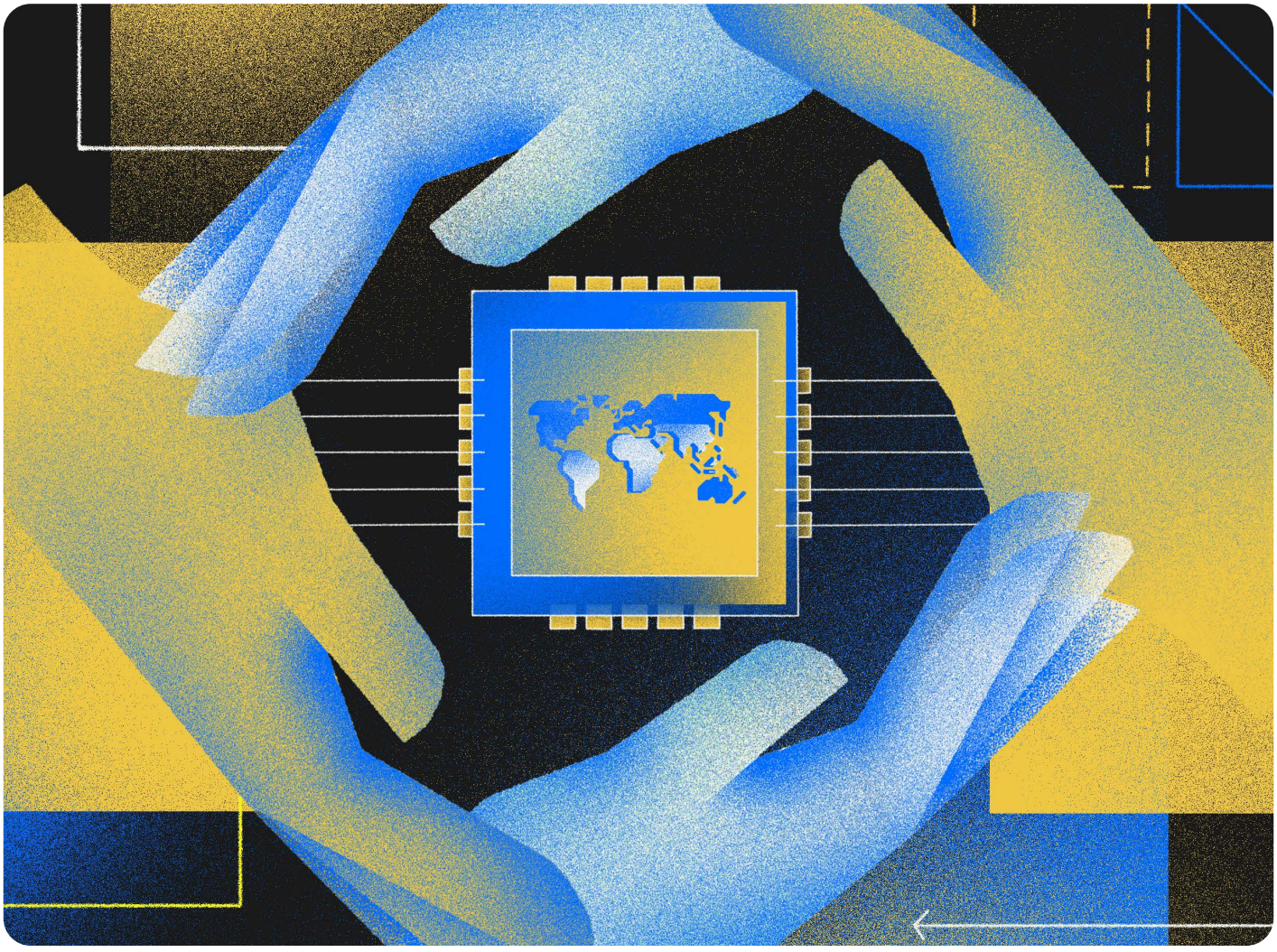
Compendium of Multistakeholder Perspectives

Cybersecurity and Sustainable Development: A Global Path Forward



Government Offices of Sweden
Ministry for Foreign Affairs

ITU

GFCE
Global Forum on Cyber Expertise

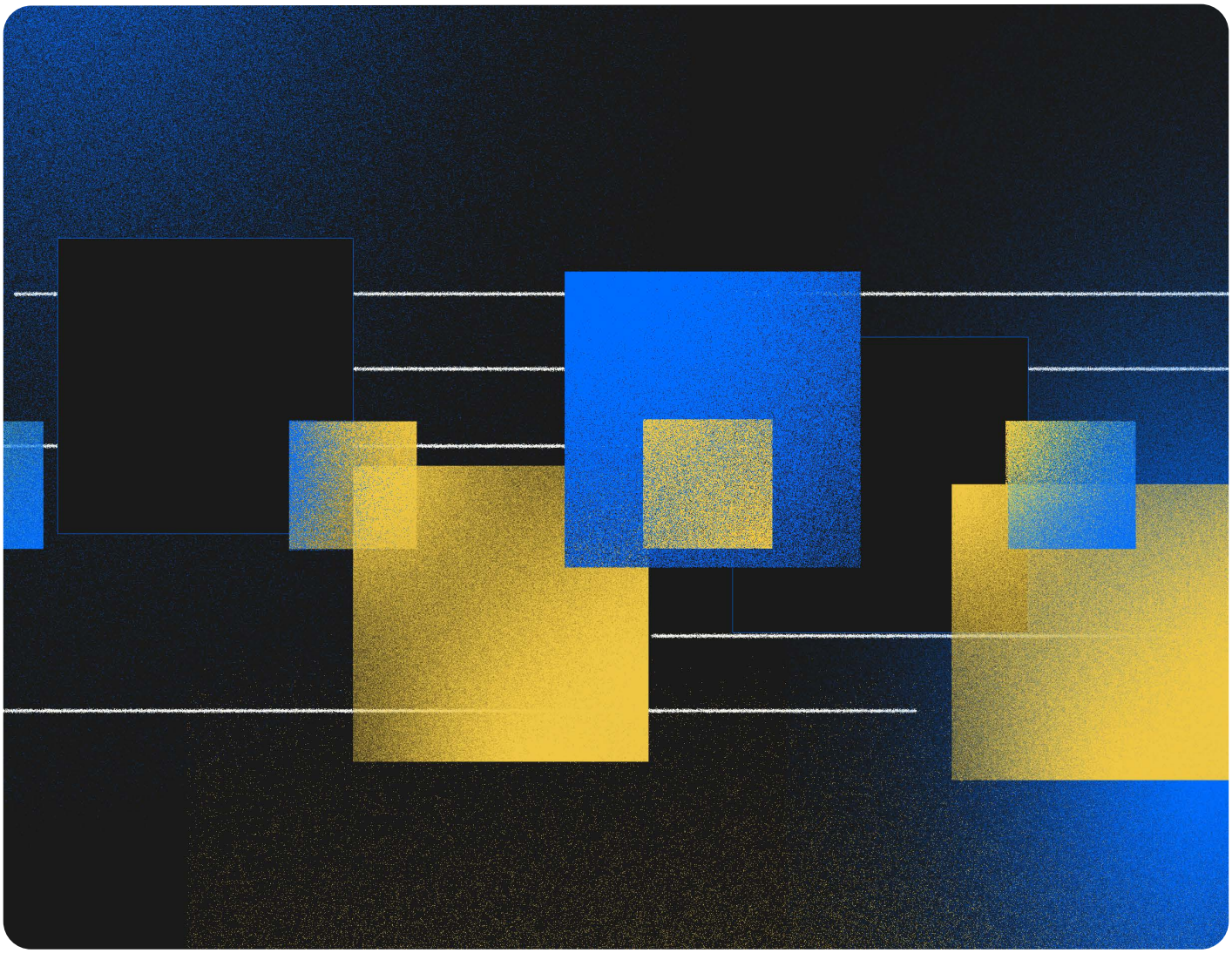
Microsoft

About this Compendium

Throughout 2023 and 2024, the Ministry of Foreign Affairs of Sweden, the International Telecommunications Union (ITU), the Global Forum on Cyber Expertise (GFCE), and Microsoft brought economic development and cybersecurity communities together through the organization of multistakeholder workshops.

During these workshops, key recommendations, lessons learned, and good practices were collected from a diverse group of experts, practitioners, and stakeholders. Based on what we heard and learned in these discussions, we have developed this Compendium titled Cybersecurity and Sustainable Development: A Global Path Forward that offers development practitioners, governments, international organizations, and other stakeholders a useful resource to support their efforts to advance cyber capacity building and inclusive development cooperation on digital issues.

The insights and ideas captured in these discussions and reported in this compendium reflect the diverse perspectives and expertise of a broad multistakeholder group, not necessarily the views of any one individual participant or the co-chairs of this project.



Executive Summary

This compendium encapsulates the key findings and insights derived from a series of workshops which took place between July 2023 and February 2024. These Workshops focused on the interplay between cyber resiliency and sustainable digital development. This initiative has been spearheaded by the Ministry of Foreign Affairs of Sweden, the International Telecommunication Union (ITU), the Global Forum on Cyber Expertise (GFCE), and Microsoft. Discussions delved into overcoming integration challenges, such as funding and timelines, the imperative of expanding awareness about cyber resilience, including both technical and policy considerations, as well as the need to continue building a pipeline of skilled cyber professionals.

The importance of multistakeholder cooperation, cross-sector partnerships, and innovative collaboration strategies were underscored to combat cyberthreats effectively. Supply chain security emerged as a significant concern, alongside the necessity to balance human-centric cyber resilience with security needs at various levels. The workshops also navigated the policy landscape and touched upon technical standardization, advocating for unified frameworks and terminologies to foster economic development goals.

Recommendations

The workshops culminated in a set of actionable recommendations applicable at the international, intra-regional, national, and local levels, aimed at comprehensively addressing the issues identified. These include:

1. **Integrating Cybersecurity into Development Initiatives:** Cybersecurity should be a fundamental and seamlessly integrated aspect of all development projects.
2. **Enhancing Cross-Sectoral Collaboration:** Encouraging diverse sectors to collaborate more effectively on cybersecurity initiatives to bolster cyber resilience.
3. **Creating Human Capacity:** Focusing on education and training to build a pool of skilled cybersecurity professionals through targeted capacity-building efforts.
4. **Enhancing Supply Chain Security:** Recognizing the importance of securing supply chains against cyberthreats by building in redundancies at multiple levels.
5. **Bridging the Gap Between Cyber Resiliency and Human Rights:** Ensuring cyber resilience efforts are aligned with human rights principles.
6. **Bridging Policy Gaps and Fostering Interoperability:** Advocating for harmonized cyber resilience policies and standards.
7. **Building Trust:** Establishing trust among development stakeholders is essential for effective cybersecurity measures.

Path Forward

Comprehensively integrating cyber resilience into development agendas requires a continuous and dedicated effort. The workshops emphasized the importance of integrating these recommendations into broader diplomatic and development efforts, particularly within the United Nations (UN) framework and in related international fora. The path forward involves enhancing existing frameworks, creating permanent mechanisms for cyber resilience, incorporating cybersecurity within the UN Sustainable Development Goals (SDGs), leveraging multistakeholder initiatives, and preparing for the post-2030 development agenda. The aim is to bridge the gap between cybersecurity capacity building and development communities, ensuring these efforts are well-anchored in ongoing and emerging initiatives globally.

Definitions

Cybersecurity

Cybersecurity is a comprehensive framework of policies, strategies, regulations, laws, standards, and practices aimed at ensuring the confidentiality, integrity, and availability of digital networks, information technology systems, and critical infrastructures. The framework is designed to protect the economy, societal functions, and the populace from a wide range of cyberthreats and potential attacks, ensuring resilience and continuity in the face of digital adversities.

Cyber Capacity

Cyber capacity refers to the expertise, competencies, technological resources, and organizational capabilities required to effectively implement and sustain cybersecurity measures. It involves developing, managing, and governing cybersecurity initiatives that align with strategic objectives and operational needs.

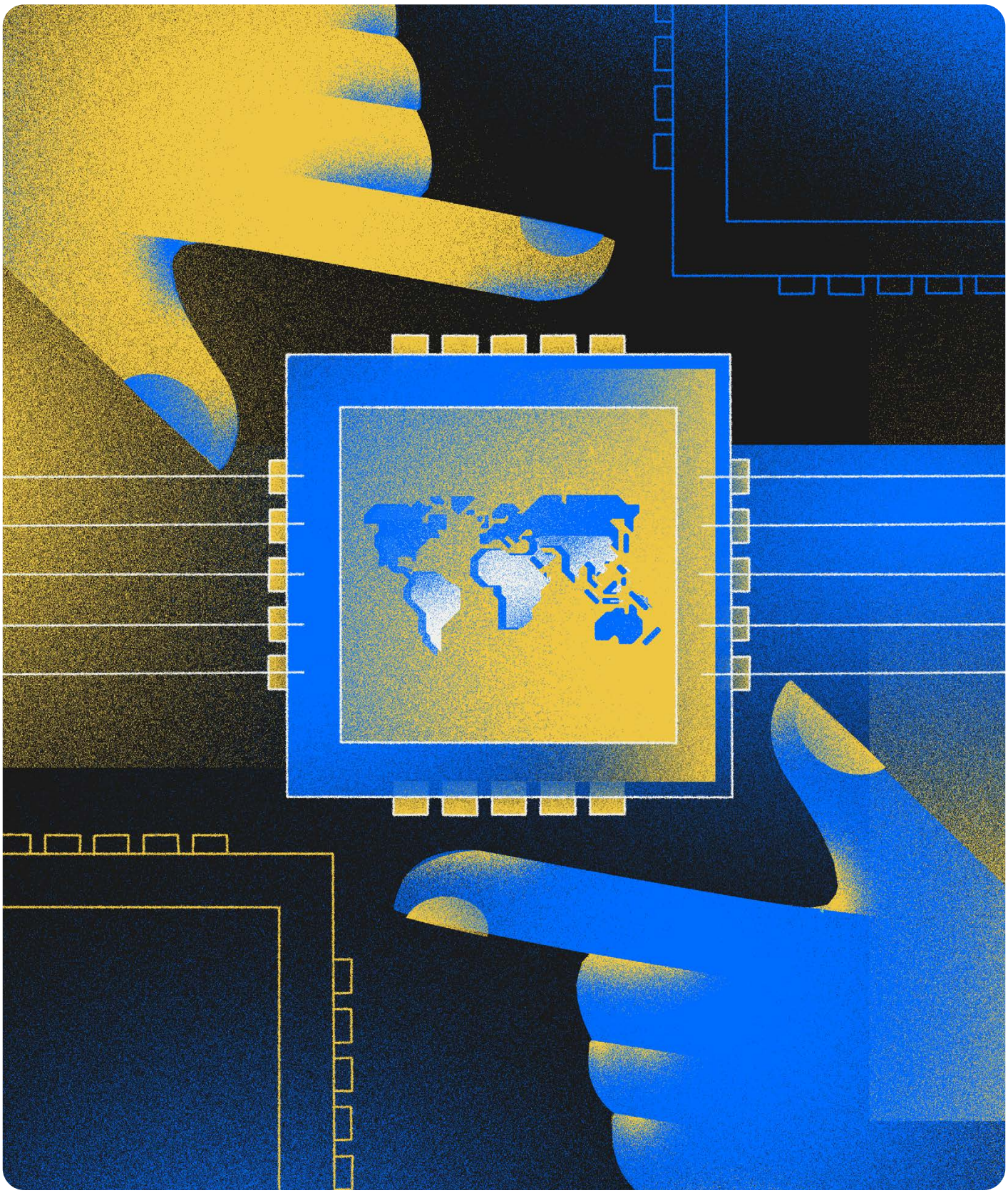
Cyber Capacity Building

Cyber capacity building is a strategic set of activities and programs that include training, advisory services, collaborative exercises, and financial support. These initiatives aim to enhance the cybersecurity readiness and responsiveness of nations, organizations, or collective entities; thereby strengthening their ability to anticipate, withstand, and recover from cyber events.

Supply Chain Security

Supply chain security is a holistic approach to safeguarding the interconnected network of participants within a supply chain. It involves governance mechanisms, regulatory frameworks, compliance standards, and risk management practices aimed at minimizing exposure to cyber risks and vulnerabilities.

Introduction



Introduction

In an era where digital transformation is essential, the International Telecommunication Union's (ITU)'s pursuit of Universal and Meaningful Digital Connectivity (UMC) by 2030 stands at the forefront of global endeavors to achieve the UN Sustainable Development Goals (SDGs). This vision – one where everyone can access a safe, enriching, and productive online experience at an affordable cost – is increasingly within our grasp. However, as we bridge the digital divide, particularly in the least developed countries, we face a crucial balancing act. While digital advancement promises substantial economic and social benefits, it also opens the door to heightened cybersecurity risks, with significant economic implications which threaten the fragile economies of these nations. The dual challenge of fostering cyber resilience alongside digital growth is not just an imperative for economic stability, but a cornerstone of trust in digital services. Addressing this tension head-on is pivotal in our journey towards a more inclusive, secure, and sustainable digital future for all.

This compendium is the product of a collaborative effort driven by a shared vision: to bridge the gap between the cyber resiliency capacity building and development cooperation communities, with the objective of mainstreaming cybersecurity into the broader framework of development work, particularly the SDGs. It has been spearheaded by a dedicated group of strategic partners: the Ministry of Foreign Affairs of Sweden, the International Telecommunication Union (ITU), the Global Forum on Cyber Expertise (GFCE), and Microsoft.

This compendium summarizes a series of workshops and engagements held across the globe, bringing together expertise from government, industry, and international organizations. By assembling cyber resiliency capacity building actors and development practitioners in diverse settings - from Accra, Singapore, New York, Paris and Kyoto - we have gained valuable insights, identified new challenges, and discovered new opportunities for collaboration. These interactions have allowed for the development of a more nuanced understanding of the complex dynamics at the intersection of cyber resilience and development. This report documents these conversations and insights, in the hope that they will lead to concrete steps and actions.

Bridging the Divide between Cyber resiliency and Development

Progress in closing the digital divide has been undeniable, with 67% of the global population now online and Internet usage in high-income countries nearing universality at 93%. While rising connectivity is creating many opportunities, however, it is also ushering in new challenges. The remarkable expansion of the digital world brings with it a paradox: digital access catalyzes social and economic growth, while simultaneously expanding the cyberthreat landscape. This is especially clear in low-income countries, with only 27% of the population being online, where the swift pace of digital adoption is surpassing local cyber resilience. As such, economies, businesses, communities, and individuals are becoming increasingly interconnected yet vulnerable to pervasive and novel cyberthreats.

Understanding and striking the delicate balance between digital inclusivity and cybersecurity is essential. It also presents the opportunity to build a more robust and equitable digital future. However, despite the evident interdependence between these domains, a lack of collaboration persists, hindering the realization of their complementary potential.

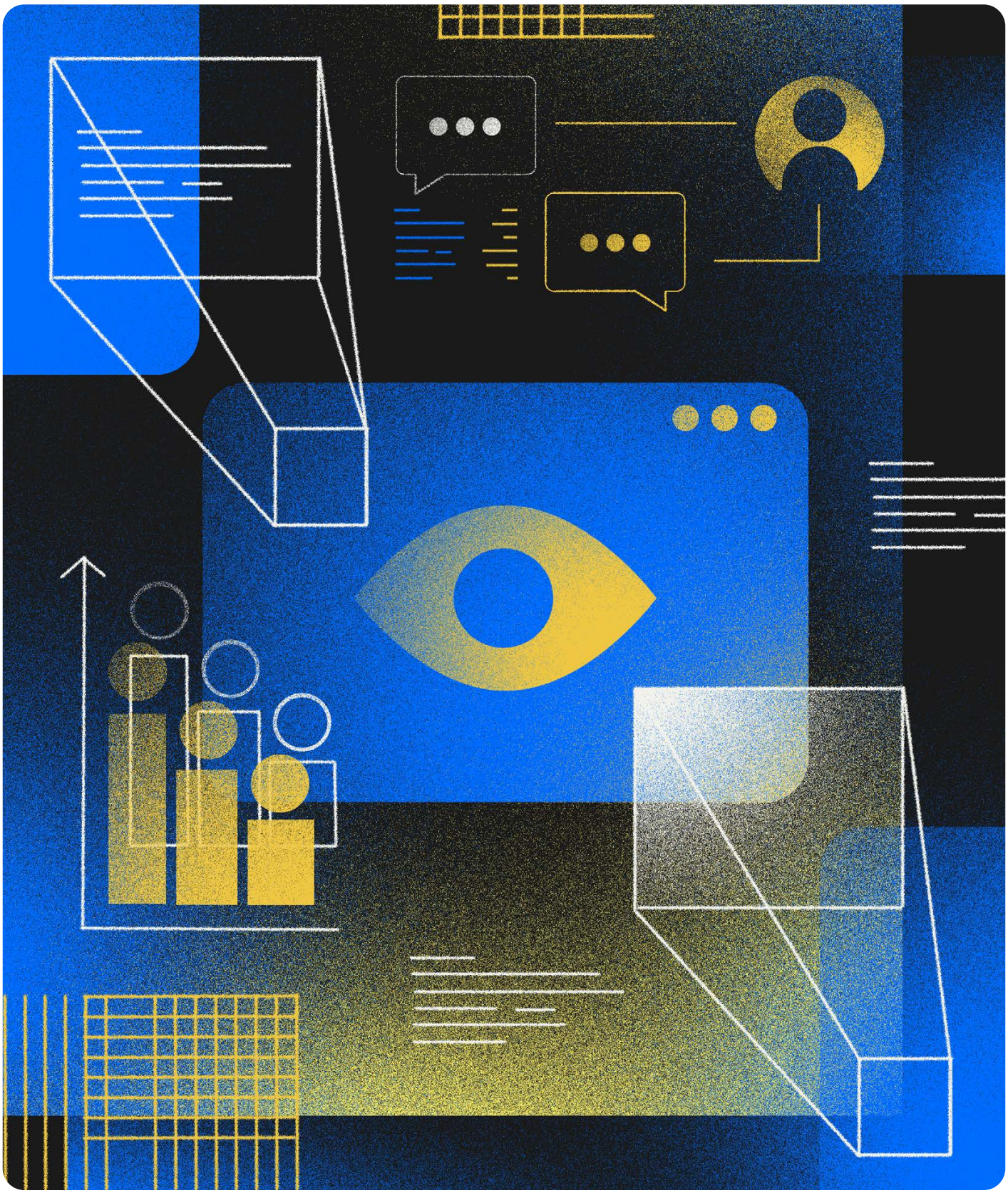
This urgency is further underscored by the emergence of cyber capacity building as a unique discipline within the broader context of global development. Its distinctiveness can be ascribed to the dynamic nature of technology and the escalating complexity of cyber resiliency challenges, thus requiring specialized expertise. Recognizing this, stakeholders across sectors and regions have taken an active role in shaping the nature of cyber capacity building as a mechanism to enhance security. However, the widespread misconception that cyber resilience is predominantly a national security concern only widens the gap between the development community and those focused on cyber capacity building. While safeguarding national interests is essential, limiting the discussion to this viewpoint overlooks the complex network of interrelated interests that shape global development.

In addition, prioritizing cyber resilience among numerous other development tasks presents a complex dilemma. The pressing demands for immediate solutions to socio-economic issues often overshadow the need for robust cyber resilience measures. This compendium delves into the challenges faced by policymakers and development practitioners in striking a balance that ensures the coexistence of developmental objectives and cyber resilience imperatives. It also explores the challenges policymakers and development practitioners face in achieving a balance that allows developmental goals and cyber resilience requirements to coexist. This compendium ultimately highlights the necessity for a shift in perspective, emphasizing that the integration of cyber resilience with development efforts is essential for creating a sustainable and secure digital future.

Workshops Overview

Event	Workshop Title
Workshop 1	Mainstreaming Cybersecurity in Development – Kickoff Event **Date:** July 25, 2023 **Location:** Side event to the Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies, New York City, United States
Workshop 2	Development Practitioners' Perspective on Mainstreaming Cybersecurity in Development **Date:** September 27, 2023 **Location:** Virtual Session
Workshop 3	Achieving the SDGs through Secure Digital Transformation **Date:** October 11, 2023 **Location:** Internet Governance Forum (IGF), Kyoto, Japan
Workshop 4	Mainstreaming Cybersecurity in Digital Transformation and Development in the Context of Southeast Asia **Date:** October 17, 2023 **Location:** Singapore International Cyber Week (SICW), Singapore
Workshop 5	Securing Digital Transformation for Sustainable Development **Date:** November 11, 2023 **Location:** Paris Peace Forum (PPF), Paris, France
Workshop 6	Mainstreaming Cybersecurity into Digital Development **Date:** November 30, 2023 **Location:** Global Conference on Cyber Capacity Building (GC3B), Accra, Ghana
Event	Presentation of Preliminary Findings **Date:** December 12, 2023 **Location:** Sideline event to the Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies, New York City, United States
Workshop 7	Mainstreaming Cybersecurity in the Development Agenda of Latin America and The Caribbean **Date:** February 20, 2024 **Location:** Virtual Session
Event	Public launch event **Date:** March 26, 2024 **Location:** Virtual session

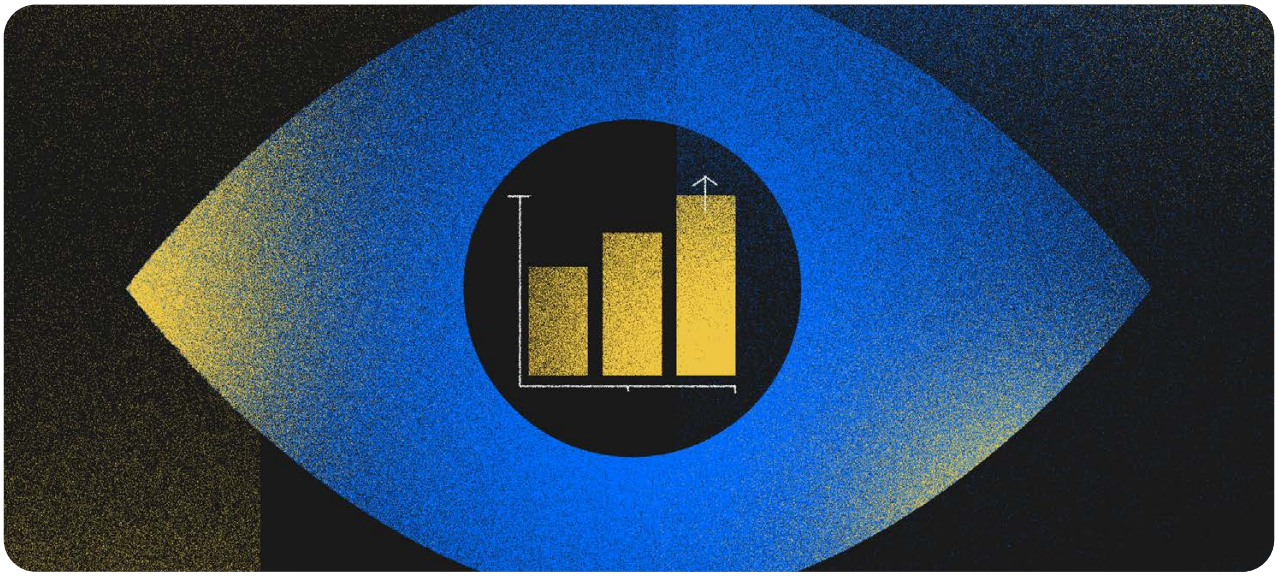
Key Findings and Insights



Key Findings and Insights

Throughout the listed workshops, participants explored fundamental questions at the intersection of cyber resiliency and development. Key discussions focused on overcoming the integration challenges of funding and timelines, as well as the importance of broadening cyber resilience awareness to include policy and technical considerations. Workshops addressed the shortage of skilled cyber professionals and highlighted the critical role of multistakeholder cooperation at all levels to combat cyberthreats, alongside the importance of cross-sector partnerships and innovative collaboration strategies.

Participants also examined supply chain security, identifying global challenges and proactive opportunities to better protect the supply chain, and debated the balance between human-centric cyber resilience and security needs at individual and state levels. Additionally, conversations touched on the policy landscape and technical standardization, exploring the varied approaches to cyber resilience across countries and suggesting ways to unify frameworks and terminologies to achieve development goals.



General Trends and Observations

Integrating Cybersecurity into Development Agendas

There was widespread recognition across the workshops that there is an insufficient integration of cyber resilience into traditional development agendas. This was frequently attributed to structural factors such as funding constraints and project timelines. Participants also consistently emphasized the urgency of raising cyber resilience awareness, stressing that it extends beyond technical considerations to encompass policy dimensions. It was evident that most development practitioners remain uncomfortable with technical aspects of cyber resilience, which continues to hinder the seamless integration of the two domains.

Despite these challenges, the participants consistently emphasized the critical role of secure digital transformation in achieving sustainable development. They acknowledged the necessity for coordination, collaboration, and capacity building across ministries, sectors, regions, civil society, and industry to succeed. The role of international frameworks, norms, and human rights in guiding state behavior in cyberspace was also emphasized, with a focus on the need for a holistic approach to fully realize the SDGs.

In certain workshops, participants noted that embracing digital transformation requires a near paradigm shift on cybersecurity within traditional development agendas. Rather than considering cybersecurity as an isolated technical aspect, it is essential to integrate it as a fundamental component in the planning and execution of development policies. As one participant put it, “The issue of awareness is important; I believe that cybersecurity is still not understood as an important factor in the different actors of the digital ecosystem.”

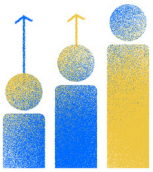
Enhancing Cross-Sectoral Collaboration

The need for greater multistakeholder collaboration emerged as another critical theme, with participants advocating for cooperative efforts across and between stakeholder groups at various levels. Bringing together diverse stakeholders was seen to enable the pooling of resources, expertise, and policies, fostering a more comprehensive and coordinated approach. Collaboration, particularly facilitated by organizations like the the Global Forum on Cyber Expertise (GFCE), was deemed crucial for boosting sustainability and avoiding duplication of efforts. Additionally, it is worth highlighting similar complementary efforts, such as the EU CyberNet's launch of the Knowledge Hub, featuring cybersecurity capacity building projects mapping and Operational Guidance for the EU's International Cooperation on Cyber Capacity Building.

Participants highlighted political support as crucial for successfully incorporating civil society and industry, stressing the importance of partnerships at all government levels. They focused similarly on the private sector's essential role, particularly in understanding and operating the technology.

Cross-sector collaboration was identified as a key necessity, particularly in the Asia-Pacific region, where innovative strategies have been sought to foster partnerships between sectors such as healthcare and finance. The discussions prioritized the need for a framework to guide collaboration and emphasized addressing cyber vulnerabilities in global supply chains. They also focused on leveraging micro, small, and medium-sized enterprises (MSMEs) for supply chain security.

Likewise, the workshop focusing on Latin America and the Caribbean highlighted that collaboration among multiple stakeholders, including governments, businesses, academia, and civil society, is essential to maximize the impact of capacity building efforts and to ensure a holistic and sustainable approach.



Creating Human Capacity

Capacity development consistently returned to the fore of discussion as many participants highlighted the shortage of skilled cyber resilience professionals, especially in emerging economies. For example, it is estimated that Africa's current level of cyber resilience awareness could be costing states up to 10% of their GDP, representing a tangible impact on economic resources. While discussions emphasized the urgency of capacity building, especially in regions with limited resources, the workshops acknowledged the complexity of making initiatives sustainable.

The post-training phase consistently emerged as a major concern, with participants questioning the efficacy of training programs if not accompanied by measures allowing for the application of acquired knowledge.

Each workshop surfaced new areas for improvement, exploring avenues to enhance capacity building and suggesting initiatives, for example the establishment of mentorship programs to link young professionals with experienced counterparts. Additionally, there were recommendations for enhancing skills at sectoral levels and promoting specialized training rather than broad education. Other participants noted that integrated capacity development initiatives can be implemented to address skills gaps, along with concrete national initiatives aimed at developing and implementing common frameworks and establishing clear and consistent cyber language.

These insights underline the potential positive impact of strategic investments in cyber resilience education and awareness. Discussions also revolved around effective cooperation between international organizations, governments, and the private sector to address the shortage of such investments. Recommendations to democratize the sector included the prioritization of soft skills, implementation of mentorship programs, and alignment of job descriptions with diverse backgrounds. Leveraging technology to bridge existing gaps and identifying specific skills needed and enhancing sectoral-level skills were also emphasized.

Enhancing Supply Chain Security

Participants agreed that addressing cyber resilience vulnerabilities in global supply chains is a complex challenge, especially given that these threats can disrupt operations, compromise sensitive information, and cause significant economic losses across interconnected global markets. The workshops underscored the need for a verification process and collaboration between governments and organizations to enhance supply chain protection. While challenges existed in determining the most effective methods for ensuring supply chain cyber resilience, opportunities were identified in leveraging micro and small enterprises (MSEs). MSEs were seen as potential collaborators that could impose requirements on their supply chains, thereby contributing to overall supply chain security. General recognition of the value of security was present among all participants: as one proactively noted, "Security is not an expense, but an investment."

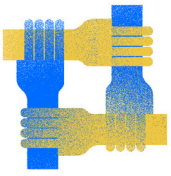
Establishing a Human-Centric Approach to Cybersecurity

All the workshops emphasized that significant challenges remain in achieving a human-centric approach to cyber capacity building, including in education, training, and literacy. Advancing both individual and state security, particularly in the context of potential tensions between cyber resilience and human rights, was raised as another area of concern. Simplifying technical and human rights concepts into understandable metrics for political leaders was identified as a key area for improvement to secure their support. Further, opportunities were recognized in closing the gaps between cyber resilience and human rights, highlighting the importance of adopting human rights-based approaches.

Bridging the Gap to Policy and Standardization

Different stakeholders' varying perceptions of, and approaches to, cyber resilience were a frequent topic of discussion. The need for a common framework and language for capacity building collaboration emerged as a consistent theme. For example, many participants highlighted how a relatively siloed approach of communities led to specific terminology that is only used within these communities. While development experts primarily relate to 'digital development', cyber capacity building experts tend to focus their attention on 'cyber resilience'. While such linguistic differences seem minor at first, they frequently lead to tangible cooperation challenges and hinder both communities from working together effectively.

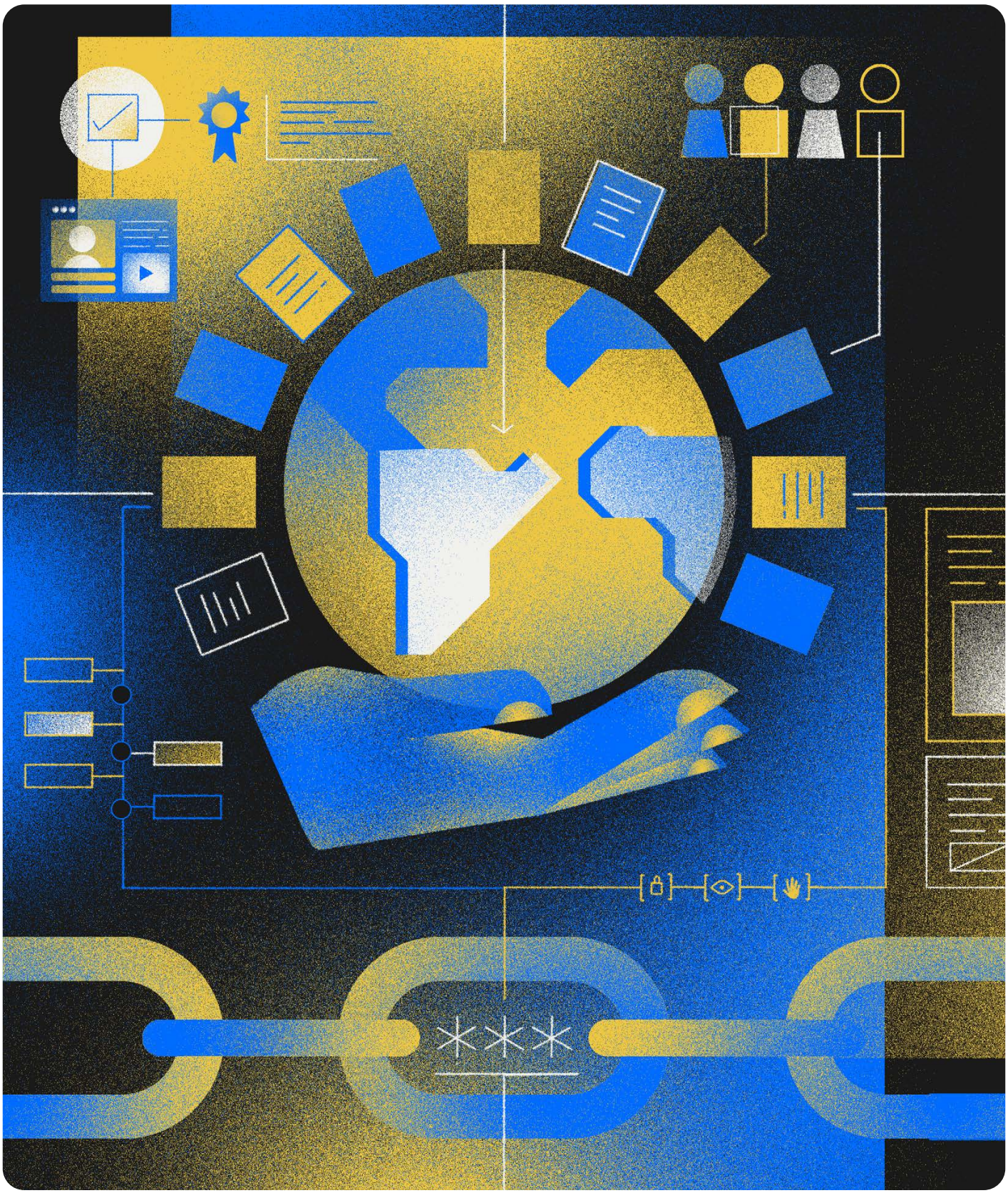
Opportunities identified for improvement included reframing discourse to align different communities, developing common frameworks, and updating metrics/indicators to contribute to development. Further, the "used responsibly" approach to digital technologies promotes their potential as catalysts for social and economic transformation.



Building Trust

In several workshops, it was noted that building trust among stakeholders is key to making meaningful progress. Understanding that different stakeholders have different motivations but can still work towards a common goal was identified as an important lesson still to be learned. As put by one participant in the Latin America and Caribbean workshop, "We definitely have to start by strengthening governance, because a solid governance model generates trust and when we generate trust, we generate interconnection...". Another participant built on this sentiment, noting that "Trust promotes the opening of the doors to an exchange of technological solutions, to the possibility of having as much information as possible."

Recommendations



Recommendations

Drawing on the rich insights identified across the workshops, several recommendations should be prioritized in future actions. These recommendations span strategic considerations, potential policy changes, and practical steps aimed at addressing the identified issues comprehensively. They are applicable at the international, intra-regional, national, and local levels. As such, they aim to catalyze transformative actions and initiatives to establish a more integrated, collaborative, and secure intersection of cyber resilience and development.

1. Integrating Cybersecurity into Development Initiatives

- Advocate for a unified framework and language to harmonize approaches to cyber resilience and digital development among governments, industry, and civil society, tackling terminological and conceptual differences. Policymakers, technical experts, and the public should have access to explanations that are clear, relevant, and meaningful.
- Collaborate to establish comprehensive, ongoing cybersecurity capacity building programs that cover both technical and policy aspects, fostering a spirit of collaboration, communication, and strategic planning. Government and industry should anchor these programs in local and international collaborations within the development community wherever possible.
- Integrate cybersecurity metrics and assessments into project monitoring and evaluation frameworks of development agencies and financial institutions, assessing the cybersecurity readiness of projects and their impact on enhancing the digital resilience of communities and nations.
- Work cooperatively across stakeholders to explore the integration of cyber resilience into existing international frameworks, such as the UN Sustainable Development Goals (SDGs), and propose clear indicators that support achieving the SDGs to measure progress in cybersecurity and digital development.
- Advocate for a common framework and language to align different communities' perceptions of cyber resilience and digital development, addressing terminological disparities. This common language should be accessible to policymakers, technical experts, and the public. Precision and clarity is key. Where existing frameworks and language have been adapted to cover a wide variety of interpretations, capturing the range of these interpretations is needed.
- Explore integration of cyber resilience into existing international frameworks, such as the SDGs. Propose clear indicators within SDGs to measure progress in cybersecurity and digital development.

Case Study

Cybersecurity and Data Protection Toolkits for SMEs

From 2019-2023, the UK Foreign, Commonwealth & Development Office (FCDO) ran a project titled "Cybersecurity and Data Protection Toolkits for SMEs – Strengthening the cybercrime defenses of South African small businesses", aimed at developing an online cybersecurity and data protection toolkit to help protect South African Small and Medium-sized Enterprises (SMEs) against cyber harms as they move to online trading. Recognizing that many African SME owners have neither the knowledge nor the funds to implement the controls and procedures they need to protect their businesses, this program blended development and cybersecurity by training over 400 SMME's with their online cyber security and data protection toolkit.

Read more here

2. Enhancing Cross-Sectoral Collaboration

- Develop frameworks for innovative strategies that foster cross-sector collaboration, for example in cyberthreat information-sharing across vital sectors like healthcare, finance, and other components of critical infrastructure which otherwise might not have sufficient cyber capacity.
- Facilitate cooperation among government agencies, in particular Computer Emergency Response Teams (CERTs) and industry, especially technology solution providers to enhance sustainability, minimize duplication, and promote information-sharing.
- Encourage and facilitate public-private partnerships in cybersecurity to leverage the expertise and resources of the private sector for public good. Such partnerships could focus on developing secure digital solutions for public services, enhancing national cybersecurity infrastructures, and fostering innovation in cybersecurity technologies.
- Emphasize the need for proper coordination, especially in establishing Security Operations Centers (SOCs) and CERTs across different sectors. Facilitate inter-ministerial dialogues to ensure a cohesive and collaborative approach to cyber resilience and development.

3. Creating Human Capacity

- Establish ongoing mentorship programs and collaboration opportunities within industry to facilitate knowledge transfer by connecting seasoned cybersecurity professionals with emerging talents.
- Governments should collaborate with private sector partners to create accessible cyber resilience education through scholarships, grants, and vocational courses. Additionally, ensure these programs integrate both technical and soft skills to address the diverse needs of the workforce.
- Curate and disseminate information resources for public use through collaboration among governments, industry, and academia, ensuring coverage of a broad range of topics and competency levels, including technical expertise, best practices, and collaborative strategies. Make these resources available in a variety of languages.
- Implement needs-based capacity building programs specifically designed to enhance the cybersecurity skills of government officials and civil servants in priority developing countries, adjusting these programs to include workshops, training sessions, and knowledge-sharing platforms that focus on areas such as cyber policy formulation, incident response, and secure digital infrastructure development.

Case Study

EU CyberNet LAC4 – Latin America and Caribbean Cyber Competence Centre

The LAC4 is a regional cybersecurity competence center with a physical facility in Santo Domingo, the Dominican Republic. This Centre serves as a focal point for sharing EU's collective expertise, building up local capacity, facilitating collaboration on joint projects and actions, and promoting the benefits of an open, free and inclusive cyberspace. By creating the spaces for a variety of cyber professionals from all backgrounds to come together, especially in a regional context, regions can strengthen the cyber knowledge and capacity within their geographies.

Read more here

4. Enhancing Supply Chain Security

- Develop and implement stringent supply chain security measures incorporating a verification process to ensure cybersecurity resilience. Governments and industry should work collaboratively to base and align processes with existing initiatives to avoid reinventing the wheel.
- Emphasize government collaboration with MSEs to ensure that measures are practical and adaptable for smaller entities, and provide guidance and resources to help MSEs meet these requirements effectively.
- Develop redundancies within supply chains to ensure adequate cyber resilience at multiple levels.

5. Bridging the gap between cyber resilience and human rights

- Advocate for a human rights-based approach that integrates human rights principles into cyber resilience. Develop comprehensive frameworks for political leadership to assess policy impacts on individuals and communities, underscoring the imperative of safeguarding human rights in the digital domain.
- Foster dialogue and collaboration between cyber resilience and human rights communities to ensure rights are respected, protected, and fulfilled; emphasizing the development of guidelines that advance state security and rights.
- Bridge the gap between cyber resilience and development by facilitating collaboration among academic institutions, industry, civil society organizations, and policymakers to create a holistic approach.

Case Study

Raising awareness of cybersecurity across Brazil – Creating a more cybersecure population

When the Brazilian government launched E-Ciber, its first ever national cybersecurity strategy, there was a need to increase public awareness across its constituents. This workstream, implemented by KPMG and Tonica, focused on making those most vulnerable in Brazil's population aware of new cyber threats they might face. For example, this included educating women, young people, under-represented minority groups and the elderly about issues ranging from online sexual exploitation to discrimination, and cyber bullying to the abuses of personal data.

Read more here

6. Bridging the Gap between Policy and Standardization

- Stress the significance of policy harmonization and structural alignment beyond sectors and national boundaries for successful cyber resilience that is scalable and easily transferrable across sectors, nations, and regions. Governments and industry should share best practices and guidelines for countries aiming to align their policies and structures effectively.
- Foster academic research that links cyber resilience and development by working together across governments and civil society, acknowledging the challenges of aligning medium to long-term development goals with shorter cyber capacity building timelines. Encourage research that addresses the specific needs and challenges at this intersection, with a focus on multidisciplinary and international studies.
- Present lessons learned from recipients of developmental aid, focusing on local impact, country interests, and structural reforms, and provide case studies that highlight successful policy and structural alignment in recipient countries.

Case Study

OAS Cybersecurity Program

The Organization of American States (OAS) runs a robust cybersecurity program spanning its member states. This program focuses on three elements: (I) policy development, (II) capacity building (including training and exercises), and (III) research and outreach; which collectively produces outputs like reports, strategies, and trainings that builds upon the experiences within the region. This kind of interregional cooperation is an ideal way to share lessons and best practices, all while maintaining a spotlight on pressing local and national issues.

Read more here

7. Building Trust

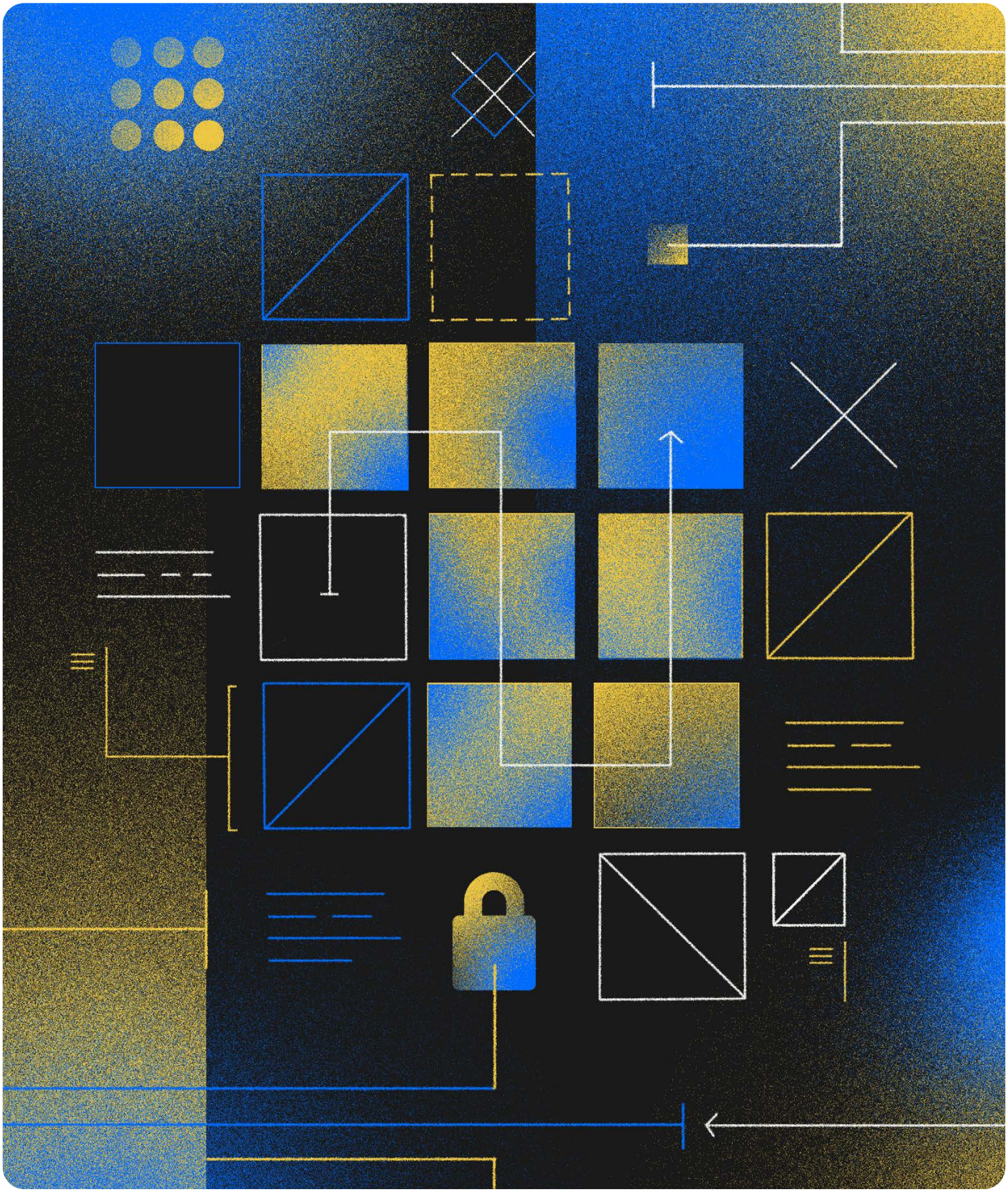
- Create a recognition that progress on bridging the gap between development and cybersecurity requires building trust between a large and diverse group of stakeholders including government, industry, and civil society.
- Establish dedicated cybersecurity advisory services within development aid agencies and international financial institutions to offer technical assistance, strategic advice, and policy guidance to countries, with a particular focus on integrating cybersecurity considerations into development projects. Collaborate with national governments to develop and implement comprehensive cybersecurity strategies that align with their development goals.
- Encourage meaningful multistakeholder engagement on cybersecurity in development by collaborating across governments, industry, academia, and civil society. Establish formal and informal mechanisms for ongoing collaboration, emphasizing inclusivity and diversity in stakeholder involvement.
- Foster academic research on the intersection of cybersecurity and development, producing insightful reports, case studies, and best practices to lead the way in understanding and addressing the unique cybersecurity challenges faced in the development context.

Case Study

The Mainstreaming Cybersecurity into Digital Development Compendium

As a final word, this compendium effort and in particular its workshops constitute an example of building trust across communities. In doing this exercise, participants witness a remarkable degree of sharing insights, practices, and lessons – and between a large variety of communities, including representatives from the private sector, academia, civil society, and the public sector. In many ways, this compendium was built on the idea of meaningful inclusivity, where it was attempted to provide stakeholders with the opportunity to highlight perspectives from both the development and cybersecurity communities. The most important result of such an exercise is arguably the trust it builds between the participants – by establishing meaningful personal relationships, everybody has a sense of ownership and is empowered to contribute in finding solutions.

Path Forward – A Vital Imperative for Sustainable Development



Path Forward – A Vital Imperative for Sustainable Development

The previous chapters outlined the findings and recommendations for actionable steps to mainstream cyber capacity building into digital development. However, it is important to contextualize these recommendations into the broader diplomatic negotiations and efforts that are occurring within the United Nations (UN) and elsewhere. The following are an effort to link up recommendations toward existing international fora and processes.

The results of this workshop series confirmed that bridging the cyber and development communities must be a continuous process and require specific efforts by all involved communities. After all, actors here do not operate in a vacuum. As the community strives to bridge the gap between the cybersecurity capacity building and the development communities, there must be a clear attempt to anchor these efforts in existing emerging initiatives, on both sides of the divide. Building on the recommendations found in the previous sections of this compendium, there are several clear next steps and opportunities for the continuation of this journey to bridge the cyber and development communities.

1. Enhancing Existing Frameworks

Capacity building lies at the heart of building an effective global cyber resilience framework. This has been recognized across several international fora, such as the current UN Open-Ended Working Group (OEWG) on cybersecurity, as well as other sectoral and regional platforms.

Participants of the OEWG consider the OEWG itself as a collaborative platform for fostering a holistic, inclusive, and needs-based approach. The OEWG members' efforts to map existing cybersecurity capacity building initiatives aim to provide UN member states with lessons learned and benchmarking opportunities with the goal of fostering more effective collaboration, enhancing implementation efforts, and leveraging the multitude of stakeholders across government, industry and civil society more effectively. Going forward, it will be important to leverage the OEWG's work to bridge the gap between the cyber resilience and digital development communities.

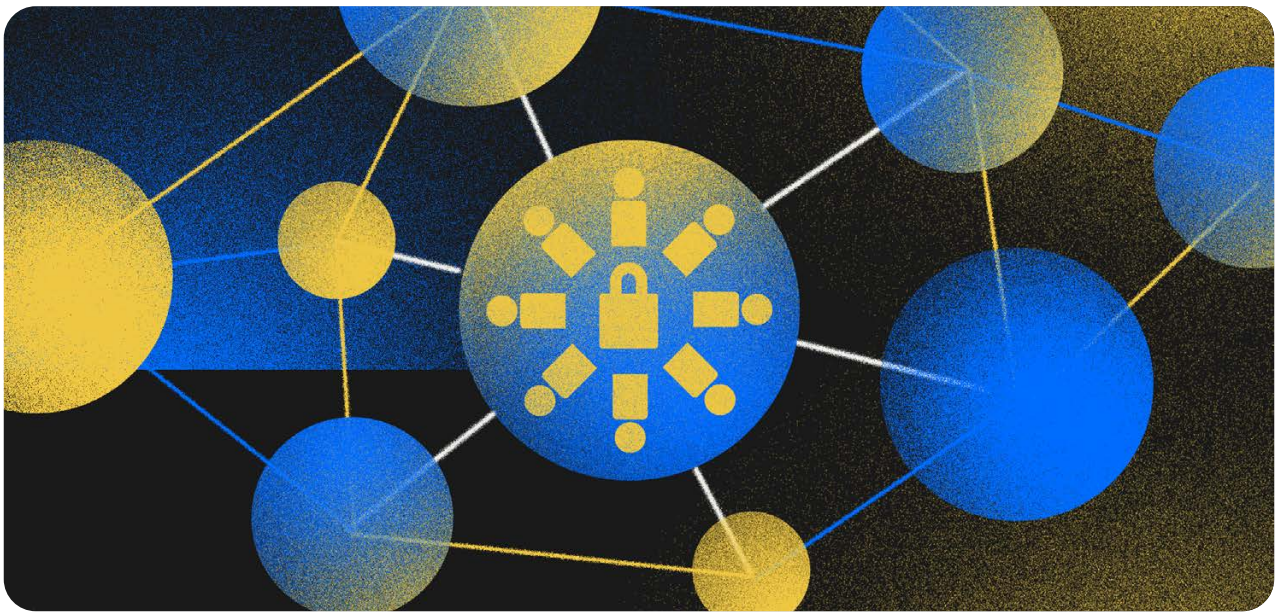
Other international processes have also recognized the linkage between digital development and cybersecurity; as well as the importance of this linkage towards capacity building efforts, particularly in the Global South. The forthcoming UN Global Digital Compact (GDC), for example, aims in part to bridge the digital divide and will also include language on cybersecurity and capacity building. Similarly, the work done in the OEWG and the proposed Programme of Action (PoA) might highlight similar connections among digital connectivity, cybersecurity, and capacity building. Going forward, it is vital to coordinate and cohere these efforts across multiple UN workstreams, not only to avoid duplicate funding requests, but also to maximize efficiencies.

2. Building a Permanent Mechanism

Additionally at the international level, states are currently determining what a possible permanent mechanism at the UN for cybersecurity could look like. Here, all options currently on the table include a strong focus on cyber capacity building. In particular, the proposal for a Programme of Action (PoA) in this space has zeroed in on this area as needing special attention.

The suggested PoA aims to build on already existing efforts in the field. Key elements when it comes to capacity building efforts of this mechanism might include:

- **Needs based Approach:** The focus must be on the needs that will be matched by capabilities.
- **Resource Allocation:** Adequate funding and resources must be allocated to capacity-building programs.
- **Skills Development:** Training programs, workshops, and certifications need to become more accessible and available globally.
- **Public Awareness:** Raising awareness about cyberthreats and best practices is essential for a cyber-literate society.



3. Leveraging Multistakeholder Initiatives

In addition to the work driven in multilateral institutions, it is crucial to leverage multistakeholder initiatives to drive implementation of the recommendations outlined within this document. Here, it is important to recognize the efforts begun through the Global Conference on Cyber Capacity Building (GC3B) and the Accra Call. For instance, the Accra Call aims to stimulate global action to elevate cyber resilience across international and national development agendas as well as promotes cyber capacity building that supports broader development goals. As a group, signatories are committed to driving forward this initiative and reporting back on it at the 2025 conference in Switzerland and participate in the buildup process leading up to this conference.

4. Linkage to the Global Digital Compact (GDC) Agenda

In spring 2024, the UN's GDC co-facilitators – Sweden and Zambia – invited member states and stakeholders to express their views on possible principles, commitments, and actions to be included in the GDC. These suggestions will be considered during the negotiations of the GDC ahead of its adoption at the September 2024 UN Summit of the Future. Contributions to this compendium make it clear that cybersecurity should be one of the priorities.

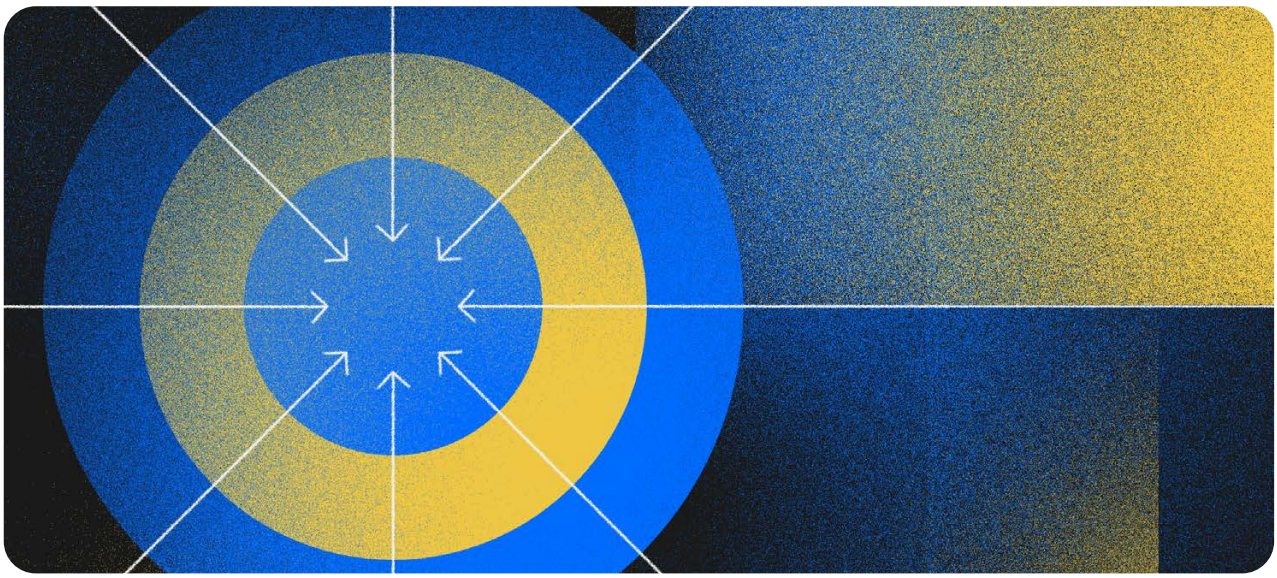
Digital transformation is essential for achieving the SDGs, but if countries do not take steps to protect themselves online and instill cyber resilience against constantly evolving threats, we risk missing those targets. Cybersecurity should not be an add-on, but a core element of trusted digital transformation and needs to be mainstreamed into development efforts at the UN and beyond. Agreeing specific goals would also generate political will, mobilize donor commitments, and inform assessments as to where more efforts are needed.

5. Elevating Cybersecurity within the Sustainable Development Goals (SDGs)

The SDGs provide a roadmap for global development, addressing challenges ranging from poverty eradication to climate action. However, the current SDGs do not explicitly address cybersecurity. This omission is concerning, given the escalating cyberthreats faced by nations, organizations, and individuals. To rectify this, all stakeholders must work together to raise awareness of the importance of cybersecurity for economic development and advocate for the creation of Cyber Development Goals (CDGs) to support the SDGs. These CDGs would emphasize the importance of secure digital infrastructure, data protection, and cyber resilience as integral components of sustainable development.

6. Lay the Groundwork for the Post-2030 Development Agenda

The development agenda looks set to go through many changes in the years to come – and this will provide opportunities to share the lessons of this compendium and advocate for greater inclusion of cybersecurity. For example, as the processes to create the post-2030 development agenda begin to take shape, it will be vital to proactively lay the groundwork for robustly integrating cybersecurity into this future framework. Recognizing the evolving nature of both digital landscapes and development priorities, it will be necessary to foster early dialogue and advocacy; develop flexible, forward-looking strategies; building partnerships for knowledge and resource sharing; and demonstrate the outcomes of integrating cybersecurity in development projects.



Conclusion

The workshops held as part of our “Cybersecurity and Sustainable Development: A Global Path Forward” compendium initiative have yielded valuable insights into the intersection of cybersecurity and digital development. Participants underscored critical challenges, identified key themes, and spotlighted potential pathways for transformative action. The collective findings emphasize the urgent need for a paradigm shift in how cybersecurity is perceived, integrated, and prioritized within traditional development agendas.

A consistent theme among the workshops was the prevailing gap in cybersecurity integration, often hindered by structural constraints and a lack of awareness. To combat this, the workshops made clear that engaging technical experts, and collaborating with key stakeholders in policy and development circles is key to success.

To push this work forward, a top priority will be capacity building, particularly in regions with a shortage of skilled cybersecurity professionals. Recommendations for soft skills development, mentorship programs, and alignment of job descriptions to attract diverse backgrounds have been proposed. Cross-sector collaboration, inclusive solutions, and robust supply chain security measures are deemed essential for enhancing overall cybersecurity defenses.

The interdependence of cybersecurity and development was a central theme, with workshops highlighting the need for coordination, collaboration, and capacity building across sectors, and regions. The role of international frameworks, norms, and human rights in guiding states’ behavior in cyberspace was underscored, emphasizing the holistic approach required to achieve the SDGs.

As we navigate the complex landscape of a digital future, these workshops have paved the way for a deeper understanding of the challenges and opportunities at the nexus of cybersecurity and digital development. The collective findings serve as a call to action for concerted, collaborative, and strategic efforts to bridge the existing gaps, fostering a resilient and secure digital transformation that aligns with global development objectives. The lessons learned from these workshops not only inform immediate actions but also lay the groundwork for sustained dialogue, knowledge sharing, and collective action to shape a digitally inclusive and secure future.

Thanks

We would like to acknowledge and thank all the speakers who took part in the various workshops:

Workshop 1: Mainstreaming Cybersecurity in Development – Kickoff Event

- **Demi Bylon,** Desk Officer for Cyber Issues and Hybrid Threats, Swedish Permanent Mission to the United Nations
- **Pavel Mraz,** Moderator, Senior Project Manager of Digital Diplomacy at Microsoft
- **Chris Painter,** President, GCFE Foundation Board Director
- **Caroline Troein,** Cross Thematic Programme Officer, International Telecommunications Union

Workshop 2: Development Practitioners' Perspective on Mainstreaming Cybersecurity in Development

- **Tereza Horejsova,** Outreach Manager, GFCE
- **Nikolas Ott,** Senior Manager, European Government Affairs, Microsoft
- **Ingela Svedin,** Digital for Development, Sida
- **Lisa Svensson,** Deputy Director, Global Cyber/Digital Affairs, Ministry of the Foreign Affairs of Sweden
- **Caroline Troein,** Cross Thematic Programme Officer, International Telecommunications Union

Workshop 3: Achieving the SDGs through Secure Digital Transformation

- **Allan Cabanlong,** Director South-East Asia Hub, GFCE
- **Johan Ekerhult,** Counsellor, Permanent Mission of Sweden to the UN and Other International Organizations in Geneva
- **Tereza Horejsova,** Outreach Manager, GFCE
- **Yasmine Idrissi Azzouzi,** Project Officer, ITU
- **Michael Kariminian,** Director of Digital Diplomacy, Microsoft
- **Christopher Painter,** President, GFCE Foundation

Workshop 4: Mainstreaming Cybersecurity in Digital Transformation and Development in the Context of Southeast Asia

- **Allan Cabanlong,** Director South-East Asia Hub, GFCE
- **Jenny Egermark,** Ambassador, Embassy of Sweden to Singapore
- **Christopher Painter,** President, GFCE Foundation

Workshop 5: Securing Digital Transformation for Sustainable Development

- **Kaja Ciglic,** Senior Director, Digital Diplomacy, Microsoft,
- **Mariana Gonzalez Carrillo,** Technical Advisor, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
- **Giacomo Persi Paoli,** Head of Programme Security and Technology, United Nations Institute for Disarmament Research (UNIDIR)
- **Moctar Yedaly,** Special Envoy for the Global Conference on Cyber Capacity Building

Workshop 6: Mainstreaming Cybersecurity into Digital Development

- **Rex Amos,** Cyber Policy Department, Foreign, Commonwealth and Development Office
- **Enrico Calandro,** Project Leader at Cyber Resilience for Development, Cyber4Dev
- **Vanessa Copetti Cravo,** Telecommunication Regulation Specialist, Anatel
- **Steven Matainaho,** Chairman, Public Service ICT Steering Committee, Papua New Guinea
- **Nikolas Ott,** Senior Manager, European Government Affairs, Microsoft
- **Caroline Troein,** Cross Thematic Programme Officer, International Telecommunications Union

Workshop 7: Mainstreaming Cybersecurity in the Development Agenda of Latin America and The Caribbean

- **Kerry-Ann Barrett,** Cybersecurity Program Manager, OAS/CICTE
- **Orlando Garcés,** Cybersecurity Program Officer, OAS/CICTE
- **Ingrid Hernández,** Presidential Advisor of the Department of Digital Transformation and Coordinator of Digital Transformation, Presidency of the Republic of Colombia
- **Carlos Leonardo,** Director of the National CSIRT, Dominican Republic
- **Gezer Molina,** Director of Cybersecurity of the Ministry of Science, Innovation, Technology and Telecommunications (MICITT) of Costa Rica
- **Valentina Name,** Program Officer, OAS and GFCE Hub for the Americas and the Caribbean
- **Mauricio Papaleo,** Director of Information Security, Agency for the Development of the Government of Electronic Management and the Information and Knowledge Society (AGESIC) of the Republic of Uruguay
- **Nikolas Ott,** Senior Manager, European Government Affairs, Microsoft
- **Caroline Troein,** Cross Thematic Programme Officer, International Telecommunications Union


Government Offices of Sweden
Ministry for Foreign Affairs

ITU

GFCE
Global Forum on Cyber Expertise

Microsoft