Global Cyber Policy Dialogues: Southern Africa

October 31-November 1, 2022
Pretoria (Tshwane), South Africa

MEETING MATERIALS

international relations & cooperation
Department: International Relations and Cooperation
REPUBLIC OF SOUTH AFRICA

Ministry of Foreign Affairs of the Netherlands

ORF AMERICA

RESEARCH ICT AFRICA

Monday, October 31

Venue: Department of International Relations and Cooperation of South Africa

10:00-10:30 REGISTRATION

10:30-10:45 WELCOME REMARKS

Zaheer Laher, Chief Director, Political, Peace and Security, Department of International Relations and Cooperation of South Africa
Bruce W. McConnell, Distinguished Fellow, Observer Research Foundation America

10:45-11:15 OPENING REMARKS

Wopke Hoekstra, Minister of Foreign Affairs of the Netherlands *(via prerecorded message)*
Nozipho Mxakato-Diseko, Ambassador at Large, Peace and Security, Department of International Relations and Cooperation of South Africa
Nathalie Jaarsma, Ambassador-at-Large, Security Policy and Cyber, Ministry of Foreign Affairs of the Netherlands

11:15-12:30 SESSION I: IMPLEMENTING THE UNITED NATIONS NORMATIVE FRAMEWORK

In 2021, two United Nations processes released consensus reports containing recommendations, norms, and principles for improving stability and security in cyberspace, namely: the UN Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE). Their agreed upon norms, confidence building measures, and capacity building principles have large implications for participating governments as they set their own policies and strategies. But participation in these processes was not universal nor is the implementation of their agreed framework. More work must be done to involve underrepresented countries in these processes and to promote the work that has already been done. This session will raise awareness about what has been agreed at the international level, bridging gaps between the diplomatic communities and other stakeholders, and identify opportunities for increased engagement in the negotiations and implementation of outcomes.

Moderator: **Bruce W. McConnell**, Distinguished Fellow, Observer Research Foundation America

Speakers: **Moliehi Makumane**, Researcher, United Nations Institute for Disarmament Research (UNIDIR); Former South African Expert to the UN Group of Governmental Experts and Open-ended Working Group
Sheetal Kumar, Head of Global Engagement and Advocacy, Global Partners Digital
Noëlle Van der Waag-Cowling, Cyber Program Lead, Security Institute for Governance and Leadership in Africa (SIGLA), Stellenbosch University

12:30-13:30 LUNCH

13:30-14:45 **SESSION II: INTERNATIONAL COOPERATION TO COMBAT CYBERCRIME**

Additional processes are taking place at the international level to foster cooperation to combat cybercrime and improve global response. In 2021, the Intergovernmental Expert Group on the Problem of Cybercrime (IEG) issued a report with consensus recommendations on international cooperation, capacity building and prevention. A new UN "Ad Hoc Committee to Elaborate a Comprehensive International Convention on countering the Use of Information and Communications Technologies for Criminal Purposes" held its first substantive meetings in 2022. Furthermore, the UN OEWG and GGE report contain norms and principles that are relevant to promoting better international cooperation on the issue of cybercrime. There are also instruments, including the Budapest Convention on Cybercrime and the African Union Convention on Cyber Security and Personal Data (Malabo Convention), which contribute model frameworks and instruments that can be used to prevent, respond to, and prosecute cybercrime. In Southern Africa as well as globally, increased digitization has brought not only economic benefit, but also opportunities for criminals to take advantage of uneven access, limited resources, low cyber literacy, and jurisdictional questions to prey on citizens and businesses alike, thereby undermining trust in ICT tools and their stability.

This session presents an opportunity to outline a way forward towards the practical implementation of the 2021 Kyoto Declarations in the area of cybercrime and cybersecurity. We will explore how the principles agreed upon at the 14th UN Crime Congress are relevant for cyber development in Southern Africa, highlighting specific connections between the norms and development goals, taking into account the ongoing negotiations for an international legally binding instrument on cybercrime at the UN Ad Hoc Committee.

Moderator: **Bruce W. McConnell**, Distinguished Fellow, Observer Research Foundation America

Speakers: **Terlumun George-Maria Tyendezwa**, Vice-Chair, UN Ad Hoc Committee on Cybercrime
Joseph Mauggo, Regional Prosecutions Officer, National Prosecutions Service of Tanzania
Ronel le Grange, Head of Electronic Communications, Communications Regulatory Authority of Namibia (CRAN)
Uchenna Jerome Orji, Assistant Professor of Law, American University of Nigeria; Fellow, African Center for Cyberlaw and Cybercrime Prevention

14:45-15:15 NETWORKING BREAK

15:15-16:45 **SESSION III: RESILIENCE IN CYBERSPACE**

As reliance on technology increases, so too must the resilience of its systems. The ability for services to withstand accidents and attacks and recover quickly is necessary for their secure adoption by the general public. This is particularly important when they are used by under-served communities, who may rely on technology for access to banking, communication, or government services. Building capacity to use technology is important, but it must go hand in hand with a capacity to keep the technology operable and secure throughout its use. One potential source of this is cooperation between Computer Emergency Response Teams

(CERTs), who have ample opportunities to promote intra-regional cooperation and share information on the threat landscape. They are not the only source, however. National strategies and policy frameworks need to consider ways to promote resilience in technology systems, but also in the organizational practices that guide the humans that manage those systems. Likewise, the private sector, as the designer and implementer of so many digital innovations, must build resilience in its own systems. This session will explore ways to build resilience vertically within countries but also horizontally across borders as stakeholders work with their counterparts throughout Southern Africa. It will pay particular attention to ways that systems can be built resiliently from the beginning as new infrastructures are put in place in the region.

Moderator: **Bruce W. McConnell**, Distinguished Fellow, Observer Research Foundation America

Speakers: **Christopher Banda**, Head of CERT, Malawi Communications Regulatory Authority (MACRA)
Codjo Roland Aikpe, Senior Analyst, Cybersecurity, National Agency for the Security of Information Systems of Benin
Kaleem Ahmed Usmani, Head, CERT Mauritius
Nick Small, Regional Coordinator, EU Cyber Resilience for Development (EU Cyber4Dev)

16:45-17:00 **SUMMARY AND SCENE-SETTING FOR DAY 2**

Sorene Assefa, Founder and Managing Director, Cyber Czar

18:30-20:30 **RECEPTION HOSTED BY THE AMBASSADOR OF THE KINGDOM OF THE NETHERLANDS TO SOUTH AFRICA**

Tuesday, November 1

Venue: Department of International Relations and Cooperation of South Africa

08:30-09:00 REGISTRATION

09:00-09:15 **DAY 2 OPENING REMARKS**

Enrico Calandro, Senior Research Associate, Research ICT Africa

09:15-10:30 **SESSION IV: BUILDING MEANINGFUL PUBLIC-PRIVATE PARTNERSHIPS FOR CYBERSECURITY**

Cyberspace is a multistakeholder environment, and thus digital development, cybersecurity, and cyber stability require engagement from not just governments, but civil society, academia, and the private sector. In previous virtual meetings, the private sector in particular was highlighted as an important partner to increase capacity to improve cybersecurity and advance development. However, more meaningful conversation with the private sector, both large tech companies and

smaller more regional and local companies, is needed to examine what kind of roles they can play and how governments can create an enabling environment for meaningful partnership in meeting cyber challenges. In the context of the international processes on cybercrime and cybersecurity, this session will explore the role of the private sector in creating and advancing cybersecurity maturity in Southern African countries. Participants will examine what conditions are necessary to create public-private partnerships that address these challenges while encouraging innovation, establishing good governance of the digital space, and bolstering respect for human rights online.

Moderator: **Enrico Calandro**, Senior Research Associate, Research ICT Africa

Speakers: **Nnenna Ifeanyi-Ajufo**, Vice-Chair, African Union Cyber Security Expert Group (AUCSEG); Associate Professor of Law and Head of Law, Buckinghamshire New University
Susan Potgieter, Lead, Cybersecurity Program and Banking CSIRT, South African Banking Risk Information Centre (SABRIC)

10:30-11:00 NETWORKING BREAK

11:00-12:15 **SESSION V: CYBER CAPACITY BUILDING FOR SUSTAINABLE DEVELOPMENT**

It has become clear that improving cyber capacity and reducing digital divides is a prerequisite for achieving the goals contained in the 2030 Sustainable Development Agenda. To achieve these goals, new capacities must be built in infrastructure, education and literacy, and governance. This session will explore the value of cyber capacity building efforts for sustainable development, discuss implementing the results of international processes, examine past success, and outline priorities for capacity development that underpin both sustainable development and cybersecurity. It will aim to take best practices learned from existing examples and seek to apply them to new situations, while always keeping in mind the value of meaningful cooperation between governments as well as through public-private partnerships.

Moderator: **Enrico Calandro**, Senior Research Associate, Research ICT Africa

Speakers: **Kiru Pillay**, Chief Director, Department of Communications and Digital Technologies of South Africa
Nthabiseng Pule, Project and Outreach Manager, Cybersecurity Capacity Centre for Southern Africa (C3SA)
Kathleen Bei, Research and Working Groups Coordinator, Global Forum on Cyber Expertise (GFCE)

12:15-12:45 **CONCLUDING REMARKS**

Andrew Rens, Senior Research Fellow, Research ICT Africa
Nathalie Jaarsma, Ambassador-at-Large, Security Policy and Cyber, Ministry of Foreign Affairs of the Netherlands

12:45-13:45 LUNCH

The Department of International Relations and Cooperation of South Africa and the Ministry of Foreign Affairs of the Netherlands, in partnership with the Observer Research Foundation America and Research ICT Africa will be hosting an in-person Global Cyber Policy Dialogues: Southern Africa meeting on October 31-November 1, 2022, in Pretoria, South Africa. This multistakeholder meeting will bring together attendees from across Southern Africa as well as some experts and stakeholders from outside the region. Participants and speakers will come from government, civil society, academia, and the private sector. This meeting also highlights the commitment of the governments of South Africa and the Netherlands to cooperate on cyberspace-related matters in the region.

Virtual preparatory meetings were held in October of 2020 and 2021 to lay the groundwork for this event, and summaries of both the 2020 and 2021 meetings are available to provide further background. Through the course of these virtual meetings, several issues were raised with particular relevance for the Southern Africa region. First, digital transformation is integral to Southern Africa's future, and cybersecurity is a necessary component of this digital revolution. Therefore, it is crucial that development efforts are linked to cybersecurity and human rights. Second, with digital transformation comes increased opportunity for misuse of ICTs, and thus concerted efforts are needed to tackle cybercrime and other cyber threats. This includes building awareness and capacities among users, law enforcement, and policymakers, as well as implementing laws that contribute to improved resilience and accountability for crimes while protecting human rights in the digital space. Third, digital transformation in Southern Africa can fundamentally alter the way that states interact with each other and their own citizens. Cyber technologies can be misused, undermining international trust and stability, and threatening to hamper digital development gains. International processes to create norms of behavior and mechanisms for improving trust in cyberspace, including confidence building measures, can be useful to guard against these risks. Participation by Southern African states in the United Nations processes on ICTs, peace and security, cybercrime, and other digital issues is important to ensure that the outcomes of these processes reflect models of governance and priorities of Southern African countries.

In order for Southern African countries to reap the benefits of digital transformation and avoid a regime of digital colonialism where rules are set without their input and digital resources are gleaned by foreign companies and governments, existing capacity gaps in the technical, policy, and governance spheres must be addressed. This includes capacities to participate and engage in the processes at the United Nations. It also includes capacities to build, maintain, and operate secure digital infrastructure from the technical side, as well as on the governance side in terms of creating and implementing policies and laws that respect security, inclusivity, accessibility, and fundamental rights in the digital space. Identifying opportunities for partnerships across sectors and regions, and finding new methods of collaborating will be key to addressing the challenges associated with digital transformation.

This meeting will look at capacity challenges as fundamental components of cyberspace security in a variety of specific contexts and identify concrete actions towards developing a regional approach to equitable, inclusive, and secure digital transformation that contributes to improved trust and cooperation in cyberspace. It will also examine ways to improve collaboration and coordination across borders to address persistent problems and better take advantage of existing capacities. To these ends, the meeting will:

1. Examine how the implementation of the UN normative framework on responsible state behavior in cyberspace can support the development goals of Southern African countries
2. Build awareness and discuss how Southern African states and stakeholders can participate more effectively in the UN processes on responsible state behavior and cybercrime
3. Outline Southern African priorities for peace and stability in cyberspace

4. Identify capacity gaps in Southern African countries, especially related to the implementation of the normative framework
5. Explore structures and processes necessary for building national capacities and regional cooperation among states and stakeholders, including the private sector, particularly related to digital resilience and cybercrime