OUTCOME REPORT

ITU INTERREGIONAL CYBERDRILL FOR AFRICA AND EUROPE
16 September 2021

Acknowledgements

This report has been produced by International Telecommunication Union (ITU). ITU would like to express their gratitude to the all participants of the interregional meeting, specifically, **Mr. Andrew Rugege,** Regional Director, ITU Regional Office for Africa, and **Mr. Jaroslaw Ponder,** Head of the ITU Office for Europe, for providing welcome remarks and informed data trends in the region. **Mr. Moses Bayingana**, Representative, AU Infrastructure and Energy, African Union Commission, **Mr. Lacina Koné**, Director General, Smart Africa Secretariat, **H.E. Ambassador Lotte Knudsen,** Head of the Delegation of the European Union to the United Nations and other international organisations in Geneva, for their respective special opening messages. ITU also sincerely thanks **Ms. Caroline Troein**, Lead Cybersecurity Research, International Telecommunication Union and **Ms. Anamaria Meshkurti,** Program Officer ITU Office for Europe for their respective moderating, and Claire Breedlove, Cybersecurity Technical Writer, for authoring this report.

In addition, ITU would like to express their appreciation to the interregional meeting speakers, **Mr. Moctar Yedaly,** Africa Program Director, Global Forum on Cyber Expertise (GFCE), **Mr. Luigi Rebuffi,** Founder and Secretary General, European Cyber Security Organization (ECSO), **Mr. Didier Nkurikiyimfura,** Chief Technology and Innovation Officer, Smart Africa, **Mr. Jean-Robert Hountomey,** Executive Director AfricaCERT for excellent contributions regarding African and European cybersecurity cooperation trends. ITU also thanks **Mr. Jeremy Ketteringham,** Representative of the Government of the United Kingdom, **Ms. Natalia Spinu,** Head of CERT Moldova, **Mrs. Connie Francis,** Director of ICT and Applications Services, Tanzania Communications Regulatory Authority, **Dr. Kaleem Ahmed Usmani,** Head, Computer Emergency Response Team of Mauritius (CERT-MU) for providing the specific context of their representative countries.

Introduction

The International Telecommunication Union improves nations' cyber security readiness, protection, and incident response capabilities by conducting CyberDrills at regional and international level. A CyberDrill is a planned event during which cyber-attacks, information security incidents, or other types of disruptions are simulated in order to test an organization's cyber capabilities. CyberDrills aim to measure how well organizations are able to detect security incidents and their ability to respond appropriately and minimize any related impact. Through a CyberDrill participants are able to validate policies, plans, procedures, processes, and capabilities that enable preparation, prevention, response, recovery, and continuity of operations.

Over the past ten years, ITU has held over thirty CyberDrills partnering with more than 100 countries committed to improving cybersecurity at both the national and global levels. This year, focused specifically on the role of national Computer Incident and Response Teams (CIRTs) and Computer Security Incident Response Teams (CSIRTs) in building cyber resilience and protecting critical information infrastructure, the 2021 CyberDrill tailored event sessions around four thematic concepts: *reflect*, *share*, *learn* and *practice*. These concepts provided an overall framework for event sessions while encouraging meaningful conversation around challenges and advancements of the past year.

- ***Reflect:*** Bring together the global cybersecurity community to review major regional cybersecurity trends and consider improvements based on the five GCA and GCI pillars.
- ***Share:*** Promote knowledge sharing of beneficial communication networks, and exchange funding stream resources.
- ***Learn:*** Build capacity for the CSIRT communities within incident response, CIIP, and detections.
- ***Practice:*** Test operational resiliency key concepts across CSIRT/CIRT/CERT community.

African and European Interregional Meeting

The first African and European interregional meeting of ITU CyberDrills was held on the 16th of September, 2021 and was attended by over 160 participants from over eighty countries around the world. Centered around the necessity for collaboration within cybersecurity in order to protect critical information infrastructure, the session posed the following questions to panelists:

- What concrete initiatives and actions could the European Union and Africa develop together in order to strengthen their cooperation in cyberspace?
- What should be in place for Africa and the countries in the European Union to step up their cooperation engagement?
- What are the main challenges and areas of cooperation going forward among regions?

