Global Cyber Policy Dialogues: Southern Africa

October 27, 2020
15:00 SAST

Meeting Summary

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

Ministry of Foreign Affairs of the Netherlands

EastWest INSTITUTE

RESEARCH ICT AFRICA

Meeting Summary

On October 27, the Department of International Relations and Cooperation of South Africa and the Ministry of Foreign Affairs of the Netherlands, in partnership with the EastWest Institute and Research ICT Africa, hosted the Global Cyber Policy Dialogues: Southern Africa meeting. Participants explored challenges and opportunities for building an inclusive, secure, safe and resilient cyberspace in the Southern African region around three pillars critical to stability and growth in the digital realm: sustainable development, peace and security, and governance.

This event reflects the commitment of the governments of South Africa and the Netherlands to support regional cooperation in Southern Africa on cybersecurity, and is intended to serve as a precursor to a more comprehensive in-person conference to be held in South Africa in 2021. The dialogue is also part of a Global Dialogue Series being undertaken by the EastWest Institute, which aims to convene regional meetings to address capacity building around key cyber challenges and complement ongoing international cyber norms processes.

The October 27 Southern Africa meeting featured speaker contributions on the three pillars of the dialogue and included opportunities for exchange with representatives from governments, businesses, civil society organizations and universities from Southern Africa and beyond. In total, over 70 attendees from twelve Southern African countries and nine countries outside the region participated in the dialogue.

The following sections briefly summarize the speaker contributions and characterize the discussions, which took place under the Chatham House Rule. The meeting was moderated by Bruce W. McConnell, President of the EastWest Institute.

OVERVIEW OF KEY POINTS

Enrico Calandro, Senior Research Associate, Research ICT Africa

The meeting focused on inclusiveness, equity, safety, security and resilience, and included a broad geographic base of attendees. There were many similarities in the challenges outlined by speakers such as skills gaps, lack of Internet access, digital divides and missing infrastructure investment, as well as the potential for development and digitalization to lead to bigger challenges if carried out without due regard for ensuring cybersecurity, improving the knowledge of users and mitigating potential threats to freedom of expression, privacy and safety. While each of these has their own solutions, one key theme that emerged throughout the presentations was the need for international cooperation to tackle cyberspace's complex challenges. To that end, presenters gave many avenues to foster and strengthen cooperation such as public-private partnerships, the UN Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG), the Global Forum on Cyber Expertise (GFCE), and a number of more focused fora such as the Intergovernmental Expert Group on the Problem of Cybercrime (IEG). The need to work through these issues in a collaborative, consensus-driven, multistakeholder way that builds trust, whether through these fora, or bilaterally as exemplified by this meeting, was the key goal that united all of the presenters and participants.

INTRODUCTORY REMARKS

Francis Moloi, Acting Deputy Director-General, Global Governance and Continental Agenda, Department of International Relations and Cooperation of South Africa

Both South Africa and the Netherlands share a determination to contribute to the development of international law, norms, standards, and values and recognize the need to collectively address the global challenges of cyberspace, especially using the mechanisms of the United Nations. The benefits and threats of cyberspace cannot be viewed separately from larger questions of global peace and sustainability. Any discussion about digitalization in Southern Africa needs to take place within this context as well as one of inclusion, accessibility and usability. Poverty, inequality and unemployment are key challenges in the Southern African region that cyber excellence could help mitigate if the principles of the Fourth Industrial Revolution are embraced.

Cyber development is a shared responsibility to be taken up by governments, the private sector and civil society together; one that is necessary to fully achieve the Sustainable Development Goals. Because security must accompany development, all governments must remain engaged in the existing governance mechanisms to build partnerships that transcend existing national and regional boundaries.

Alison Gillwald, Executive Director, Research ICT Africa; Adjunct Professor, Nelson Mandela School of Public Governance, University of Cape Town

Digital inequality is no longer just about connectivity. It now exists not only between those offline and online but also between those with limited and full access to cyberspace. The primary determinant of access is education with a correlating determinant of income; therefore, access is limited by factors related to poverty. This is a classic demand-side development challenge, which will require coordination between the public and private sectors to tackle the larger issues rather than a simple focus on increasing access.

It is also important to discuss technical issues such as cybersecurity and data protection in a context of developing countries. Best practices are often modelled on more mature markets and then implemented in countries that do not have the resources to match. Likewise, global policies and governance need to address the local issues that face these developing economies.

Most pushes for development do not take into account the risks that digitalization exacerbates. The rise of the Internet as a global public good requires new forms of global cooperation, and developing countries, who are often invisible in these discussions, must navigate complementary and competing systems of governance. But Internet governance and cybersecurity are only as strong as their weakest link, therefore, taking into account the opinions of African and other developing nations, becomes critical as these global governance policies take shape.

SUSTAINABLE DEVELOPMENT

Esther Mwema, Founder and Chief Strategist, Digital Grassroots

COVID-19 has amplified the demand to bridge the digital divide in Southern Africa, and resulted in rapid digitization efforts in order to keep economies afloat, particularly in urban areas. The increase in mobile phone ownership has improved Internet penetration and consequently strengthened voices demanding equality through social media. Digital innovation is also creating opportunities for social mobility and autonomy, especially for young people and women, but some capacity challenges still remain.

There is a pressing need for skills training to allow the entire population to take advantage of the Internet, not only as a tool of empowerment, but also for economic reasons. In many areas, especially rural ones, there is a

need for improved infrastructure to provide more Internet bandwidth. However, competition policies must be carefully crafted to avoid monopolistic practices by the companies investing in that infrastructure. There also needs to be a focus on online safety: as social media supplants real, human connections, the psychosocial and emotional consequences of cyber bullying, revenge porn and reduced self-confidence, particularly for women, often prevent equal participation.

There are three priorities for addressing the needs on the ground. First, governments should keep the Internet on. Free speech should be protected and digital citizenship must be built in a way that respects privacy and the protection of personal information, and governments that shut down the Internet must be held to account. Second, investments in digital skills training and capacity building should be focused at the grass roots level and carried out in ways that support local innovation and autonomy. Third, policymakers and implementers should collect and disaggregate data on ICT access and use, and digital policies should take into account the specific challenges that marginalized and vulnerable groups (e.g. young people, persons living with disabilities, the LGBTQ community and women) face in joining the digital economy.

Susan Potgieter, Head, Strategic Services, South African Banking Risk Information Centre (SABRIC)

There has never been a better time to explore partnerships between the public and private sectors to strengthen resilience at both the regional and global levels. The pandemic has shown how quickly people can adapt to using the Internet; this momentum should be maximized towards improving cybersecurity through additional training and education. Expanding access to the Internet must be balanced with education for people to understand how to protect themselves, which is why SABRIC has partnered with the South African National Cybersecurity Hub on initiatives to create awareness for good cyber hygiene, improve cyber skills and educate the public on crime risks. Additionally, the costs of protection for users must be factored into the creation of security policies to increase compliance. For example, users with limited resources will be less likely to download a security update for their phone if it uses the last of their limited data.

The financial sector is known for optimizing technology: digital financial products have dominated innovation for some time now. With the good, however, comes the bad. Without proper risk management, digitalization and the Internet of Things increase the attack surface exponentially to the benefit of cyber criminals. Hence, public-private partnerships are important. Governments have the authority to create regulations that protect the national interest and citizens, which helps create trust in ICT, while the private sector has a responsibility to offer safe and secure digital services. If they work together, there can be good security standards that keep compliance costs manageable.

PEACE AND SECURITY

Karen Allen, Senior Research Advisor and Head of Emerging Threats, Institute for Security Studies (ISS)

In order to harness the potential of the digital revolution, we need to understand the risks. One of the biggest risks is defining threat actors and threats too narrowly. Most cybersecurity efforts are focused on technical aspects, for instance network intrusions, but cyber threats should be understood as more of an ecosystem with many possibilities and perils.

One example within this ecosystem are the risks associated with biometric surveillance. These systems include not only cameras and facial recognition, but also AI algorithms and centralized government databases which contain highly sensitive information. Potential risks associated with these systems include algorithmic bias, data theft (which is amplified by centralized databases where cyber criminals can access large amounts of data), and "function creep," where cyber tools designed for one purpose are repurposed without appropriate safeguards or oversight. In addressing these issues, policymakers must balance freedom of expression and the right to

privacy while being cautious about bulk surveillance becoming a norm and threatening democratic institutions. In countries like South Africa with a strong civil society, questions about some of these risks are already being raised.

Other peace and security threats in the cyber ecosystem include information operations, mobilizing social media platforms by malicious actors and the weaponization of drones. Social media platforms have already been used to manipulate elections in South Africa, Madagascar and Kenya, and hate groups have tapped these platforms to gain access to larger audiences and activate real world consequences on touchstone issues.

South Africa is working hard to counter both cyber crime and cybersecurity threats. Despite new laws on cyber crime and personal data protection as well as significant involvement in UN processes, South Africa still faces capacity challenges particularly in enforcement and prevention. As it, and other developing countries, rely on outside help for building digital infrastructure and the foundations of digital economies, they should take care not to trade away the data of its citizens or import norms contrary to democratic values.

Moctar Yedaly, Head, Department of Information Society, African Union Commission

Digital transformation is a requirement for the survival of Africa, but also remains a geopolitical challenge. It will happen whether African countries desire it or not. Digitization will touch many sectors and it is important to have cross-sector conversations to prepare for it.

The race for data collection will inform the economy of the future. African leaders must know that the industries of the future will be artificial intelligence, advanced life sciences, the development of algorithms for behavioral manipulation and especially big data. Data has become the geography of future markets, and these markets must be mastered. Because of this it must also be acknowledged that, whether it is morally good or reprehensible, any data that can feasibly be collected, likely will be.

The current geopolitical climate is characterized by a Cold War 2.0. While the European Union is looking for new positions in its alliances with Africa and fights with international tech companies, the U.S. and Russia are seeking to counterbalance their strategic retreat through domination of the Internet economy and tools of destabilization respectively. This new Cold War is based on the tools of cyber warfare, but states are losing power as networks are increasingly controlled by large corporations. Players who have emerged from this new economy, such as data centers and smart manufacturing, are racing to see how much they can control. Most of these companies and platforms are non-African and they are motivated by profits on the continent. If Africans wish to stay out of this race, they must create safeguards.

African leaders need to act swiftly to avoid digital colonization by enhancing their capacity and reducing knowledge gaps. To this end, the African Union has been pushing for the ratification of a convention on cybersecurity, electronic transactions and personal data protection as well as advocating for the adoption of cybersecurity strategies and CERTs in each African country.

GOVERNANCE

Nathalie Jaarsma, Ambassador-at-Large, Security Policy and Cyber, Ministry of Foreign Affairs of the Netherlands

Trust is an important precondition for the use of digital technology for development. Trust is needed between governments and citizens, between companies and citizens, and between companies and governments. All malicious behavior in cyberspace erodes that critical trust. There are three ways to build trust in the face of

these challenges: multilateral norms development, international cooperation in countering cyber crime and capacity building.

On the first, there has been great success in the work of the UN norms processes such as the GGE and the OEWG as well as the general acknowledgement that international law applies in cyberspace. But much work remains to be done to reach an understanding of how international law applies, and to create the accountability needed to hold malicious actors in check.

Secondly, international cooperation is required to counter cyber crime. UN processes such as the IEG has been invaluable in promoting the sharing of information and best practices. The Netherlands is also aware that many states see the need to negotiate a new treaty on cyber crime through the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the use of ICTs for Criminal Purposes, but it is important that anything new builds on the experience and expertise of existing instruments and is pursued through an international process that is based on consensus, inclusivity, transparency and respect for fundamental freedoms.

Finally, capacity building is needed to level the unequally distributed development of cyberspace which currently amplifies vulnerability in an interconnected world. The Global Forum on Cyber Expertise (GFCE) stands as a model in this field by bringing together its 100 state, civil society members and the private sector to identify needs, pool resources and expertise.

Doctor Mashabane, South African Representative to the UN Group of Governmental Experts; Chair, Intergovernmental Expert Group to Conduct a Comprehensive Study of the Problem of Cybercrime

The IEG has generated more interest in solving cyber crime challenges. In order to do so, states need to understand their capabilities, before they begin to address the gaps. The IEG's report will focus on electronic evidence, criminal justice, law enforcement and investigation, prevention, and criminalization to help determine where those gaps are as well as understand the complex nature of this global challenge. The groups' recommendations will be discussed at the IEG's stocktaking exercise in 2021. In the meantime, it is encouraging to see that approximately 16 African states have cyber crime strategies and that they generally agree on the principles of international cooperation, public-private partnerships, rule of law, harmonization, accountability, a multistakeholder approach and governance.

Cyber crime is just as important a topic as international cyber policy, and it should be discussed in international groups such as a the GGE and OEWG, and also at the regional and subregional level. Here we see interesting work from the African Union and there is hope that the work will also be replicated in the South African Development Community (SADC).

Cybersecurity frameworks should not be designed from a threat-centric lens, but from the perspective of higher ambitions: economic benefit, social prosperity, resilience and safe ICT environments, regional security and international influence. The UN is the center of gravity on all matters of global concern so it is important that it plays a leading role in norms development and cyber crime prevention.

DISCUSSION

Throughout the event participants posed questions to speakers and offered their thoughts on the presentations. The notion of the Internet as a public good, even as it is built and controlled by companies that are focused on profit, was discussed as one potential way to ensure more equitable digital development. Participants also engaged with the idea that the COVID-19 pandemic, while revealing the ways we are

dependent on technology and related threats, may present an opportunity to integrate cybersecurity (and cybersecurity capacity building) as a foundational element for sustainable development. As such, participants questioned the maturity of the cybersecurity legislative landscape on the African continent, as initiatives such as the African Continental Free Trade Area are being taken forward without much emphasis on digital trade as of yet. Cyber policy capacity building was also specifically addressed as a priority for international efforts, to ensure that African countries are able to have sufficient voice in cybersecurity discussions.

Further discussion focused on the nexus of cybersecurity and development. Questions were raised about whether and how African-owned technology companies are investing in cybersecurity or looking at innovative ways to make security compliance less costly for users. Focusing on the differentiated impacts of cybersecurity on women and marginalized groups was highlighted as a way to ensure that digital-enabled development is holistic and addresses the needs of people who are not prioritized by for-profit corporations or governments. Finally, the presenters were asked about the feasibility of cooperation in cyberspace in an already contentious international environment. While it was acknowledged that agreement and cooperation on these issues will be difficult and require time, the risks are simply too great. All countries are only as safe as the most vulnerable, and thus there is no other option but to work together.