Global Cyber Policy Dialogues: Southern Africa

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

MEETING SUMMARY

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

Ministry of Foreign Affairs of the Netherlands

ORF AMERICA

RESEARCH ICT AFRICA

On October 31-November 1, 2022, 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 (ORF America) and Research ICT Africa, held an in-person roundtable in Pretoria, South Africa, as part of its Global Cyber Policy Dialogues series. The meeting focused on improving the security and stability of cyberspace and building cyber capacity in Southern Africa in several key areas. The meeting brought together over 60 participants from across Southern Africa representing government, civil society, academia, multilateral institutions, and the private sector. It also served to highlight 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 the protection of 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, to implement technological and security standards 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.

Accordingly, the 2022 meeting examined capacity challenges as fundamental components of cyberspace security in a variety of specific contexts and identified concrete actions towards developing a regional approach to equitable, inclusive, and secure digital transformation that contributes to improved trust and cooperation in cyberspace. It also explored ways to improve collaboration and coordination across borders to address persistent problems and better take advantage of existing capacities.

This two-day event was convened as part of the Global Cyber Policy Dialogue Series, a project undertaken by ORF America and the Ministry of Foreign Affairs of the Netherlands. This project consists of regional meetings which seek to address key cyber challenges, strengthen multistakeholder networks, and increase coordination of regional capacity building initiatives. These meetings are intended to complement ongoing international-level cyber processes, such as the United Nations Open-ended Working Group and the Ad Hoc Committee tasked with elaborating a "comprehensive international convention on countering the use of information and communications technologies for criminal purposes".

The discussions took place under the Chatham House Rule. Opening remarks for the meeting were provided by Mr. Zaheer Laher, Chief Director: Political, Peace and Security at the Department of International Relations and Cooperation of South Africa; Nozipho Mxakato-Diseko, Ambassador at Large for Peace and Security at the Department of International Relations and Cooperation of South Africa; and Nathalie Jaarsma, Ambassador-at-Large for Security Policy and Cyber of the Ministry of Foreign Affairs of the Netherlands.
The first day was moderated by Bruce W. McConnell, Distinguished Fellow at ORF America. The second day was moderated by Enrico Calandro, Senior Research Associate, Research ICT Africa.

October 31

Implementing the United Nations Normative Framework

The first session of the event sought to raise awareness about what has been agreed at the United Nations Group of Governmental Experts (UN GGE) and the United Nations Open-ended Working Group (UN OEWG), bridge gaps between the diplomatic communities and other stakeholders, and identify opportunities for increased engagement in the negotiations and implementation of outcomes. In 2021 these two UN Working Groups adopted consensus reports containing recommendations, norms, and principles for improving stability and security in cyberspace. Their agreed-upon outcomes, including international law, 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, and more work must be done to involve underrepresented countries in these processes.

The session began with remarks by Moliehi Makumane (UNIDIR), Sheetal Kumar (Global Partners Digital), and Noëlle Van der Waag-Cowling (Stellenbosch University). The discussion highlighted recent progress made in the United Nations processes, where negotiations currently stand and what issues remain. Southern African countries are particularly engaged in the processes but, like in most regions of the world, implementation of the norms needs to be strengthened. In Southern Africa, capacity gaps have proven to be significant barriers to this so there needs to be a stronger focus on next steps: instead of implementing everything at once, states should work in areas where they have capacity and buy-in. The norms on the respect for human rights and privacy (13e), cooperation against cybercrime and terrorism (13d), and on the protection of critical infrastructure (13g) were singled out as good candidates for earlier implementation in Southern Africa.

Despite engagement from Southern African countries on the normative framework at the United Nations, there remains a need to engage all sectors of society in the process of creating and implementing the normative framework. Success will require engagement from civil society and the private sector in all Southern African countries and this is only possible if they feel a sense of ownership over the decisions made. Similarly, human-centric approaches, those that prioritize rights and increase trust in the system, are necessary to enact the kind of holistic approach that is needed to get implementation right. A successful holistic approach will also understand that cybersecurity touches all aspects of society: making systems more resilient and preventing cybercrime are just as much part of implementing the normative framework as they are separate topics of discussion.

International Cooperation to Combat Cybercrime

The second session of the event focused on ways to effectively fight cybercrime and coordinate global responses to it. Numerous international and regional processes exist to foster international cooperation among law enforcement agencies and judicial authorities. Chief among these is the new UN "Ad Hoc Committee to Elaborate a Comprehensive International Convention on countering the Use of Information and Communications Technologies for Criminal Purposes" which held its first substantive meetings in 2022, but others exist as well. In 2021, the Intergovernmental Expert Group on the Problem of Cybercrime (IEG), chaired by South Africa, issued a report with consensus recommendations on international cooperation, capacity building, and prevention. Additionally, the UN OEWG and GGE reports 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 Protection (Malabo Convention), which contribute model frameworks and instruments that are widely used to prevent, respond to, and prosecute cybercrime.

The session began with remarks by Terlumun George-Maria Tyendezwa (Vice-Chair on behalf of the Africa Group to the UN Ad Hoc Committee on Cybercrime), Joseph Mauggo (National Prosecutions Service of

Tanzania), Ronel le Grange (Communications Regulatory Authority of Namibia), and Uchenna Jerome Orji (African Center for Cyberlaw and Cybercrime Prevention). The discussion explored the existing instruments to foster cooperation and ways that they can help law enforcement and other government agencies successfully prosecute cybercrime. The Ad Hoc Committee was singled out in importance because of its role in fostering greater international cooperation but also in highlighting the value of existing conventions and resources. These processes are designed to be collaborative and iterative, and they work better with more participation. Regional instruments such as the Malabo Convention on Cyber Security and Personal Data Protection and the Budapest Convention on Cybercrime were also heavily featured in the discussion. Regarding the latter, experts discussed both the importance and challenges of engaging with a treaty designed specifically for another region (in this case, Europe) but noted that it had practical value in specific areas such as its discussion on information sharing and data integrity. Its potential synergy with the Malabo Convention was also noted, but it is too soon to tell because the Malabo Convention has not yet come into effect. The effect of many of its provisions (as well as ways to improve them) will not become clear until after it is ratified by two more African states to make the required 15 ratifications to come into force. South Africa indicated its intention to sign and ratify this Convention during the 2023 Ordinary Session of the African Union in January 2023.

Participants also stressed the need to think beyond international negotiations and formal agreements and focus on the practical matters of dealing with individual crimes. The need for more formal (and informal) channels between regional law enforcement agencies and judicial authorities was of particular concern: cybercrime is a global problem and without close cooperation between agencies, it becomes easier for criminals to exploit gaps between jurisdictions. At the same time standards of evidence must be maintained. It is not enough to share information between law enforcement, it must be done through proper channels, with data integrity, and in a timely fashion. Similar to the normative framework, there is a need to take a holistic approach to solving cybercrime as well. Civil society's role as an educator to improve cyber hygiene and advertise the dangers of cybercriminals as well as regulators' and policymakers' role in reducing the vulnerabilities that make cybercrime possible were noted as they often get forgotten in conversations about cybercrime.

Resilience in Cyberspace

The third session of the event focused on building a more resilient cyberspace, which has become ever more important as reliance on technology has increased especially among 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. Computer emergency response teams (CERTs) are a key component of building such capacity due to their responsibility to deal with threats and the opportunities they present to foster intra-regional cooperation and information sharing. National strategies and policy frameworks are also important ways that governments can promote resilience, and the private sector, as the designer and implementer of digital innovation, is also a critical pillar of support.

The session began with remarks by Christopher Banda (Malawi Communications Regulatory Authority), Codjo Roland Aikpe (National Agency for the Security of Information Systems of Benin), Kaleem Ahmed Usmani (CERT Mauritius), and Nick Small (EU Cyber4Dev). Participants noted the numerous achievements in CERT cooperation recently: the Botswana National CERT and Malawi National CERT have signed an agreement showing cross-national cooperation for sharing information on cyber threats, and CERT Mauritius launched MAUSHIELD, an open-source platform for sharing cyber threat intelligence in real-time. Despite these successes, challenges remain of course. Only 26 countries in Africa have national CERTs, so for many countries, improving resilience will need to start with creating one. Additionally, there is a need to integrate resilience into national cyber strategies, as well as create more robust methods of communication and points of contact between existing CERTs. The new Botswana-Malawi agreement and MAUSHIELD represent the early steps on a path to greater CERT cooperation.

Participants noted the need to view resilience as a journey: it is not an end state but a constantly changing pursuit. It is also a pursuit that is particularly impacted by shortages of capacity in Southern Africa. CERTs are not the only stakeholder on this journey; resilience must be built vertically within a country and horizontally between them and that requires engagement with other stakeholders. Lack of accessible educational resources and lack of interest in pursuing cybersecurity careers, or a disconnect between education and professional requirements, limit the pool of talent necessary to make cyberspace more resilient. There is also the danger of paralysis in starting new cooperative endeavors focused on resilience: many new efforts get bogged down in defining threats or creating frameworks and never get off the ground. Each sector will have its own different requirements on what is necessary to start cooperating on improving resilience, but participants agreed that the best path forward was to get started however possible and refine the process along the way.

November 1

Building Meaningful Public-Private Partnerships for Cybersecurity

This session explored the role of the private sector in creating and advancing cybersecurity maturity in Southern African countries, in particular, it examined the conditions necessary to create public-private partnerships to help improve cybersecurity in Southern Africa. Numerous international processes and instruments suggest or require governments to work closely with private sector counterparts, among these the 3rd session of the UN Ad Hoc Committee and the Malabo Convention, particularly Article 26. Deeper and more meaningful connections between the public and private sectors are a necessity to improving capacity and creating sustainable development. But critical questions remain about what these partnerships will look like and how to create an environment that is mutually beneficial.

The session began with opening remarks by Nnenna Ifeanyi-Ajufo (AUCSEG) and Susan Potgieter (SABRIC). A major topic of discussion was the necessary conditions for effective partnerships between the public and private sector: questions about whether collaboration should be through a normative, obligatory, or hybrid model were heavily discussed. As with many things, a common issue is lack of trust and accountability, both of which can be increased through greater transparency. Governments do not trust that the private sector will be a reliable partner, and companies do not trust that governments will place any value in the partnership. Consultation, early and often, was noted as a potential way to avoid this issue as well as clear methods of accountability within a formal mechanism. All parties need to come to the table knowing what they would like and communicate clearly with each other. Each partnership should look different and be guided by different frameworks and relationships based on the participants and goals.

At the same time, there was focus on the way that this session connected with the others. It will be impossible to implement the normative framework, create workable cybercrime solutions, and promote resilience without significant buy-in from the private sector. Both Ghana and Mauritius have led the way in this regard by creating sectoral CERTs that bring together different stakeholders from a specific sector to work holistically on cybersecurity issues, of which SABRIC in South Africa is also an example.

Civil society is also often underrepresented in conversations about partnerships. These organizations have much to learn from their counterparts but can also be helpful in building capacity for the government and companies, and can also allow them to reach new constituencies. There is a danger in thinking that you need capacity to enter into these partnerships (particularly on the part of civil society organizations), but in many cases, participating in public-private partnerships is the best way to build that capacity. There was consensus that civil society organizations can play a meaningful role in protecting internet freedoms and fundamental human rights.

Cyber Capacity Building for Sustainable Development

A core prerequisite of many of the previous sessions was the need to have additional cyber capacity. Without additional capacity in Southern Africa, it will be difficult to create sustainable development, produce new infrastructure necessary for improved connectivity, have access to the talent needed to make cyberspace resilient, implement the normative framework, and reduce susceptibility to cybercrime. This session explored the value of cyber capacity building, examined past successes, and outlined priorities and next steps.

The discussion began with remarks by Kiru Pillay (Department of Communications and Digital Technologies of South Africa), Nthabiseng Pule (Cybersecurity Capacity Centre for Southern Africa), and Kathleen Bei (GFCE). Experts shared numerous ongoing success stories in capacity building and drew lessons from them. Among these were Africa's School of Internet Governance (AfriSIG), Cybersecurity Capacity Centre for Southern Africa (C3SA), CyberSmart Botswana, and the Global Forum on Cyber Expertise (GFCE). Participants noted the need to decouple training efforts from specific stakeholder interests, the need to keep gender and cultural dynamics in mind when making programs and to have wide engagement from the start, as well as the value of building upon existing frameworks and institutions. Access was also stressed. Without making the tools of capacity building broadly accessible, it will not provide equitable gains to societies.

Trust again was a key issue here. Without ownership and transparency, efforts are likely to be hamstrung from the start. Instead, capacity building partnerships should be demand-driven to ensure that both sides of the relationship feel a degree of ownership on the process and that localization of content and shared values are accounted for. In order to help foster this, South-South, North-South, and triangular cooperation should be considered when starting new capacity building programs to take advantage of different points of view. Similarly, efforts should be thought of as iterative processes that further the cybersecurity strategy and posture of a country; capacity building needs to be seen as a necessary part of these national initiatives. As part of that, capacity building must be institutionalized and become continuous otherwise it will not be a sustainable effort. Similar to resilience, capacity building is a journey with no end state.

Concluding Remarks

Concluding remarks at the end of the conference provided an overview of themes from the dialogue, including the normative framework, cybercrime, CERT cooperation and the role of CERTs, the need for and challenges to public-private partnerships, and effective means of building the capacities necessary to tackling all of these challenges. Lack of equitable access, jurisdictional issues, low cyber literacy, and better laws and policies were challenges that repeatedly arose from the discussion but participants agreed that there were numerous viable paths forward for each. Furthermore, Southern Africa is a cooperative environment with governments working together on issues related to capacity challenges, law enforcement, and resilience. The discussions identified several areas for potential future research or projects which are outlined below.

Implementing the United Nations Normative Framework:

- **Consider a more human-centric approach**: Norms implementation needs to be human rights-based. Governments have a responsibility to their citizens and if they do not take that seriously when implementing norms, they won’t be able to build the trust necessary to do so. Implementation is not a top-down action that can be imposed on society, but must be a conversation that takes a whole-of-society approach.
- **Focus on actionable norms to build momentum**: Implementation of the entirety of the normative framework is a daunting challenge and states should focus on components that can be more easily implemented to build momentum. Norms 13d (cybercrime and terrorism), 13e (human rights) and 13g (critical infrastructure protection) were suggested as good starting points for Southern African countries.

- **Think beyond government implementation**: Government has an important role to play in the implementation of the normative framework, but it is not the only role. Civil society and the private sector are critical players, but their roles are often ignored. Work needs to be done to ensure that they are aware of their part in implementation and that they feel a sense of ownership and buy-in to the norms.

International Cooperation to Combat Cybercrime:

- **Improve and strengthen international engagement on cybercrime**: Cybercrime is an international problem with national implications. Without international cooperation, criminals can commit crimes with impunity as long as they are not based in the country they are targeting with their crime. In order to prevent this, agencies must develop the tools to work together in a timely manner while respecting each other's legal requirements (such as maintaining evidence integrity or protection of human rights).
- **Think beyond law enforcement in combating cybercrime**: Cybercrime is a societal problem and requires societal solutions. Just as law enforcement agencies have a role in catching cybercriminals after they have committed crimes, regulators and policymakers have a role as well. Regulators can work to make cyberspace safer by helping to reduce vulnerabilities in sectors they oversee, and policymakers have an active role in engaging with citizens and creating more effective legal frameworks for law enforcement to use.
- **Engage with civil society and the public**: There is an important role for civil society in educating the public on the dangers of cybercrime. Cyber hygiene and literacy are important components of preventing crime at the source and more efforts need to be put into creating programs to improve these throughout the Southern Africa region.

Resilience in Cyberspace:

- **Improve formal and informal communication between CERTs**: CERTs look at a global threat landscape and it is critical to their efforts to have the most up-to-date information. Sharing between CERTs can help them gain access to that information, but structures for sharing information effectively remain in early stages. Work should be done to improve these as quickly as possible, especially as new national CERTs are created in Southern Africa. At the same time, because relationships and trust are so important to effective communication, CERT leaders should work to instill cultures of informal sharing to supplement, but not replace, the formal structures wherever possible.
- **Center resilience in national cyber strategies**: Cyber resilience is not something that can be left up to CERTs alone; they need help from other government agencies and society at large. As governments create and update their national cyber strategies, they should be sure to consider resilience throughout: it should not be a separate topic but a component of every cyber conversation.
- **Create more educational opportunities for cyber talent**: Building resilience often requires technical skills. Without access to appropriate talent, it can prove impossible to create resilience. Care needs to be taken to create the educational resources in each country to ensure that there is access to the talent necessary in the future to build and maintain resilience. This requires cooperation between government, civil society, and academia to ensure those resources exist and the opportunity is available to all.

Building Meaningful Public-Private Partnerships for Cybersecurity:

- **Engage early and often**: Ensuring that all members of the partnership trust each other and the structures that they are building is critical to continued success. Consultation when creating structures and ongoing discussion about how partnerships are working and any changes that need to be made should be regular. Governments should refrain from unilaterally creating structures for partnerships with the private sector and then inviting them to join; it must be collaborative from the start.

- **Customize solutions for their specific problem**: Every partnership will look different. In some industries informal structures will work best when connecting with government counterparts; in others (such as financial services or law enforcement) there are strict legal requirements that must be followed when partnering. Each relationship can and should look different to tackle the problems that are facing the members, and creators should refrain from cookie-cutter approaches to public-private partnerships.

Capacity Building for Sustainable Development:

- **Take advantage of different points of view**: It is important to incorporate different points of view when creating capacity building programs. Regional, gender, and cultural dynamics should be considered when crafting programs to avoid alienating local audiences and to ensure that the program will be inclusive and beneficial for everyone. No two capacity building programs should look the same; they should be customized for the audience they are working with.
- **Engage with the local community when creating programs**: Often capacity building programs are designed by external funders or organizations without input from people on the ground of those receiving the training. Instead, those who design these programs should change their frame of reference: programs should be demand-driven and build the capacities that are required by those in the region. Without this, there is likely to be a lack of buy-in at the local level and an inability to sustainably build the capacities actually desired.
- **Build on success to sustain political will**: Capacity building efforts should be incorporated into the national strategies and policy frameworks to ensure that political will does not evaporate. As part of this, care should be taken to build the capacities necessary for those frameworks to succeed so that future efforts can build upon first successes.

Sorene Assefa from Cyber Czar assisted in the preparation of this summary.