CYBER STABILITY CONFERENCE

PROTECTING CRITICAL INFRASTRUCTURE AND SERVICES ACROSS SECTORS

2022 Conference Report

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

ACKNOWLEDGEMENTS

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. The 2022 Cyber Stability Conference (CS2022) was supported by the generous contributions of UNIDIR's Security and Technology Programme core donors: France, Germany, the Netherlands, Norway, Switzerland, and Microsoft.

ABOUT UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

NOTE

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members, or sponsors.

THE AUTHOR

Dr. Camino Kavanagh is Visiting Senior Fellow at King's College London and Non-resident Scholar at the Carnegie Endowment for International Peace. Beyond current contracts, she served as Rapporteur/Consultant to the 2016–2017 Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security, and as lead consultant to the Organization for Security and Cooperation in Europe on confidence-building measures, conflict and information and communications technology.

TABLE OF CONTENTS

1. INTRODUCTION

▲ UNIDIR Director Dr. Robin Geiss opening the Cyber Stability Conference 2022.

UNIDIR's 2022 Annual Cyber Stability Conference 'Protecting Critical Infrastructure and Services Across Sectors' brought together experts and practitioners from different sectors to discuss existing and emerging approaches to critical infrastructure (CI) protection with the aim of informing ongoing multilateral discussions relevant to information and communication technologies (ICTs) and international security and stability and efforts by national governments to strengthen the resilience of critical infrastructure.

Several recent systemic events, including the COVID pandemic, the conflict in Ukraine and climate action, have elevated the importance of protecting critical infrastructure on the international policy agenda, and made more evident the interdependencies among infrastructures/sectors and their transnational character. These developments press home the urgent need to strengthen efforts underway to strengthen the resilience of critical infrastructure, including much-needed collaboration among relevant disciplines, industries and organizations.

Discussions throughout the Conference confirmed the value of the framework for responsible behaviour that has emerged at the United Nations over the past two decades through its work on ICTs and international security. The framework provides a basis for discussing threats posed to critical infrastructure and associated harms to people, society and the economy. It also provides a basis for governments to assess how they can best protect against and respond to malicious ICT/cyber activity targeting their national assets, including through the lens of existing international law, norms of responsible behaviour, and confidence-building measures that can help to build trust among all relevant CI stakeholders.

▲ Ambassador Jürg Lauber of Switzerland delivering his remarks at Concluding Session moderated by Dr. Cecile Aptel, Deputy Director, UNIDIR.

More specifically, speakers from across a range of sectors (health, humanitarian, financial, digital, transport, energy and water) discussed key aspects of resilience, notably the ability of their respective sectors to anticipate, prepare for and adapt to changing conditions, as well as to withstand and recover rapidly from disruptions. Despite significant progress in strengthening resilience across CI sectors, the Conference laid bare the need to continue evolving CI-related strategic planning and risk management models, notably where CI cross-dependencies are concerned, as well as the importance of strengthening intra- and cross-sectoral threat intelligence- and information-sharing and other forms of public–private collaboration. Discussions also highlighted the need to ensure greater accountability for lax cyber security practices within and across CI sectors, and for perpetrators of malicious activity targeting critical infrastructure. Importantly, speakers stressed the importance of moving certain CI-related policy discussions and high-level commitments forward. This includes ensuring more effective and sustainable funding models for supporting developing countries in their efforts to strengthen the resilience of their national assets.

This report identifies key take-aways from the Conference and provides a short overview of issues discussed during the panels. Recordings of the presentations are available on UNIDIR's website.[1] Discussions at the meeting were conducted under the Chatham House Rule.

1 Please see: https://unidir.org/events/2022-cyber-stability-conference-protecting-critical-infrastructure-and-services-across

2. MAIN TAKE-AWAYS

▲ Participants arriving at the venue of the Cyber Stability Conference, Campus Biotech.

THREATS AND VULNERABILITIES

- Critical infrastructure is considered vital to a country's economy and prosperity. It forms the backbone of a society's vital functions, services and activities. Increasingly, to enable real time monitoring and control, such systems couple computer control systems with physical processes. The coupling of physical and cyber systems[2] often presents vulnerabilities that, if exploited, can cause disruption or damage to the physical system producing effects within and across sectors. Recent years have witnessed a greater level of cyber-related activity targeting critical infrastructure that is considered **systemically important** for **broader economic and social development** and for international stability. The **harms** that such activity poses to **people**, **the public purse and businesses** across the globe are significant.

- **Interdependencies** within and across sectors are growing, but these interdependencies and associated risks are **not consistently or properly mapped**.[3] Geopolitical and other major events are accelerating the uptake of new technologies in some sectors, yet these often carry new risks, particularly when these technologies interact with legacy systems. The **poor cyber security practices** of **third-party manufacturers and vendors** and associated **supply chain risks** were among those considered of most concern.

- **Threat actors** include States, non-State actors acting under the authority or control of a State, criminal groups and individuals. Their tools, techniques and procedures continue to evolve, in some cases in the form of highly sought-after **professional** and **specialized services**. The general availability of vulnerability-related information across the globe makes such activity highly accessible. While identifying and assigning

2 These are often referred to as Cyber–Physical Systems (CPS).
3 For example, a water treatment or a water distribution plant requires power to operate. If the power distribution source is disrupted, the effects can be felt across both sectors.

responsibility for State activity affecting critical infrastructure has improved, accountability remains a significant problem. So too does accountability for financially motivated criminal activity such as ransomware, which law enforcement has struggled to keep pace with.

- In addition to the cyber-specific risks noted above, **poorly conceived** or non-adaptive **CI-related policy and regulation** also pose important risks where protecting critical infrastructure is concerned, as do **non-adaptive risk management frameworks**. Despite a growing number of incidents affecting critical infrastructure sectors, including in countries with mature cyber capacities, it is not evident that lessons from these incidents—many which have had **global effects**—have been properly integrated into follow-on strategies. **Accountability** for not having **anticipated or prevented** them, despite several warning signs, remains a challenge which some States and regions are beginning to address.

STRENGTHENING RESILIENCE

- Threats will continue to evolve and vulnerabilities will always exist, hence ensuring that efforts are centred on strengthening the resilience of infrastructure and minimizing disruptive effects remains critical. This includes ensuring the **capacity to anticipate/identify, prepare for, respond to and recover from cyber incidents** affecting critical infrastructure, including through more effective and comprehensive strategic planning, risk awareness and management, and greater cooperation and engagement between and across sectors and actors—nationally, regionally and internationally.
- The framework for responsible behaviour agreed at the United Nations provides a basis for governments to work with other key stakeholders to identify needs and to strengthen the resilience of their national assets. Determining which sectors and infrastructures should be prioritized or designated as critical is an important first step in this regard. Sometimes this will include infrastructures that provide services across several States; such prioritization is often outlined in national policy, strategy and legislative documents.
- Enhancing resilience across infrastructures that have been designated as critical involves significant **planning** to set objectives, to determine the necessary institutional arrangements, processes and actions, to allocate resources, to assess progress and to learn from past actions. This is an **iterative and incremental process** that builds on achievable objectives while also **incorporating feedback and improvements** into the process **at every stage**.
- **Risk-management frameworks** also play an important role in strengthening the resilience of critical infrastructure. While governments will set the relevant policy and regulation, it is broadly acknowledged, including in relevant international standards, that risk management—be it cyber-related or otherwise—is a shared responsibility among all CI stakeholders including governments, industry partners, first responders, academia and civil society. Risk-management frameworks are **evolving across sectors**, although much more needs to be done to get the right focus within and across sectors, particularly since critical infrastructures can be interconnected and dependent on each other.

- Managing **third-party risk**, particularly where the safety and cyber security practices of **third-party manufacturers and vendors** are concerned, is a shared concern of public and private CI actors, requiring greater attention of regulators and standards-setting bodies. Contracting parties need to introduce better **due diligence** practices and more consistent **auditing** of third-party vendors into their work processes. This applies particularly to new technologies emerging on the market: whether it be in the financial services sector, the energy sector (e.g., renewables/clean energy), the ICT sector broadly (security appliances, etc.) or others, more effort needs to be made to ensure that third-party manufacturers and vendors can **guarantee** that their products and services will contribute to greater resilience of critical infrastructure rather than undermine it.
- Given the **cross-sectoral cascading effects** of recent cyber incidents, it is important that public and private sectors map **cross-sectoral interdependencies** and associated risks and identify a shared awareness and common understanding of the roles, responsibilities and capabilities of each stakeholder in identifying, assessing and responding to said risks. **Investment** in **academic and other such studies** that **investigate the cascading effects of cyberattacks on coupled critical infrastructure** as well as **operational exercises** that actively demonstrate the **benefits of shared threat intelligence to interdependent sectors** can prove valuable in this regard.
- Strengthening the resilience of critical infrastructure assumes the prior existence of **skilled personnel** within the public and private sectors, from the policy level all the way through to the operational level, a challenge that States across the globe continue to struggle with. Dealing with this challenge and its cyber-related dimensions cannot be overcome solely by one-off or short-term capacity-building initiatives, as well-intentioned as they may be. It also requires heavy **public and private investment in more systemic long-term approaches to education**, including blended tertiary education programmes that can equip policymakers and leaders across the public and private sectors with the vision and expertise (social, technical, legal, economic, environmental, cultural) needed to navigate current and future CI-related risks and challenges.
- Governments and industry actors alike are finding that working with **civil society** to strengthen the resilience of critical infrastructure is equally important. For instance, beyond its traditional **oversight and advocacy** roles, civil society can support both public and private CI actors in **crisis management**, from the pre-crisis phase through to the recovery phase, especially where awareness-raising, communications, incident-tracing and information-sharing are concerned. Some of these efforts have led to the publication of useful compendiums on how to protect certain sectors from cyber harms.[4] **Ethical hackers and security researchers** are also key to building resilience. They can help to identify gaps and vulnerabilities and bring them to the attention of the right people in a timely manner. In several jurisdictions efforts are being made to ensure appropriate guarantees and protections for their activity.

4 See "Compendium of Multistakeholder Perspectives: Protecting the Healthcare Sector from Cyber Harm", https://www.mzv.cz/jnp/en/issues_and_press/press_releases/the_ministry_of_foreign_affairs_together.html

INTERNATIONAL COOPERATION AND UNITED NATIONS PROCESSES

- **International cooperation** is critical to the strengthening of critical infrastructure, be it national or transnational in character. Again, the framework of responsible behaviour for States in their use of ICTs lays out a series of assessments and recommendations that can significantly contribute to this objective. Beyond existing obligations under international law, three of the eleven non-binding political norms specifically cover critical infrastructure, including restraint measures and positive duties that can help to protect critical infrastructure from malicious ICT activity involving States.[5] These complement earlier General Assembly resolutions on CI protection that remain relevant today.

- Several, if not all, of the **confidence- and capacity-building measures** recommended at the United Nations over the years are essential to strengthening resilience of critical infrastructure, and for ensuring that all States, not just technologically advanced ones, have the **resources and capacities** required to **anticipate/identify, prepare for, respond to and recover from cyber incidents affecting critical infrastructure**. While much progress has been made in putting in place the relevant policies, strategies and action plans, implementation continues to fall short, including in terms of **funding arrangements for CI-related projects in developing countries**. Most countries continue to struggle with the most basic aspects of critical infrastructure protection. In developing countries, the impact can be significant, including in terms of the ability to **fully recover** from a serious ICT incident.

- The **current Open-ended Working Group (OEWG)** on developments in the field of information and telecommunications in the context of international security 2021–2025 has, like previous groups, highlighted concerns regarding malicious ICT activity affecting critical infrastructure and critical information infrastructure and will continue discussing appropriate responses to said threats within its mandated areas of focus, notably international law, norms, confidence-building measures and capacity-building. There are growing **expectations** that the Group will invite **relevant stakeholders** from industry, academia and civil society to **inform its discussions**. Finally, it is hoped that this report from UNIDIR's 2022 Cyber Stability Conference can constructively contribute to future substantive sessions of the OEWG, and to other ongoing efforts to build the resilience of critical infrastructure and to better protect it and the essential services it provides to societies across the globe.

5 See General Assembly, "Report of the Group of Governmental Experts", UN document A/70/174, 22 July 2015, para. 13(f–g); the 2021 GGE report (A/76/135, 14 July 2021) and OEWG report (A/AC.290/2021/CRP.2, 10 March 2021), as well as the current OEWG, build upon these norms.

3. SUMMARY OF DISCUSSIONS

▲ Mr. Doug Greene, Director of the Division of Information Systems and Telecommunications, UNHCR at Scene-setting Panel: Cybersecurity and Critical Infrastructure moderated by UNIDIR Director Dr. Robin Geiss.

3.1 CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION AT THE UNITED NATIONS

In the first and last panels of the Conference, discussions focused on how critical infrastructure has figured in the consecutive GGE and OEWG reports and how these efforts can be brought forward in the current OEWG. The work of these groups—both past and present—has focused on existing and emerging threats, international law, norms of responsible State behaviour, confidence-building measures and capacity-building, all of which include elements relevant to CI protection. Determining which infrastructures, sectors, functions or services should be designated as critical is a national prerogative and is an essential first step that States take to protect a nation's assets. In some countries, critical sectors or services are outlined in national policy or legislation. Both the GGE and OEWG reports provide examples of which infrastructures might be deemed critical or important. They can include infrastructure such as health, energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes. Designating certain infrastructures or sectors as critical and allocating resources is important, especially for those sectors/institutions that do not necessarily have the requisite resources to ensure adequate protection. In this regard, the process is generally accompanied with decisions on relevant institutional arrangements, guidelines or regulatory requirements (e.g., regarding incident notification, information-sharing and incident response and recovery), and the allocation of adequate resources.

Critical infrastructure can also refer to infrastructures that provide services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet and which may be critical to international trade, financial markets, global transport, communications, health or humanitarian action.[6] The latter often collect and store highly sensitive data and provide essential services to at-risk populations across multiple jurisdictions, thus meriting prioritization and assignation of appropriate resources by relevant authorities or Member States, as required.

Undoubtedly, States have ultimate responsibility for national security and for ensuring that national policies and strategies are developed, and adequate resources are allocated to ensure the security and resilience of infrastructure that has been designated as critical or essential. At the same time, the effectiveness of such national efforts is highly dependent on collaboration within and across sectors and between public and private actors. This collaborative aspect is addressed in consecutive GGE reports (2010, 2013, 2015, and 2021), the OEWG report (2021) and in the current OEWG.[7] Many national cyber security laws or strategies include provisions for public–private collaboration around critical infrastructure protection.

Engaging key stakeholders, particularly infrastructure owners and operators, to inform and implement CI-related decisions is essential since governments and the public purse alone are not sufficient to build resilience. In some countries CI is entirely owned and operated by private companies. In others it is publicly owned or operated. In yet others it is a mix of these. These factors, alongside the political culture of a country, generally determine the type of engagement between public and private actors, including how best to work together to anticipate/identify, prepare for, respond to and recover from cyber incidents affecting critical infrastructure, and cover related costs.

6 See General Assembly "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", UN Document A/76/135, 14 July 2021, Paragraph 45

7 For further information please see: https://www.un.org/disarmament/ict-security

▲ Ms. Moliehi Makumane, Researcher, UNIDIR moderated Panel on Curing the world: Health and Healthcare with Ms. Francesca Bosco, Chief of Strategy at Cyber Peace Institute and Mr. Flavio Aggio, Chief Information Security Officer, WHO.

3.2 THE HUMANITARIAN AND HEALTH SECTORS

Speakers discussed the main characteristics of attacks affecting humanitarian and health organizations, the critical services they deliver, and the harms that disruption of these services have caused for peoples across the world. There has been a significant increase in the number of threats affecting humanitarian organizations over the past few years, including the infrastructure and services upon which highly vulnerable populations are reliant. Where healthcare is concerned, the COVID-19 pandemic has served as an accelerator of malicious activity, ransomware attacks in particular, involving both State and non-State actors targeting public and private hospitals, research institutes, laboratories and a range of other entities across the globe responsible for delivering health services or hosting patient data.

The cascading effects of some of these attacks have been significant (e.g., disruption of vaccine development), including with regard to the harms posed to ordinary citizens, the impact on the public purse and on private businesses. In addition, the recovery costs of the attacks combined with new investments in cyber security and broader resilience efforts has diverted funding away from research at a moment when significant investment in research was most needed.

Speakers discussed how their respective organizations are responding to threats affecting their sectors since the onset of the pandemic. The COVID-19 pandemic as well as the uptick in ransomware attacks has accelerated these different efforts. For instance, where incident identification and classification are concerned, the World Health Organization

(WHO) is collaborating more closely with Member States, the private sector (including cyber security and technology companies), and with academia and specialized non-governmental organizations on incident mapping and response as part of broader efforts to build resilience.[8] Organizations such as the WHO manage huge amounts of sensitive data, which logically implies direct and indirect risks, some of which became painfully evident during the pandemic. Through the adoption and implementation of data management strategies and plans of action, global health and humanitarian organizations are also ensuring greater attention to data protection and privacy.

Integrating cyber security and resilience into senior management structures is enabling this progress, as is a stronger focus on cyber hygiene across relevant organizations, regular cyber security assessments and regular data protection impact assessments, some of which are conducted jointly with private companies. More systematized approaches to information-sharing across the health and humanitarian ecosystems are also proving valuable to the organizations' cyber defence posture.

In addition, some non-governmental organizations have fixed their sights on creating new tools to provide information on the harms that cyber incidents in these ecosystems pose to citizens and vulnerable populations. In this regard, new cyber incident tracing tools are being made publicly available. These provide additional insights into how the threat landscape is evolving and complement existing tools or methodologies that government entities, international organizations, infrastructure operators and private cyber security companies already use. One of these, the Cyber Incident Tracer, developed since the onset of the pandemic, collects data on the tools, techniques and procedures used by attackers and, where possible, on the civilian impacts of such incidents, including when healthcare- or humanitarian-related data is compromised or delivery of relevant services is disrupted or delayed.

Speakers also discussed innovative models of public–private cooperation within the health and humanitarian ecosystems or between these and other sectors, stressing the importance of transparency when networks and systems are breached, the willingness to take tough decisions about the products they use (including with regard to dealing with legacy products), and working together to shape policy and practice. With regard to the latter, for instance, a recent collaboration between the Czech Republic, Microsoft and the Cyber Peace Institute has provided insights into multilateral perspectives in protecting the healthcare sector from cyber harm.[9]

Speakers representing both public and private sectors also spoke of the need to invest more in risk-based approaches to cyber security and resilience, including for managing cross-sectoral dependencies. While capacity-building efforts continue to mature, the need for more structural, long-term approaches to cyber security education and workforce up-scaling requires urgent attention.

8 For instance, the WHO has conducted an extensive mapping of incidents targeting hospitals.
9 See note 3 above.

▲ Discussion during Panel II – Growing the world: International Trade and Finance, with Mr Justin McCall, Head of Demand Generation and Partnerships, Hewlett Packard Enterprise, moderated by Dr. Andraz Kastelic, Researcher, UNIDIR.

3.3 THE FINANCIAL SERVICES SECTOR

Speakers discussed the evolution of cyber-related threats affecting financial services and trade, with very specific emphasis on the former. For evident reasons, the financial services sector is one of the most targeted sectors and threats continue to evolve in tandem with technological developments which are driving changes within the sector, if not fragmentation. In addition to risks emerging around growing cross-sector dependencies (financial/ICT in particular) and challenges in constantly updating risk management models that capture these trends, speakers highlighted vulnerabilities in new payment systems (mobile money), attacks against crypto-currency exchanges as well as supply chain and third-party attacks as issues of particular concern.

Levels of cybersecurity maturity and resilience across the sector are shifting in a positive direction. For one, traditional banks have been forced to reconsider their security models to ensure that the highest levels of management understand that greater resilience—anticipating risk, preparing for and adapting to shifting conditions, recovering from incidents when they occur, learning and continuously evolving—is a multi-layered responsibility requiring adequate skills and resource allocation. Yet, efforts to strengthen resilience of the financial services sector differ significantly across countries and regions, for reasons ranging from the growing fragmentation of public and private initiatives, acute differences in policy and regulatory maturity across countries, to available resources and capacities.

▲ Discussion during Panel II – Growing the world: International Trade and Finance, with Mr Justin McCall, Head of Demand Generation and Partnerships, Hewlett Packard Enterprise, moderated by Dr. Andraz Kastelic, Researcher, UNIDIR.

Significant investments are being made in new approaches to modelling risk in the financial services sector in some countries. The lessons from these experiences could be valuable to other sectors. Finding ways to map risk in a smart and nimble manner is becoming a new priority. More comprehensive approaches to risk mapping are also needed to capture cross-sector interdependencies and vulnerabilities and to better align incentives across public and private sectors. For instance, there are growing interdependencies between the banking and ICT/digital sectors. This also comes with vulnerabilities for which joint risk management, including clarity on roles and responsibilities for building resilience, is required. Managing third-party risk, especially where vendors are concerned, is also a problem, and lax due diligence and auditing practices continue to spread risk across the sector.

▲ Panel III on Connecting the world: Information and Communication Technologies and Transport moderated by Dr. Samuele Dominioni, Researcher, UNIDIR, with Ms Jaya Baloo, Chief Information Security Officer at Avast.

3.4 INFORMATION AND COMMUNICATION TECHNOLOGIES AND TRANSPORT SECTORS

Speakers discussed the evolution of cyber-related threats and vulnerabilities across the ICT, telecoms and aviation sectors. Each sector is faced with the challenge that the number and character of threat actors is changing. The tailored services these actors provide is increasing every year, as is the speed at which these services are provided. These factors challenge the way risk is managed and are making it more difficult for traditional incident response efforts to keep pace.[10] Most organizations do not have the cyber maturity or capacity to keep up with the number of vulnerabilities that are being reported. Where criminal activity is concerned, law enforcement has struggled to keep pace with the growing professionalization of threat actors and the array of services they provide, demonstrated by the low volume of actors that have been apprehended and held accountable for their activity to date. Ransomware continues to be an issue of common concern.

More specifically, the ICT sector has seen an increase in the targeting of third-party vendors (hardware, software) or service (email, cloud etc.) providers. As recent incidents have amply demonstrated, when one such third party is breached, threat actors can gain access to hundreds if not thousands of customers. For the telecoms sector, participants noted that poor security practices of some hardware and software manufacturers, combined with weak vulnerability disclosure practices are also a problem. For instance, the absence of basic security protocols in key hardware components such as modems remains a challenge, despite the fact that the associated technical and regulatory risks are well known. Firewall and other security applications are being exploited at scale, sometimes by State actors, to generate botnets. The aviation industry, too, is reporting an increase in malicious activity. Most of this activity remains criminal in character, with financial gain (e.g., credit card data theft, ransomware) being the main objective.

10 For instance, the speed with which organizations have to patch vulnerabilities poses new risks since there is limited time to ascertain the effectiveness of each patch.

The telecoms and aviation sectors are highly regulated. In the former, regulation is centred around availability management, i.e., ensuring that networks are up and running, that the right frequencies are being used, and so forth. Telecommunications operators also must meet other requirements relevant to data protection and consumer protection. And since the telecommunications sector is generally designated as a critical sector, operators increasingly have to meet other more national security-oriented requirements. Within the sector itself, incident management, including sharing information with other operators in accordance with regulatory requirements, and regular cooperation among computer emergency response teams (CERTs) is critical, as is cooperation through organizations such as the Forum of Incident Response and Security Teams (FIRST).

In the aviation sector, civil aviation authorities set safety and mitigation measures based on regulatory requirements. There is a long tradition of collaboration between these authorities and the International Civil Aviation Organization (ICAO) and the broad range of industry associations (e.g., IATA, ACI, IFATCA) where the sharing of best practices, information and threat intelligence (via the aviation ISAC) is concerned. Risk management is a continuous concern of this sector which is global and highly diverse in terms of the industries and organizations constituting it, all of which have varying levels of cyber maturity. Expenditure in cyber security across the aviation sector has increased and the sector appears to be following a trajectory similar to that of the financial services sector in terms of maturity and layered responsibilities. The sector is currently working to integrate cyber security provisions not only into the maintenance and repair of current-generation aircraft and spare parts, but also into the manufacturing, on-boarding and management of next-generation air traffic systems which will be completely digitalized. As with other sectors, ensuring the security of Operational Technology (OT) systems[11] will be key, requiring tight collaboration with manufacturers and engineers from the outset. Another critical focus of the sector at present is aligning cyber security maturity across the highly complex aviation supply chain.

The ICT sector is the least regulated, although in some jurisdictions this is beginning to change. For evident reasons there is increasing emphasis on responsibility and liability of manufacturers across supply chains and not just the end users as has tended to be the case. Acknowledging that it will be increasingly difficult to avoid regulation, many companies are engaging with regulators and standard-setting bodies in ongoing efforts to increase security and resilience of ICT products and services. The sector continues to expend significant energy on raising awareness and building capacity around basic cybersecurity practices such as using an anti-virus application, regularly updating software and implementing multi-factor authentication. For some organizations or businesses, moving their networks and systems to the cloud brings certain security advantages, as long as the cloud host itself can guarantee security.

For each sector, intra-and cross-sectoral collaboration as well as public–private cooperation (around policy, regulation, standards, risk management, information-sharing) and the engagement of academia and civil society in these efforts are critical to dealing with challenges in both ICT and transport sectors.

11 Operational technology (OT) is the use of hardware and software to monitor and control physical processes, devices, and infrastructure. IT and OT are often confused, but the main difference is that IT controls data and data flows, OT controls physical equipment.

▲ Discussion on Panel IV on Sustaining the world: Energy & Water with Ms. Ayhan Gucuyener, Kadir Has University and Ms. Chris Kubecka, Founder and Chief Executive Officer of Hypasec.

3.5 ENERGY AND WATER SECTORS

The energy and water management sectors are facing manifold threats, with the energy sector one of the most targeted. Like other sectors, these threats and associated risks continue to evolve and are becoming more complex.

Where energy is concerned, transnational pipelines are dispersed nationally, regionally and internationally and represent not just the backbone of other sectors, but also a huge part of national GDP. Current policy trajectories which are accelerating the uptake of new technologies into energy sectors are posing new challenges. Yet, while the introduction of new technologies or new software into established infrastructures can provide new opportunities for efficiencies and help to ensure redundancy, it can also create new risks when technology developers they fail to consider security in the conception and design of their products. For instance, a study conducted by one of the speakers demonstrated that all the wind turbines in a given country were highly vulnerable to remote access because of weaknesses on the manufacturing front. Security is a vitally important element of decisions to roll out renewable energy technologies because they interconnect with legacy energy systems meaning that certain points of connection can be exploited for malicious spurposes. Another concern is the fact that renewable/clean energy technologies are also being attacked for industrial espionage purposes.

In some regions or subregions, States have made the protection of water infrastructure and supplies a strategic priority, since disruption of supplies, including through ICT/cyber means, could be catastrophic. In most countries, the water sector is highly regulated, and risk and resilience assessments are key requirements; yet, these need to be able to adapt to new risks. For instance, in some regions ensuring redundancy in the water sector is becoming increasingly difficult due to the effects of climate change and overlapping

▲ Dr. Giacomo Persi Paoli, Head of Security and Technology Programme at UNIDIR moderating Panel IV on Sustaining the World: Energy & Water.

energy supply challenges.[12] In response, some water and wastewater facilities are incorporating renewable electricity sources into their systems to ensure redundancy in the event that regular supplies are disrupted.

Energy and water infrastructure owners and operators have made increasing investments in cyber security over the past decade. These investments contribute to broader energy security goals such as availability, accessibility, acceptability and affordability of energy resources. Speakers discussed the challenges of managing dependencies across the energy, water and other sectors. Despite acknowledgement of the potential cascading effects of cyber-related incidents, there is still limited cooperation among the sectors where cyber security is concerned, and in many countries governments have yet to allocate adequate budgets to strengthen public–private collaboration and to support industry and other relevant actors take on additional responsibilities. It is evident that more needs to be done to distribute costs and to ensure more burden-sharing.

In both the energy and water sectors, public–private collaboration is improving. These tend to be issue-specific forms of collaboration and are highly contextualized. For instance, according to one speaker, cybersecurity collaboration between operators of transnational pipeline, water and waste-water infrastructures in certain regions have seen positive improvements, reflecting a greater awareness of the threats and associated dependencies by national governments and related operators and owners across the region. National water sectors are also benefitting from greater collaboration as well as helping to inform and to operationalize government-led initiatives such as making available emergency numbers for sharing information on suspicious cyber-related activity relevant to the sector at national

12 Sometimes greater focus might be placed on water infrastructure protection in some regions or subregions because of climate change effects such as desalinisation

and subnational levels. Importantly, in some jurisdictions progress is being made with regard to the identification and disclosure of vulnerabilities affecting these sectors, with several States now providing legal protections for ethical hackers who share information on vulnerabilities with relevant infrastructure operators or a national computer emergency response team (CERT).

Not every State or region has the resources to move in this direction. Many are being left behind, pointing at the need to look at infrastructure, technology and associated challenges from a systemic perspective to ensure that critical goals such as the SDGs can be met. In addition, greater attention will need to be paid to emerging issues relevant to clean energy and related technologies so that advances made thus far in securing and protecting energy and water infrastructure and services are not undermined by poor security practices, but are rather underpinned by common security standards from design all the way through to implementation and deployment.

4. ANNEX 1: AGENDA

The full conference programme, including panel descriptions and speakers' biographies can be accessed on the event page: https://unidir.org/events/2022-cyber-stability-conference-protecting-critical-infrastructure-and-services-across

09:15-09:20: Conference opening – Welcome remarks by Dr. Robin Geiss, Director, UNIDIR

09:20-10:20: Scene-setting Panel: Cybersecurity and Critical Infrastructure
(Moderated by Dr. Robin Geiss, Director, UNIDIR)

- *H.E. Mr. Guilherme Patriotas* – Consul-General of Brazil and Former Chair of the GGE 2019–2021
- *Mr. Doug Greene* – Director of the Division of Information Systems and Telecommunications, UNHCR
- *Ms. Latha Reddy* – Former Co-Chair, Global Commission on the Stability of Cyberspace

---

10:25-11:30: **Panel I – Curing the world: Health and Healthcare**
(Moderated by Ms. Moliehi Makumane, Researcher, UNIDIR)

- *Mr. Brian Cincera* – Chief Information Security Officer, Pfizer
- *Ms. Francesca Bosco* – Chief of Strategy, Cyber Peace Institute
- *Mr. Flavio Aggio* – Chief Information Security Officer, WHO

11:45-13:00: Panel II – Growing the world: International Trade and Finance
(Moderated by Dr. Andraz Kastelic, Researcher, UNIDIR)

- *Mr. Arthur Nelson* – Deputy Director of the Technology and International Affairs Program, Carnegie Endowment for International Peace
- *Mr. Justin McCall* – Head of Demand Generation and Partnerships, Hewlett Packard Enterprise
- *Ms. Maria Ceccarelli* – Chief, Trade Facilitation Section, Economic Cooperation and Trade Division, UNECE
- *Ms. Susan Potgieter* – Head of Strategic Services, South African Banking Risk Information Centre

---

14:00-15:10: Panel III - Connecting the world: Information and Communication Technologies and Transport *(Moderated by Dr. Samuele Dominioni, Researcher, UNIDIR)*

- *Ms. Jaya Baloo* – Chief Information Security Officer, Avast
- *Mr. Kevin Reifsteck* – Director for Critical Infrastructure Protection, Microsoft
- *Mr. Pascal Buchner* – Director ITS and Chief Information Officer, IATA

15:15-16:25: Panel IV – Sustaining the world: Energy & Water
(Moderated by Dr. Giacomo Persi Paoli, Head of Programme, UNIDIR)

- *Ms. Ayhan Gucuyener* – Project Specialist at Kadir Has University Cybersecurity and Critical Infrastructure Protection, Khas University
- *Ms. Chris Kubecka* – Founder and Chief Executive Officer, Hypasec
- *Dr. David Mussington* – Executive Assistant Director For Infrastructure Security, Cybersecurity and Infrastructure Security Agency

---

16:40-17:45: Concluding session – Critical Infrastructure Protection in the context of International Cyber Security
(moderated by Dr. Ceciles Aptel, Deputy-Director, UNIDIR)

- Opening Remarks by *H.E. Ambassador Burhan Gafoor*, Permanent Representative of the Republic of Singapore to the United Nations, Chair of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021–2025
- Rapporteur Recap of the Day with *Dr. Camino Kavanagh*, Visiting Senior Fellow, King's College London; Non-resident Scholar, Carnegie Endowment for International Peace
- *H.E. Mr. Jürg Lauber* – Permanent Representative of Switzerland to the United Nations and other International Organizations, and former Chair of the OEWG 2019-2021
- *Ms. Marina Kaljurand* – Member of the European Parliament
- *Mr. Vladimir Radunovic* – Director, E-diplomacy and Cybersecurity, DiploFoundation
- *Ms. Beyza Unal* – Head of the Science and Technology Unit, UNODA

17:45-18:00: Conference closing

2022 Conference Report

CYBER STABILITY CONFERENCE

PROTECTING CRITICAL INFRASTRUCTURE AND SERVICES ACROSS SECTORS

This report provides a short summary of the 2022 edition of UNIDIR's Cyber Stability Conference (CS2022) held in Geneva on 5 July 2022. The event focused on discussing the protection of critical infrastructure and critical information infrastructure supporting essential services to the public. The conference convened representatives from international organizations, industry, governments, and civil society to reflect on how to further progress in multilateral discussions and support more efficient policy interventions by national governments for critical infrastructure protection.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH