Cybersecurity Agreements

Background paper to the IGF Best Practices Forum on Cybersecurity

Editor:
Maarten Van Horenbeeck, BPF Lead Expert (maarten@first.org)

Key contributors:
Sheetal Kumar, Global Partners Digital
Frans van Aardt, Private
Susan Mohr, CenturyLink
Carina Birarda, Centro de Ciberseguridad del GCBA
Louise Marie Hurel, Instituto Igarapé
John Hering, Microsoft
Klée Aiken, APNIC
Duncan Hollis, Temple Law School
Joanna Kulesza, University of Lodz, Poland
Anahiby Anyel Becerril Gil, Infotec

Many thanks to all participants of the IGF Best Practices Forum on Cybersecurity, led by Markus Kummer and Ben Wallis, and UN consultant Wim Degezelle. We are an open, multi-stakeholder group conducted as an intersessional activity of the Internet Governance Forum.
Join us at https://www.intgovforum.org/multilingual/content/bpf-cybersecurity

- July 2019 -

Feedback on the background paper is welcome and can be submitted to bpf-cybersecurity-contribution@intgovforum.org

Disclaimer:

The IGF Secretariat has the honour to transmit this paper prepared by the 2019 Best Practice Forum on Cybersecurity. The content of the paper and the views expressed therein reflect the BPF discussions and are based on the various contributions received and do not imply any expression of opinion on the part of the United Nations.

Table of Contents

Table of Contents 3

List of abbreviations and acronyms 5

Introduction to the Best Practices Forum on Cybersecurity 6

Spaces for agreement 8

- Within a stakeholder group 8
- Between stakeholder groups 10
- Within the United Nations 10

State of existing agreements 11

- How we scoped agreements 11
- The binding or non-binding nature of agreements 11
- Overlapping elements of agreements 11
- Analysis of each agreement 13
  - African Union Convention on Cyber Security and Personal Data Protection 13
  - Southern African Development Community Model Laws on Cybercrime 14
  - Paris Call for Trust & Security in Cyberspace 15
  - UNGGE Consensus Report of 2015 16
  - Cybersecurity Tech Accord 17
  - Siemens Charter of Trust 17
  - GCSC Six Critical Norms 18
  - Freedom Online Coalition Recommendations for Human Rights Based Approaches to Cybersecurity 20

Shanghai Cooperation Organization Agreement on Cooperation in the Field of Ensuring the International Information Security 21

Mutual Agreed Norms for Routing Security (MANRS) 22

Brazzaville Declaration 23

Budapest Convention 23

EU Cybersecurity Act 25

EU NIS Directive 26

Draft EAC Framework for Cyber Laws 26

ECOWAS Directive C/DIR. 1/08/11 28

NATO Cyber Defence Pledge 28

EU Joint Communication: Resilience, Deterrence and Defence 29

CSDE Anti-botnet Guide 30

The next step: assessing implementation of agreement elements 33

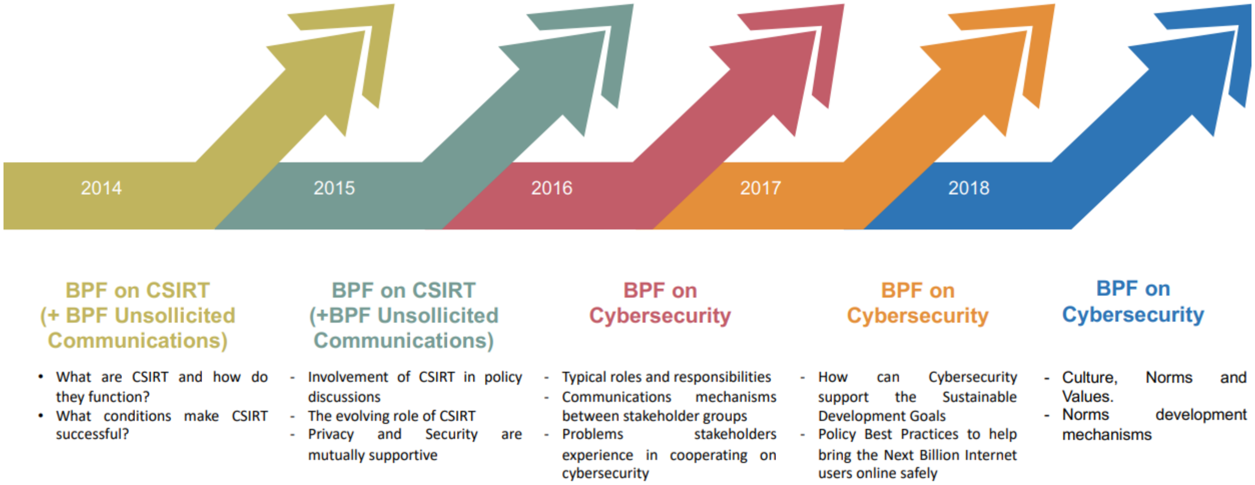
Further resources 33

List of abbreviations and acronyms

AMCC	ASEAN Ministerial Conference on Cybersecurity
ASEAN	Association of Southeast Asion Nations
BPF	Best Practice Forum
Budapest Convention	Council of Europe Convention on Cybercrime
CBM	Confidence Building Measure
CSDE	Council to Secure the Digital Economy
EAC	East African Community
ECCAS	Economic Community of Central African States
ECOWAS	Economic Community of West Adrican States
ENISA	European Union Agency for Cybersecurity
EU	European Union
GCSC	Global Commission on the Stability of Cyberspace
ICT	Information and communication technologies
IGF	Internet Governance Forum
ITU	International Telecommunication Union
MANRS	Mutually Agreed Norms for Routing Security
NATO	North Atlantic Treaty Organization
NIS Directive	EU Directive on Security of Network and Information Systems
NRIs	National, Sub-Regional, Regional and Youth IGF initiatives
OEWG	Open Ended Working Group
Paris Call	Paris Call for Trust and Security in Cyberspace
SCO	Shanghai Cooperation Organization
UNGA	United Nations General Assembly
UNGGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
UNODA	United Nations Office for Disarmament Affairs

Introduction to the Best Practices Forum on Cybersecurity

To enrich the potential for Internet Governance Forum (IGF) outputs, the IGF has developed an intersessional programme of Best Practice Forums (BPFs) intended to complement other IGF community activities. The outputs from this programme are intended to become robust resources, to serve as inputs into other pertinent forums, and to evolve and grow over time. BPFs offer substantive ways for the IGF community to produce more concrete outcomes.



BPF on CSIRT (+ BPF Unsollicited Communications)

- What are CSIRT and how do they function?
- What conditions make CSIRT successful?

BPF on CSIRT (+BPF Unsollicited Communications)

- Involvement of CSIRT in policy discussions
- The evolving role of CSIRT
- Privacy and Security are mutually supportive

BPF on Cybersecurity

- Typical roles and responsibilities
- Communications mechanisms between stakeholder groups
- Problems stakeholders experience in cooperating on cybersecurity

BPF on Cybersecurity

- How can Cybersecurity support the Sustainable Development Goals
- Policy Best Practices to help bring the Next Billion Internet users online safely

BPF on Cybersecurity

- Culture, Norms and Values.
- Norms development mechanisms

Since 2014, the IGF has operated a Best Practices Forum focused on cybersecurity. In 2014-2015, the BPF worked on identifying Best Practices in Regulation and Mitigation of Unsolicited Communications and Establishing Incident Response Teams for Internet Security. Later, the BPF has been focused on cybersecurity; identifying roles and responsibilities and ongoing challenges in 2016, and identifying policy best practices in 2017.

For 2018, the Best Practices Forum focused its work on the culture, norms and values in cybersecurity. The plan of action we took to approach this topic consisted of the following:

- The BPF started the process by building on its previous work on the roles and responsibilities of the IGF stakeholder groups in cyberspace and explored what norms have developed that apply to each of these groups. Some of the questions we explored relate to the behaviour of each stakeholder group, such as “state behaviour” or “industry behaviour”. The discussion of civil society’s role in norms development includes social norms of safe and secure online behaviour by individual users.
- We identified sample norms established by various forums, documenting and comparing them. We did so by engaging experts, BPF contributors and the IGF’s network of

National and Regional IGF initiatives (NRIs). Through this network, BPFs can bring in a developing country perspective and connect the NRIs with the norms development communities, to promote a culture of cybersecurity. We collected information on how they are articulated, implemented and whether they are successful.

- The BPF leveraged the work from 2017 to identify if any of the policy recommendations may see widespread acceptance, and may have developed into a recognized "best practice".
- We aimed to understand the impact of a "digital security divide". This refers to the situation where there's no coherent or universal implementation of a norm, or if the implementation of the norm has unintended consequences, or has different impacts in a different context (e.g. those with and those without effective rule of law), it may result in a group of "haves" and "have nots" in terms of the protection the norms offer. Security controls will be sufficient or meaningful in some parts of the world, and not in others. While these differences may exist regardless of norms, inappropriate norms operationalization also may adversely affect users. This makes it an interesting area for investigation into the reasons for non-adherence or potential barriers preventing the implementation.
- At the beginning of 2018, we published a Background document that was developed with support from participants in the Best Practice Forum, and served as an introduction to the wider area. It was provided as background reading to anyone responding to the public call for Input, which was released on August 15th 2018.
- Finally, we convened a meeting during the Paris IGF, bringing in experts from the norms development community to discuss the key issues in this space.

In 2019, the BPF continues this work by identifying best practices related to implementation of the different elements (e.g. principles, policy approaches) contained within various international agreements and initiatives on cybersecurity.

The first phase of the work, this document, identifies all relevant initiatives and agreements. The analysis will look for horizontal / overlapping elements (those appearing in more than one initiative) as well as for initiative-specific elements (which only appear in one).

As a follow-up to this document, the BPF will then agree which particular elements its work should focus on, and collect and share best practices around the implementation of these elements, including through related mechanisms and measures. The BPF's existing participants, stakeholders and knowledge base will enable it to identify these best practices. The BPF could also identify existing forums and networks that are currently addressing, or are well-placed to address, the elements that it has decided to cover, and provide an understanding on how stakeholders can participate in those existing processes. The resulting work would serve as a concrete contribution into relevant processes in the field of cybersecurity.

Spaces for agreement

Agreements among and between stakeholders to address and promote cybersecurity internationally take different forms. In this research paper, we have chosen to classify the agreements analysed under three headings:

- Agreements within a stakeholder group: These can include agreements agreed in multilateral forums among states but also agreements among private sector or nongovernmental actors
- Agreements across stakeholder groups: These are often termed 'multistakeholder initiatives', and can include agreements which are led by a state actor but which include multiple stakeholders or non governmental actors in their elaboration and implementation
- Agreements within the UN 1st Committee: We have chosen to situate the UN 1st Committee on international peace and security separately from the other agreements due to role the unique role the UN plays, and the position it holds as a multilateral forum which encompasses a very wide range of state actors, and thereby plays a unique and high-level norm-setting role.

Within a stakeholder group

Several examples of agreements within a specific stakeholder group, that describe general support for cybersecurity principles, exist:

- The G20, in their Antalya Summit Leaders' Communiqué, noted that "affirm 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".
- The G7, in their Charlevoix commitment on defending Democracy from foreign threats, committed to "Strengthen G7 cooperation to prevent, thwart and respond to malign interference by foreign actors aimed at undermining the democratic processes and the national interests of a G7 state."
- The Cybersecurity Tech Accord is a set of commitments promoting a safer online world through collaboration among technology companies.
- The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security frames cyber security approaches in a human rights context, and originates from a set of member governments.
- In the Shanghai Cooperation Organization's Agreement on cooperation in the field of ensuring the international information security member states of the Shanghai Cooperation Organization agree on major threats to, and major areas of cooperation in cybersecurity.
- The African Union Convention on Cyber Security and Personal Data Protection assists in harmonizing cybersecurity legislation across member states of the African Union.

- The Council to Secure the Digital Economy is a group of corporations which together published an International Anti-Botnet guide with recommendations on how to best prevent and mitigate the factors that lead to widespread botnet infections.
- The League of Arab States published a Convention on Combating Information Technology Offences which intends to strengthen cooperation between the Arab States on technology-related offenses.
- Perhaps one of the oldest documents, the Council of Europe developed and published a Convention on Cybercrime, also known as the Budapest Convention. Adopted in November 2001, it is still the primary international treaty harmonizing national laws on cybercrime.
- The East African Community (EAC) published its Draft EAC Framework for Cyberlaws in 2008, which contains a set of recommendations to its member states on how to reform national laws to facilitate electronic commerce and deter conduct that deteriorates cybersecurity.
- The Economic Community of Central African States (ECCAS) in 2016 adopted the Declaration of Brazzaville, which aims to harmonize national policies and regulations in the Central African subregion.
- The Economic Community of West African States (ECOWAS) Directive C/DIR. 1/08/11 on Fighting Cyber Crime within ECOWAS, agree with central definitions of offenses and rules of procedure for cybercrime investigations.
- The European Union in 2016 adopted, and in 2018 enabled its Directive on Security of Network and Information Systems (NIS Directive). The Directive provides legal measures to improve cybersecurity across the EU by ensuring states are equipped with incident response and network information systems authorities, ensuring cross-border cooperation within the EU, and implement a culture of cybersecurity across vital industries.
- In December of 2018, the EU reached political agreement on a EU Cybersecurity Act, which reinforces the mandate of the EU Agency for Cybersecurity (ENISA) to better support member states. It also built in a basis for the agency to develop a new cybersecurity certification framework. In May 2019, the EU adopted and authorized the use of sanctions in response to unwanted cyber-behavior.
- The NATO Cyber Defence Pledge, launched during NATO's 2016 Warsaw summit, initiated cyberspace as a fourth operational domain within NATO, and emphasizes cooperation through multinational projects.
- In 2017, the EU Council published to all delegations its conclusions on the Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. This reinforced several existing EU mechanisms, such as the EU Cyber Security Strategy, and further recognized other instruments such as the Budapest Convention, while calling on all Member States to cooperate on cybersecurity through a number of specific proposals.
- The Mutually Agreed Norms for Routing Security (MANRS), an initiative by the Internet Society, is a voluntary set of technical good common practices to improve routing security compiled primarily by members of the network operators community.

Between stakeholder groups

Several cross-stakeholder initiatives exist, which are essentially multi-stakeholder in nature, yet still identify areas of overall agreement on actions to be taken to improve cybersecurity internationally.

Perhaps one of the most visible examples, the Paris Call for Trust and Security in Cyberspace, launched by France at the 2018 IGF, currently has 547 official supporters, including 65 states.

The Charter of Trust consists of private sector companies, in partnership with the Munich Security Conference, endorsing minimum general standards for cybersecurity through ten principles. Some of their associate members also include the German Federal Office for Information Security and Graz University of Technology.

The Global Commission on the Stability of Cyberspace is a multi-stakeholder group of commissioners which together develop international cybersecurity related norms related initiatives. Their most recent publication is a draft of Six Critical Norms, also known as the "Singapore Norms Package". It is a set of six new norms proposed by a multi-stakeholder group intended to improve international security and stability in cyberspace.

Within the United Nations

The key United Nations agreement we investigated as part of this project is the 2015 consensus report of the UNGGE on Developments in the Field of Information and Telecommunications in the Context of International Security. It proposed several norms, rules and principles for the responsible behavior of States. A new group being established in 2019 through resolution 73/226 of the United Nations General Assembly will continue to explore this topic.The UNGGE has a narrow set of participants from member states.

As of 2019, there is also a new initiative, initiated based on resolution 73/27, which is an Open Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, that is open to the entire UN membership. This new 2019 group will reportedly study the norms proposed by the prior UNGGE and identify potential new ones. Both initiatives are supported by the UN Office for Disarmament Affairs (UNODA).

The General Assembly requested UNODA to collaborate with relevant regional organizations to convene a series of consultations that can provide input to the UNGGE process.

In the case of the OEWG, the General Assembly requested UNODA to provide the possibility of holding intersessional consultative meetings with interested parties, in particular business, non-governmental organizations and academia, to share input on issues within the OEWG's mandate.

State of existing agreements

How we scoped agreements

We scoped agreements into the project based on the following rough criteria:

- The agreement describes specific commitments or recommendations that apply to any or all signatory groups (typically governments, non-profit organization or private sector companies);
- The commitments or recommendations must have a stated goal to improve the overall state of cybersecurity;
- The agreement must be international in scope - it must have multiple well known actors that either operate significant parts of internet infrastructure, or are governments (representing a wide constituency).

Agreements were identified by experts participating in the Best Practices Forum.

The binding or non-binding nature of agreements

Of note, the agreements we scoped can be considered binding to various degrees. Some documents, such as the Budapest convention, is a legally binding instrument. Others, such as the African Union Convention on Cybersecurity, can become binding once ratified by sufficient states (15, as opposed to 4 to date).

Others are normative rather than binding. They are not legally binding but affect behavior by incentivizing or motivating the parties to comply. Examples include the UNGGE norms of 2015 for states, or the MANRS norms proposed by the Internet Society. These are often codified after best practices or agreements have had some chance to settle in the international system, and violation of these best practices is at least considered undesired by a large number of parties.

For the purpose of this document, we decided to include documents originating from both sets of backgrounds, as each of them can have a positive influence on the cyber security environment, through different means.

Overlapping elements of agreements

We identified a number of key elements that affected more than a single agreement, and mapped these against specific agreements:

- **Further multi-stakeholderism:** identify or support that cybersecurity depends on the presence in debate and coordination of all stakeholder groups.
- **Vulnerability equities processes:** the realization that stockpiling of vulnerabilities may reduce overall cybersecurity, and processes can be implemented to help identify the appropriate course of action for a government when it identifies a vulnerability.

- **Responsible disclosure:** the need to coordinate disclosure of security issues between all stakeholders, including the finder, vendor and affected parties.
- **Reference to International Law:** whether the agreement mentions the importance of international law, or commits the signatories' behavior to international law.
- **Definition of Cyber threats:** whether the agreement proposes a clear or aligned definition of cyber threats.
- **Definition of Cyber-attacks:** whether the agreement proposes a clear or aligned definition of cyber attacks.
- **Reference to Capacity Building:** whether the agreement makes specific references to Capacity Building as a needed step to improve cybersecurity capability.
- **Specified CBMs:** whether the agreement describes or recommends specific Confidence Building Measures.
- **Reference to Human Rights:** whether the agreement reflects on the importance of human rights online.
- **References to content restrictions:** whether the agreement discusses the need for content restrictions online.

Analysis of each agreement

African Union Convention on Cyber Security and Personal Data Protection

Agreement element	African Union Convention on Cyber Security and Personal Data Protection	Notes
Further multi-stakeholderism	Yes	
Vulnerability equities processes	No	
Responsible disclosure	No	
Reference to International Law	Indirect	The document does not speak directly of international law but speaks of agreements on mutual legal assistance: “Those parties that do not have agreements shall undertake to encourage signing of such agreements on mutual legal assistance in conformity with the principle of double criminal liability”
Definition of Cyber threats	No	There is no definition, but categories that would be deemed criminal offenses like child pornography, unlawful access to computer systems, unlawfully damaging or altering of data, unlawful interception are described.
Definition of Cyberattacks	Indirect	
Reference to Capacity Building	Yes	
Specified CBMs’	Yes	Focus on education and certification.
Reference to Human Rights	Yes	In line with African Charter on Human and People’s Rights and UN declarations.
References to content restrictions	Yes	Child pornography, Racism, Xenophobia, threatening to commit a criminal offense through a computer system, insults based on race gender religion ethnic

		descent and deliberately deny, justify or approve of act such as genocide and crimes against humanity are noted as restrictions.

The convention contains several elements unique to its goal to enable e-commerce more effectively, such as an overview of contractual obligations in electronic transactions.It also covers data privacy matters, such as the right to object or erase data that has been collected on an individual. Fifteen AU states must ratify the convention for it to enter into force; to date, 4 have done so.

Southern African Development Community Model Laws on Cybercrime

Agreement element	Southern African Development Community Model Laws on Cybercrime	Notes
Further multi-stakeholderism	No	
Vulnerability equities processes	No	
Responsible disclosure	No	
Reference to International Law	No	
Definition of Cyber threats	No	
Definition of Cyberattacks	No	
Reference to Capacity Building	No	
Specified CBMs'	No	
Reference to Human Rights	No	
References to content restrictions	Yes	Covers pornography and child pornography, in addition to racist and xenophobic materials, and the denial of genocide and crimes against humanity.

The Southern African Development Community Model Laws on Cybercrime were developed with the intent of harmonizing ICT policies in sub-saharan Africa.

As is common with most other model laws reviewed in this document, it describes additional elements such as evidence collection procedures, but does not cover most of the norms objectives visible in the other agreements.

Paris Call for Trust & Security in Cyberspace

Agreement element	Paris Call for Trust & Security in Cyberspace	Notes
Further multi-stakeholderism	Yes	
Vulnerability equities processes	No	
Responsible disclosure	Yes	
Reference to International Law	Yes	"We also reaffirm that international law, including the United Nations Charter in its entirety, international humanitarian law and customary international law is applicable to the use of information and communication technologies (ICT) by States."
Definition of Cyber threats	No	
Definition of Cyberattacks	No	
Reference to Capacity Building	Yes	
Specified CBMs’	No	CBMs are mentioned, but not enumerated
Reference to Human Rights	Yes	“We reaffirm that the same rights that people have offline must also be protected online, and also reaffirm the applicability of international human rights law in cyberspace.”
References to content restrictions	No	

The Paris Call for Trust and Security in Cyberspace was launched at the IGF in Paris on November 12th, 2018. It represents signatories from both government, private sector and civil society. Unique elements included in the Paris Call include:

- Signatories commit to preventing activity that “intentionally and substantially damages the general availability or integrity of the public core of the internet”;
- Take steps to prevent non-state actors from hacking back;
- Promote international norms of responsible behavior;
- The principle on foreign electoral interference (e.g., malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities") was a

major contribution, although a version of it appeared earlier in 2018 in a G7 Ministers' Declaration.

- It acknowledges the Budapest convention as a key tool in preventing cyber criminality.

UNGGE Consensus Report of 2015

Agreement element	UNGGE Consensus Report of 2015	Notes
Further multi-stakeholderism	Yes	
Vulnerability equities processes	No	
Responsible disclosure	Yes	
Reference to International Law	Yes	
Definition of Cyber threats	No	Discussion of threats that use ICTs to target infrastructure, but no express definition is written.
Definition of Cyberattacks	No	
Reference to Capacity Building	Yes	
Specified CBMs’	Yes	The UNGGE report lists out specific CBM’s in section IV.
Reference to Human Rights	Yes	
References to content restrictions	Yes	Not an express reference to content restriction, but a norm to cooperate in opposing abuse of technologies by extremists

As described in the 2018 Background paper of the BPF, “*The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security is a UN mandated group of experts which has been established five times since 2004. It is convened under the UN’s First Committee. The GGE will meet for four one-week sessions. When consensus is reached, the group publishes an outcome report, which has happened in 2010, 2013 and 2015. In particular the 2013 and 2015 edition discussed norms development, with the 2015 report offering a proposal for voluntary cybersecurity norms. Outcomes and inputs to the UNGGE process have been echoed by other bodies, showing some level of adoption*”. In 2015, the GGE published a set of 11 recommendations for non-binding norms. The outcome of this report was later supported by other organizations such as ASEAN.

Unique elements of the GGE norms include that states should not conduct or knowingly support activity to harm the information systems of the authorized Computer Emergency Response

Teams of another state, as well as that they ”*should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public*”.

Cybersecurity Tech Accord

Agreement element	Cybersecurity Tech Accord	Notes
Further multi-stakeholderism	Yes	
Vulnerability equities processes	No	Not in the agreement, but the Tech Accord have published statements to this effect.
Responsible disclosure	Yes	
Reference to International Law	No	
Definition of Cyber threats	No	No definitions in the agreement, but have issues call for comment on cybersecurity definitions
Definition of Cyberattacks	No	
Reference to Capacity Building	Yes	
Specified CBMs’	No	
Reference to Human Rights	No	
References to content restrictions	No	

The Tech Accord contains several product development norms and operational norms, such as “opposing cyberattacks on users from anywhere”, which are less relevant to some of the inter-state norms. The document also proposes joint initiatives between different stakeholders to uphold these principles.

Siemens Charter of Trust

Agreement element	Siemens Charter of Trust	Notes
Further multi-stakeholderism	Yes	"In this document, the undersigned outline the key principles for a secure

		digital world – principles that they're actively pursuing in collaboration with civil society, government, business partners and customers."
Vulnerability equities processes	No	
Responsible disclosure	Yes	"8. Transparency and response: Participate in an industrial cybersecurity network in order to share new insights, information on incidents et al.; report incidents beyond today's practice which is focusing on critical infrastructure."
Reference to International Law	No	
Definition of Cyber threats	No	
Definition of Cyberattacks	No	
Reference to Capacity Building	Yes	Focus on education.
Specified CBMs'	No	
Reference to Human Rights	No	
References to content restrictions	No	

The Charter of Trust contains several product development norms, such as "user-centricity" and "security by default", which are less relevant to some of the inter-state norms. The document also proposes joint initiatives between different stakeholders to uphold these principles.

GCSC Six Critical Norms

Agreement element	GCSC Six Critical Norms	Notes
Further multi-stakeholderism	Yes	
Vulnerability equities processes	Yes	
Responsible disclosure	Yes	
Reference to International Law	Yes	"Despite these difficulties, it should be recalled that state sovereignty is the cornerstone of the rules-

		based international system of peace and security. States have a monopoly on the legitimate use of force, strictly bound by international law. If states permit such action, they may therefore be held responsible under international law”
Definition of Cyber threats	No	
Definition of Cyber Attacks	No	
Reference to Capacity Building	Indirect	“states should work towards compatible and predictable processes”
Specified CBMs’	Indirect	Compatible and predictable VEP
Reference to Human Rights	No	
References to content restrictions	No	

At the time of writing, the six critical norms are still in draft, and published for public input. They are the result of a multistakeholder group developing cybersecurity norms and sharing them with the wider community through consultation sessions for input. The six specific norms consist of:

- Norm to Avoid Tampering
- Norm Against Commandeering of ICT Devices into Botnets
- Norm for States to Create a Vulnerability Equities Process
- Norm to Reduce and Mitigate Significant Vulnerabilities
- Norm on Basic Cyber Hygiene as Foundational Defense
- Norm Against Offensive Cyber Operations by Non-State Actors

Several of these, such as the norm against offensive operations by non-states, the vulnerabilities equities process, and the norm to avoid tampering, are unique across the documents we reviewed.

Prior to this release, the GCSC also released a norm to “Protect the Public Core of the Internet”, and, in May of 2018, that “*State and non-state actors should not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites*.”

Freedom Online Coalition Recommendations for Human Rights Based Approaches to Cybersecurity

Agreement element	Freedom Online Coalition Recommendations for Human Rights Based Approaches to Cybersecuriyt	Notes
Further multi-stakeholderism	Yes	
Vulnerability equities processes	No	
Responsible disclosure	No	
Reference to International Law	Indirect	
Definition of Cyber threats	No	
Definition of Cyberattacks	Indirect	The FOC WG1 definition of cybersecurity is "Cybersecurity is 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”. However, there is no explicit definition of an attack.
Reference to Capacity Building	Yes	
Specified CBMs’	Yes	
Reference to Human Rights	Yes	Multiple references (see recommendations 1, 2, 4, 5,6, 8, 9, 11, 12, 13)
References to content restrictions	Yes	Focus lies on freedom of expression.

This document contains the outcomes of multistakeholder dialogue between states, private sector, academia and civil society, framing cybersecurity in the light of human rights. The text is very focused on representing human rights online.

Shanghai Cooperation Organization Agreement on Cooperation in the Field of Ensuring the International Information Security

Agreement element	SCO Agreement on Cooperation in the Field of Ensuring the International Information Security	Notes
Further multi-stakeholderism	No	
Vulnerability equities processes	No	
Responsible disclosure	No	
Reference to International Law	Indirect	Reference is more to how implementation must take into account international law, not whether international law applies online.
Definition of Cyber threats	Yes	Information terrorism means using information resources in the information space and/or influencing on them for terrorist purposes;
Definition of Cyberattacks	Indirect	Focus on illegal activity
Reference to Capacity Building	Yes	
Specified CBMs'	Yes	
Reference to Human Rights	Yes	"Taking into account the important role of information security in ensuring the fundamental human and civil rights and freedoms". However, this is more around the protection of rights than the potential impact of security measures.
References to content restrictions	Yes	"Dissemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States."

The Shanghai Cooperation Organization's Agreement on Cooperation in the Field of Ensuring the International Information Security was signed in 2009 as an agreement between SCO states on Cybersecurity.

Mutual Agreed Norms for Routing Security (MANRS)

Agreement element	Mutual Agreed Upon Norms for Routing Security	Notes
Further multi-stakeholderism	Yes	Although focus tends to be towards the technical community/private sector, this document relates to all network operators in all communities, including government, academia, and civil society, and is developed under the principles of open, bottom-up, collaborative, and multistakeholder best practice development.
Vulnerability equities processes	No	
Responsible disclosure	Yes	
Reference to International Law	No	
Definition of Cyber threats	Yes	MANRS focuses on addressing a specific set of technical challenges outlined in the original document but provided as a package with further resources.
Definition of Cyberattacks	No	
Reference to Capacity Building	Yes	Although capacity building is not explicitly outlined, the document is joined by an implementation guide, dissemination of best practices is highlighted, and the wider MANRS program includes a heavy focus on capacity building
Specified CBMs'	No	
Reference to Human Rights	No	
References to content restrictions	No	

MANRS is a set of technical recommendations, developed by a number of network operators, in partnership with the Internet Society, on how to build a more secure global routing platform through Filtering, Anti-Spoofing, Coordination and Global Validation.

Brazzaville Declaration

Agreement element	Brazzaville Declaration	Notes
Further multi-stakeholderism	Indirect	The text indicates sub-regional development and support from ITU. It thus does not indicate the stakeholders in such sub-regional development of support areas.
Vulnerability equities processes	No	
Responsible disclosure	No	
Reference to International Law	No	
Definition of Cyber threats	No	
Definition of Cyberattacks	No	
Reference to Capacity Building	Yes	
Specified CBMs’	Yes	Refers to institution of awareness campaigns.
Reference to Human Rights	No	
References to content restrictions	No	

The Brazzaville Declaration makes recommendations to the secretariat of the Economic Community of Central African States, the member states and the ITU to better align laws and develop capacity building across the region on cybersecurity.

Budapest Convention

Agreement element	Budapest Convention	Notes
Further multi-stakeholderism	Yes	Chapter III talks about International co-operation. It however nor specifically talking about multistakeholder in the true sense although such cooperation will require Government and Private sector cooperation but this excludes civil society etc

		Chapter II covers Article 23 – General principles relating to international co-operation Article 24 – Extradition Article 25 – General principles relating to mutual assistance Article 26 – Spontaneous information Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements Article 28 – Confidentiality and limitation on use Article 29 – Expedited preservation of stored computer data Article 30 – Expedited disclosure of preserved traffic data Article 31 – Mutual assistance regarding accessing of stored computer data Article 32 – Trans-border access to stored computer data with consent or where publicly available Article 33 – Mutual assistance regarding the real-time collection of traffic data
Vulnerability equities processes	No	
Responsible disclosure	Yes	
Reference to International Law	Yes	
Definition of Cyber threats	Indirectly	The convention is more focused on cybercrime and as such has an extensive range of definitions for such activities deemed as criminal. Indirectly threats and cyberattacks can make use of some of these categories which are

		considered cybercrime.
Definition of Cyberattacks	Indirectly	
Reference to Capacity Building	No	
Specified CBMs’	No	
Reference to Human Rights	Yes	
References to content restrictions	Yes	Article 9 – Offences related to child pornography

The Budapest convention is an international legal framework with development starting in the late 90s. It pre-dates a lot of the language which is common today, but defines types of cybercrime, and cooperation models on how to address trans-border crime.

EU Cybersecurity Act

Agreement element	EU Cybersecurity Act	Notes
Further multi-stakeholderism	Yes	Delegates most of the responsibilities of "relevant" stakeholders- inclusion to ENISA (i.e.: Article 4, 7, 9). It also establishes the Stakeholder Cybersecurity Certification Group with greater emphasis on engaging multiple stakeholders from the technical community and private sector (i.e.: Article 8; Section 4, Article 21, 22).
Vulnerability equities processes	Yes	Article 6, 7.
Responsible disclosure	Yes	Article 6(b). 7, 51(a)
Reference to International Law	No	
Definition of Cyber threats	Yes	Article 2(8)
Definition of Cyberattacks	No	
Reference to Capacity Building	Indirectly	Article 6
Specified CBMs’	Yes	
Reference to Human Rights	Yes	

References to content restrictions	No	

The EU Cybersecurity act proposes a wide set of activities and CBMs for building stronger cybersecurity across the EU. Most dominantly, it also builds out a permanent mandate for the EU Agency for Cybersecurity ENISA, and drives towards an EU-wide cybersecurity certification framework.

EU NIS Directive

Agreement element	EU NIS Directive	Notes
Further multi-stakeholderism	Yes	
Vulnerability equities processes	No	
Responsible disclosure	Indirectly	
Reference to International Law	No	
Definition of Cyber threats	No	
Definition of Cyberattacks	No	
Reference to Capacity Building	Indirectly	
Specified CBMs’	Yes	
Reference to Human Rights	No	
References to content restrictions	No	

The EU NIS Directive is unique in that it sets out minimum standards for what are to be considered “service providers” who have an obligation to report outages and breaches. It also defines a National Competent Authority in each state, which is to be defined by the government.

Draft EAC Framework for Cyber Laws

Agreement element	Draft EAC Framework for Cyber Laws	Notes
Further multi-stakeholderism	Yes	The document is a Framework with the goal to promote harmonisation of legal responses by issues created by the increased use of ICT and cyberspace. It is primarily providing

		recommendations. It involves the participation of states which may exclude private sector and Civil society, and as such is multilateral rather than multistakeholder. However, the document does refer to enabling “private sector participation” and the need for a strong private sector to allow for a co-regulatory approach and as such it contains some limited elements to encourage partnerships across two stakeholder groups.
Vulnerability equities processes	No	
Responsible disclosure	No	
Reference to International Law	Yes	
Definition of Cyber threats	Indirectly	
Definition of Cyberattacks	No	
Reference to Capacity Building	No	
Specified CBMs’	No	
Reference to Human Rights	Yes	
References to content restrictions	Indirectly	“Where illegal content is made accessible over the Internet in contravention of applicable national rules, states will often require a Internet service provider (ISP) to hand over any details which may establish the real-world identity of the content provider. “

The East African Community’s draft framework for cyber laws contains recommendations for member states of the EAC on reforming laws to accommodate electronic commerce.

ECOWAS Directive C/DIR. 1/08/11

Agreement element	ECOWAS Directive C/DIR. 1/08/11	Notes
Further multi-stakeholderism	No	
Vulnerability equities processes	No	
Responsible disclosure	No	
Reference to International Law	Indirect	Reference to coordinating legal frameworks, but not per se to international law.
Definition of Cyber threats	Yes	Definition of offenses
Definition of Cyberattacks	Yes	Definition of offenses
Reference to Capacity Building	No	
Specified CBMs'	No	Only refers to judicial cooperation in terms of international activity.
Reference to Human Rights	No	
References to content restrictions	Yes	Defines racism and xenophobia in content, and child pornography, and how creating this content is an offense.

ECOWAS is the Economic Community of West African State. The ECOWAS Directive is an overview of events considered to be offences, and a definition of what traditional offences are incorporated in information and communication technology offences. It has an overview of procedures and sanctions applicable to either.

NATO Cyber Defence Pledge

Agreement element	NATO Cyber Defence Pledge	Notes
Further multi-stakeholderism	Indirect	Some reference to the value of educational institutions and defence stakeholders.
Vulnerability equities processes	No	
Responsible disclosure	No	
Reference to International Law	Yes	International law and norms: “We reaffirm the applicability of international

		law in cyberspace and acknowledge the work done in relevant international organisations, including on voluntary norms of responsible state behaviour and confidence-building measures in cyberspace.”
Definition of Cyber threats	No	
Definition of Cyberattacks	No	
Reference to Capacity Building	Yes	“Enhance skills and awareness, among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences;”
Specified CBMs’	Yes	
Reference to Human Rights	No	
References to content restrictions	No	

The NATO Cyber Defence Pledge contains a provision to perform an annual progress review against the commitments outlined in the document.

EU Joint Communication: Resilience, Deterrence and Defence

Agreement element	EU Joint Communication: Resilience, Deterrence and Defence	Notes
Further multi-stakeholderism	Yes	
Vulnerability equities processes	No	
Responsible disclosure	Yes	
Reference to International Law	Yes	
Definition of Cyber threats	No	
Definition of Cyberattacks	Indirect	Refers to third agreement for definition of criminal behavior
Reference to Capacity Building	Yes	
Specified CBMs’	Yes	
Reference to Human Rights	Yes	“A comprehensive approach to cybersecurity

		requires respect for human rights, and the EU will continue to uphold its core values globally, building on the EU's Human Rights “
References to content restrictions	No	

In addition to these elements, the EU Joint Communication contains specific language focusing on deterrence, certification schemes for cybersecurity and threat sharing.

CSDE Anti-botnet Guide

Agreement element	CSDE Anti-botnet Guide	Notes
Further multi-stakeholderism	Yes	“Security relies on mutually beneficial teamwork and partnership among governments, suppliers, providers, researchers, enterprises, and consumers, built on a framework that takes collective action against bad actors and rewards the contributions of responsible actors.”
Vulnerability equities processes	No	
Responsible disclosure	Yes	“Coordinate with customers and peers”
Reference to International Law	Indirect	There is mention to domestic law enforcement coordination, but not directly to international law: “Coordination with law enforcement during address domain seizure and takedown.”
Definition of Cyber threats	Yes	The paper addresses Botnets and provides a description for them.
Definition of Cyberattacks	No	
Reference to Capacity Building	Yes	“While the industry leaders who have developed this

		Guide recognize that no combination of measures can guarantee the elimination of all threats and risks, they believe these practices, both baseline and advanced, present a valuable framework for ICT stakeholders to reference in identifying and choosing practices of their own to mitigate the threats of automated, distributed attacks. “
Specified CBMs’	Yes	Signature Analysis and Packet Sampling best practices, amongst others. While not directly CBMs, when universally applied they could be considered confidence building.
Reference to Human Rights	No	
References to content restrictions	Yes	Mostly describes techniques: blackholing, sinkholing, scrubbing and filtering and not categories of content.

The CSDE Anti-botnet guide is an industry driven document that focuses more on technical elements than the other documents we reviewed. Its primary purpose is to highlight voluntary practices that each segment of the ICT sector (e.g. infrastructure, software development, devices and device systems, home and small business systems installation, and enterprises) could implement, according to their circumstances, to mitigate the impact of botnet infections.

OAS - Organization of American States

Agreement element	AG/RES. 2004 (XXXIV-O/04)	Notes
Further multi-stakeholderism	Yes	
Vulnerability equities processes	Yes	
Responsible disclosure	Yes	
Reference to International Law	Yes	
Definition of Cyber threats	Yes	

Definition of Cyberattacks	Yes	
Reference to Capacity Building	Yes	
Specified CBMs´	Yes	10. The importance of promoting cooperation in the public sector with the private and academic sectors to strengthen the protection and protection of said infrastructure.
Reference to Human Rights	Yes	
Reference to content restrictions	Yes	Face and respond to cyber attacks, whatever their origin, fighting against cyber threats and cyber crime, typifying attacks against cyberspace, protecting critical infrastructure and securing networks of systems.

Adoption of a comprehensive Inter-American strategy to combat threats to cybersecurity: A multidimensional and multidisciplinary approach to creating a culture of cybersecurity (Adopted at the fourth plenary session, held on June 8, 2004).

Members States: Antigua and Barbuda, Argentina, Bahamas, Barbados, Belize, Bolivia, Brazil, Canada, Chile, Colombia, Costa Rica, Cuba, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyane, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Saint Lucia, St. Kitts & Nevis, Saint Vincent and the Grenadines, Suriname, Trinidad and Tobago, United States of America, Uruguay, Venezuela (Bolivarian Republic of).

The next step: assessing implementation of agreement elements

As part of its work, the Best Practices Forum will contact signatories and initiative holders of the agreements, as well as do a public Call for Contributions to learn about initiatives that have been implemented to achieve elements of each agreement.

Our goal is by the publication date of our final report, to have a list of initiatives that others can look towards to understand how to better achieve the outcomes intended by these cyber security agreements. These initiatives can then serve as “norms catalysts” to further spread awareness of the importance of some points on which wide agreement has been reached, and help further improve the ability of these agreements to increase cybersecurity.

Further resources

https://carnegieendowment.org/publications/interactive/cybernorms

The Carnegie Endowment for International Peace’s Cyber Norms Index “tracks and compares the most important milestones in the negotiation and development of norms for state behavior in and through cyberspace”.

https://cyberregstrategies.com/an-analytical-review-and-comparison-of-operative-measures-included-in-cyber-diplomatic-initiatives/

This excellent research by the Research Advisory Group of the Global Commission on the Stability of Cyberspace includes a thorough overview of Cyber Diplomatic Initiatives.

https://cyberpolicyportal.org/en/

The United Nations Institute of Disarmament Research published the Cyber Policy Portal as a comprehensive overview of cyber policy documents published by UN member states.

____________________ *End of document* ___________________