Outline

Module objectives

Welcome to the knowledge module on cyber diplomacy and international cooperation, as part of the GFCE-Africa project.

This knowledge module discusses emerging cybersecurity risks for international peace and security, introduces the existing international framework for responsible state behaviour in cyberspace, maps the major diplomatic and multistakeholder processes that shape this agenda, and reviews experiences related to establishing national cyber diplomacy capabilities.

The Cyber Security Policy and Strategy theme may be understood as the 'foundation' for the other identified themes in the GFCE Global Agenda for Cyber Capacity Building.

Recognising the importance of cyber norms and cyber diplomacy, the GFCE Working Group A, which discusses policy and strategy issues, has created a Task Force 'CBMs, Norms Implementation, and Cyber Diplomacy'.

See more at:
https://thegfce.org/working-groups/working-group-a/

By the end of this module, you will be able to respond to and find additional resources for the following questions:

- How can cyberattacks impact national economies and political relations? Why are cyberattacks used for military and political gains? Are states developing their offensive cyber capabilities?
- What are the current 'rules of the road' for states in cyberspace? (How) Does international law apply to cyberspace?
- What are the norms? How do they interplay with international law? How to implement them across African states?
- What are the confidence-building measures (CBMs)? What is the significance of regional CBMs? What are the main cyber capacity-building principles set by the UN?
- What is the link between human rights and cyber norms? How does cybersecurity impact economic development and SDGs?
- What is the history of the negotiations and dialogue under the UN? What are the current and possible future elements of the institutional dialogue? What other major diplomatic and political processes have cybersecurity elements on the agenda?
- What are the major instruments developed on regional levels? How can those instruments assist African developments?
- What is the value of multistakeholder discussions for cyber diplomacy efforts? Which are the most relevant multistakeholder fora that African states should be engaged with?
- Is cyber diplomacy about cybersecurity only?
- What role non-state stakeholders play in cyber diplomacy, especially at the regional levels? Why is inclusiveness of stakeholders important for reaching meaningful agreements?

- What are the skills that cyber diplomats require? What are the skills that other stakeholders need to contribute to cyber processes? (Why and how) Should diplomats and non-diplomats work together? What is the role of other stakeholders?

1 Risks for international peace and cyber stability

> *I am absolutely convinced that, differently from the great battles of the past, which opened with a barrage of artillery or aerial bombardment, the next war will begin with a massive cyberattack to destroy military capacity ... and paralyse basic infrastructure such as the electric networks.*
> António Guterres, UN Secretary-General (Reuters, 2018)

There are growing concerns that cyberattacks could be used for, or escalate into, cross-border conflicts. In this part, we will look into major cases of cyberattacks that had economic and political consequences, the role of cyberattacks and disinformation as part of hybrid warfare, and trends with cyber-armament of countries.

1.1 Cyberattacks and geopolitics

- □ *How can cyberattacks impact national economies and political relations?*

Dozens of cases of cyberattacks have had serious consequences for global and regional economies, well-being, and political relations. These include distributed denial of service (DDoS) attacks and hacks that paralyse critical national infrastructures, cases of political and economic espionage, ransomware operations, stealing massive amounts of personal data, surveillance operations, as well as regional provocations, cyberattacks conducted to support warfare, and conventional strikes in response to cyberattacks.

Figure 1 maps key examples of such major events from the past 20 years. This is not a comprehensive review but serves as an illustration of some important examples, types of attacks, and possible effects.

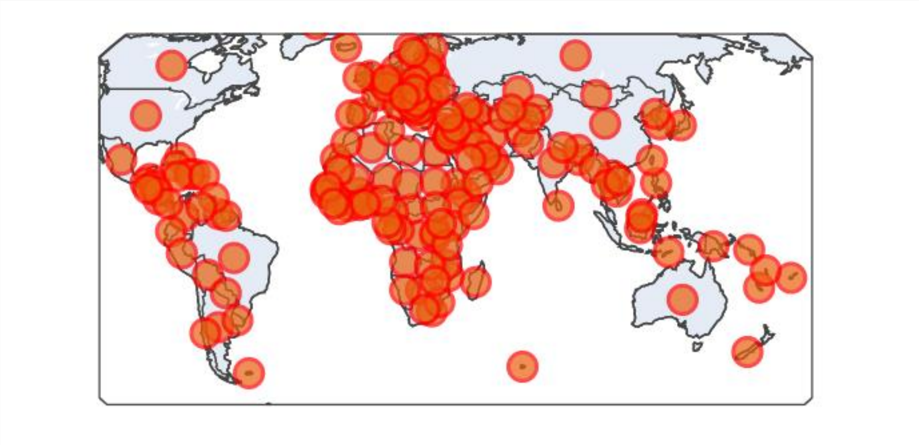

Figure 1: Interactive map of some major cyberattacks with political backgrounds and consequences ([DiploFoundation](), 2022)

□ **Reflection point**

Are there relevant examples from your region? What were the targets? What were the political and economic consequences?

Leave your comment below.

1.2 Cyber as part of hybrid warfare

- □ *Why are cyberattacks used for military and political gains?*

The Munich Security Conference perceived cyberattacks as an important segment of hybrid warfare back in 2015 (Munich Security Conference, 2015).

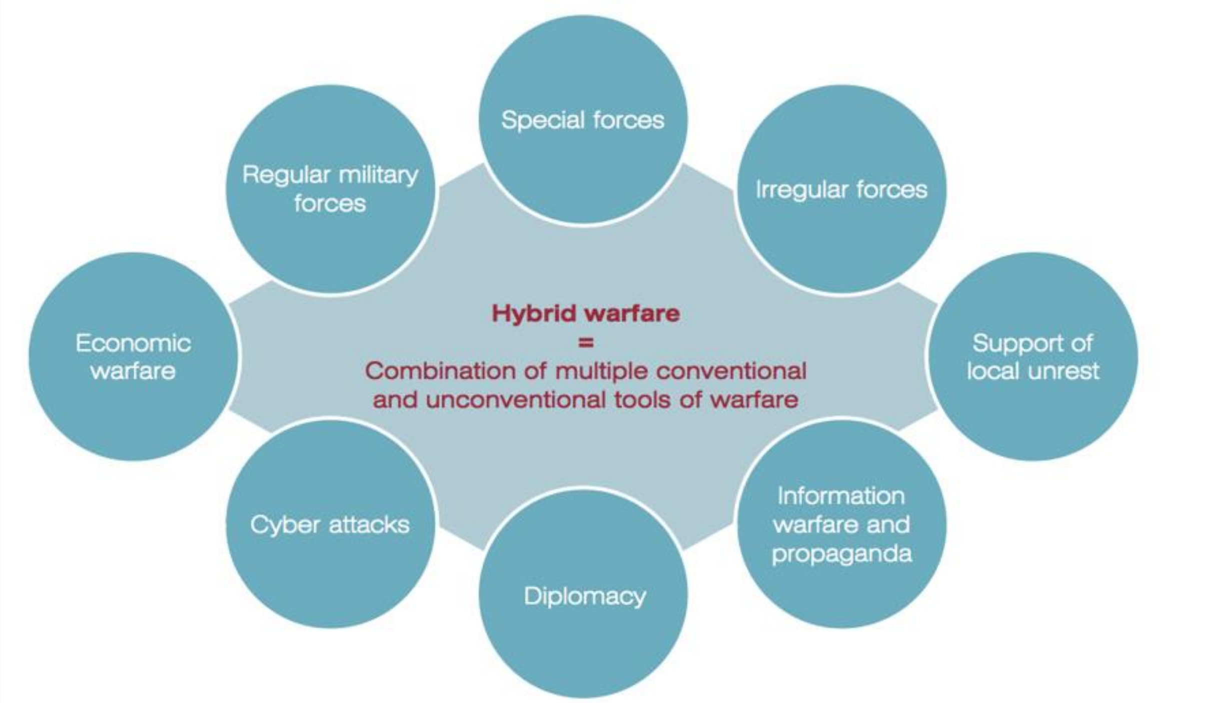

Figure 2: Cyberattacks are one of the important components of hybrid warfare (Source: Munich Security Conference, 2015)

On the one hand, this means cyberattacks may, in future, be used in combination with conventional operations. On the other hand, cyberattacks become popular means of weakening the opponents – particularly in 'peacetime' (short of the criteria of armed attack in conventional understanding) – due to being able to be customised for particular activities (from espionage to disrupting digital systems without causing physical damage, even to disabling physical industrial facilities, but without casualties), and even more due to deniability (high complexity of attribution).

In addition to conducting cyberattacks, states turn to information warfare using digital platforms. In practice, this often takes the form of disinformation campaigns targeting interference with elections, efforts to combat diseases (as witnessed during COVID-19 pandemic), or causing political division and unrest. While the deceptive use of information for hostile purposes has a long history, the internet, and especially the social media, allow for an near-instant targeting and manipulation of masses at rather low costs. Some countries have already embedded threats from malign influence and information campaigns, propaganda, and disinformation into their national strategies.

1.3 Cyber-armament

- *Are states developing their offensive cyber capabilities?*

Incidents of cybersabotage or cyberespionage have accelerated cyber-armament. NATO considers cyber to constitute one of the five military domains (along with land, sea, air, and space). Many countries have established significant budgets for building military cyber capabilities, both offensive and defensive. The mapping of publicly available documents, such as national strategies, military doctrines, official statements, and credible media reports, presents evidence and indications that offensive cyber capabilities (OCCs) exist or are being built in over 50 states (figure 3).

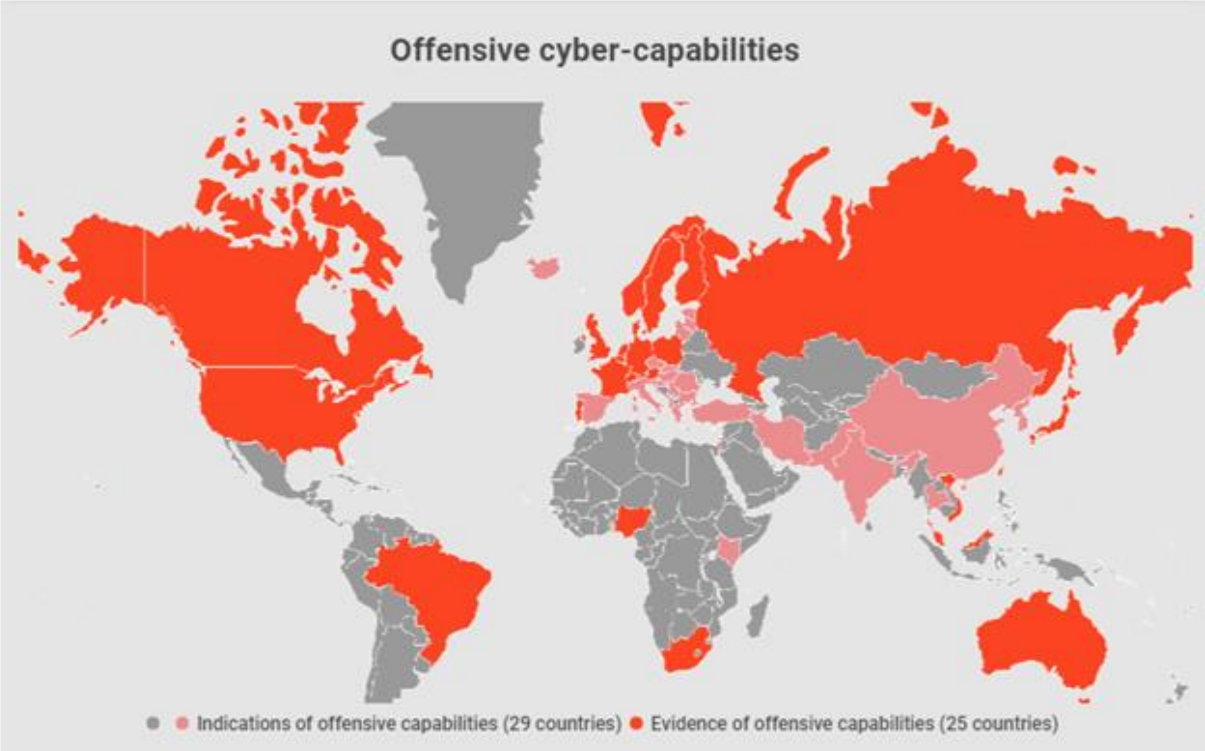
Offensive cyber-capabilities
● ● Indications of offensive capabilities (29 countries) ● Evidence of offensive capabilities (25 countries)

Figure 3. Interactive map of states with offensive cyber capabilities (DiploFoundation, 2021)

□ **Reflection point**

Is your country developing offensive cyber capabilities? How transparent are the plans for development and deployment of OCCs?

Leave your comment below.

2 Towards an international agreement

The fact that potential future cyberattacks, while possibly causing widespread destruction, could also initiate conventional warfare, has fuelled initiatives to codify diplomatic response, as well as to disentangle the challenges of the application of international law to cyberspace and formulate a framework for responsible state behaviour.

Negotiations in this context fall into three main areas:

- Criteria for entering a war or invoking *jus ad bellum* ('right to war', i.e. the body of international law governing the right of states to resort to war), and in particular, how principles and specific articles of the UN Charter apply to cyberspace.
- International humanitarian law or *jus in bello* ('law in war', i.e. laws that govern the conduct of conflict), in particular, how to apply The Hague Conventions and the Geneva Conventions in cyberspace.
- Weapons and disarmament, and questions like how (and if) to introduce cyberweapons into the disarmament process.

Even though, for many countries, these issues are new at the foreign affairs agenda, they have been discussed within the UN context since 1998. A brief history of the UN cyber processes is illustrated in video 1, while more details are discussed later in the module.

[Embed video: https://www.youtube.com/watch?v=JbMn_9uzxfk]

Video 1. An Animated History of United Nations Cyber Processes. (UNIDIR, 2021)

Besides clarifying how international law applies to cyberspace, the UN deliberations have also discussed how to address peacetime incidents, for example, cyberattacks that fall under the threshold of armed attacks. In this regard, a set of voluntary norms, confidence-building measures (CBMs), and capacity-building principles have been developed by the UN and regional organisations.

2.1 Framework for responsible state behaviour in cyberspace

- □ *What are the current 'rules of the road' for states in cyberspace?*

The UN negotiations have given birth to a framework for responsible state behaviour in cyberspace (further referred to as the Framework), consisting of four pillars: international law, norms, CBMs, and capacity building (video 2).

[Embed video: https://ad-aspi.s3-ap-southeast-2.amazonaws.com/2020-09/UN-framework_ENGLISH.mp4]

Video 2. UN framework on responsible state behaviour in cyberspace (ASPI, 2020)

The framework is defined by the body of existing international agreements under the UN (informally known as the "*acquis*", reminding of the term used as a reference to the EU's body of laws), in particular the reports of UN Group of Governmental Experts (GGE) and the UN Open-ended Working Group (OEWG).

The proposed UN General Assembly (UNGA) Resolution A/C.1/76/L.13, tabled jointly by the USA and Russia in autumn 2021, clarifies that the two core instruments which should guide states in their use of information and communication technologies (ICT) are:

- The 2021 report of the Open-ended Working Group (OEWG) (UNGA Res. A/75/816)
- The 2021 report of the Group of Governmental Experts (GGE) (UNGA Res. A/76/135)

In addition, the resolution reiterates the importance of the three previous consensus reports of the GGE: from 2010 (A/65/201), 2013 (A/68/98* and A/RES/68/243), and 2015 (A/70/174 and A/RES/70/237).

□ **Resources**

Ambassador Jürg Lauber, Permanent Representative of Switzerland to the United Nations and other Organizations in Geneva, gave a 'masterclass' interview for 'Inside Cyber Diplomacy' podcast. In his discussion with Jim Lewis and Chris Painter, he shared experiences from his work as Chair of the OEWG, how his previous UN experience helped him increase engagement in the process, and where to go from here.

Similarly, Ambassador Guilherme Patriota, Brazil's Consul General in Mumbai and Chair of the UN GGE on Advancing responsible State behaviour in cyberspace in the context of international security, gave an interview for 'Inside Cyber Diplomacy' podcast. There, he discussed the influence his past negotiating experience had in how he chaired the group, how they had to adjust to negotiating during Covid to achieve a consensus report, and whether his future plans will involve ICTs.

2.2 Applicability of international law

- □ *(How) Does international law apply to cyberspace?*

According to the Framework, states agree that existing international law and the UN Charter apply to cyberspace. Established international law regulates the conduct of armed conflict and seeks to limit its effects.

It is, however, less clear how it applies in practice and in particular circumstances. The UN Charter, as the foundation of the body of international law that provides grounds to justify entry into a conflict, grants (Article 51) the right of individual or collective self-defence if an armed attack occurs against a member state. Yet, what exactly is an armed attack and use of force in cyberspace – and what is its threshold? Is it limited to attacks that cause physical damage and injury, or would other effects (e.g. financial, environmental, economic, or political) of a cyberattack fall under it as well? When (and if) does a cyberattack violate another state's sovereignty? Should the attacked state be allowed to respond by any and all means, including all out military options with traditional warfare methods?

It is equally hard to understand how the international humanitarian law (IHL) governing the use of force in armed conflicts, such as protecting civilian populations and infrastructure, will apply. For years, states failed to reach an agreement about whether the IHL applies at all or whether its application would actually militarise cyberspace. It was only in 2021 that the GGE confirmed that the IHL applies only in situations of armed conflict, thus, not in peacetime. The GGE also says that applying the core IHL principles to the use of ICTs needs further study.

One of the main challenges is how to hold states accountable for their operations, from reliably attributing the attack, to responding without risking the escalation of political tensions. Invoking international law provisions, and using elements of the Framework, is of relevance when raising a responsibility of certain states for a cyberattack, and holding states accountable for their cyber operations. The 2021 GGE report in particular provides space for progress since it prescribes elements for the attribution of cyberattacks, i.e. 'the incident's technical attributes; its scope, scale, and impact; the wider context, including the incident's bearing on international peace and security; and the results of consultations between the States concerned' (UN GGE, 2021, Par. 24).

The most authoritative and comprehensive research that discusses the applicability of international law to cyberspace and the related challenges is the Tallinn Manual on the International Law Applicable to Cyber Warfare, developed in 2013 by an independent international group of experts who were invited by the NATO CCDCOE. It was updated in 2017 - dubbed the Tallinn Manual 2.0.

□ Contribute and engage

The CCDCOE invites experts to contribute to the development of the Tallinn Manual 3.0. Your country experts may seek options to engage and contribute.

The UN GA resolutions of 2021 related to the reports of the GGE and the OEWG invite states to share their own positions on how international law applies to cyberspace. Indeed, an increasing number of states are developing and publishing their national positions. A good overview of open issues and general positions of states on the applicability of international law is available at the Digital Watch Observatory.

□ Resources

The Cyber Law Toolkit is a dynamic interactive web-based resource for legal professionals who work with matters at the intersection of international law and cyber operations. The Toolkit may be explored and utilised in a number of different ways. At its core, it presently consists of 25 hypothetical scenarios. Each scenario contains a description of cyber incidents inspired by real-world examples, accompanied by detailed legal analysis. The aim of the analysis is to examine the applicability of international law to the scenarios and the issues they raise.

□ **Reflection point**

Is there awareness about the existing framework and the related processes in your Ministry of Foreign Affairs, and in your government more generally? Are there already discussions about a national position related to the applicability of international law to cyberspace, as invited by the UN GA?

Leave your comment below.

2.3 Norms, confidence-building measures, and capacity building

2.3.1 Voluntary norms

- □ *What are the norms?*
- □ *How do they interplay with international law?*
- □ *How to implement them across African states?*

Norms present standards of behaviour, shaped through terms of rights and obligations. Though non-binding, they reflect expectations, increase predictability, reduce risks of misperceptions, and contribute to conflict prevention.

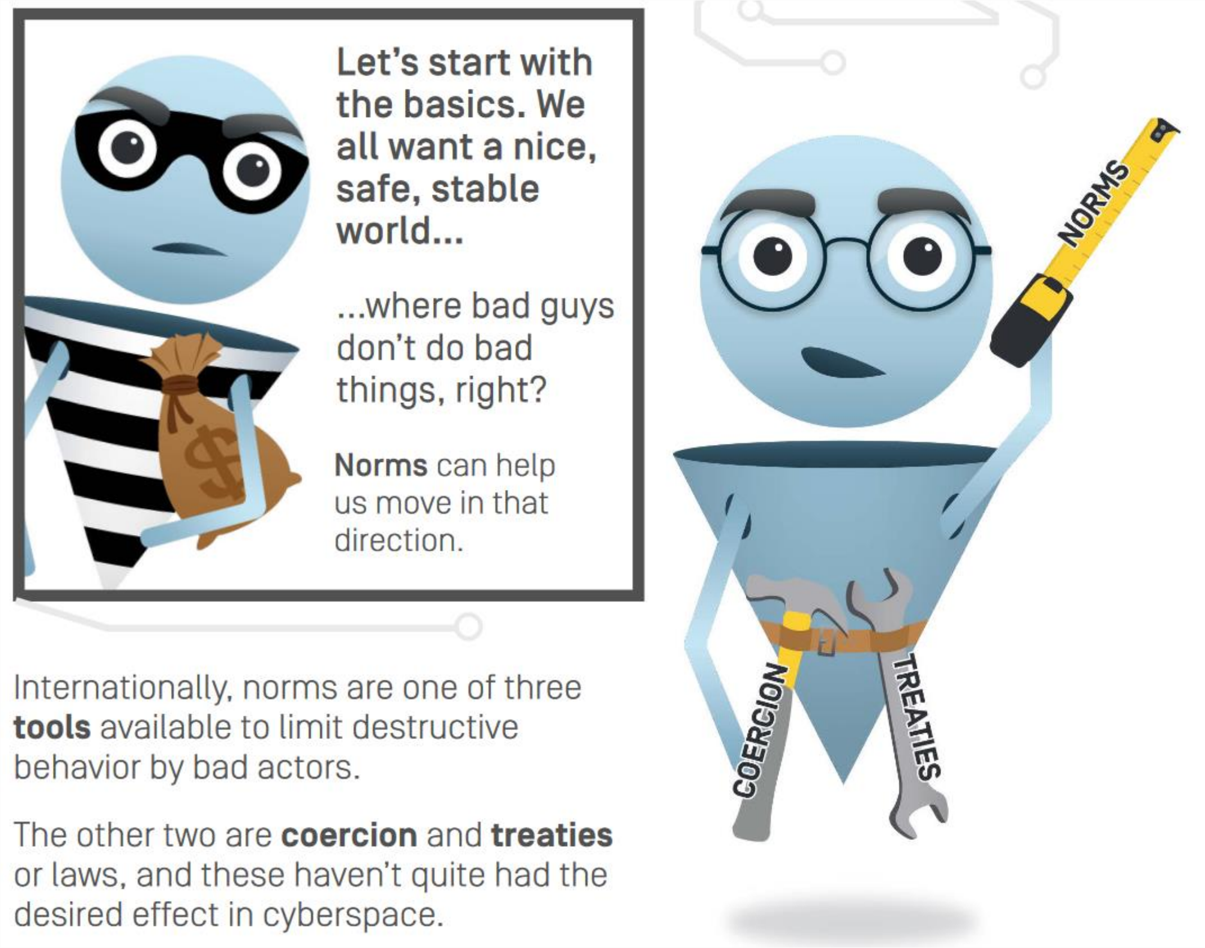
Let's start with the basics. We all want a nice, safe, stable world...
...where bad guys don't do bad things, right?
Norms can help us move in that direction.
Internationally, norms are one of three **tools** available to limit destructive behavior by bad actors.
The other two are **coercion** and **treaties** or laws, and these haven't quite had the desired effect in cyberspace.
NORMS
COERCION
TREATIES

Figure 4: Professor Cy Burr's Graphic Guide to: INTERNATIONAL CYBER NORMS (New America, 2016)

While not replacing binding obligations of states under international law, the norms and principles agreed on by the UNGA have the highest authority. In the context of cyberspace, norms are particularly important for peacetime operations to address aspects that are not sufficiently or clearly covered by existing international law.

The Framework outlines and elaborates on 11 norms for responsible state behaviour in cyberspace (figure 5).

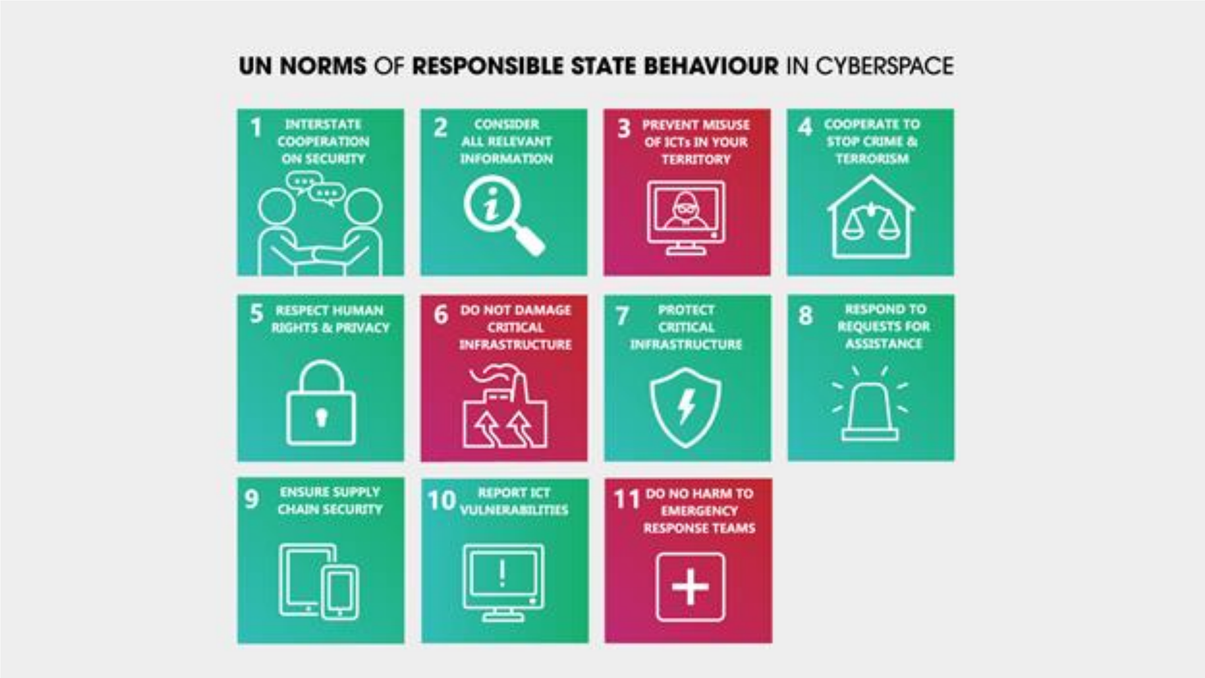
UN NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE
1 INTERSTATE COOPERATION ON SECURITY
2 CONSIDER ALL RELEVANT INFORMATION
3 PREVENT MISUSE OF ICTs IN YOUR TERRITORY
4 COOPERATE TO STOP CRIME & TERRORISM
5 RESPECT HUMAN RIGHTS & PRIVACY
6 DO NOT DAMAGE CRITICAL INFRASTRUCTURE
7 PROTECT CRITICAL INFRASTRUCTURE
8 RESPOND TO REQUESTS FOR ASSISTANCE
9 ENSURE SUPPLY CHAIN SECURITY
10 REPORT ICT VULNERABILITIES
11 DO NO HARM TO EMERGENCY RESPONSE TEAMS

Figure 5. Eleven UN norms for responsible state behaviour in cyberspace adopted by the UN GGE in 2015 (ASPI, 2020)

□ **Case study**

"Putting Cyber Norms in Practice: Implementing the UN GGE 2015 recommendations through national strategies and policies", a report written by Mika Kerttunen and Eneken Tikk, commissioned by the GFCE with support from the UK FCDO through the Global CCB Research Agenda 2021 process, provides number of case studies to showcase approaches that can be, and have been, adopted to implement norms of responsible state behaviour which are part of the Framework. The guide includes notable examples from African countries as well.

Mauritius, for instance, has undertaken number of steps towards stopping crime and terrorism, which have directly contributed to implementing the UN GGE norm on cooperating to stop crime and terrorism (13(d)). Major steps include: Prevention of Terrorism Act (2002) has included information systems in the decription of terrorism acts; Computer Misuse and Cybercrime Act" has defined cybercrimes (2003); Mutual Assistance in Criminal and Related Matters Act (2003) which sets the basis for international cooperation; National Cyber Security Strategy (2014) prioritised defence against cybercrime; Cybercrime Strategy (2017) calls for a more effective law enforcement and criminal justice response, emphasises the harmonisation of legal frameworks in its anti-cybercrime approach, and sets working with international counterparts as one of the seven goals; Mauritian Cybercrime Online Reporting System (MAUCORS) was designed to facilitate secure online cybercrime reporting and develop a better understanding of the cybercrime affecting citizens. Kenya is another good example of contributing to this norm, as it is a member of the Commonwealth, Harare Scheme and London Scheme relating to Mutual legal assistance in criminal Matters within the Commonwealth.

Notable examples of contributions to implementation of the norm related to interstate cooperation on cybersecurity (13(a)) are the Economic Community of West African States (ECOWAS) Regional Cybersecurity and Cybercrime Strategy (2021), and the South African National Cybersecurity Policy Framework (2015). Norm related to respect human rights and privacy (13(e)) is moved forward by the parliament of the Ivory Coast, which recognised and affirmed that access to the Internet and to electronic communication networks is a fundamental human right and a universal good. Similarly, Ghana Cybersecurity Act which facilitates the cooperation between the national CERT with CERTs from other countries contributes to the norm related to not harming the emergency response teams (13(k)).

2.3.2 Confidence building measures

- □ *What are the confidence-building measures (CBMs)?*
- □ *What is the significance of regional CBMs?*

CBMs aim to prevent hostility, reduce tension, avert conflict escalation, and build mutual trust between states. The UN Framework outlines a number of voluntary CBMs to increase cooperation and predictability, and reduce misunderstanding. CBMs call for, among other:

- *Exchange of information* on national strategies and policies, decision-making processes, and relevant national organisations and national terminology; on national and transnational threats, identified cyber incidents, product vulnerabilities and hidden functions, best practises in dealing with cyber incidents, and national classifications of incidents;
- Appointment of *national points of contact* on policy and technical levels, as well as creation of related directory of contacts;
- Establishment of, and cooperation among *national CERT/CSIRTs*, including for critical infrastructure;
- Protection of *infrastructure that states consider critical*, including industrial systems, through exchange of information and a repository of laws and policies related to critical infrastructure (CI), and developing technical, diplomatic and legal mechanisms to protect CI, as well as public-private partnership and multistakeholder cooperation for that;
- Cooperation in *investigating cybercrime and terrorism*, through cooperation of law enforcement authorities, and appointing focal points for the exchange of information on incidents and assistance in investigations;
- Developing mechanisms and processes for bilateral, regional, subregional, and multilateral *consultation to avoid misperception and escalation*;
- Developing *workshops, seminars and exercises* to prevent and manage cyber incidents.

Since regional organisations like the OSCE, ASEAN and the OAS have developed their own CBMs and principles, some of which fed into the UN Framework, it encourages further sharing of information about CBMs developed in regional and multilateral forums. We will discuss the work of regional organisations later in this module.

□ **Resources**

The GFCE paper Overview Of Existing Confidence Building Measures As Applied To Cyberspace provides an overview of the CBMs developed by the UN and the regional organisations by 2020.

□ **Reflection point**

One of the main elements of building confidence is enhanced information sharing among states and other actors, and establishing trust relations. In this regard, what are the good examples across Africa which follow the UN CBMs?

What are other CBMs that could be of particular relevance for African cooperation?

Leave your comment below.

Exercise (for in-situ and webinar format – breakout session)

To be further developed

1) Discuss the relevance and implementation of UN and regional CBMs (such as from the OSCE, the OAS or ASEAN) in national contexts.

2) Create a list of those CBMs that apply to the African context, as well as those that are possibly irrelevant.

3) Discuss what each African country has done (or could easily do) to implement those (e.g. assigning a point of contact, sharing information about national laws, connecting CERTs, etc.)

4) Discuss additional CBMs that might be developed to address the specific context of Africa that is not ‘covered’ by the existing UN and regional CBMs.

5) Consider whether asking African Ministers to publicly commit to existing CBMs (even if only the UN ones) could increase commitment with implementation, as well as their awareness.

2.3.3 Capacity building

- □ *What are the main cyber capacity-building principles set by the UN?*

Capacity building is the third pillar of the international cyber stability framework. There is general agreement on the importance of capacity building, and both the UN processes and various regional organisations develop specific measures and principles.

UN OEWG report of 2021 recommends that capacity building should be a sustainable process, comprising specific activities by and for different actors, results focused and with a clear purpose, evidence-based, politically neutral, transparent, accountable, and without conditions, and undertaken with full respect for the principle of State sovereignty. Further, it should be based on mutual trust, with voluntary participation, demand-driven and tailored to specific needs, correspond to nationally identified needs and priorities, undertaken in full recognition of national ownership, and protecting confidentiality of national policies and plans. Finally, capacity building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal, and non-discriminatory.

UN GGE report of 2021 further calls for capacity building to be voluntary, politically neutral, mutually beneficial and reciprocal in nature, and suggests it should help states to: develop and implement national policies and strategies, strengthen CERTs, improve resilience of the critical infrastructure, build competences and capacities to respond to incidents, deepen common understanding on how international law applies to cyberspace, and implement voluntary norms.

Resources

In the video by Diplo, several cyber ambassadors discuss Cyber capacity building, in particular what are the needs to develop cyber diplomacy capacities.

Contribute and engage

To learn more about cyber capacity building, education, and developing skills, refer to the Knowledge Module 4.

2.4 Broader context

- □ *What is the link between human rights and cyber norms?*
- □ *How does cybersecurity impact economic development and SDGs?*

Deliberations about cybersecurity and related norms don't happen in vacuum. In order to observe a broader context, cybersecurity should be connected with policy discussions related to digital aspects of human rights, and economic development.

The link between cyber norms and human rights may not be immediately obvious. Report of the APC and Global Public Digital, Unpacking the GGE's Framework on Responsible State Behaviour: Cyber Norms, clarifies that the goal of cyber norms of promoting responsible state behaviour in cyberspace contributes to the underlying conditions that are needed for the exercise of human rights today. The report further elaborates on how each of the norms relates to human rights.

In addition, the relationship between the Women, Peace and Security (WPS) agenda and cyber-enabled threats and cybersecurity is explored in the report "System Update: Towards a Women, Peace and Cybersecurity Agenda" by the United Nations Institute for Disarmament Research (UNIDIR). The paper analyses the linkages between WPS priority themes – gender equality, women's participation in international security, prevention and protection of violence against women, gender-differentiated needs – and international cybersecurity. It identifies priority areas that should be addressed to ensure a gender-inclusive cyberspace that protects the rights of women and girls.

On the other hand, sustainable development heavily relies on digitalisation and digital technologies, as the link between digital transformation and the Sustainable Development Goals showcase. 'The Global Risks Report 2022' of the World Economic Forum emphasises the link between the two particular digital concerns, 'digital inequality' and 'cybersecurity failure'. A GFCE report 'Integrating Cyber Capacity into the Digital Development Agenda' underlines that digitisation and resilience are two sides of the same coin, and identifies pathways to bridge the commonly detached topics and communities – development and cybersecurity communities, particularly in the field of capacity building.

African context

In his interview for 'Inside Cyber Diplomacy' podcast, co-hosted by Mr Jim Lewis and Mr Chris Painter, Mr Moctar Yedaly, Africa Program Director for the GFCE, and former Head of the Information Society department within the African Union Commission, discusses the African context and cybersecurity negotiations. Mr Yedaly also provides a cross-link of security with development, discusses the need for high-level political interest and attention to the issues of ICTs, and the value of including more stakeholders in multilateral negotiations.

Contribute and engage

To learn more about the broader context of cybersecurity, refer to the introductory Knowledge Module.

3 International cooperation

3.1 The United Nations

- *What is the history of the negotiations and dialogue under the UN?*
- *What are the current and possible future elements of the institutional dialogue?*

3.1.1 Institutional dialogue

Issues related to cybersecurity are not new to the UN. In 1998, the Russian Federation introduced the draft resolution *Developments in the Field of Information and Telecommunications in the Context of International Security*, of the First Committee of the UNGA, which was adopted without a vote.

The increasing cyber armament of states led to the establishment of the UN GGE in 2004, which consisted of experts from several states. The group ended its work without producing a final report, yet the GGE's mandate was renewed for 2009/10, 2012/13, 2014/15, 2016/17, and 2019–2021 (together referred to as the GGEs).

A breakthrough occurred in 2013 when the final report (adopted by consensus of the, then, 15 countries of the GGE, including all the permanent members of the Security Council – P5) clearly outlined growing trends of cyber militarisation and confirmed that international law applies to cyberspace. The GGE report of 2015 was another breakthrough and resulted in a landmark document – 20 countries, including the P5, specified the voluntary and non-binding normative framework for state behaviour and agreed on a set of voluntary norms, CBMs and capacity-building provisions.

The 2016/17 GGE, which was extended to include 25 countries, was unable to reach consensus on its final report, in particular, due to disagreement over what options states have to respond to cyberattacks. In 2021, however, the GGE managed to again reach consensus on a final report that has become a cornerstone of the framework of responsible behaviour. It has confirmed the applicability of the IHL during armed conflicts, suggested what should be treated as critical infrastructure, elaborated in greater depth on the previously agreed voluntary norms and CBMs, and set out capacity-building principles.

In 2018, besides a US-sponsored resolution that renewed the GGE for 2018–2020, the UNGA adopted another resolution (A/RES/73/27) sponsored by Russia that set in place a parallel process, the Open-ended Working Group (OEWG), which involved all interested states and allowed inputs from other stakeholders. While the two groups worked in parallel in somewhat different settings, considerable cooperation was established between the chairs of the two groups (Brazil and Switzerland), and most countries expressed an interest in ensuring that both succeed.

Indeed, in March 2021, the OEWG reached consensus, the first UN agreement on cybersecurity in almost six years, since the GGE report of 2015. The OEWG final report confirmed the agreed points from 2015, suggested what should be understood as CI clusters, invited agreement to ensure the integrity of the internet and of the ICT supply chain, asked for prevention of the proliferation of malicious tools and use of harmful hidden functions (aka backdoors), defined additional specific CBMs (such as appointing national points of contact), and set out capacity-building principles. Notably, the report also recommended that regular institutional dialogue should continue under the auspices of the UN, including the 2021–2025 OEWG, with equal state participation, although also opening the door for other types and formats of processes.

The GGE was not renewed in 2021, and the 2021–2025 OEWG remains as the only active format of institutional dialogue within the UN.

Reflection point

According to Mr Abdul-Hakeem Ajijola (Chair, African Union Cyber Security Expert Group (AUCSEG) and Commissioner, Global Commission for the Security of Cyberspace), the international community is building norms and these will have consequences for Africa. Therefore, it is crucial for Africa to be at the table, engaging with its partners as an empowered peer. Cyber is only as strong as the weakest link, so it is imperative that Africa will not be that weak link. (From the panel 'Cyber diplomacy in Africa and digital transformation', IGF 2021)

How to better engage African countries to take meaningful part in the institutional dialogue and other related cyber negotiations?

Leave your comment below.

Contribute and engage

Enrol in the Diplo's online course on Cybersecurity Diplomacy (facilitated small-group tailored learning), with four modules: strategic impact of cyber(in)security, issues on the diplomatic agenda (international law, norms, CBMs and capacity building, critical infrastructure, supply chain, attribution issues, links to human rights and development), roles of different stakeholders, mapping of multilateral and multistakeholder processes, and preparing a state for cyber diplomacy.

Enrol in the UNODA online Cyberdiplomacy Training (self-paced course), with five pillars: existing and emerging threats; international law; norms, rules and principles; confidence-building measures; international cooperation and assistance in capacity building.

Engage your Ministry of Foreign Affairs to take active part in the institutional dialogue and the other cyber-related processes.

3.1.2 Future processes

There are, however, different views and positions on how institutional dialogue should look like in future. For instance, there are calls for a long-term process rather than a limited mandate of a few years, as the OEWG currently is. Another open question is the mandate of future dialogue: should it focus on the implementation of the already agreed norms, CBMs, and capacity-building measures, or should it (also) develop new norms and measures? And should it expand the list of topics on the agenda, or remain focused on peace and security issues since the dialogue runs under the First Committee of the UN?

One concrete proposal to address some of those questions is already tabled by France and Egypt, with the support of 40 other states – a proposal for a Programme of Action (PoA) as a long-term and inclusive process. The PoA should create a framework and a political commitment based on the Framework, with regular annual working-level meetings focused on the implementation of the existing framework and periodic review conferences to consider whether additional norms should be developed. The OEWG 2021 final report names PoAs as one possibility for future institutional dialogue(s).

A particularly important question is whether there is a need for a cyber treaty of some kind. Six countries of the Shanghai Cooperation Organisation (SCO) proposed an International Code of Conduct for Information Security to the UN in 2011 and again in 2015. The proposal envisaged that the code of conduct would cover more than just cyber conflict, including provisions about information warfare in cyberspace and other internet governance issues, surveillance, content policy, and sovereignty. The USA, the EU and their partners have strongly resisted such initiatives, arguing that these would introduce greater censorship and internet content control in countries around the world. Since the UN OEWG is inclusive to all states, the question of a binding treaty or convention is getting addressed as part of the discussion on the future institutional dialogue.

It is important to mention, however, another important process which is distinguished from the dialogue related to peace and security, but may influence it indirectly. The UN resolution on countering the use of ICT for criminal purposes, adopted in 2019, established the open-ended ad hoc international committee of experts (known as the Ad hoc committee) under the Third Committee of the UN, tasked with developing a new global cybercrime treaty. The ad hoc committee should provide a draft convention to the UN General Assembly in August 2023. One of the main questions in these negotiations is about coherence of the possible global convention with the Convention on Cybercrime of the Council of Europe (known as the Budapest Convention) of 2001. Another question is how to preserve human rights while accommodating demands for greater sovereignty of states in cyberspace.

Contribute and engage

To learn more about cybercrime and related issues and processes, as well as the capacity-building opportunities, refer to the Knowledge Module 3.

3.2 Other multilateral forums

- *What other major diplomatic and political processes have cybersecurity elements on the agenda?*

Diplomatic and political processes that are not focused on cybersecurity increasingly consider cybersecurity aspects as well.

Cyberespionage appeared on the agenda of the G20, a group of 20 major economies, in 2015, when it agreed 'that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors' (G20, 2015, art. 26). The G20 Cybersecurity Dialogue Working Group, as part of the G20 Digital Economy Task Force, is a venue for multistakeholder, cross-sectoral discussion on security in the context of the digital economy, such as exchanging good national practises. In addition, the G20 Osaka Track, initiated in 2019, intensified international rule-making efforts in the digital economy, especially on data flows and e-commerce, while promoting enhanced protections for intellectual property, personal information, and cybersecurity.

Similarly, in the past, the Group of Seven (G7) has reflected on the need for responsible state behaviour in cyberspace and, in particular, on its relevance for intellectual property theft and economic cyberespionage.

The World Trade Organization (WTO), under its plurilateral negotiations on e-commerce carried out under the Joint Statement Initiative (JSI), promotes cybersecurity as one of the issues on its agenda. Accordingly, discussions about cybersecurity have focused on strengthening national capacities for incident response, encouraging cooperation, and fostering sharing of information (JSI Focus Group D), but have also considered cross-border data flows (Focus Group B) and electronic authentication (Focus Group A).

The Global Forum on Digital Security for Prosperity of the Organisation for Economic Co-operation and Development (OECD) offers a multilateral and multidisciplinary setting that, since 2018, brings together experts and policymakers to share experiences and good practises on digital security and discuss the economic and social aspects of cybersecurity. In addition, the OECD's Working Party on Security and Privacy in the Digital Economy (SPDE) brings together stakeholders to shape high-level policy recommendations, such as those related to the security of digital technologies and products.

3.3 Regional efforts

- *What are the major instruments developed on regional levels?*
- *How can those instruments assist African developments?*

3.3.1 OSCE

Diplomatic efforts within several regional organisations seek to formulate CBMs for cyberspace to enhance cooperation and prevent misunderstanding and possible conflicts. Of particular relevance is the set of CBMs to reduce the risk of conflict stemming from the use of ICTs, adopted in 2013 (Decision No. 1106) and extended in 2016 (Decision No. 1202), by the Organization for Security and Co-operation in Europe (OSCE). The decision outlines measures that participating states are invited to follow voluntarily, including: sharing national views on threats and best practises; cooperating with competent national bodies; consulting to reduce risks of misperception and possible tension or conflict; building up of national legislation to allow information sharing; sharing and discussing national terminology related to cybersecurity; cooperating in critical infrastructure protection; disclosing vulnerabilities; promoting public-private partnerships; and involving the private sector, academia, centres of excellence, and civil society in cybersecurity measures.

Contribute and engage

Enrol the OSCE online course on Cyber/ICT security Confidence-Building Measures (self-paced learning), with three modules: a brief overview of the four pillars of the international framework for stability in cyberspace and roles of regional organisations, development of cyber/ICT security in the OSCE and the 16 CBMs, and a closer look at each of the 16 cyber CBMs individually, with a specific focus on practical implementation.

3.3.2 ASEAN and the ARF

The ASEAN Regional Forum (ARF) has followed the OSCE example with its 2015 Work Plan on Security of and in the Use of Information and Communications Technologies, which came as a result of the 2012 statement by ASEAN ministers of foreign affairs. In 2018, the ASEAN countries agreed that a formal ASEAN cybersecurity mechanism for cyber diplomacy and policy and operational issues should be established. The ASEAN countries also decided to subscribe to the 11 voluntary, non-binding norms recommended in 2015 by the UN GGE, as well as to focus on regional capacity building in implementing these norms. The UN-Singapore Cyber Programme (UNSCP) was launched, focusing on cyber norms, awareness building, and cyber policy scenario planning. In 2020, the ASEAN ministers further agreed to develop a long-term regional cybersecurity action plan to implement the norms. Building on the norms chart that the ASEAN countries developed in 2019, Singapore and the UN Office for Disarmament Affairs (UNODA) agreed to establish a norms implementation checklist, making it applicable to a broader range of UN member states.

In Asia, the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF) also addresses cybersecurity confidence-building measures and combating cybercrime. In 2012, the ARF produced a ministerial statement intensifying regional cooperation on ICT security (ARF, 2012). In 2017, ASEAN adopted a Cybersecurity Cooperation Strategy, which guides the organisation and its member states in a coordinated approach to building their cybersecurity capacity. In addition, the ASEAN-Singapore Cybersecurity Centre of Excellence and the ASEAN-Japan Cybersecurity Capacity Building Centre were established to raise the level of cyber expertise.

3.3.3 OAS

In 2018, the OAS adopted a resolution stressing the need to prepare and agree on a set of CBMs for cyberspace, and starting with the two voluntary measures: sharing information on cybersecurity policies and identifying a national point of contact at the policy level. In 2019, four additional CBMs were recommended, including designating points of contact in ministries of foreign affairs and strengthening capacity building in cyber diplomacy.

The Organization of American States (OAS) established the *Inter-American Cybersecurity Strategy* in 2003. This strategy pools the efforts of three related groupings of the organisation: The Inter-American Committee against Terrorism (CICTE), Ministers of Justice or other Ministers or Attorneys General of the Americas (REMJA), and the Inter-American Telecommunication Commission (CITEL). These groups work with member states to implement programmes that prevent cybercrime and protect the CI by legislative and other procedural measures. REMJA fosters cooperation in combating cybercrime through its Working Group on Cybercrime and the Inter-American Cooperation Portal on Cybercrime. Further OAS declarations – Strengthening Cyber Security in the Americas in 2012 and the Declaration on the Protection of Critical Infrastructure from Emerging Threats in 2015 – and CICTE's Declaration on Strengthening Hemispheric Cooperation and Development in

Cybersecurity and Fighting Terrorism in the Americas, renewed the OAS's commitment to regional cybersecurity.

3.3.4 Africa

The African Union's Convention on Cyber Security and Personal Data Protection (known as a Malabo Convention), adopted in 2014, provides a legal framework for promoting cybersecurity, combating cybercrime, conducting electronic commerce, and protecting personal data. However, its influence on national legal frameworks remains limited so far, as only 19 of 55 member states had signed or ratified it by mid-2020.

While there are no regional CBMs, there are many cybersecurity and cyber diplomacy efforts on the regional and subregional levels: the Cybersecurity Expert Group (AUCSEG), the Cybersecurity flagship in the AU Agenda 2063, the Policy and Regulations Initiative for Digital Africa (PRIDA), the Programme for Infrastructure Development for Africa (PIDA), the Digital Transformation Strategy for Africa, the Smart Africa Alliance, the ECOWAS' cybersecurity strategy and the SADC's action plan on cybersecurity. "Africa as a Cyber Player", a research conducted by the EU ISS under the EU Cyber Direct initiative, provides a good overview of main players and instruments in the continent, in the fields of cybersecurity and cyber diplomacy.

Reflection point

In her Master thesis "International Cyber Security Diplomatic Negotiations: Role of Africa in Inter-Regional Cooperation for a Global Approach on the Security and Stability of Cyberspace", Ms Souhila Amazouz suggest that, to accelerate the ratification process of the Malabo Convention within AU Member States, the AUC has to escalate the issue to the Ministerial Committee on the Challenges of Ratification/Accession and Implementation of AU Treaties, and engage in reflections to find the appropriate way of transposing the Malabo convention provisions to national laws to harmonise cybersecurity frameworks at continental level. She also suggests that African countries should care about mainstreaming cybersecurity into their foreign and security policies, along with the development of their digital agenda.

What are the measures that could steer a greater uptake of cybersecurity as an issue among the African Ministries of Foreign Affairs, and consequently their role in shaping the African and global instruments?

Leave your comment below.

Resources

Global Forum on Cyber Expertise (GFCE) provides an 'Overview Of Existing Confidence Building Measures As Applied To Cyberspace'. The paper "Towards a secure cyberspace via regional cooperation" by the Geneva Internet Platform offers a comparative analysis of the thematic areas covered by cyber norms, CBMs and capacity-building measures by the regional organisations.

3.4 Multistakeholder efforts

- *What is the value of multistakeholder discussions for cyber diplomacy efforts?*
- *Which are the most relevant multistakeholder fora that African states should be engaged with?*

3.4.1 Internet Governance Forum

The UN Internet Governance Forum (IGF) is a non-decision-making forum that involves a variety of stakeholders to openly discuss internet governance issues, including security and privacy. While the IGF does not make decisions or recommendations, it provides the opportunity for open dialogue and partnership, the exchange of information, and useful voluntary policy guidance through the Best Practice Forum (BPF) on Cybersecurity, the Dynamic Coalition (DC) on Internet Standards, Security and Safety (DC-ISSS), and reports from the thematic sessions held each year. In addition, the secretary general's Roadmap for Digital Cooperation envisages a strengthened role for the IGF (the so-called IGF+) in global digital cooperation and the establishment of a high-level multistakeholder body within the IGF, which will work on translating discussions into impact, increasing the importance of the IGF for coordinated discussions on cybersecurity.

Resources

BPFs offer substantive ways for the IGF community to produce more concrete outcomes. Through an open dialogue and exchange, BPF Cybersecurity has developed number of relevant reports:
- Exploring Best Practices in Relation to International Cybersecurity Initiatives (2020)
- BPF Cybersecurity on International Cybersecurity Agreements (2019)
- Cybersecurity Culture, Norms and Values (2018)
In 2021, BPF has turned to testing existing norms against historical cybersecurity events.

African context

African Internet Governance Forum (AfIGF) was officially recognized by ICT Ministers as a necessary continental platform, with the Secretariat hosted by the AUC. It organises annual events to discuss a broad range of internet governance issues, including cybersecurity, in a multistakeholder format. In addition, all the five regions of Africa have established subregional IGFs, in order to bring together national IGFs, and promote local policy dialogues. According to the UN IGF, 30 African countries have established their national IGFs.

3.4.2 The GFCE

The Global Forum on Cyber Expertise (GFCE) is a platform joined by 60 countries and many international and regional organisations, companies, and civil society organisations to collaborate on capacity building in cybersecurity. The Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building, adopted in 2017, set several priority areas for global capacity building and enabled the GFCE to create corresponding thematic working groups for the cooperation of its members and partners. These priority areas include developing national frameworks, incident response and protection of the CI, combating cybercrime, and developing cybersecurity culture and skills. In addition, the GFCE aims to establish a 'clearing house mechanism' to enable its members to get any support needed from other members. To map its work and available global knowledge, resources, and capacity-building activities in the field of cybersecurity, the GFCE launched its CyBil knowledge portal.

3.4.3 Paris Call

Together with the French government, Microsoft launched the Paris Call for Trust and Security in Cyberspace, a high-level declaration on the development of common principles for securing cyberspace. The Paris Call was signed by over 80 countries and over 1000 businesses and organisations worldwide. The Call affirmed the importance of voluntary norms of responsible state behaviour to cybersecurity, drawing on the 2015 GGE norms and the GCSC norms.

3.4.4 The GCSC

The Global Commission on the Stability of Cyberspace (GCSC), a multistakeholder think tank established in 2015, proposed a set of new norms for consideration by various forums, such as the GGE. The proposals include the Call to Protect the Public Core of the Internet, a Call to Protect Electoral Infrastructure, and the Singapore Package of six norms that ask states to avoid tampering with products, to create vulnerability equities processes and mitigate significant vulnerabilities, to enhance cyber hygiene, and to abstain from using botnets or driving offensive operations through non-state actors. These norms are intended to be complementary to norms developed within the context of the UN.

3.4.5 The FOC

Freedom Online Coalition (FOC) works on raising the profile of human rights as an integral consideration in cybersecurity policymaking. The FOC has issued a Joint Statement on a Human Rights Based Approach to Cybersecurity Policy Making, and provided a definition of cybersecurity as ‘the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline.’

4 Cyber diplomacy

Digitalisation and related topics have reached almost all aspects of foreign policy. This is not a new realisation, but ministries of foreign affairs have only recently begun to address this in a more comprehensive way. Hence, we are now seeing the emergence of 'digital foreign policy', in particular digital foreign policy *strategies* that offer a comprehensive overview of countries' approaches to digital topics, actors and processes, and the establishment of cyber departments and portfolios within the Ministries of Foreign Affairs.

Resources

"Improving the practice of cyber diplomacy: Training, tools, and other resources", research developed by the GFCE and Diplo, explains who the cyber diplomacy practitioners are, where cyber diplomacy is conducted, and which countries are the most active and inactive. The study also maps available training, tools, and other resources available, as well as how they help diplomats engage in cyber diplomacy. Importantly, the study also presents the findings of a survey and analyses how widely used these tools and resources are by diplomats around the world, with a focus on the countries and regions that are not as active in cyber diplomacy.

Through several thematic video interviews, cyber representatives look at the scope of cyber diplomacy, inclusiveness and roles of stakeholders, and skill sets that should be developed for cyber diplomacy. The interviews include:

- Amb. Nathalie Jaarsma (Ambassador-at-Large for Security Policy & Cyber, Netherlands)
- Mr Chris Painter (President, Global Forum on Cyber Expertise (GFCE) Foundation)
- Amb. Tobias Feakin (Ambassador for Cyber Affairs and Critical Technology, Australia)
- Mr David Koh (Commissioner of Cybersecurity and Chief Executive of the Cyber Security Agency of Singapore)
- Amb. Asoke Mukerji (former Ambassador of India)

4.1 Scope

- *Is cyber diplomacy about cybersecurity only?*

Experiences shared by Mr Painter, Ms Jaarsma, and Mr Feakin:
Cyber diplomacy beyond security (video)

4.2 Inclusiveness and roles of stakeholders

- *What role non-state stakeholders play in cyber diplomacy, especially at regional levels?*
- *Why is inclusiveness of stakeholders important for reaching meaningful agreements?*

Experiences shared by Mr Koh:
Regional processes and role of stakeholders (Mr Koh) (video)

Experiences shared by Amb Mukerji:
Inclusiveness and possible agreements (Amb Mukerji) (video)

4.3 Skill sets

- *What are the skills that cyber diplomats require?*
- *What are the skills that other stakeholders need to contribute to cyber processes?*
- *(Why and how) Should diplomats and non-diplomats work together? What is the role of other stakeholders?*

Experiences shared by Amb Jaarsma and Amb Feakin:
Skill set for cyber diplomats (video)

Experiences shared by Mr Painter, Amb Mukerji, and Mr Koh:
Skill set for cyber non-diplomats (video)

Experiences shared by Mr Koh and Amb Mukerji:
Diplomats and non-diplomats working together (video)

Contribute and engage

Engage with the GFCE Working Group A, especially its Task Force 2 on cyber diplomacy, to share your perspectives on the matter, and assist with shaping further capacity-building resources, toolkits, and activities.

Contribute to the CyBil portal through submitting information about available resources, toolkits, and activities in Africa.

5 Conclusion

Congratulations, you have reached the end of the module. The concluding part reflects on the key takeaways from this module.

- Cyberattacks against critical systems and components of society can cause severe disruptions to a digitalised nation's economy and security. A combination of high-impact operations conducted remotely, with relatively high deniability, make them suitable for hybrid warfare, especially in peacetime (short of an open conflict).

- The UN recognises the risks from increasing cyber armament of states – that is, the development of offensive cyber capabilities. Cyber is increasingly recognised by states as a new military domain, along with land, sea, air, and space. This, in turn, introduces dangers of escalations of cyberattacks into conflict with cyber, as well as other conventional means.

- More than two decades ago, it became clear that there is a need for certain ‘rules of the road’ related to the use of cyberattacks, and their implications for international peace and security. Since 2004, the dialogue has been ongoing within the UN – and it did bring (some) results.

- The international framework of responsible state behaviour in cyberspace is based on the agreements of several rounds of meetings of the Group of Governmental Experts (GGE) and one Open-ended Working Group (OEWG), which were subsequently endorsed by the UN General Assembly. Even though it is non-binding in nature, the framework creates the basis for predictability and holds states accountable for their actions in cyberspace.

- Within the framework, states have agreed that the existing international law and the UN Charter do apply to cyberspace, and that the international humanitarian law applies in cases of conflict. The framework outlines a number of cyber norms that define what states should and should not do, confidence building measures which encourage states to exchange information and cooperate in preventing misunderstanding that could lead to escalations, and capacity building principles. The framework also establishes further steps in the institutional dialogue under the UN.

- However, there are still many open issues to be resolved. In particular, how the international law applies in terms of understanding what constitutes an armed attack in cyberspace, in which cases the right to self-defence applies, and how it can be operationalised, how to monitor the adherence of states to the agreed norms, how to hold countries accountable for cyberattacks having in mind great complexities with attribution, how to better engage other stakeholders, and whether new norms, or an international treaty, are needed.

- Several regional organisations have developed their own strategies and measures that address regional specificities, and have found ways to ensure that states commit to the global framework. Africa, however, needs to enhance its regional cooperation on this matter.

- In practice, cyberspace is mainly owned, managed, and used by the private sector, while the civil society (including technical and academic community) possesses an in-depth understanding of how it works and impacts the society, and operates vast global communities that shape the development and use of the internet. It is therefore essential that other stakeholders are involved in shaping and implementing cyber norms and agreements. Number of global and regional multistakeholder initiatives exist that are of particular relevance, such as the UN Internet Governance Forum, and the GFCE

- Cyber diplomacy is the key element for reaching global agreements, as well as implementing them. On one hand, states have to develop cyber diplomacy capacities and structures within public institutions, particularly within the Ministries of Foreign Affairs. On the other hand, the civil society and the private sector also need to be involved and prepared for participating in global processes, and working with the officials on applicability of international law, and shaping and implementing norms and principles.

- Finally, it is important to note that cyber diplomacy is not only about cybersecurity, but that it needs to address challenges holistically. Cyber diplomats, therefore, should equally address digital aspects of economic development and human rights – and the cross links between those three dimensions.

Reflection point

What are your main takeaways from this knowledge module – important points that are not included above?

Leave your comment below.