consider a potential collective course of action.









Key Insights from the Session

- **Policy and institutional measures for effective response and recovery.** Speakers stressed the need for strong policy and institutional frameworks to create synergies across people, technology, skills, and processes. Key measures discussed included early threat detection systems, information-sharing standards, comprehensive sector-specific risk assessments, and regular internal audits to identify and patch vulnerabilities. Effective governance should define clear roles and responsibilities, establish communication and escalation pathways, ensure compliance checks, and promote continuous capacity-building to maintain high standards of cyber hygiene. Furthermore, cooperation among national CERTs and robust public–private partnerships were emphasized as good practices for national response frameworks to enhance coordination and resilience. Bilateral regional cooperation, particularly for States with shared infrastructure and limited capacities, was particularly highlighted. Special attention was given to critical infrastructure preparedness, including the designation of such infrastructure at the national level and the establishment of tailored responses to sector-specific threats. The 11 norms of the framework for responsible State behaviour were emphasized as a key starting point for the development of national policies.
- **Legal frameworks to strengthen national ICT incident response.** Speakers emphasized the need for comprehensive national legal frameworks to support effective and lawful ICT incident response. They identified four key domestic legal areas that could strengthen preparedness, response and recovery: i) preventive cybersecurity legislation that sets minimum and sector-specific standards and enforcement mechanisms; ii) strategic and operational frameworks and action plans for cybersecurity; iii) effective criminal law, including to combat cybercrime obligations; and (iv) implementation of international legal obligations pertaining to cybersecurity and cybercrime. In this regard, national legal frameworks should also incorporate relevant bilateral, regional and international agreements to ensure cross-border legal interoperability and cooperation. Moreover, speakers highlighted the role of attribution—including technical, legal and political considerations—in assessing an ICT incident and for fostering accountability.
- **Role of international law in securing ICT environment.** Speakers emphasized the importance of advancing common understandings of how international legal rules and principles apply to State use of ICTs. These foundational rules and principles are essential for promoting the security and stability of the ICT environment. In this regard, the development of national or regional positions was highlighted as a useful way to advance transparency in how States and regional organizations apply international law in cyberspace. In particular, speakers highlighted the need to clarify how international legal principles governing the peaceful settlement of disputes—such as good faith and the underlying duty of non-aggravation—should be applied in the cyber context to minimize escalation. This includes better alignment of expectations for State behaviour in relation to disputes involving ICT incidents.

- **Multilateralism for accomplishing preparedness.** According to speakers, multilateral dialogue plays a crucial role in advancing a more resilient cyberspace, including on building a shared understanding of the application of international law to cyberspace. It can also help States to align their national priorities with global perspectives and to adopt good practices in ICT incident response. However, effective international cooperation depends on strong national capacities and coordination mechanisms. Disparities in capabilities among States remain a barrier to collaboration and increase overall vulnerability.
- **The role of regional organizations in preparedness and ICT incident response.** The pivotal role of regional organizations in cybersecurity was emphasized, including through their assistance in developing effective national frameworks that adhere to international standards and enhance regional cooperation. Moreover, regional confidence-building measures, such as those developed within the Organization of American States and Organization for Security and Cooperation in Europe, could enhance information-sharing frameworks, help to prevent ICT incident response errors, and promote transparency to support regional and global stability. They also encourage cross-institutional cooperation. Regional organizations also contribute to cyber confidence-building by facilitating CERT-to-CERT coordination, maintaining 24/7 directories of points of contact, and supporting real-time incident communication. Finally, speakers highlighted the role of regional organizations in promoting capacity-building, for example, by offering support for peer learning and strategic development of limited national resources.

Lessons Learned

Cyber resilience should integrate robust legal, policy and institutional frameworks and governance structures to leverage technical capacities, political leadership, strategic coordination, and national, regional and international cooperation to the end of effective preparedness for ICT incident response and recovery. The Dystopia scenario served to illustrate how a comprehensive and multidimensional framework for dealing with ICT incidents could have resulted in more effective, coordinated and timely response to a large-scale incident. It also demonstrated how political will and national consensus are precursors to a robust national policy framework for ICT incident preparedness and coordinated response.

Panel 5 speakers. Credit: © UNIDIR/Pierre Albouy

2.6 Session 5. Advancing Collective Cyber Resilience through Diplomacy

The final session shifted focus from scenario-based discussions to strategic foresight, exploring the diplomatic dimensions of advancing collective cyber resilience. This session addressed the broader implications of international cooperation and diplomacy in bridging the digital divide, supporting capacity-building, fostering trust, managing risks, and advancing the implementation of the framework for responsible State behaviour. Speakers also discussed the potential role of the permanent mechanism in accelerating multilateral implementation efforts.

Key Insights from the Session

- **Cyber diplomacy as a tool for deterrence.** Speakers agreed that sustained diplomatic engagement is essential for deterring malicious actors. Specifically, they stressed the importance of short-, medium-, and long-term diplomatic initiatives—such as sharing information and good practices, collective capacity-building and coordinated response strategies—to support swift recovery and long-term resilience.
- **Multilateral diplomacy to manage risk and prevent escalation.** According to the speakers, multilateral diplomacy was recognized as essential for fostering transparency and predictability, reducing misperceptions, and prompting shared responsibility in cyberspace. The United Nations, and especially the permanent mechanism, was seen as a key multilateral platform for institutional trust-building and cyber de-escalation efforts.
- **Multistakeholder approaches for collective cyber resilience.** Speakers emphasized the critical role of non-State stakeholders in enhancing cyber resilience. The private sector drives innovation and research and development in ICTs, while the technical community steers interoperability through standard-setting. Civil society, acting as a bridge between governments and the public, was seen as a valuable source of feedback, helping to highlight overlooked societal concerns and promote transparency. Speakers emphasized the importance of diversity in the permanent mechanism, particularly in thematic group discussions.
- **Operationalizing norms requires practical tools and inclusive cooperation.** There was strong consensus among speakers that high-level cyber norms must be translated into concrete and actionable implementation frameworks. Speakers also stressed to the importance of cooperative approaches in norms implementation, pointing to norm 13(d), which encourages States to consider how best to cooperate to address cross-border cyber threats. Multi-stakeholder involvement was highlighted as an essential element to ensure that norms implementation reflects operational realities.
- **Strengthening implementation through regional synergies.** Some speakers noted that greater efforts are needed to facilitate the meaningful participation of developing countries in multilateral discussions—particularly in the permanent mechanism. Speakers highlighted the value of regional approaches for complementing global efforts by adapting implementation to specific regional contexts. Such synergy enhances culturally appropriate solutions and can foster trust among neighbouring States. Furthermore, ensuring broader inclusion would help to address disparities in cyber capacities and broaden perspectives and insights.
- **Capacity-building must be strategic, sustainable and anchored in local ownership.** Speakers noted that effective cyber capacity-building should avoid donor-driven fragmentation and focus on aligning with national needs, local realities, and human rights principles. Speakers emphasized the importance of capacity-building being inclusive, demand driven, tailored to local contexts, and sustainable. Effective capacity-building was cited as being essential for closing the digital divide and ensuring the meaningful participation of developing countries in shaping the direction and outcomes of multilateral processes

Conference Closing. Credit: © UNIDIR/Pierre Albouy

3. Conference Closing

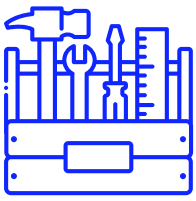
Giacomo Persi Paoli, Head of UNIDIR's Security and Technology Programme, closed the 2025 Cyber Stability Conference by expressing appreciation to the speakers, audience, and the Programme team. He emphasized the importance of sustaining momentum through further research and continued multi-stakeholder engagement.

Using the analogy of cyber resilience as a team sport, in which mere participation is insufficient and achieving success is the only imperative, he outlined a six-step pathway for cyber resilience to summarize the day's discussions. The initial step of team sport involves comprehensively understanding the 'rules of the game', namely the governing frameworks—including national, regional, and international cyber regulations—as well as the influence of technological standards on the ICT environment. The second component is 'understanding your team', which necessitates recognizing and collaborating with key stakeholders such as governments, academic institutions, CERTs, industry, civil society, and other relevant actors. The third step focuses on identifying potential adversaries by assessing both internal vulnerabilities and external threats. The fourth step involves developing a 'game plan', notably a dynamic strategic framework encompassing policies, strategies, techniques, tools, and competencies that adapt in response to the evolving ICT environment.
The fifth step emphasizes the necessity of continuous training to guarantee preparedness. Fifth, 'practice' in implementing the game plan is key and, in the case of cyber resilience, requires effective implementation of the framework for responsible State behaviour. Finally, we must 'play the game' and actively engage in ongoing discussions at the political, technical and societal level.

Concluding Session. Credit: © UNIDIR/Pierre Albouy

4. Options for Action

Based on the rich discussions of the 2025 Cyber Stability Conference, the following options for action can be identified for Member States to take into consideration for strengthening cyber resilience.



Leverage the full toolkit of statecraft to mitigate cyber threats

Cyber threats are complex, diverse, and evolving—posing risks to the economic and national security of all Member States. In response, States should actively draw on the full toolkit of statecraft to counter and mitigate these threats. This includes fostering partnerships, employing diplomacy, leveraging economic influence, and enacting policies, among others, to ensure mutual security in cyberspace.

Embed supply chain security in ICT incident response planning

Global ICT supply chains are highly interconnected and involve a wide range of national, regional and international stakeholders. Securing the openness, integrity and resilience of supply chains is critical for both international security and sustainable economic development. Given that hidden vulnerabilities in any part of the supply chain can have widespread effects, future United Nations discussions could further address the practical implementation of relevant norms and the framework for responsible State behaviour to enhance ICT supply chain security.

Strengthen capacity-building through regional cooperation

Regional cooperation provides shared situational awareness of cyber threats, context-aware regulatory understanding, and culturally appropriate solutions—essential components for effective capacity-building. Tailored programmes should be grounded in local contexts while also contributing to national response frameworks and complementing global initiatives. Regional organizations are uniquely positioned to translate global guidance into local action and ensure smoother adaptation.

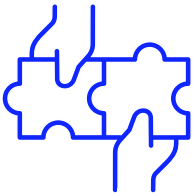
Establish comprehensive domestic legal frameworks for ICT crisis prevention and incident response

Establishing comprehensive and coherent domestic legal frameworks is essential for preventing and mitigating ICT incidents. National-level legal measures serve as the foundation for enhancing a State's cybersecurity posture and its ability to effectively respond to incidents. A well-structured legal framework ensures clarity of responsibilities, enables coordinated action among stakeholders, and provides the necessary tools for law enforcement and regulatory bodies to act decisively. These frameworks should encompass sector-specific legislation. Furthermore, domestic legal measures should be aligned with international norms and good practices to facilitate cross-border cooperation and mutual legal assistance.

Take preventive action

States should strengthen prevention efforts by improving early detection systems, facilitating real-time threat intelligence sharing and vulnerability disclosure, increasing transparency with cloud service providers, and conducting regular integrity checks and audits of supply chain security. Additional preventive measures could include enforcing data-protection legislation, developing certification schemes, and ensuring compliance with established technical standards.

Foster public–private collaboration for coordinated ICT incident response



To avoid fragmented responses to ICT incidents, the public and private sectors should collaborate on the development of national ICT frameworks and scalable deployment strategies for ICT incident response with clearly defined roles, timelines, and procedures. Regular, large-scale joint exercises are recommended to test coordination mechanisms, refine strategies, and ensure effective collective response.

Integrate cybersecurity as a foundational element of digital transformation

As digital technologies become increasingly critical for the delivery of essential services, integrating cybersecurity considerations into digital transformation efforts from the outset may help to protect systems, data, and users from evolving cyber threats. Governments and organizations should prioritize embedding cybersecurity in the design, development, and deployment of digital systems to build secure and trustworthy environments. Doing so will support innovation, drive economic growth, and maintain public confidence in the digital future.

Credit: © UNIDIR/Pierre Albouy

Annex: Conference Agenda

09:00–09:30 CONFERENCE OPENING

Opening Address: **Robin Geiss**, Director, UNIDIR

Keynote Address: **Will Smart**, Director, CareTech Partners Ltd (Former CIO, NHS England)

09:30–09:40 WELCOME TO DYSTOPIA

Giacomo Persi Paoli: Head of Programme, Security and Technology, UNIDIR

09:40–10:55 SESSION 1

Outside the Perimeter: Strengthening Digital Supply Chains

Ernst Noorman: Ambassador-at-Large for Cyber Affairs, the Netherlands

Shariffah Rashidah binti Syed Othman: Director, Cyber Security Policy and International Cooperation, National Cyber Security Agency (NACSA), Malaysia

Katitza Rodriguez Pereda: Policy Director for Global Privacy, Electronic Frontier Foundation, United States of America

Patricia Ephraim Eke: Director, Cybersecurity and Emerging Tech Policy, Microsoft

Moderator: **Pavel Mraz:** Researcher, Security and Technology, UNIDIR

10:45–11:55 COFFEE BREAK

11:15–12:30 SESSION 2

On the Perimeter: Enhancing Endpoint Security and Protecting Critical Systems

Haider Pasha: Senior Director & Chief Security Officer (CSO), EMEA & LATAM, Palo Alto Networks

Serge Droz: Chair of the Board of Directors, FIRST

Catalina Vera Toro: Deputy Permanent Representative of Chile, the Organization of American States (OAS)

Eva Nthoki: Principal Foreign Service Officer, UN & Multilateral Affairs, State Department for Foreign Affairs, Kenya

Moderator: **Samuele Dominioni:** Researcher, Security and Technology, UNIDIR

12:30–13:30 LUNCH BREAK

13:30–14:45 SESSION 3

Inside the Perimeter: Preventing Cascading Effects Across Essential Services

Andrew Lee: Vice President of Government Affairs, ESET

Ithabeleng Chabana: Chief Information Security Officer (CISO), The Global Fund

Thilina Dissanayaka: Manager, Cyber Security Capacity Building (Research, Policies & Projects), CERT Sri Lanka

Rania Toukebri: Senior Team Leader and Business Manager, Akkodis Aerospace and Defence

Moderator: **Lenka Filipova:** Coordinator, Security and Technology, UNIDIR

14:45–15:15 COFFEE BREAK

15:15–16:30 SESSION 4

Beyond the Perimeter: From National Crisis to Regional Response

Athena Matalavea: Principal Cyber Incident Response Coordinator and Analyst, Ministry of Communications & Information Technology, Samoa

Alison Treppel: Executive Secretary, Inter-American Committee against Terrorism (CICTE), Organization of American States (OAS)

Emmanuella Darkwah: Senior Manager, International Cooperation, Cyber Security Authority, Ghana

Marta Pelechová: Cyber Affairs and Cyber Diplomacy, Ministry of Foreign Affairs, Czechia

Andraz Kastelic: Senior Researcher, Security and Technology, UNIDIR

Moderator: **Dominique Steinbrecher:** Researcher Security and Technology, UNIDIR

16:30–17:30 SESSION 5

Advancing Collective Cyber Resilience through Diplomacy

Anne-Marie Buzatu: Executive Director, ICT4Peace Foundation, Switzerland

Diego Brasioli: Special Envoy for Cyberspace, Ministry of Foreign Affairs, Italy

Joanna Lahaie: Director, International Engagement & Capacity Building Office, International Cyberspace Security Policy Unit, State Department's Cyberspace and Digital Policy Bureau, United States of America

Larissa Schneider Calza: Head of Cyber Defence and Security Division, Ministry of Foreign Affairs, Brazil

Moderator: **Andrea Gronke:** Deputy Head of Programme for Cyber, Security and Technology, UNIDIR

17:30-17:45 CONFERENCE CLOSING

Giacomo Persi Paoli: Head of Programme, Security and Technology, UNIDIR


CYBER S
CONFE
Cyber governa
technologic
4–5 May 2026
UNIDIR
GENEVA 2026
CYBER WEEK


TABILITY
RENCE
nce in an era of
al revolution
Geneva and online
#CS26

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

UNIDIR

Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG