UNIDIR

Accelerating ICT Security Capacity-Building

Take Aways from the Global Roundtable on ICT Security Capacity-Building

GIACOMO PERSI PAOLI · SAMUELE DOMINIONI · AAMNA RAFIQ · LENKA FILIPOVÁ

Acknowledgments

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This study is part of UNIDIR's Security and Technology Programme cyber workstream, which is funded by the Governments of Australia, Canada, Czechia, France, Germany, Italy, the Netherlands, Norway, Switzerland and by 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.

Authors

This report was produced by the UNIDIR Security and Technology Programme.

Giacomo Persi Paoli

Head, Security and Technology

Dr. Giacomo Persi Paoli is the Head of the Security and Technology Programme at UNIDIR. His expertise spans the science and technology domain with emphasis on the implications of emerging technologies for security and defence. Before joining UNIDIR, Giacomo was Associate Director at RAND Europe where he led the defence and security science, technology and innovation portfolio as well as RAND's Centre for Futures and Foresight Studies. He holds a PhD in Economics from the University of Rome, Italy, and a Master's degree in political science from the University of Pisa, Italy.

Samuele Dominioni

Researcher, Security and Technology Programme

Dr. Samuele Dominioni is a researcher in the Security and Technology Programme at UNIDIR. Before joining UNIDIR, he held research positions in both academic and think tank settings. He holds a PhD in international relations and political history from Sciences Po, France, and the IMT School for Advanced Studies, Italy.

Aamna Rafiq

Researcher, Security and Technology Programme

Aamna Rafiq is a Researcher (Cyber) within the Security and Technology Programme at UNIDIR. She has expertise in securitization of cyberthreats at national, regional and international levels. She is also interested in the military applications of emerging technologies specially ICTs and their integration into warfare strategies and doctrines.

Lenka Filipová

Coordinator, Security and Technology Programme

Lenka is a Coordinator with the Security & Technology Programme at UNIDIR. Prior to this role, Lenka held various positions in different international organizations and government.

Contents

“

Excellencies, ladies and gentlemen,

Peace and security in the physical world demand new approaches to peace and security in the digital world. Your Roundtable highlights this vital link.

Unlocking the benefits of digital technology means closing the digital divide, and ensuring its many benefits are shared by all people. But closing the digital divide also means closing the glaring gaps in the security of information and communication technology.

Such gaps place countries and, most importantly, people at risk. More than ever, global security depends on the security of digital technology.

We need to ensure that States fully implement the agreed norms of responsible behaviour in their use of digital technology. This is the only way to protect not only people, but the infrastructure they depend on. And we need to support developing countries to increase their digital security capacity.

Digital security is a critical part of the New Agenda for Peace.

We need strong frameworks for collaboration on threats to global peace and security, in line with international law, human rights, and the UN Charter. This Roundtable is a key opportunity for countries to share their ideas, experiences, and commitment to this vital issue.

Thank you all for being part of this essential work.

”

Secretary-General’s video message to the Global Roundtable on Information and Communications Technologies Security Capacity-Building, 10 May 2024

1. The Road to the Global Roundtable on ICT Security Capacity-Building

The Global Roundtable on ICT Security Capacity-Building held in New York on 10 May 2024 was the first event organized under United Nations auspices fully dedicated to this important issue. It was organized by the Chair of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 (OEWG) as requested by Member States in the second Annual Progress Report of the OEWG.[1]

While this event was the first of its kind, capacity-building in the field of information and communication technology (ICT) has been on the multilateral agenda pertaining to international peace and security in the ICT domain for more than a decade. The consensus report of the 2010 Group of Governmental Experts on advancing responsible State behavior in cyberspace noted that "Capacity-building is of vital importance to achieve success in ensuring global ICT security, to assist developing countries in their efforts to enhance the security of their critical national information infrastructure, and to bridge the current divide in ICT security".[2] Since then, capacity-building has been progressively recognized as a key enabler underpinning the implementation of, and adherence to, the Framework for responsible State behaviour in cyberspace, including voluntary norms, principles and rules, international law and confidence-building measures.

With the consensus report of 2019–2021 Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, Member States achieved an important milestone by agreeing on a set guiding principles for ICT capacity-building in relation to process and purpose, partnerships and people (see Box 1).[3]

---

[1] Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/78/265, para. 48, 1 August 2023, https://documents.un.org/symbol-explorer?s=A/78/265&i=A/78/265_8759712.

[2] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201, para. 17, 30 July 2010, https://documents.un.org/symbol-explorer?s=A/65/201&i=A/65/201_5194277.

[3] Final Substantive Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, A/AC.290/2021/CRP.2, para. 56, 10 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

BOX 1.

Principles for capacity-building in relation to State use of ICTs in the context of international security

Source: Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report, para. 56

Process and Purpose

- Capacity-building should be a sustainable process, comprising specific activities by and for different actors.
- Specific activities should have a clear purpose and be results focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.
- Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.
- Capacity-building should be undertaken with full respect for the principle of State sovereignty.
- Access to relevant technologies may need to be facilitated.

Partnerships

- Capacity-building should be based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership. Partners in capacity-building participate voluntarily.
- As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.
- The confidentiality of national policies and plans should be protected and respected by all partners.

People

- Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.
- The confidentiality of sensitive information should be ensured.

The ongoing 2021–2025 OEWG has put an even stronger emphasis on capacity-building, adopting a total of 12 recommendations in its first[4] and second[5] Annual Progress Reports, with responsibilities divided among Member States, the Chair of the OEWG, and the United Nations Secretariat (see Box 2).

BOX 2.

Summary of recommended next steps on capacity-building produced by the 2021–2025 OEWG

Source: Open-ended Working Group on security of and in the use of information and communications technologies, First Annual Progress Report, para. 17, August 2022

In the first Annual Progress Report, States were encouraged to:

- Continue exchanging views at the OEWG on capacity-building on security in the use of ICT.
- Engage in focused discussions on a number of issues including funding specifically for capacity-building efforts, better coordination and integration of existing initiatives, best practices and lessons learned and gender dimensions of ICT security.
- Survey their capacity needs including through the National Survey of Implementation or other tools.
- Continue to support capacity-building programmes, including in collaboration, where appropriate, with regional and subregional organizations and other interested stakeholders, including businesses, non-governmental organizations and academia.

Source: Open-ended Working Group on security of and in the use of information and communications technologies, Second Annual Progress Report, paras. 44–51, August 2023

In the second Annual Progress Report, States were encouraged to:

- Continue exchanging views at the OEWG on capacity-building related to security in the use of ICT, and continue focused discussions on how the principles of capacity-building as adopted in the 2021 OEWG report can be further mainstreamed within capacity-building initiatives on security in the use of ICT.
- Continue to discuss the proposal for a Global Cyber Security Cooperation Portal as a 'one-stop shop' tool for States, developed under the auspices of the United Nations and in synergy with existing portals as appropriate.

---

[4] Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/77/275, 8 August 2022, https://documents.un.org/symbol-explorer?s=A/77/275&i=A/77/275_0643976.

[5] Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/78/265, 1 August 2023, https://documents.un.org/symbol-explorer?s=A/78/265&i=A/78/265_8759712.

- Support the United Nations Secretariat in updating the Cyber Diplomacy e-learning course for diplomats.
- Develop and share voluntary checklists and other tools to assist States in mainstreaming the capacity-building principles from the 2021 OEWG report into capacity-building initiatives related to ICT security, as well as to develop and share tools that would assist States in incorporating a gender perspective into such capacity-building efforts.
- Continue to support capacity-building programmes, including in collaboration, where appropriate, with regional and subregional organizations and other interested stakeholders, including businesses, non-governmental organizations and academia.

The OEWG Chair was requested to:

- Engage with relevant United Nations entities and international organizations offering capacity-building programmes on security in the use of ICT and encourage them to align their capacity-building programmes, where relevant and appropriate and in accordance with their respective mandates, to further support States in their implementation of the framework for responsible State behaviour in the use of ICT and efforts to build an open, secure, stable, accessible and peaceful ICT environment.
- Convene a dedicated Global Roundtable meeting on ICT security capacity-building during the intersessional period to allow for an exchange of information and best practices.

The United Nations Secretariat was requested to:

- Conduct a 'mapping exercise', in consultation with relevant entities, in order to survey the landscape of capacity-building programmes and initiatives within and outside of the United Nations and at the global and regional levels, including by seeking the views of Member States.
- Update the Cyber Diplomacy e-learning course for diplomats, with the aim of producing an updated course in 2024.

2. Format and Structure of the Roundtable

The Global Roundtable on ICT Security Capacity-Building was organized in the format of an in-person, high-level meeting to provide an action-oriented platform for Member States and the stakeholder communities. It brought together more than 100 delegations, of which 53 took the floor,[6] and 56 stakeholders. It was organized as a full-day event alternating plenary sessions and breakout groups with a dedicated 'matchmaking' session for ICT security capacity-building providers and implementers to offer an overview of their work.[7]

The plenary session offered a platform for Member States to share their views, experiences and good practices related to ICT security capacity-building. The breakout groups provided an opportunity for more in-depth discussions on concrete and action-oriented measures that States, international organizations and stakeholders should take to improve capacity-building measures.

The following sections in this report provide a high-level summary of the key themes that emerged from the event. The report is not meant to be an exhaustive recount of all individual interventions, for which we invite readers to consult the event recordings[8] and the repository of statements.[9]

3. Highlights from the Plenary Session and Signature Panel

After the opening remarks by Ambassador Burhan Gafoor, Permanent Representative of Singapore to the United Nations and Chair of the OEWG, and a video message from Secretary-General of the United Nations António Guterres, the Global Roundtable continued with high-level statements from distinguished speakers that shared perspectives on the importance of ICT security and related capacity-building efforts. Interventions were made by:

- Ambassador Collen Kelapile, Chef de Cabinet, who delivered remarks on behalf of

---

[6] 52 national delegations, plus the European Union. See Appendix A.

[7] See Appendix B for the list of organizations that took the floor during the matchmaking session.

[8] Please note that the recordings of the event are accessible via UN Web TV at the following links—Part 1: https://webtv.un.org/en/asset/k18/k18of23xwc ; Part 2: https://webtv.un.org/en/asset/k10/k100ujzq24.

[9] All statements delivered during the plenary sessions of the Global Roundtable can accessed at the following link: https://meetings.unoda.org/meeting/57871/statements?f%5B0%5D=segment_statements_%3A2024%20inter-sessional.

the President of the General Assembly, Mr. Dennis Francis;[10]

- Ms. Doreen Bogdan-Martin, Secretary-General, International Telecommunication Union;[11]
- Mr. Achim Steiner, Administrator, United Nations Development Programme;[12] and
- Ms. Josephine Teo, Minister for Communications and Information, Singapore.[13]

Following this high-level opening segment, the Global Roundtable continue with a Signature Panel titled "Building Cyber Resilience for Sustainable Development by Bridging the Global Capacity Gap". During this session, moderated by UNIDIR Director Dr. Robin Geiss (morning session) and Ambassador Burhan Gafoor (afternoon session), national delegations were invited to share their views on barriers faced at the national level in building the ICT security capacities, avenues to overcome or mitigate such barriers and lessons learned in capacity-building to be shared and applied internationally.

Two key messages emerged from the day, both equally supported by hard evidence: a message of urgency and a message of hope.

The sense of urgency is the product of several worrying trends, both quantitative and qualitative. If on one side the recognition of the importance of digital transformation for the achievement of the Sustainable Development Goals is undisputed, on the other **many critical vulnerabilities persist at the global level:**

1. Cyber insecurity now figures among the top 10 most severe global risks over the short and long term, according to the World Economic Forum's 2024 Global Risks Report and in 2024 alone the projected cost of cybercrime to the global economy is over 9 trillion US dollars.
2. The ICT domain is playing an increasingly relevant role in the context of armed conflicts, posing new challenges to civilians and critical infrastructure.
3. The threat landscape is continuously evolving: as digital transformation and connectivity increase for the great benefit of societies, so does the attack surface that malicious actors can exploit; technological advancements, including but not limited to artificial intelligence, are increasing the sophistication, scale and speed of traditional cyberattacks (e.g. ransomware) and have the potential to unlock new attack vectors, posing significant risks to national security, organizational integrity and the global economy.
4. There is a global shortage of nearly 3.5 million ICT professionals and a significant gender gap with only 25% of ICT

---

[10] Link to statement: https://www.un.org/pga/78/2024/05/10/pga-remarks-at-the-global-roundtable-on-ict-security-capacity-building-as-delivered-by-chef-de-cabinet-ambassador-collen-kelapile/.

[11] Link to statement: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/10052024_Global_Roundtable_on_ICT_Security_Capacity_Building_OEWG_ITU_SG_FINAL.pdf .

[12] Link to statement: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/240510_Remarks_by_UNDP_Administrator-_Global_Roundtable_on_ICT_Security_Capacity_FINAL.pdf.

[13] Link to statement: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Opening_Remarks_by_Minister_Josephine_Teo_at_UN_Roundtable_on_ICT_Security_Capacity_Building__10_May_.pdf.

professionals being women. Beyond the community of ICT professionals, there is a persistent issue related to the lack of digital literacy, including awareness of cyber threats and basic principles of cyber hygiene at the individual and organizational level.

5. Despite the general acknowledgement of the growing importance of ICT security as a global issue and as a key enabler for economic and social development, digital divide continues to be a significant barrier for many developing countries and 60% of the least developed countries currently lack a national cybersecurity strategy.

However, **the Global Roundtable also delivered a clear message of hope** based on (a) the consensus on the gravity of the problem and the need to act, (b) the strong evidence presented to illustrate the scale and scope of current and past initiatives related to ICT security capacity-building, and (c) the general commitment to do more and work cooperatively, within and outside the United Nations, to address ICT security capacity gaps.

Two key areas of intervention were frequently mentioned. The first is **education and upskilling** with a view to creating a workforce that possesses the range of skills required to effectively mitigate the risks pertaining to ICT security domestically and internationally, including the technical, legal and diplomatic. Several examples of initiatives conducted at the national, bilateral, regional or global level were described by speakers.

The second area of intervention is the provision of **technical/specialized assistance and organizational/institutional support**, including but not limited to incident response. The combination of training, organizational support, technical expertise and—where relevant and feasible—technology transfer, emerged as a key component to **enhance national, regional and global cyber resilience** in the face of rapidly evolving ICT threats.

Beyond the 'what' of ICT capacity-building, the global roundtable also offered **important insights into the 'how' and the 'who'.** In relation to the 'how', the **importance of the capacity-building principles** agreed under United Nations auspices (see Box 1 above) was reiterated, with particular emphasis on issues pertaining to **human rights and gender** as well as on characteristics such as **inclusivity, universality and non-discrimination**.

In relation to the 'who', interventions during the Global Roundtable recognized the importance of the United Nations, of Regional and other intergovernmental initiatives, and of the multi-stakeholder community.

States recognized the **important role played by all stakeholders**, including industry, the scientific and academic communities, and civil society and NGOs in informing, shaping and delivering capacity-building initiatives. Both donors and recipients of capacity-building programmes can benefit from the meaningful engagement of a wide range of stakeholders that can provide support across all stages of a programme life cycle, from design to delivery and evaluation.

Many interventions also recognized the **essential role played by many regional and subregional organizations** in the design and delivery of capacity-building initiatives that are contextualized, demand-driven and tailored to local needs and capacities. Regional organizations often act as the intermediary between donors, recipients and implementers, adding the knowledge of local context and needs to the subject matter expertise brought by project implementers.

Lastly, there was **large support for the role of the United Nations as fundamental player** in the area of ICT security capacity-building. In general terms, there was the recognition that the United Nations plays a vital role as a global platform for Member States to engage in productive discussion on ICT security, including capacity-building, and for its ability to convene the multi-stakeholder community.

More specifically, interventions highlighted **the pivotal role played by the current OEWG** in further advancing the multilateral agenda on ICT security, including on capacity-building, and **the need for these discussions to continue in an institutionalized, permanent and action-oriented mechanism under United Nations auspices** that will follow after the current OEWG concludes its mandate.

4. Highlights from the Breakout Groups

Following the opening plenary session and the briefings by the stakeholders, the Global Roundtable provided an opportunity for Member States to engage in more focused discussions through the participation in two breakout groups. In these sessions, discussions sought to unpack the five pillars of the foundational cyber capabilities identified in the UNIDIR report *Unpacking Cyber Capacity Needs: Part I – Mapping the Cyber Foundational Capabilities*: policies, processes, people and skills, partnerships, and technology.[14] The first group focused on strengthening governance policies and processes, in particular through the development of national cyber strategies and other regulatory instruments as well as through the creation or improvement of dedicated structures and process to enable the implementations of such governance instruments. The second group focused on developing talent, partnerships and technologies in particular through the development of operational and technical capacities, the growth of the talent pipeline and the establishment of new partnerships across relevant stakeholders. Both groups started with some framing remarks by a small group of panellists followed by a moderated discussion with the whole group. The list of panellists and guiding questions can be consulted in appendix C.

An important note on terminology was made at the start of the discussions to clarify how the terms capability and capacity relate to each other. As working definitions, **capability** refers to the **ability to perform a given task**, while **capacity** refers to the **ability to sustain and maintain** such capability over time. In the context of ICT security, both are important and required.

In relation to **national cybersecurity strategies**, there was agreement that such strategies are not only important, but an essential

[14] Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, UNIDIR, July 2023, https://unidir.org/publication/unpacking-cyber-capacity-building-needs-part-i-mapping-the-foundational-cyber-capabilities/.

prerequisite for any State interested in developing a safe and secure digital ecosystem. Without a national cyber strategy, States **may lack a structured response** to cyber threats, leading to disjointed and inefficient handling of cyber incidents.

National cybersecurity strategies serve as a clear declaration of a State's commitment to cybersecurity, helping to mobilize necessary funding and other resources, and ensuring the sustainability of cybersecurity initiatives beyond traditional political cycles. Additionally, strategies lay the groundwork for digital transformation—a critical factor for the social and economic development of any country.

Two important characteristics were highlighted in relation to strategies: they should be **progressive** and **continuously evolving**. The first point builds on the assumption that strategies can be broken down into three generations, each with a different priority and focus. The **first generation of strategies** primarily focuses on **raising awareness** about the significance of cybersecurity and putting in place **basic national-level policies, processes and structures**, marking the initial steps towards national cybersecurity readiness. As such, first generation strategies tend to be inward facing, prioritizing domestic interventions. **The second generation of strategies** builds on the first and adds the **cooperation element**, both internal with the clarification of roles and responsibilities of different national stakeholders (e.g. incident response teams, various ministries, private sector) as well as external, covering the issue of international cooperation. **The third generation** builds on the previous two to further advance the cybersecurity discourse by **recognizing the transverse nature of cybersecurity**, acknowledging that its impact extends across all sectors of society and government. Such holistic view supports a more **integrated and strategic approach** to cybersecurity.

This approach is useful in illustrating how States that have yet to develop their first cybersecurity strategy should not feel overwhelmed by the complexity of the issue: not everything has to be dealt with at once, but it is essential to take the first step.

This is supported also by the second characteristic of strategies: that they should be **continuously evolving**. This is particularly relevant given the rapid evolution of the technology and the associated threat landscape which requires a continuous reassessment of the national approach as showcased by a recurring trend in many States where the 'shelf-life' of national cybersecurity strategies has been progressively reduced from five years to only two or three years.

Developing, and regularly updating, **a national cybersecurity strategy** and other regulatory instruments is a **necessary but not sufficient condition** to enable a safe and secure digital ecosystem. Discussions in the breakout groups emphasized the critical importance of **the practical elements of implementation** and the need for a step-by-step approach to avoid setting expectations that are not aligned with resources, which can itself be a risk if not managed properly. Strategies alone are not sufficient if they are not designed with implementation in mind and matched with adequate resources. Thinking about implementation means thinking about the establishment of **structures and processes** to oversee such implementation, the development of **human, organizational and technical capacities** to implement such plans **in partnership** with a wide range of relevant governmental and **non-governmental stakeholders** as required. All of these elements are required to improve the prevention and mitigation of, and the response to, cyber incidents, ultimately increasing national cyber resilience.

Sustained **access to, and retention of, skills and talent remain a critical challenge** across the globe, particularly for governments that face strong competition from the private sector. As such, it is important for governments to both cultivate a talent pipeline in a new generation of civil servants and to offer upskilling and professional development opportunities to the current workforce. This could be achieved, for example, through cyber apprenticeship programmes, dedicated courses, and certifications. **Regional and subregional organizations already play an important role** in making such opportunities available to States that do not have the national resources to set up and sustain a national training programme.

Within the wider context of supporting sustainable development through digital transformation, participants agreed that **technical and organizational capacity together with partnerships are essential** for a wide range of purposes: from supporting operational capabilities related to incident response and cyber law enforcement, including the sharing of threat intelligence and preservation of digital evidence, to ensuring the cybersecurity of critical infrastructure and securing supply chains.

Finally, the breakout session highlighted the **critical importance of multi-stakeholder engagement** across all capability areas: from strategy development, to incident response, efficient and structured engagement with civil society organizations, the private sector, academia and—where relevant—regional organizations, such engagement was flagged as an essential component for enhancing national cyber resilience.

5. Addressing Barriers to ICT Capacity-Building

Over the course of the day, participants highlighted a number of barriers to building ICT security capacities and provided an overview of current practices aimed at mitigating, at least in part, such barriers. Table 1 below provides a summary of the main barriers identified matched with mitigation strategies that emerged from the interventions during the day, both in plenary and in the breakout sessions.

Beyond individual barriers and mitigation strategies, it is important to highlight how participants recognized **the critical role that the United Nations must play** both through the current OEWG and even more through the future action-oriented, permanent mechanism, in the area of ICT security capacity-building. In addition, the Global Roundtable also highlighted the **essential role played by regional organizations and national-led initiatives** which, by leveraging the wealth of **knowledge and expertise available across the multi-stakeholder community** have been able to achieve remarkable results in recent years.

TABLE 1.

Summary of Identified Barriers to ICT Security Capacity-Building and Possible Mitigation Strategies

BARRIERS	MITIGATION STRATEGIES FOR CONSIDERATION
Lack of political support at the national level due to limited awareness of the issue and/or competing policy priorities	• Identify and cultivate 'cyber champions' within political leadership who can advocate for the inclusion of ICT security on the political agenda and drive policy development. • Work with the multi-stakeholder community, particularly civil society and academia, to raise the overall level of awareness. • Work with the multi-stakeholder community, particularly with critical infrastructure owners/operators and providers of critical services, to create strong business cases illustrating the importance of ICT security for national security and economic prosperity.
Limited access to, or retention of, talent in the public sector	• Expand the talent pool through the creation of dedicated education programmes at all levels with a particular focus on addressing the significant gender disparity that currently affects the cyber workforce. • Implement upskilling and professional development programmes for the current workforce, leveraging regional and subregional organizations as necessary and appropriate. • Implement efficient public–private partnerships for the provision of specialized capabilities.
Lack of organizational structures and/or coordination amongst them	• Develop a national cybersecurity strategy and implementation plan that establish a clear distribution of roles and responsibilities across existing structures/entities and/or create new ones. • Leverage the expertise of the multi-stakeholder community to mitigate some of the inefficiencies as appropriate (e.g., to support better coordination). • Leverage regional and multilateral forums to exchange views on good practices.
Affordability of technical solutions	• Leverage international cooperation and assistance opportunities. • Implement efficient public–private partnerships for the provision of technology and/or services. • Leverage regional and subregional synergies for the harmonization of requirements and the design of shared solutions.
Limited alignment between needs and resources due to lack of awareness, lack of coordination and duplication of efforts	• Leverage regional and multilateral forums for exchanging information on needs and available resources. • Use existing (or create as required) digital tools, platforms and portals to increase situational awareness of current supply and demand of capacity-building programmes. • Leverage the United Nations, and in particular the future permanent mechanism, as a 'clearing house' for ICT security capacity-building to increase awareness and coordination among donors, recipients and implementers.

6. Conclusion

The first United Nations Global Roundtable on ICT security capacity-building offered a unique platform for Member States, intergovernmental organizations and representatives from the multi-stakeholder community to meet and exchange views on barriers and solutions to building a more resilient global ICT ecosystem where States, societies and people can thrive in a safe and secure digital environment.

While the roundtable highlighted **how much is already happening** thanks to national or regional programmes or multi-stakeholder initiatives such as the Accra Call for Cyber Resilient Development,[15] it also highlighted the **urgent need to do more,** including by **enhancing synergies** to advance the international community's work on **capacity-building in a coherent and sustainable way**. The roundtable also highlighted that in light of a continuously evolving threat landscape, **ICT security itself needs to evolve** and as a result capacity-building should be considered as a **continuous need** that will persist across generations and require **strategic partnerships and resource optimization** to ensure successful implementation. It is in this context that the **United Nations can reaffirm its centrality** by providing a platform that facilitates dialogue and exchange of good practices, and enhance coordination and coherence across different layers of intervention (national, regional and multilateral).

The **Global Roundtable gave a strong input to the work of the OEWG** both in relation to how the group can carry forward the ICT security capacity-building agenda in its mandate as well as how capacity-building will feature in the scope, structure, content and modalities of the future permanent mechanism, which the OEWG will determine.

While being its first iteration, the Global Roundtable on ICT security capacity-building represented an important step for the **international community's commitment to enhance cyber resilience at the global level.** In a year characterized by many multilateral initiatives outside of the First Committee of the General Assembly that will have an impact on the digital domain such as the Global Digital Compact[16] and the Pact for the Future,[17] the theme of ICT security capacity-building is likely to establish itself as a cross-cutting issue that is of critical importance for security and development alike. As such, Member States should leverage the OEWG to further advance this important issue and work together to address one of the greatest challenges of our times, and of the times to come.

---

[15] See https://gc3b.org/the-accra-call-for-cyber-resilient-development/.

[16] See https://www.un.org/techenvoy/global-digital-compact.

[17] See https://www.un.org/en/summit-of-the-future.

APPENDIX A.

List of Registered Speakers for the Signature Panel

States only, in alphabetical order

Albania	Ecuador	Latvia	Spain
Argentina	El Salvador	Malaysia	Sri Lanka
Belgium	European Union	Mexico	Sweden
Brazil	France	Morocco	Switzerland
Burkina Faso	Germany	Pakistan	Syrian Arab Republic
Cambodia	Guatemala	Paraguay	Thailand
Canada	India	Philippines	Ukraine
China	Indonesia	Poland	United Arab Emirates
Côte d'Ivoire	Ireland	Portugal	United Kingdom
Cuba	Islamic Republic of Iran	Qatar	United States
Czechia	Israel	Russian Federation	Uruguay
Denmark	Italy	Saudi Arabia	
Djibouti	Jordan	Sierra Leone	
Dominican Republic	Kingdom of the Netherlands	South Africa	

APPENDIX B.

List of Registered Speakers for the Matchmaking Session

Organizations only, in alphabetical order

BAE Systems	ICT4Peace Foundation
Cipher	Independent Diplomat
CREST	Institute for Security and Technology
Department of States, United States	Internet Corporation for Assigned Names and Numbers
Digital Agenda for Tanzania Initiative	INTERPOL
DiploFoundation	Japan International Corporation Agency
Ensign Infosecurity	MITRE
EU CyberNet	S. Rajaratnam School of International Studies
European Union Institute for Security Studies	SafePC Solutions
Federal Foreign Office, Germany	Temple University Institute for Law, Innovation & Technology (iLIT)
Forum of Incident Response and Security Teams (FIRST)	Third Eye Legal
Global Cyber Alliance	UNIDIR
Global Forum on Cyber Expertise (GFCE)	Write Pilot
Hikanotes Consultancy Limited (Hikanotes Cyber Program)	Youth for Privacy

APPENDIX C.

Speakers and Guiding Questions for Breakout Groups

Breakout Group 1: Strengthening Governance Policies and Processes

Speakers

Ms. Kerry Ann Barrett, Cybersecurity Programme Manager at the OAS; Mr. Chris Painter, President of the Global Forum on Cyber Expertise; and Mr. Eng. Abdulrahman Bin Ali Al Farahid Al Malki, President of the National Cyber Security Agency of Qatar.

Moderator

Dr. Giacomo Persi Paoli, Head, Security & Technology Programme, UNIDIR

Rapporteur

Ms. Lenka Filipová, Coordinator, Security & Technology Programme, UNIDIR

Guiding Questions

- Why it is important to develop national cyber strategies and other regulatory instruments?
- What are the risks associated with not having such instruments or dedicated structures in place for their implementation?
- Which policies, regulations, and structures are crucial for implementing various elements of the Framework of Responsible State behaviour (the Framework) and why these elements are essential?
- Which aspects of the Framework are the most challenging to implement in terms of policies and regulations?
- What resources do Member States require to effectively strengthen these policies, regulations, and structures?
- What are the potential roles of civil society, the private sector, and academia in these efforts?
- What are good practices to strengthen policies and regulations necessary for the Framework's implementation, as well as effective methods for establishing or improving national structures to support this implementation?

Breakout Group 2: Developing Technology, Talent and Partnerships

Speakers

Ms. Lee Pei Ling, Head of Strategy, Interpol, Singapore; Mr. Hitoshi Tojima, Chief Digital Officer, Japan International Cooperation Agency; Ms. Timea Suto, Global Digital Policy Lead, International Chamber of Commerce (ICC).

Moderator

Dr. Samuele Dominioni, Researcher, Security & Technology Programme, UNIDIR

Rapporteur

Ms. Aamna Rafiq, Researcher, Security & Technology Programme, UNIDIR

Guiding Questions

- What technological capabilities and partnerships may be crucial for the implementation of multiple elements of the Framework and why?
- What are the challenges of developing technology, talents, and partnerships in relation to what is outlined by the Framework?
- What resources would Member States require to effectively develop these capabilities? And what could be the role of the private sector, civil society, and academia?
- What are good practices in developing technical and operational capabilities?
- What are good practices for growing and retaining talent?
- What are good practices for establishing effective partnerships?
- What technology/talents/partnerships should a Member State employ/establish to implement the following norm (as an example)?
    - » Norm G States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199.

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

Palais des Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG