CYBER CONFLICT PREVENTION ON THE EU-AFRICA SECURITY AGENDA

Co-organised by the EU Institute for Security Studies and the Portuguese Presidency of the Council of the European Union

10 May 2021, Online event

In 2020, the European Union outlined its vision for a more comprehensive EU-Africa partnership focused on digital transformation and peace, security and governance, among others. These two aspects gain particular relevance in the context of the COVID-19 pandemic which makes cooperation between the two regions critical - both to ensure the suitable conditions for a sustainable and resilient recovery as well as to counter the challenges and negative security spill-overs. Yet, the link between the stability of the cyber domain and international security has so far remained largely unexplored in the dialogue between EU and Africa, despite the fact that Africa remains the primary theatre for the EU-led CSDP missions and operations.

The use of cyber means in the midst of an ongoing conventional conflict is not the only way a cyber conflict can play out. The focus on attacks above the threshold of the 'use of force' and an 'armed attack' has progressively allowed for a more tacit challenge to emerge: malicious cyber activities that damage state infrastructure, the economy or institutions over an extended period of time. While initially cyber-specific in nature, these situations can lead to the escalation of a political conflict. Cyber-attacks can also target the key elements of internet infrastructure which now forms an indispensable element of modern societies: telecommunications networks (radio, telephone lines, undersea cables, satellites), information systems, as well as the processes and protocols underlying the use of the above can all be subjected to attacks. Such activities might destroy or severely affect the proper functioning of these systems (the use of ransomware against hospitals is one example). These hostile activities may involve cyber-specific units, the equivalent to combat arms in traditional conflicts, but states also do not shy away from making use of proxy groups as part of their cyber campaigns. The high risk of miscalculation and the escalatory potential of seemingly 'harmless' cyber operations are the reasons why the prevention of conflict in cyberspace plays such a critical role. The more we learn to understand conflict as a manifestation of the failed management of mutual disagreements, the better the chances are for crafting effective and timely measures of conflict prevention.

The EU and its African counterparts have a well-established pattern of cooperation on international security issues. The recently established European Peace Facility offers a new opportunity for further strengthening this cooperation. However, the discussion about conflict prevention and stability in cyberspace has so far remained largely unexplored. How can the EU and Africa leverage their ongoing security dialogue and cooperation to better coordinate and cooperate on topics such as responsible state behaviour in cyberspace, with particular focus on countries where cybersecurity threats are the highest or the global venues where their cooperation can be most impactful? Recognising that digital economic growth and development need to go hand in hand with increased cybersecurity and resilience, the main questions that this conference aims to address are the following: How can the EU and the African partners build a comprehensive and strategic security agenda fit for the digital age? How can they work better to preserve the value of multilateral institutions as fully representative and legitimate venues for international negotiations and global governance?

PROGRAMME

10:00-10:10

OPENING REMARKS

Gustav LINDSTROM

Director, EU Institute for Security Studies

10:10-10:40

ROUNDTABLE DISCUSSION

Chair

Patryk PAWLAK

Brussels Executive Officer, EU Institute for Security Studies

Speakers

Joanneke BALFOORT

Director, Security and Defence Policy, European External Action Service

Moliehi MAKUMANE

Assistant Director, Department of International Cooperation, South Africa

Camino KAVANGH

Visiting Senior Fellow, King's College London; Non-resident Fellow, Carnegie Endowment for International Peace

10:40-11:45

INTERVENTIONS FROM PARTICIPANTS

Chair

Janne TAALAS

CEO, CMI – Martti Ahtisaari Peace Foundation, Finland

11:45-12:00

CLOSING REMARKS

Luís BARREIRA DE SOUSA

Ambassador for Cyber Issues, Ministry of Foreign Affairs, Portugal