Opening Remarks and Special Messages

Mr. Andrew Rugege, Regional Director, ITU Regional Office for Africa
Mr. Jaroslaw Ponder, Head of the ITU Office for Europe
Mr. Moses Bayingana, Representative, AU Infrastructure and Energy, African Union Commission
Mr. Lacina Koné, Director General, Smart Africa Secretariat
H.E. Ambassador Lotte Knudsen, Head of the Delegation of the European Union to the United Nations

The opening of the session commenced with remarks from both African and European continental representatives emphasizing the important legislative and strategic steps each region has taken to further secure cyberspace. In particular, African delegates highlighted the newly published African Union *Digital Transformation Strategy for Africa*, which envisions a secure digital single market on the continent by 2030 with the free movement of people, services, and capital. While additions to the strategy continue to be drafted (including a child online safety policy, a complete cybersecurity strategy for Africa, and a data policy framework), the *Digital Transformation Strategy for Africa* intends to address global cybersecurity threats with a comprehensive continental response.

As broadband connections continue to increase across the African continent, so do the potential for cyber-attacks, and therefore it is critical to reinforce human and institutional capacity to secure cyberspace by building trust and confidence in the use of cyber technology. Globally, cybercrime continues to rise, and is projected to cost the global economy $10.5 trillion annually by 2025. Simultaneously, the continent faces a serve shortage of cybersecurity talent; 2020

registered a shortage of 100,000 roles within the sector, and this number is only expected to increase in the future. Acknowledging the risks that Internet users across the continent will take in order to participate in an increasingly data driven society means that governments and regional representatives must develop new rules to generate trust and protect data across the entire value chain, and particularly for vulnerable and marginalized groups. In addition to the *Digital Transformation Strategy for Africa*, the African Union encourages member states to sign and ratify the *Convention on Cybersecurity and Personal Data Protection* "Malabo Convention" which targets cybersecurity, privacy, and data protection as central themes to strengthen cybersecurity at the regional, national, and continental levels.

Recognizing that cyberthreats across the African continent are borderless, collaboration is essential to these strategies. The current fragmented continental cybersecurity approach must be reconstructed to promote harmonization of cybersecurity regulations and policy adoption, enhance peer learning and sharing of best practices, and the development of measures that ensure the protection of African critical information infrastructure. Over sixty percent of the countries within the African continent are classified as a Least Developed Country (LDC), with a high population of unconnected peoples. As cyberthreats continue to evolve, it is necessary that the protection and preservation of critical information infrastructure does as well, especially as streams of new users come on line.

Within Europe an emphasis was placed upon the COVID-19 pandemic's acceleration of societal digital transformation both within services accessible in the digital space, and the increase in sophistication of cyber-attacks. The necessary response to this increase of attacks on critical information infrastructure, in particular healthcare, is to build a cyber resilience strategy at the national, regional and international level; cybersecurity threats exploit vulnerabilities in technology regardless of geographical location. The European Union has recently adopted a cyber security strategy for the digital decade which includes enhancing collaboration mechanisms along with legislation on the security of networks and information systems. The best way forward for both continents, is to increase transparent information sharing to cooperate in preventing and responding to cyber incidents.

Panel I: Cooperation Between Europe and Africa

The main aim of this panel was to identify and address the cybersecurity cooperation needs, current trends, good practice, innovative approaches and lessons learned to identify common challenges across the regions. Emphasized by all speakers was the common challenge of identifying partnerships that are productive while creating a more efficient cybersecurity ecosystem. Well-functioning cyber partnerships must rely on trust, mutual and clear goals, frequent communication, adaptability, and leadership at both the technical and political level. Additionally, in order for a nation, or region, to develop a diverse cybersecurity ecosystem with embedded cooperation mechanisms, it is essential that all stakeholders understand the defined purpose. Outlining a clear purpose and buy-in from various national actors can be a challenge both within Europe and Africa.

Europe and Africa also face the same daily cybersecurity challenges, the possibility of attacks, security threats, vulnerabilities on critical assets, etc. The readiness of individual countries, however, varies throughout both continents. While some may have the right infrastructure and frameworks in place to deal with these attacks, not all do, and it is important to create partnerships that work to elevate the readiness of the whole. Partnership organizations like SmartAfrica, European Cyber Security Organization, and AfricaCERT work to put the correct policy, regulatory, and technical teams in place to encourage collaboration and reduce potential effects of cyber-attacks. Partnerships between governments and the private sector are also critical for success as these businesses have the capacity to innovate and invest in research and development often beyond the means of the government. Finally, capacity building efforts that work to address the cyber skills gap, both within the technical fields, and the general public, are critical to ongoing cybersecurity efforts. An environment where all citizens are better prepared for cyber-attacks, and understand basic cyber hygiene principles would significantly impact the resiliency of the cybersecurity ecosystem.

Important Notes

- Collaboration within cybersecurity is extremely important, and new strategic plans for increased cooperation must complement existing efforts. A well-functioning partnership depends on set of attributes: trust, defined purpose, clearly articulated goals, measurable progress and outcomes, leadership involvement at the technical and political levels, clear and frequent communication, flexibility and adaptability.
- Interregional exchanges can be strengthened with diversified team collaborations. Groups should have varied maturity levels, economic backgrounds, political associations, etc. and work jointly on technical projects and knowledge exchange.
- Preventing cyber-attacks is impossible as they continue to evolve at a rapid pace. Instead, both African and Europe should aim to work towards for higher resilience. Resilience, especially, is a cross border effort that governments and non-state actors can work on collaboratively to elevate the general readiness of all cyber efforts.
- National CIRTs are an essential tool in a national cybersecurity strategy, and information exchange between national CERTs can only be further encouraged.

Panel II: Critical Information Infrastructure Protection, Identifying and Sharing Good Practices

Within the cyber threat landscape protecting Critical Information Infrastructure (CII) is an incredible task that varies state to state. While often these sectors are siloed within their approach to cybersecurity, it is essential for the overall security of CII to acknowledge their interconnectedness. The greater the connection, the greater the dependency, and therefore the greater potential impact of a security incident on essential government services. Assessing impact, however, cannot just be done at the traditional service level. Considering a broader view of impact that includes the economy, citizens, public trust and confidence, reputation, essential services and health helps to better map the potential effect of a cyber incident.

Using national risk assessments to identify CII and essential digital services is a key component in protecting critical information infrastructure, and should be integrated with other assessments to help shape National Cybersecurity Strategies. Risk assessment outcomes can also help governments to prioritize initiatives, and therefore allocate essential investment and resources to the most at-risk industries. Building a community where the system as a whole is evaluated (people, processes, informational technology, and facilities) allows for targeted capacity building trainings, exercising, and testing, to help mitigate the larger CII risk. Countries that have not updated national cybersecurity strategies, however, or continued to perform risk assessments throughout the COVID-19 pandemic should consider doing so as the digital priorities and risks of governments and citizens have changed dramatically over the past two years.

Important Notes

- Critical information infrastructure risk must be seen as an intersection of overall impact and overall likelihood. In order to properly assess the overall risk, analysis at the service/integrated system level provides the best context.
- National impact level definition specificity is essential for identifying the critical information infrastructure in each member state, and thus tailoring risk assessments.
- The national CII risk assessment should be integrated with other critical assessments to help shape a National Cybersecurity Strategy. For example, the capacity maturity model assessment, the national cyber risk assessment, and capacity building programmes and projects.
- Cybersecurity threats are becoming more complex: a complex and non-transparent supply chain, an increase in devices online instigated by the COVID-19 pandemic, new viruses, poorly educated cyber-hygiene practices of the general public, etc.
- Cybersecurity threats have increased in severity over the past year, with over 50% of threats being logged critical in nature compared with medium or high in Moldova.
- Efficient cybersecurity governance must include improvement of technological resources used in proactive and reactive threat measures, education of citizens, legal framework that is able to be constantly adapted, and international cooperation.
- No government has the resources to tackle cybersecurity without partnership from the private sector, and international organizations.
- Modern governments cannot operate without access to CII which are mostly Internet dependent. Acknowledging that this puts critical operations and assets at risk, allows for better preparedness and resilience planning.

Key Takeaways

The COVID-19 pandemic has thoroughly demonstrated that though digital technology is a critical enabler of social and economic development, it must become the foundation upon which economic and social resiliency is built in order to carve out a more equitable, prosperous and

sustainable future for all. The interregional meetings at the 2021 CyberDrill provided an opportunity for member state and organizational representatives to offer their expertise on both global and regional cybersecurity issues, to report upon successful collaboration projects, and to highlight cooperation opportunities in the future. Specifically, an emphasis on the need for stronger official cooperation mechanisms between member states and that have made significant steps towards creating confidence and security of ICT use by governments, businesses, and the general public, and those member states that are at the beginning of that path.

The exchange of experiences and knowledge between the African and European continent is an opportunity to reinforce human and institutional capacity to further secure cyberspace by building trust and confidence. A continued investment in regional partnerships and involvement with organizations like ITU, SmartAfrica, and ECSO are encouraged to recognize the role they play both regionally and globally to enhance cyber resilience.