Internet Governance Forum

IGF 2020

Best Practice Forum on Cybersecurity

Exploring Best Practices in Relation to International Cybersecurity Agreements

draft Research paper

September 2020

Exploring Best Practices in Relation to International Cybersecurity Agreements

The IGF 2020 Best Practice Forum (BPF) on Cybersecurity's first workstream is focused on updating and further advancing the analysis of the 2019 BPF report on the state of international cybersecurity agreements, with a more narrow focus on cyber norms agreements. Its work includes:

- Identifying new agreements and developments since last year to include in the analysis.
- Reviewing and refining the scope of agreements to be included in the report.
- Identifying a core group of agreements to include in the 2020 analysis.
- Identifying trends and commonalities between contents of cyber norms agreements.
- Releasing a call for contributions to gain further input on these selected agreements and their implementation.
- Updating last year's research paper with new learnings about implementation regarding these core agreements.

Authors
John R. Hering
Louise Marie Hurel
Frans van Aardt
YingChu Chen
Carina Birarda
Ayesha Khan
Wim Degezelle

IGF 2020 BPF Cybersecurity webpage

www.intgovforum.org/multilingual/content/bpf-cybersecurity

Table of contents

Table of Contents

Scope of analysis – international agreements on cyber norms

In order to update the content of the 2019 BPF Cybersecurity report, a similar method was used in determining which international agreements would be included in the analysis for this year's report. We scoped agreements into the project based on the following 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; and
- 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).

In addition to these three criteria that were used in the previous BPF report, this year's report is also exclusively including in its analysis international agreements which *include voluntary, nonbinding norms for cybersecurity*, among and between different stakeholder groups. This is intended to help focus the analysis of the 2020 BPF, and the requests for contribution, on the impact of international agreements on cyber norms, areas of emerging consensus on cyber norms, and best practices for such efforts moving forward. It also will help to identify which norms are being more commonly included in different international agreements – said differently, *which norms are becoming "the norm" to include.*
Agreements were identified by experts participating in the Best Practices Forum.

Classification of agreements

In our analysis, we classify agreements analysed under three headings:

- 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 UN plays, and the position it holds as a multilateral forum which encompasses a wide range of state actors. It thereby plays a unique and high-level norm-setting role. Indeed, the cyber norms set out by the UN 1st Committee report serve as the foundation for our analysis of the other agreements in this report.
- Agreements within a stakeholder group: These can include agreements established in multilateral forums among states but also agreements among private sector or other 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.

The agreements below between and among different stakeholder groups reflect the scope for analysis in this year’s report. Building on the work of the 2019 BPF, it includes many of the same agreements included in the previous report, as well as new agreements and developments achieved over the past year. It does not include agreements which may have been included in the 2019 report but which are exclusively legally-binding or otherwise do not include specific voluntary cybersecurity norms.

Agreements included

In total, the BPF has identified 22 international agreements on cybersecurity norms for inclusion in this report, based on the scoping criteria above and split between three categories -- UN agreements, agreements within a stakeholder group, and agreements between multiple stakeholder groups.

UN Agreements

For this analysis, we have included the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security combined consensus reports from 2010/2013/2015, often referred to as the   "The Framework for Responsible State Behavior in Cyberspace" – which includes the 11 norms featured in the 2015 consensus UN-GGE report. The contents of the 2015 report, including its eleven norms, were formally adopted by the UN General Assembly in resolution 70/237, by consensus. The resolution "calls upon Member States to be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts."

A new iteration of the GGE – now labelled the GGE on "Advancing responsible State behaviour in cyberspace" – was established in 2019 through resolution 73/226 of the United Nations General Assembly, which will continue to explore these topics through 2021. The UNGGE has a narrow set of participants from UN member states, with 25 states included in the current body. As of 2019, there is also a new parallel UN initiative on these topics, established by resolution 73/27, the Open Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, which is open to the entire UN membership.

The two bodies have had successive rounds of meetings across 2019 and 2020, including several informal sessions. Both the UNGGE and the OEWG 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 an intersessional consultative meeting with interested parties, in particular business, nongovernmental organizations and academia, to share input on issues within the OEWG's mandate. This meting took place in December of 2019, at the UN headquarters in New York City.

Agreements within a single stakeholder group

Below are the agreements within stakeholder groups that are included in this report. These types of agreements, within a single stakeholder group (states, non-profits, private sector, academia, technical community, ...etc), were by far the most common form of cybersecurity norms-setting agreements we encountered in this initiative. They largely take advantage of existing institutions and forums, exclusive to certain stakeholders, in order to be established.

- 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."
- In 2017, the G7 also released its Declaration on Responsible States Behavior in Cyberspace, intended to promote "a strategic framework for conflict prevention, cooperation and stability in cyberspace, consisting of the recognition of the applicability of existing international law to State behavior in cyberspace, the promotion of voluntary, non-binding norms of responsible State behavior during peacetime, and the development and the implementation of practical cyber confidence building measures (CBMs) between States."
- 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 cybersecurity 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 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 African Union Convention on Cyber Security and Personal Data Protection assists in harmonizing cybersecurity legislation across member states of the African Union.
- 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
- The East African Community (EAC) Draft EAC Framework for Cyberlaws 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) 2016 Declaration of Brazzaville, aims to harmonize national policies and regulations in the Central African subregion.
- 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.
- The EU Council's 2017 Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, which was published to all EU delegations. 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, which how now expanded to include internet exchange points, as well as
- The Commonwealth Cyber Declaration, launched in 2018, is a commitment among the Commonwealth Heads of Government to “a cyberspace that supports economic and social development and rights online,” “build the foundations of an effective national cybersecurity response,” and “promote stability in cyberspace through international cooperation.”

Multistakeholder agreements on cyber norms

Below are the multistakeholder cybersecurity agreements we included in this report. By comparison to agreements within stakeholder groups, multistakeholder agreements on cybersecurity norms and principles were found to be less common, and frequently reflect the output or launch of a new initiative to build cooperative relationships across stakeholder groups that have not previously existed.

- The Paris Call for Trust and Security in Cyberspace is a multistakeholder agreement on cybersecurity principles. It was launched by the French foreign ministry at IGF2018. The currently has over 1,000 official supporters, including 78 national governments.
- The Siemens 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 (GCSC) 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.
- The World Wide Web Foundation’s Contract for the Web was launched in 2019 to create a “a global plan of action to make our online world safe and empowering for everyone.” The agreement includes roles for governments, organizations and individuals alike.
- Ethics for Incident Response and Security Teams (EthicsfIRST) is “designed to inspire and guide the ethical conduct of all Team members, including current and potential practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way.” The initiative includes security teams across sectors.

Trends in international cyber norms

Due to the unique responsibility the United Nations has in matters of international peace and security, and the recognition of the GGE's 11 norms by consensus of the UN General Assembly, the BPF has used these norms as the basis for analysis of the other agreements included in this report. This was in an effort to determine whether or not these multilateral cyber norms are being recognized and reinforced in other agreements in order to be strengthened, implemented, or enforced – including with non-state stakeholders.

An expert contributor to the BPF on Cybersecurity reviewed each of the agreements included in this year's report in order to determine if they reflect any of the 11 cyber norms identified by the 2015 UN GGE consensus report. As various agreements apply to different stakeholder groups, and the GGE norms are written strictly to guide state behavior in cyberspace, the BPF used a simplified, up-leveled, version of each of the 11 UN cyber norms – focused on the resources being protected or the behavior being prohibited/promoted by the norm – when considering whether a similar norm existed in another agreement. The resulting simplified 11 norms considered include:

1. States should not allow territory be used for international wrongful acts via ICTs
2. Do not conduct or support ICT activity that harms critical infrastructure.
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools.
4. Recognizing computer emergency response teams as a protected and benign group.
5. Recognizing human rights online and/or right to privacy.
6. Cooperation with states to increase stability and security in use of ICTs.
7. States (or other stakeholders) should consider all relevant information following ICT incidents.
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.
9. States (or other stakeholders) should protect their own critical infrastructure.
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.
11. Encourage responsible reporting of ICT vulnerabilities and share remedies.

The following charts reflect the frequency with which each of the 11 norms above have been reflected in each of the agreements included in the analysis, as determined by the team of experts. The sixth norm, calling for cooperation to promote stability and security in cyberspace, was the norm most commonly reflected in the other agreements, with some form of it being evident in 77% of the agreements reviewed. It is perhaps unsurprising that the norm most commonly found in such agreements that there should be partnership and cooperation between the parties in the agreement. The next most frequently recognized norm was number five, which is reflected in 68% of the agreements and recognizes of either human rights or privacy rights online. States preventing their own territory from being used in wrongful ICT acts, norm number one, was the UN norm least often reflected in other agreements.

<u>A note on the charts below and the analysis</u>:

Comparing international agreements across regions, and stakeholder groups, necessarily requires that those conducting the analysis make informed assumptions about intentions and meaning in different agreements. It also requires an expansive understanding of each of the norms included, in order to capture when they are reflected in other agreements. Indeed, language reflecting the 11 GGE norms was often found within the preamble of an agreement, or as part of another norm entirely. While the specific language in international agreements is generally carefully crafted and highly intentional, the analysis here focuses less on the specific language and more on the spirit of the norm itself. After all, a norm by definition is not an explicitly defined rule with narrow boundaries but a general principle to be adhered to.

In addition, while the analysis here focuses on the 11 norms established by the UN-GGE for the reasons described above, this is not meant to imply causality or influence in terms of why similar norms are included in other agreements. Several of the agreements included below actually pre-date the 2015 UN-GGE report, so their content could not have been influenced by that report – In fact, it is possible that they would have been influencers of the GGE. Of course, other agreements may have simply independently reached similar conclusions about what norms should be established in cyberspace.

<u>Chart I: frequency of each norm in other agreements</u>

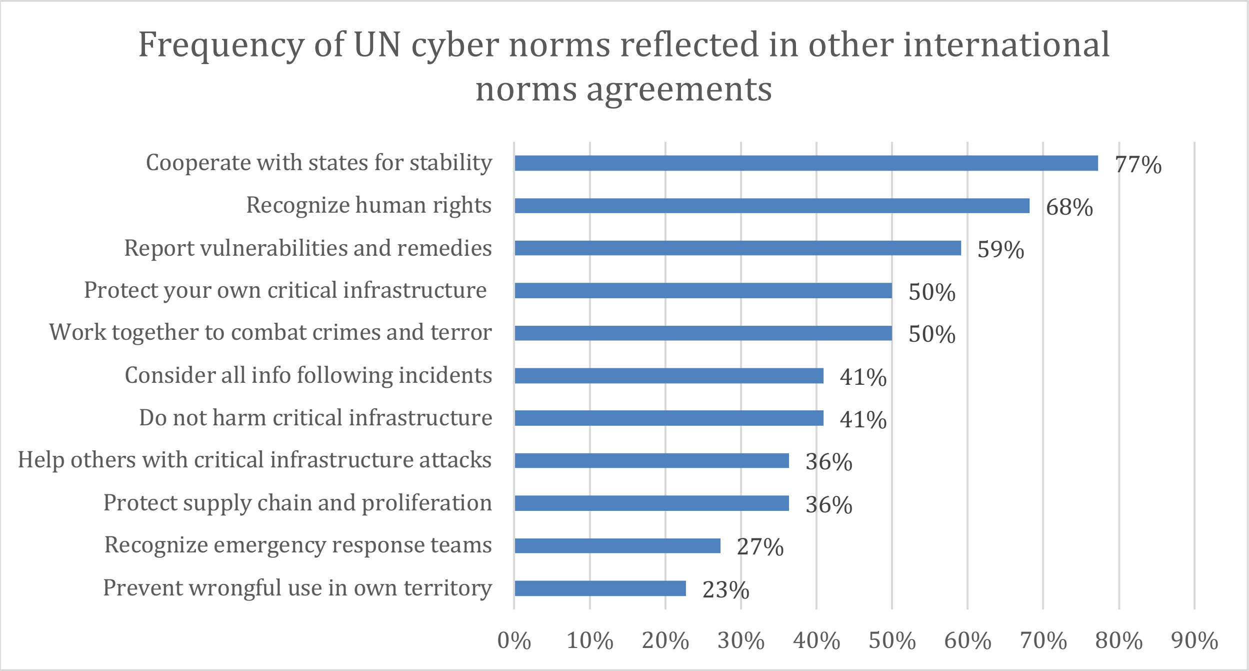

Chart II – UN Cyber norms reflected in each agreement

UN cyber norms reflected in international cybersecurity agreements

		Simplified UN Cyber Norms										
	International Agreements	#1 Prevent wrongful use in territory	#2 Do not harm critical infrastructure	#3 Protect supply chain & against proliferation	#4 Recognize emergency response teams	#5 Recognize human rights/privacy	#6 Cooperate with states for stability	#7 Consider all info following incidents	#8 Work together to combat criminals & terorrists	#9 Protect your own critical infrastructure	#10 Help others with critical infrastructure attacks	#11 Report vulnerabilities and remedies
1	The G20 Antalya Summit Leaders' Communiqué					🟩						
2	The G7 Charlevoix commitment on defending Democracy from foreign threats						🟩					
3	G7 Declaration on Responsible States Behavior in Cyberspace	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
4	The Cybersecurity Tech Accord			🟩			🟩		🟩			🟩
5	The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to cybersecurity					🟩						
6	Shanghai Cooperation Organization Agreement on cooperation in international information security						🟩	🟩	🟩	🟩		
7	The African Union Convention on Cyber Security and Personal Data Protection	🟩	🟩	🟩		🟩	🟩		🟩	🟩	🟩	🟩
8	The Council to Secure the Digital Economy International Anti-Botnet guide		🟩		🟩	🟩	🟩	🟩			🟩	🟩
9	The League of Arab States Convention on Combating Information Technology Offences	🟩	🟩			🟩	🟩	🟩	🟩	🟩	🟩	
10	The East African Community (EAC) Draft EAC Framework for Cyberlaws					🟩	🟩					
11	The Economic Community of Central African States (ECCAS) Declaration of Brazzaville				🟩		🟩					
12	The NATO Cyber Defence Pledge	🟩	🟩	🟩		🟩	🟩	🟩	🟩	🟩	🟩	🟩
13	The EU Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU					🟩	🟩	🟩		🟩		🟩
14	The Mutually Agreed Norms for Routing Security (MANRS)								🟩			🟩
15	The Southern African Development Community Model Laws on Cybercrime		🟩									
16	The Paris Call for Trust and Security in Cyberspace		🟩	🟩		🟩	🟩			🟩	🟩	🟩
17	UN-GGE 2015 consensus report*	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
18	The Siemens Charter of Trust"			🟩			🟩		🟩	🟩		
19	GCSC's Six Critical Norms		🟩	🟩		🟩	🟩	🟩	🟩	🟩		🟩
20	Commonwealth Cyber Declaration				🟩	🟩	🟩			🟩	🟩	🟩
21	World Wide Web Foundation's Contract for the Web					🟩	🟩					🟩
22	Ethics for Incident Response and Security Teams (EthicsfIRST)				🟩	🟩		🟩	🟩			🟩

*all norms are reflected in the 2015 UN-GGE report

Analysis of Agreements

Each of the international cybersecurity agreements featuring cyber norms identified above is reviewed below based on i) when they were initiated, ii) which stakeholders are included, iii) the total number of supporters/signatories, iv) whether there is an organization responsible for maintaining the agreement, v) whether any of the eleven UN-GGE norms are reflected in the agreement, and vi) what other norms are featured.

#	**Agreement** (links included as available)
I.	The G20 Antalya Summit Leaders’ Communiqué
II.	The G7 Charlevoix commitment on defending Democracy from foreign threats
III.	G7 Declaration on Responsible States Behavior in Cyberspace
IV.	The Cybersecurity Tech Accord
V.	The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security
VI.	In the Shanghai Cooperation Organization’s Agreement on cooperation in the field of ensuring the international information security
VII.	The African Union Convention on Cyber Security and Personal Data Protection
VIII.	The Council to Secure the Digital Economy International Anti-Botnet guide
IX.	The League of Arab States Convention on Combating Information Technology Offences
X.	The East African Community (EAC) Draft EAC Framework for Cyberlaws
XI.	The Economic Community of Central African States (ECCAS) Declaration of Brazzaville
XII.	The NATO Cyber Defence Pledge
XIII.	The EU Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU
XIV.	The Mutually Agreed Norms for Routing Security **(**MANRS**)**
XV.	The Southern African Development Community Model Laws on Cybercrime
XVI.	The Paris Call for Trust and Security in Cyberspace
XVII.	UN Group of Governmental Experts (GGE) on information security combined consensus reports from 2010/2013/2015 – “The Framework for Responsible State Behavior in Cyberspace” – which includes the 11 norms featured in the 2015 consensus report.
XVIII.	The Siemens Charter of Trust”
XIX.	GCSC’s Six Critical Norms
XX.	Commonwealth Cyber Declaration
XXI.	World Wide Web Foundation’s Contract for the Web
XXII.	Ethics for Incident Response and Security Teams (EthicsfIRST)

I. G20 Leaders' Communiqué, Antalya Summit

A. Date it was signed/launched: November, 2015

B. Stakeholders who are party to the agreement: Governments

C. Total number of signatories/supporters of the agreement: 19 member-states.

D. Organization responsible for the agreement: G20

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

The Communiqué welcomes the 2015 report of the GGE and affirms that "international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs in accordance with UN resolution A/C.1/70/L.45."

1. States should not allow territory be used for international wrongful acts via ICTs. **– N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. **– N/A**
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. **– N/A**
4. Recognizing computer emergency response teams as a protected and benign group. **– N/A**
5. Recognizing human rights online and/or right to privacy. **– Yes.**
    a) *"All states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications."*
    b) Cooperation with states to increase stability and security in use of ICTs. **– N/A**
    c) States (or other stakeholders) should consider all relevant information following ICT incidents. **– N/A**
    d) States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. **– N/A**
    e) States (or other stakeholders) should protect their own critical infrastructure. **– N/A**
    f) States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack. **– N/A**
    g) Encourage responsible reporting of ICT vulnerabilities and share remedies. **– N/A**

F. Additional norms included in the agreement:

"[W]e 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."

II. G7 Declaration on Responsible States Behavior in Cyberspace

A. Date it was signed/launched: April, 2017

B. Stakeholders who are party to the agreement: Governments

C. Total number of signatories/supporters of the agreement: 7 Countries

D. Organization responsible for ongoing management of the agreement: N/A

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

IMPORTANT*: The Lucca Declaration restates **all 2015 GGE** norms and 2015 G20 Leaders' Communiqué, quoting the resolution/communiqué. That repetitive norms language is reflected below in red. Meanwhile, in black are references reflected in other sections of the document and that might contain a different approach or nuance than the list of norms at the end of the document.

1. States should not allow territory be used for international wrongful acts via ICTs
   a) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
2. Do not conduct or support ICT activity that harms critical infrastructure.
   a) A State 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;
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools.
   a) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;
4. Recognizing computer emergency response teams as a protected and benign group.
   a) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.
5. Recognizing human rights online and/or right to privacy
   a) Indirect reference to the UNGA Resolution on the Right to Privacy in the Digital Age: "*We also reaffirm that the same rights that people have offline must also be protected online and reaffirm the applicability of international human rights law in cyberspace, including the UN Charter, customary international law and relevant treaties*".
   States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;
   b) Cooperation with states to increase stability and security in use of ICTs
   "*We recognize the urgent necessity of increased international cooperation to promote security and stability in cyberspace, including on measures aimed at reducing the malicious use of ICTs by State and non-State actors*".
   Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;
   c) States (or other stakeholders) should consider all relevant information following ICT incidents.
   States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats.
   States may need to consider whether new measures need to be developed in this respect; In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

d) States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs;
States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

e) States (or other stakeholders) should protect their own critical infrastructure
States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

f) States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.
States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

g) Encourage responsible reporting of ICT vulnerabilities and share remedies
States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

F. Additional norms included in the agreement:

It should be noted that, unlike other declarations that only reinforce their commitment to the GGE 2015 norms, the Lucca Declaration of the G7 indicates a future pathway of commitment towards the promotion of "a strategic framework for conflict prevention, cooperation and stability in cyberspace" that observes the applicability of IL to state behavior in cyberspace, promotion of voluntary, non-binding norms of responsible State behavior during peacetime and the implementation and development of CBMs.

- Specific note on cyber attribution: *"We note that the customary international law of State responsibility supplies the standards for attributing acts to States, which can be applicable to activities in cyberspace. In this respect, States cannot escape legal responsibility for internationally wrongful cyber acts by perpetrating them through proxies […] In this context, a State assesses the facts and is free to make its own determination in accordance with international law with respect to attribution of a cyber-act to another State;"*
- Calls for public explanation from states on how IL applies to cyberspace.
- Refers to 2016 G7 document on "Principles and Actions on Cyber" that recognized the right of states to exercise collective or individual self-defense in accordance with Art. 51 of the UN Charter: "*We also recognized that States may exercise their inherent right of individual or collective self-defense as recognized in Article 51 of the United Nations Charter and in accordance with international law, including international humanitarian law, in response to an armed attack through cyberspace;"*
- Endorses CBMs as an "essential element to strengthen international peace and security".
- Calls against intellectual property theft and espionage; "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.

Not necessarily a norm, but more of a general comment. The G7 Lucca Declaration highlights member-states' position on what norms are and their importance for international cybersecurity:

> "In addition, we support the promotion of voluntary, non-binding norms of responsible State behavior in cyberspace during peacetime, which can reduce risks to international peace, security and stability. Such norms do not seek to limit or prohibit any action that is

otherwise consistent with international law. Nor do norms limit a State’s obligations under international law, including with regard to human rights**. Norms reflect the current expectations of the international community, set standards for responsible State behavior, and allow the international community to assess the activities and intentions** of States. **Norms can help to prevent conflict in the ICT environment** and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development.”

III. G7 Charlevoix Commitment on Defending Democracy from Foreign Threats

A. Date it was signed/launched: June, 2018

B. Stakeholders who are party to the agreement: Governments

C. Total number of signatories/supporters of the agreement: 7 member-states.

D. Organization responsible for the agreement: N/A

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs**– N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. **– N/A**
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. **– N/A**
4. Recognizing computer emergency response teams as a protected and benign group. **– N/A**
5. Recognizing human rights online and/or right to privacy. **– N/A**
6. Cooperation with states to increase stability and security in use of ICTs **– Yes.**

   Establish a G7 Rapid Response Mechanism to strengthen our coordination to identify and respond to diverse and evolving threats to our democracies, including through sharing information and analysis, and identifying opportunities for coordinated response.

   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.
7. States (or other stakeholders) should consider all relevant information following ICT incidents. **– N/A**
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. **– N/A**
9. States (or other stakeholders) should protect their own critical infrastructure. **– N/A**
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack. **– N/A**
11. Encourage responsible reporting of ICT vulnerabilities and share remedies. **– N/A**

F. Additional norms included in the agreement:

It calls for cross-sector collaboration in sharing lessons and best practices in promoting a peaceful, stable, secure and rights-respecting approach to defending democracy against foreign threats: *"Share lessons learned and best practices in collaboration with governments, civil society and the private sector that are developing related initiatives including those that promote free, independent and pluralistic media; fact-based information; and freedom of expression."*

It also singles out ISPs and social media platforms as key actors in information sharing practices to ensure privacy and prevention of illegal use of personal data: *"Engage directly with internet service providers and social media platforms regarding malicious misuse of information technology by foreign actors, with a particular focus on improving transparency regarding the use and seeking to prevent the illegal use of personal data and breaches of privacy."*

Given the scope of the Charlevoix Commitment, G7 countries also endorsed the following norms:

- Media literacy/Education: *Support public learning and civic awareness aimed at promoting critical thinking skills and media literacy on intentionally misleading information, and improving online security and safety.*
- Transparency in reporting during elections: *In accordance with applicable laws, ensure a high level of transparency around sources of funding for political parties and all types of political advertising, especially during election campaigns.*

IV. Cybersecurity Tech Accord

A. Date it was signed/launched: April, 2018

B. Stakeholders who are party to the agreement: Industry – Technology Industry.

C. Total number of signatories/supporters of the agreement: 145

D. Organization responsible for the agreement: There is a secretariat responsible for managing the agreement and its efforts.

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs. – **N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. – **N/A**
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. – **Yes.**
   We will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use.
4. Recognizing computer emergency response teams as a protected and benign group. – **N/A**
5. Recognizing human rights online and/or right to privacy. – **N/A**
6. Cooperation with states to increase stability and security in use of ICTs. – **Yes**
   We will support civil society, governments and international organizations in their efforts to advance security in cyberspace and to build cybersecurity capacity in developed and emerging economies alike.
7. States (or other stakeholders) should consider all relevant information following ICT incidents – **N/A**
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. – **Yes**
   We will encourage global information sharing and civilian efforts to identify, prevent, detect, respond to, and recover from cyberattacks and ensure flexible responses to security of the wider global technology ecosystem.
9. States (or other stakeholders) should protect their own critical infrastructure – **N/A**
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack – **N/A**
11. Encourage responsible reporting of ICT vulnerabilities and share remedies. – **Yes.**
   We will work with each other and will establish formal and informal partnerships with industry, civil society, and security researchers, across proprietary and open source technologies to improve technical collaboration, coordinated vulnerability disclosure, and threat sharing, as well as to minimize the levels of malicious code being introduced into cyberspace.

F. Additional norms included in the agreement:

1. We will protect all of our users and customers everywhere.
   a. We will strive to protect all our users and customers from cyberattacks – whether an individual, organization or government – irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical.
   b. We will design, develop, and deliver products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability, and severity of vulnerabilities.
2. We will oppose cyberattacks on innocent citizens and enterprises from anywhere.
   a. We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere.
3. We will help empower users, customers and developers to strengthen cybersecurity protection.
   a. We will provide our users, customers and the wider developer ecosystem with information and tools that enable them to understand current and future threats and protect themselves against them.
4. We will partner with each other and with likeminded groups to enhance cybersecurity.

V. Freedom Online Coalition

A. Date it was signed/launched: September 2015

B. Stakeholders who are party to the agreement: Governments

C. Total number of signatories/supporters of the agreement: 32

D. Organization responsible for the agreement: Freedom Online Coalition

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs **– N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. **– N/A**
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. **– N/A**
4. Recognizing computer emergency response teams as a protected and benign group. **– N/A**
5. Recognizing human rights online and/or right to privacy **– Yes.**
    a. *1. Cybersecurity policies and decision-making processes should protect and respect human rights.*
    b. *2. The development of cybersecurity-related laws, policies, and practices should from their inception be human rights respecting by design.*
    c. *4. The development and implementation of cybersecurity-related laws, policies and practices should be consistent with international law, including international human rights law and international humanitarian law*
    d. *5. Cybersecurity-related laws, policies and practices should not be used as a pretext to violate human rights, especially free expression, association, assembly, and privacy*
    e. *6. Responses to cyber incidents should not violate human rights.*
    f. *8.Cybersecurity-related laws, policies and practices should reflect the key role of encryption and anonymity in enabling the exercise of human rights, especially free expression, association, assembly, and privacy."*
    g. *9. Cybersecurity-related laws, policies and practices should not impede technological developments that contribute to the protection of human rights.*
    h. *10. Cybersecurity-related laws, policies, and practices at national, regional and international levels should be developed through open, inclusive, and transparent approaches that involve all stakeholders.*
    i. *11. Stakeholders should promote education, digital literacy, and technical and legal training as a means to improving cybersecurity and the realization of human rights.*
    j. *12. Human rights respecting cybersecurity best practices should be shared and promoted among all stakeholders.*
    k. *13. Cybersecurity capacity building has an important role in enhancing the security of persons both online and offline; such efforts should promote human rights respecting approaches to cybersecurity*
6. Cooperation with states to increase stability and security in use of ICTs. **– N/A**
7. States (or other stakeholders) should consider all relevant information following ICT incidents. **– N/A**
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. **– N/A**
9. States (or other stakeholders) should protect their own critical infrastructure. **– N/A**
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack. **– N/A**
11. Encourage responsible reporting of ICT vulnerabilities and share remedies. **– N/A**

F. Additional norms included in the agreement: N/A

VI. Agreement in Ensuring International Information Security Between Member States of the Shanghai Cooperation Organization.

A. Date it was signed/launched: June, 2009

B. Stakeholders who are party to the agreement: Governments

C. Total number of signatories/supporters of the agreement: 6

D. Organization responsible for ongoing management of the agreement: Shanghai Cooperation Organization

E. Norms adapted from 2015 UN-GGE consensus report reflected in the agreement

Even though the SCO Agreement precedes the GGE report, it does mention the UNGA on "Developments in the field of information and telecommunications in the context of international security" – probably the latest report A/RES/63/37 Jan 2009.

Overall, the agreement establishes the conditions through which information security cooperation should be conducted in the SCO. It provides a list of common key threats and *basic* threats (annex) to international information security (Art. 2), establishes main areas, principles, formats and mechanisms for collaboration and specifications on the protection of information, funding and relationship of the agreement with other international treaties.

1. States should not allow territory be used for international wrongful acts via ICTs **– N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. – **N/A**
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. – **N/A**
4. Recognizing computer emergency response teams as a protected and benign group. – **N/A**
5. Recognizing human rights online and/or right to privacy – **N/A**
6. Cooperation with states to increase stability and security in use of ICTs – **Yes**
    - *defining, coordinating and implementing necessary joint measures in the field of ensuring international information security; (Art. 3)*
    - *conducting expertise, research and evaluation in the field of information security necessary for the purposes of this Agreement; (Art. 3)*
    - *promoting secure, stable operation and governance internationalization of the global Internet network; (Art. 3)*
    - *creating of a system of joint monitoring and response to emerging threats in this area; (Art. 3)*
    - *developing and implementing joint measures of trust conducive to ensuring international information security*
7. States (or other stakeholders) should consider all relevant information following ICT incidents – **Yes**
    - *exchanging information on issues related to the cooperation in the basic areas listed in this Article (Art.3)*
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. – **Yes**
    - *[SCO parties shall cooperate in] countering threats related to the use of information and communication technologies for terrorist purposes (Art. 3)*
    - *Combatting cybercrime (Art.3)*
9. States (or other stakeholders) should protect their own critical infrastructure – **Yes**
    - ensuring information security of the critically significant structures of the Parties (Art.3)
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack – **N/A**
11. Encourage responsible reporting of ICT vulnerabilities and share remedies – **N/A**

F. Additional norms included in the agreement:

- Capacity building:

    - exchanging experience, training of specialists, holding working meetings, conferences, seminars and other forums of authorized representatives and experts of the Parties in the field of information security; (Art. 3(15))
    - creating conditions for cooperation between the competent authorities of the Parties in order to implement this Agreement (Art. 3(13)).
- Data protection and cross-border data flows: developing and implementing coherent policies and organizational and technical procedures for the implementation of digital signature and data protection in the cross-border exchange of information (Art.3(10))
- More on cooperation and knowledge exchange:
    - exchanging information on the legislation of the Parties on issues of information security (Art.3(11)).
    - interacting within international organizations and fora on issues of international information security (Art.3(14))
    - elaborating joint measures for the development of the provisions of the international law limiting the spread and use of information weapons threatening defense capacity, national security and public safety (Art.3(3)).
- Cooperation will be conducted in a way that is consistent “with universally recognized principles and norms of the international law, including the principles of peaceful settlement disputes and conflicts, non-use of force, non-interference in internal affairs, respect for human rights and fundamental freedoms, as well as the principles of regional cooperation and non- interference in the information resources of the Parties” (Art.4 (1)).

VII. African Union Convention on Cyber Security and Personal Data Protection

A. Date it was signed/launched: June 2014

B. Stakeholders who are party to the agreement: Governments in Africa

C. Total number of signatories/supporters of the agreement: 14/55 Signed 8/55 Ratified and Deposited

D. Organization responsible for the agreement: African Union

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs – **Yes**
    - *Article 29*
    - *Offences specific to Information and Communications Technologies*
    - *"Participate in an association formed or in an agreement established with a view to preparing or committing one or several of the offences provided for under this Convention."*
2. Do not conduct or support ICT activity that harms critical infrastructure. – **Yes**
    - *Article 25*
    - *" 4. Protection of Critical Infrastructure*
    - *Each State Party shall adopt such legislative and/or regulatory measures as they deem necessary to identify the sectors regarded as sensitive for their national security and well-being of the economy, as well as the information and communication technologies systems designed to function in these sectors as elements of critical information infrastructure; and, in this regard, proposing more severe sanctions for criminal activities on ICT systems in these sectors, as well as measures to improve vigilance, security and management."*
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. – **Yes**
    - *Article 29*
    - *Offences specific to Information and Communications Technologies*
    - *"g. Adopt regulations compelling vendors of information and communication technology products to have vulnerability and safety guarantee assessments carried out on their products by independent experts and researchers, and disclose any vulnerabilities detected and the solutions recommended to correct them to consumers;*
    - *h. Take the necessary legislative and/or regulatory measures to make it a criminal offence to unlawfully produce, sell, import, possess, disseminate, offer, cede or make available computer equipment, program, or any device or data designed or specially adapted to commit offences, or unlawfully generate or produce a password, an access code or similar computerized data allowing access to part or all of a computer system"*
4. Recognizing computer emergency response teams as a protected and benign group. – **N/A**
5. Recognizing human rights online and/or right to privacy – **Yes**
    - *Article 25*
    - *"In adopting legal measures in the area of cyber security and establishing the framework for implementation thereof, each State Party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others."*
6. Cooperation with states to increase stability and security in use of ICTs – **Yes**
    - *Article 28*
    - *International cooperation*
    - *" 1. Harmonization*
    - *State Parties shall ensure that the legislative measures and/or regulations adopted to fight against cyber-crime will strengthen the possibility of regional harmonization of these measures and respect the principle of double criminal liability."*
7. States (or other stakeholders) should consider all relevant information following ICT incidents – **N/A**

8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs – **Yes**
    - *Article 28*
    - *International Cooperation*
    - *"2. Mutual legal assistance*
    - *State Parties that do not have agreements on mutual assistance in cyber-crime shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal liability, while promoting the exchange of information as well as the efficient sharing of data between the organizations of State Parties on a bilateral and multilateral basis."*
9. States (or other stakeholders) should protect their own critical infrastructure – **Yes**
    - *Article 25*
    - *" 4. Protection of Critical Infrastructure*
    - *Each State Party shall adopt such legislative and/or regulatory measures as they deem necessary to identify the sectors regarded as sensitive for their national security and well-being of the economy, as well as the information and communication technologies systems designed to function in these sectors as elements of critical information infrastructure; and, in this regard, proposing more severe sanctions for criminal activities on ICT systems in these sectors, as well as measures to improve vigilance, security and management."*
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack – **Yes** (indirectly)
    - *Article 28*
    - *International Cooperation*
    - *" 2. Mutual legal assistance*
    - *State Parties that do not have agreements on mutual assistance in cyber-crime shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal liability, while promoting the exchange of information as well as the efficient sharing of data between the organizations of State Parties on a bilateral and multilateral basis."*
11. Encourage responsible reporting of ICT vulnerabilities and share remedies – **Yes**
    - *Article 29*
    - *Offences specific to Information and Communications Technologies*
    - *"g. Adopt regulations compelling vendors of information and communication technology products to have vulnerability and safety guarantee assessments carried out on their products by independent experts and researchers, and disclose any vulnerabilities detected and the solutions recommended to correct them to consumers;"*

F. Additional norms included in the agreement:

Promotion of Cybersecurity Governance

"Article 27

National cyber security monitoring structures

Cyber security governance

a) *Each State Party shall adopt the necessary measures to establish an appropriate institutional mechanism responsible for cyber security governance;*

b) *The measures adopted as per paragraph 1 of this Article shall establish strong leadership and commitment in the different aspects of cyber security institutions and relevant professional bodies of the State Party. To this end, State Parties shall take the necessary measures to:*

i) Establish clear accountability in matters of cyber security at all levels of Government by defining the roles and responsibilities in precise terms;

Express a clear, public and transparent commitment to cyber security;

Encourage the private sector and solicit its commitment and participation in government-led initiatives to promote cyber security.

c) *Cyber security governance should be established within a national framework that can respond to the perceived challenges and to all issues relating to information security at national level in as many areas of cyber security as possible."*

<u>Promote Multi stakeholder</u>

"Article 26

National cyber security system

1. *Culture of Cyber Security*

a) *Each State Party undertakes to promote the culture of cyber security among all stakeholders, namely, governments, enterprises and the civil society, which develop, own, manage, operationalize and use information systems and networks. The culture of cyber security should lay emphasis on security in the development of information systems and networks, and on the adoption of new ways of thinking and behaving when using information systems as well as during communication or transactions across networks.*

b) *As part of the promotion of the culture of cyber security, State Parties may adopt the following measures: establish a cyber-security plan for the systems run by their governments; elaborate and implement programmes and initiatives for sensitization on security for systems and networks users; encourage the development of a cyber-security culture in enterprises; foster the involvement of the civil society; launch a comprehensive and detailed national sensitization programme for Internet users, small business, schools and children.*

3. *Public-Private Partnership*

Each State Party shall develop public-private partnership as a model to engage industry, the civil society, and academia in the promotion and enhancement of a culture of cyber security."

<u>Confidence Building Measures</u>

"Article 26

National cyber security system

2. Role of Governments

Each State Party shall undertake to provide leadership for the development of the cyber security culture within its borders. Member States undertake to sensitize, provide education and training, and disseminate information to the public.

4. Education and training

Each State Party shall adopt measures to develop capacity building with a view to offering training which covers all areas of cyber security to different stakeholders, and setting standards for the private sector.

States Parties undertake to promote technical education for information and communication technology professionals, within and outside government bodies, through certification and standardization of training; categorization of professional qualifications as well as development and needs-based distribution of educational material."

VIII. The Council to Secure the Digital Economy International Anti-Botnet guide (2018 & 2020)

A. Date it was signed/launched: Initial document was finished in November 2018, while the latest one on their website was finished in November 2019 (2020)

B. Stakeholders who are party to the agreement: Industry

C. Total number of signatories/supporters of the agreement: 14 enterprises / companies

D. Organization responsible for the agreement: Council to Secure the Digital Economy (CSDE)

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs. **– N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. – **Yes.**

   The global economy, critical infrastructure and government operations have increased their dependence on software.

3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. **– N/A**
4. Recognizing computer emergency response teams as a protected and benign group. **– Yes**

   REAL-TIME INFORMATION SHARING*: Enterprises should be prepared to receive and act responsively and responsibly upon cyber threat information provided by information sharing activities even when not yet committed to actively share information. Examples include information from government and law enforcement information sharing activities, various CERTs, industry groups, network providers, RFC2142 addresses, and updates and alerts from vendors and other sources. (2018/ P.34; 2020/p.41)*

5. Recognizing human rights online and/or right to privacy. **– Yes.**

   Whether inadvertent or malicious, improper actions by privileged users can have disastrous effects on IT operations and the overall security and privacy of organizational assets and information. (2018/p. 36; 2020/p.44)

6. Cooperation with states to increase stability and security in use of ICTs **– Yes.**
   - *They are able to work in partnership with government and industry to take down malicious botnets. They may also offer commercial services such as scrubbing traffic and DDoS protection. (2018/p.18; 2020/p.23)*
   - *Threat modeling and analysis of risks to architecture: Companies that work with governments or whose operations are highly sensitive may hire teams of experts to determine how malicious actors would hypothetically create or exploit vulnerabilities in a system to achieve nefarious ends. A threat model may consider many types of risks, including those involving automated, distributed attacks.(2018/p.24; 2020/p29)*
7. States (or other stakeholders) should consider all relevant information following ICT incidents. – **Yes**.

   The entirety of the “secure-by-design” section.

8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. **– N/A**
9. States (or other stakeholders) should protect their own critical infrastructure. **– N/A**
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack. **– Yes.**

    Enterprises should be prepared to receive and act responsively and responsibly upon cyber threat information provided by information sharing activities even when not yet committed to actively share information.(2018/p.34; 2020p.41)

11. Encourage responsible reporting of ICT vulnerabilities and share remedies. **– Yes.**

    Enterprises should maintain contact with sharing communities and be aware of the processes and safeguards to properly report/share cyber security incidents within their region and industry. (2018/p.34; 2020/p.42)

F. Additional norms included in the agreement: N/A

IX. Arab Convention on Combating Information Technology Offences

https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab Convention on Combating Information Technology Offences.pdf

A. Date it was signed/launched: Adopted on 21 December 2010 and came into force in 2014 (after the ratification of seven states).[1]

B. Stakeholders who are party to the agreement: Governments **–** Jordan, Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, United Arab Emirates, Tunisia, Algeria, Djibouti, Sudan, Syria, Somalia, Iraq, Palestine, Comoros, Lebanon, Libya, Egypt, Morocco, Mauritius and Yemen.

C. Total number of signatories/supporters of the agreement: 22

D. Organization responsible for the agreement: General Secretariat of the Council of Arab Interior Ministers (CAIM) and the Technical Secretariat of the Arab Justice Ministers.

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs. – **Yes.**
   a) *Desiring to enhance cooperation between themselves to combat information technology offences threatening their security, interests and the safety of their communities, (Preamble)*
   b) *Convinced of the need to adopt a common criminal policy aimed at protecting the Arab society against information technology offences, (Preamble)*
   c) *to enhance and strengthen cooperation between the Arab States in the area of combating information technology offences to ward off the threats of such crimes in order to protect the security and interests of the Arab States and the safety of their communities and individuals. (Preamble)*
   d) ***Article 9**: **Offence of Misuse of Information Technology Means** (1)- The production, sale, purchase, import, distribution or provision of: a- any tools or programmes designed or adapted for the purpose of committing the offences indicated in Articles 6 to 8. b- the information system password, access code or similar information that allows access to the information system with the aim of using it for any of the offences indicated in Articles 6 to 8. (2)- The acquisition of any tools or programmes mentioned in the two paragraphs above with the aim of using them to commit any of the offences indicated in Articles 6 to 8.*
2. Do not conduct or support ICT activity that harms critical infrastructure. – **Yes.**

   ***Article 6: Offense of Illicit Access**: (1)- Illicit access to, presence in or contact with part or all of the information technology, or the perpetuation thereof. (2)- The punishment shall be increased if this access, presence, contact or perpetuation leads to: a- the obliteration, modification, distortion, duplication, removal or destruction of saved data, electronic instruments and systems and communication networks, and damages to the users and beneficiaries. b- the acquirement of secret government information*
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. -- **– N/A**
4. Recognizing computer emergency response teams as a protected and benign group. **– N/A**
5. Recognizing human rights online and/or right to privacy – **Yes.**
   a) *Adhering to the relevant Arab and international treaties and charters on human rights, and guaranteeing, respecting and protecting them (Preamble)*
   b) ***Article 14**: **Offence Against Privacy** - Offence against privacy by means of information technology*
6. Cooperation with states to increase stability and security in use of ICTs. – **Yes.**
   a) *The purpose of this convention is to enhance and strengthen cooperation between the Arab States in the area of combating information technology offences to ward off the threats of such crimes in order to protect the security and interests of the Arab States and the safety of their communities and individuals (Preamble)*
7. States (or other stakeholders) should consider all relevant information following ICT incidents **– Yes.**

[1] https://www.unescwa.org/sites/www.unescwa.org/files/uploads/policy-recommendations-cybersafety-arab-region-summary-english.pdf & https://www.chathamhouse.org/sites/default/files/publications/research/2018-07-04-cybercrime-legislation-gcc-hakmeh.pdf

a) ***Article 28: Expeditious Gathering of Users Tracking Information** – (1)- Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to: a- gather or register using technical means in the territory of this State Party. b- require the service provider, within his technical competence, to: - gather or register using technical means in the territory of this State Party, or - cooperate with and help the competent authorities to expeditiously gather and register users tracking information with the relevant communications and which are transmitted by means of the information technology. (2)- If, because of the domestic legal system, the State Party is unable to adopt the procedures set forth in paragraph 1(a), it may adopt other procedures in the form necessary to ensure the expeditious gathering and registration of users tracking information corresponding to the relevant communications in its territory using the technical means in that territory. (3)- Every State Party shall commit itself to adopting the procedures necessary to require the service provider to maintain the secrecy of any information when exercising the authority set forth in this Article.*

b) ***Article 33 - Circumstantial Information:** (1)- A State Party may – within the confines of its domestic law – and without prior request, give another State information it obtained through its investigations if it considers that the disclosure of such information could help the receiving State Party in investigating offences set forth in this convention or could lead to a request for cooperation from that State Party. (2)- Before giving such information, the State Party providing it may request that the confidentiality of the information be kept; if the receiving State Party cannot abide by this request, it shall so inform the State Party providing the information which will then decide about the possibility of providing the information. If the receiving State Party accepts the information on condition of confidentiality, the information shall remain between the two sides.*

8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. **– Yes.**

   ***Article 32: Mutual Assistance** – (1)- All State Party shall lend assistance to each other to the fullest extent for the purposes of investigation, procedures related to information and information technology offences or to gather electronic evidence in offences.*

9. States (or other stakeholders) should protect their own critical infrastructure – **Yes.**

   a) ***Article 5: Criminalization** - Every State Party shall commit itself to the criminalization of acts set forth in this chapter, according to its legislations and statutes.*

   b) ***Article 21: Increasing Punishment for Traditional Crimes Committed by Means of Information Technology** - Every State Party shall commit itself to increasing the punishment for traditional crimes when they are committed by means of information technology*

10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack **– Yes.**

    Article 32: Mutual Assistance – (1)- All State Party shall lend assistance to each other to the fullest extent for the purposes of investigation, procedures related to information and information technology offences or to gather electronic evidence in offences.

11. Encourage responsible reporting of ICT vulnerabilities and share remedies. – **N/A.**

F. Additional norms included in the agreement:

1) Sovereignty:

   i. ***Article 4: Safeguarding Sovereignty** - (1)- Every State Party shall commit itself, subject to its own statutes or constitutional principles, to the discharge of its obligations stemming from the application of this convention in a manner consistent with the two principles of equality of the regional sovereignty of States and the non-interference in the internal affairs of other States.*

   ii. ***Article 35: Refusal of Assistance** - In addition to the grounds for refusal set forth in Article 32, paragraph 4, the State Party from which assistance is requested may refuse assistance if: 1- the request relates to an offence that the* *law of the State Party from which assistance is requested considers as a political offence. 2- It considers that implementing the request could constitute a violation of its sovereignty, security, order or basic interests.*

2) Principles of Sharia Law as a Determinative Legal Framework:

   iii. Taking into account the high religious and moral principles, especially the ordinances of Islamic Law (Shari'a), as well as the human heritage of the Arab Nation which rejects all forms of crimes, and having regard to public order in every State. (Preamble)

X. AC Framework for Cyberlaws

A. Date it was signed/launched: May 2010

B. Stakeholders who are party to the agreement: Governments in East African Community - Burundi, Kenya, Rwanda, Tanzania, and Uganda

C. Total number of signatories/supporters of the agreement: 5

D. Organization responsible for ongoing management of the agreement: N/A

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs. – **N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. – **N/A**
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. – **N/A**
4. Recognizing computer emergency response teams as a protected and benign group. – **N/A**
5. Recognizing human rights online and/or right to privacy –**Yes**
    - *“The Task Force recognises the critical importance of data protection and privacy and recommends that further work needs to carried out on this issue, to ensure that (a) the privacy of citizens is not eroded through the Internet.*
    - *2.5Data Protection and Privacy For the purposes of the Framework, ‘data protection’ is used here to describe those obligations placed upon those entities that process information about living individuals, generally referred to as ‘personal data’. A data protection regime will also grant certain rights upon individual data subjects. The application of data protection rules may be limited only to private sector entities or public bodies. A sectoral regulatory response may be appropriate to address specific uses and abuses of personal data, whether driven by domestic or foreign concerns, such as the financial services sector. In terms of the entity responsible for the processing, the following minimum obligations represent international best practice in the area:*
    - *18 •To comply with certain ‘principles of good practice’ in respect of their processing activities, including accountability, transparency, fair and lawful processing, processing limitation, data accuracy and data security. •To supply the individual with a copy of any personal data being held and processed and provide an opportunity for incorrect data to be amended.”*
6. Cooperation with states to increase stability and security in use of ICTs. -- **Yes**
    - *“The purpose of developing a Cyberlaw Framework for the EAC Partner States is to promote regional harmonisation in the legal response to the challenges raised by the increasing use and reliance on ICT for commercial and administrative activities, specifically in an Internet or cyberspace environment. Such a Framework details those agreed features that should be transposed into national laws and regulations in order to address the various issues identified in respect of the five topics discussed below. These features will include matters that are considered part of an essential response to a specific problem, as well as matters on which the Partner States may optionally choose to adopt measures.”*
7. States (or other stakeholders) should consider all relevant information following ICT incidents – **N/A**
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. -- **N/A**
9. States (or other stakeholders) should protect their own critical infrastructure – **N/A**
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack. -- **N/A**
11. Encourage responsible reporting of ICT vulnerabilities and share remedies. – **N/A**

F. Additional norms included in the agreement: N/A

XI. Declaration of Brazzaville

A. Date it was signed/launched: November 2016

B. Stakeholders who are party to the agreement: Governments [Member States of the Economic Community of States of Central Africa (ECCAS)]

C. Total number of signatories/supporters of the agreement: 11

D. Is there an organization responsible for ongoing management of the agreement: N/A

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs – **N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. – **N/A**
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. – **N/A**
4. Recognizing computer emergency response teams as a protected and benign group. – **Yes**
   - *To support member states in setting up Centers for National Cyber Incident Alerts and Response (CIRT) and in the constitution of a sub-regional CIRT;"*
5. Recognizing human rights online and/or right to privacy – **N/A**
6. Cooperation with states to increase stability and security in use of ICTs – **Yes**

   "1.To support member states in the process of transposing Model laws relating to Telecommunications / ICT and cybersecurity
   2. To facilitate the development of a regulatory reference framework cross-border interconnection;
   3. To support member states in the process of Strengthening capacities and development of Human Resources in terms of cybersecurity;
   4. Support member states in setting up CIRTs national and a sub-regional CIRT;
   5. To assist member states in setting up programs of child protection"
7. States (or other stakeholders) should consider all relevant information following ICT incidents – **N/A**
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs – **N/A**
9. States (or other stakeholders) should protect their own critical infrastructure – **N/A**
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack – **N/A**
11. Encourage responsible reporting of ICT vulnerabilities and share remedies – **N/A**

F. Additional norms included in the agreement: N/A

Confidence Building Measures "To institute awareness campaigns for the whole of the population to the culture of cybersecurity;To promote the establishment of training courses in cybernetics…

XII. NATO - Cyber Defence Pledge

A. Date it was signed/launched: Jul, 2016

B Stakeholders who are party to the agreement: Allied Heads of State and Governments

C. Total number of signatories/supporters of the agreement: NATO is an alliance that consists of 30 independent member countries

D. Organization responsible for the agreement: NATO, e-mail information not available.

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs. **– Yes.**

   ”1. In recognition of the new realities of security threats to NATO, we, the Allied Heads of State and Government, pledge to ensure the Alliance keeps pace with the fast evolving cyber threat landscape and that our nations will be capable of defending themselves in cyberspace as in the air, on land and at sea.”

2. Do not conduct or support ICT activity that harms critical infrastructure. **– Yes.**

   ”2. We reaffirm our national responsibility, in line with Article 3 of the Washington Treaty, to enhance the cyber defences of national infrastructures and networks, and our commitment to the indivisibility of Allied security and collective defence, in accordance with the Enhanced NATO Policy on Cyber Defence adopted in Wales. We will ensure that strong and resilient cyber defences enable the Alliance to fulfil its core tasks. Our interconnectedness means that we are only as strong as our weakest link. We will work together to better protect our networks and thereby contribute to the success of Allied operations.”

3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. **– Yes.**

   ” 5. We, Allied Heads of State and Government, pledge to strengthen and enhance the cyber defences of national networks and infrastructures, as a matter of priority. Together with the continuous adaptation of NATO’s cyber defence capabilities, as part of NATO’s long term adaptation, this will reinforce the cyber defence and overall resilience of the Alliance.”

4. Recognizing computer emergency response teams as a protected and benign group. -- **N/A**
5. Recognizing human rights online and/or right to privacy

   ”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.”

6. Cooperation with states to increase stability and security in use of ICTs

   ” I. Develop the fullest range of capabilities to defend our national infrastructures and networks. This includes: addressing cyber defence at the highest strategic level within our defence related organisations, further integrating cyber defence into operations and extending coverage to deployable networks; deepen co-operation and the exchange of best practices;”

7. States (or other stakeholders) should consider all relevant information following ICT incidents. **– Yes.**

   ”V. Improve our understanding of cyber threats, including the sharing of information and assessments.”

8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. **– Yes.**

   4. We emphasise NATO’s role in facilitating co-operation on cyber defence including through multinational projects, education, training, and exercises and information exchange, in support of national cyber defence efforts. We will ensure that our Alliance is cyber aware, cyber trained, cyber secure and cyber enabled.

9. States (or other stakeholders) should protect their own critical infrastructure. **– Yes.**

   5. We, Allied Heads of State and Government, pledge to strengthen and enhance the cyber defences of national networks and infrastructures, as a matter of priority.

10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack. **– Yes.**

    NATO Policy on Cyber Defence adopted in Wales. We will ensure that strong and resilient cyber defences enable the Alliance to full its core tasks. Our interconnectedness means that we are only as strong as our weakest link. We will work together to better protect our networks and thereby contribute to the success of Allied operations.

11. Encourage responsible reporting of ICT vulnerabilities and share remedies. **– Yes.**
    - *We emphasise NATO's role in facilitating co-operation on cyber defence including through multinational projects, education, training, and exercises and information exchange, in support of national cyber defence eorts. We will ensure that our Alliance is cyber aware, cyber trained, cyber secure and cyber enabled.*
    - *IV. Improve our understanding of cyber threats, including the sharing of information and assessments;*

F. Additional norms included in the agreement:

Article 3 of the Washington Treaty

XIII. Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

A. Date it was signed/launched: September, 2017

B. Stakeholders who are party to the agreement: Governments

C. Total number of signatories/supporters of the agreement: N/A

D. Organization responsible for ongoing management of the agreement: European Union

E. Norms adapted from 2015 UN-GGE consensus report included in the agreement

The Joint statement is a summary of the different initiatives set out by the EU to enhance cyber resilience. With that in mind, it provides a perspective on best practices in operationalizing some of the 2015 GGE norms while restating some of the guiding principles and policy documents guiding this strategic vision of cybersecurity within the Digital Single Market – therefore a bit beyond the scope of the exercise here. Other docs such as the NIS directive, Cybersecurity Act or Blueprint for coordinated cyber attack response. I've added a couple of examples related to the norms below.

However, it also does explicitly endorse the GGE voluntary non-binding norms: "The EU strongly promotes the position that international law, and in particular the UN Charter, applies in cyberspace. As a complement to binding international law, the EU endorses the voluntary non-binding norms, rules and principles of responsible State behaviour that have been articulated by the UN Group of Governmental Experts84; it also encourages the development and implementation of regional confidence building measures, both in the Organisation for Security and Co-operation in Europe and other regions."

1. States should not allow territory be used for international wrongful acts via ICTs – **N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. – **N/A**
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. – **N/A**
4. Recognizing computer emergency response teams as a protected and benign group. – **N/A**
5. Recognizing human rights online and/or right to privacy

   The EU will prioritise international security issues in cyberspace in its international engagements, while also ensuring that cybersecurity does not become a pretext for market protection and the limitation of fundamental rights and freedoms, including the freedom of expression and access to information. 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 Guidelines on online freedom. In that regard, the EU emphasises the importance of all stakeholders' involvement in the governance of the internet.

6. Cooperation with states to increase stability and security in use of ICTs

   A rapid and shared understanding of threats and incidents as they unfold is a prerequisite for deciding whether joint mitigation or response action supported by the EU is needed. Such information exchange requires the involvement of all relevant actors – EU bodies and agencies, as well as Member States – at technical, operational and strategic levels. ENISA, in cooperation with the relevant bodies at Member State and EU level, notably the network of Computer security incident response teams, CERT-EU, Europol and the EU Intelligence and Situation Centre (INTCEN), will also contribute to EU-level situational awareness.

7. States (or other stakeholders) should consider all relevant information following ICT incidents – **Yes**

   Countering hybrid threats: *The EU and NATO will also foster cyber defence research and innovation cooperation, andbuild on the current technical arrangement on cybersecurity information sharing between their respective cybersecurity bodies.*

8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. – **N/A**
9. States (or other stakeholders) should protect their own critical infrastructure – **Yes.**

   The EU cybersecurity certification framework would operate as a voluntary scheme whereby all 'relevant stakeholders' would be called to take measures to deal with the evolving cybersecurity landscape – paying attention to the preservation of ‘essential services’ (transport, energy, health care, banking, financial market infrastructures, drinking water or digital infrastructure).

10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack – **N/A**
11. Encourage responsible reporting of ICT vulnerabilities and share remedies – **Yes.**

    Mentioned under the wider objective of the establishment of an EU cybersecurity certification framework. The Joint communication document recognizes the important role of third party security researchers in discovering vulnerabilities and notes that “conditions to enable coordinated vulnerability disclosure should be created across Member States, building on best practice and relevant standards.”

F. Additional norms included in the agreement:

Reinforces the role of cyber capacity building for global cyber stability: *The EU will continue to promote a rights-based capacity building model, in line with the Digital4Development approach. The priorities for capacity-building will be the EU’s neighborhood and developing countries experiencing fast growing connectivity and rapid development of threats. EU efforts will be complementary to the EU's development agenda in light of the 2030 Agenda for Sustainable Development and overall efforts for institutional capacity building.*

XIV. Mutually Agreed Norms for Routing Security (MANRS)

A. Date it was signed/launched: 2014 (Current version 2.3 updated Sept. 2019)

B. Stakeholders who are party to the agreement: Multistakeholder Network Operators, Internet Exchange Points (IXPs), and Content Delivery Networks (CDNs)

C. Total number of signatories/supporters of the agreement: 528 total members

- 460 – Network Operators
- 56 – IXPs
- 12 – CDN & Cloud Providers

D. Organization responsible for the agreement: The Internet Society

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory to be used for international wrongful acts via ICTs – **N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. – **N/A**
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. – **N/A**
4. Recognizing computer emergency response teams as a protected and benign group. – **N/A**
5. Recognizing human rights online and/or right to privacy. – **N/A**
6. Cooperation with states to increase stability and security in use of ICTs – **N/A**
7. States (or other stakeholders) should consider all relevant information following ICT incidents – **N/A**
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. – **Yes**
   a. CDN & Cloud Providers – "Facilitate global operational communication and coordination"
   b. IXP's – "Facilitate global operational communication and coordination between network operators."
   c. Network Operators – "Coordination – Maintain globally accessible up-to-date contact information"
9. States (or other stakeholders) should protect their own critical infrastructure – **N/A**
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack – **N/A**
11. Encourage responsible reporting of ICT vulnerabilities and share remedies – **Yes.**

    IXP's – "Action 5. Provide monitoring and debugging tools to the members."

F. Additional norms included in the agreement:

CDN & Cloud Providers actions:

- Prevent propagation of incorrect routing information
- Prevent traffic of illegitimate source IP addresses
- Facilitate validation of routing information on a global scale
- Encourage MANRS adoption
- Provide monitoring and debugging tools to peering partners (optional)

IXP Actions:

- Action 1. Prevent propagation of incorrect routing information. (Mandatory)
- Action 2. Promote MANRS to the IXP membership.
- Action 3. Protect the peering platform.
- Action 4. Facilitate global operational communication and coordination between network operators.

Network operator actions:

- **Filtering** – Ensure the correctness of your own announcements and of announcements from your customers to adjacent networks with prefix and AS-path granularity

- **Anti-spoofing** – Enable source address validation for at least single-homed stub customer networks, your own end-users, and infrastructure
- **Coordination** – Maintain globally accessible up-to-date contact information
- **Global Validation** – Publish your data, so others can validate routing information on a global scale

XV. Southern Africa Model Laws

A. Date it was signed/launched: November 2012

B Stakeholders who are party to the agreement: Governments of SADC

C. Total number of signatories/supporters of the agreement: N/A

D. Organization responsible for ongoing management of the agreement: International Telecommunication Union (ITU) and the European Commission through HIPSSA project

C. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs – **N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. – **Yes**

   "A person who intentionally, without lawful excuse or justificationor in excess of a lawful excuse or justificationhinders or interferes with a computer system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure the punishment shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both"

3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. – **N/A**
4. Recognizing computer emergency response teams as a protected and benign group. – **N/A**
5. Recognizing human rights online and/or right to privacy – **N/A**
6. Cooperation with states to increase stability and security in use of ICTs – **N/A**
7. States (or other stakeholders) should consider all relevant information following ICT incidents – **N/A**
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. – **N/A**
9. States (or other stakeholders) should protect their own critical infrastructure. -- **N/A**
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack -- **N/A**
11. Encourage responsible reporting of ICT vulnerabilities and share remedies – **N/A**

F. Additional norms included in the agreement:

It does not address norms but more specific to offences thus indirectly addressing norms such as harmful use of ICT's, criminalising hate speech and denial of genocide and crimes against humanity.

XVI. Paris Call for Trust and Security in Cyberspace.

A. Date it was signed/launched: November, 2018

B. Stakeholders who are party to the agreement: Multistakeholder – governments, industry, civil society, academia, public sector

C. Total number of signatories/supporters of the agreement: 1105

D. Organization responsible for the agreement: French Ministry of European and Foreign Affairs

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs – **N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. – **Yes**

   Protect individuals and infrastructure *– Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure.*

3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. – **Yes**.
   a. ***Lifecycle security*** *– Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain.*
   b. ***Non-proliferation*** *– Develop ways to prevent the proliferation of malicious software and practices intended to cause harm.*
4. Recognizing computer emergency response teams as a protected and benign group. – **N/A**
5. Recognizing human rights online and/or right to privacy – **Yes.**

   In order to respect people's rights and protect them online as they do in the physical world, States must work together, but also collaborate with private-sector partners, the world of research and civil society.

6. Cooperation with states to increase stability and security in use of ICTs – **Yes.**

   ***Supporters of the Paris Call [including states] are therefore committed to working together to: [list all nine principles*]**

7. States (or other stakeholders) should consider all relevant information following ICT incidents – **N/A**
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. – **N/A**
9. States (or other stakeholders) should protect their own critical infrastructure – **Yes.**

   Protect individuals and infrastructure *– Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure.*

10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.

    Protect individuals and infrastructure *– Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure.*

11. Encourage responsible reporting of ICT vulnerabilities and share remedies – **Yes.**

    Non-proliferation *– Develop ways to prevent the proliferation of malicious software and practices intended to cause harm.*

F. Additional norms included in the agreement:

- **Protect the Internet** – Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet.
- **Defend electoral processes** – Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.

- **Defend intellectual property** – Prevent 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 sector.
- **Cyber hygiene** – Support efforts to strengthen an advanced cyber hygiene for all actors.
- **No private hack back** – Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors.
- **International norms** – Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.

XVII. Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security

A. Date it was signed/launched: July 2015

B. Stakeholders who are party to the agreement: UN Member States by General Assembly resolution adopting the report.

C. Total number of signatories/supporters of the agreement: 193

D. Organization responsible for ongoing management of the agreement: N/A

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

Note: This is the agreement which established all the of the GGE norms. They are all reflected.

1. States should not allow territory be used for international wrongful acts via ICTs – **Yes**

   "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;"

2. Do not conduct or support ICT activity that harms critical infrastructure. **– Yes**

   "A State 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;"

3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. **– Yes**

   "States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions"

4. Recognizing computer emergency response teams as a protected and benign group. **– Yes**

   "States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity."

5. Recognizing human rights online and/or right to privacy. **– Yes**

   "States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;"

6. Cooperation with states to increase stability and security in use of ICTs. **– Yes**

   "Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;"

7. States (or other stakeholders) should consider all relevant information following ICT incidents. **– Yes**

   "In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;"

8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. **– Yes**

   "States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;"

9. States (or other stakeholders) should protect their own critical infrastructure. **– Yes**

   "*States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;"*

10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack. **– Yes**

    "States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty."

11. Encourage responsible reporting of ICT vulnerabilities and share remedies. **– Yes**

    "*States should encourage responsible reporting ofICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure."*

F. Additional norms included in the agreement:

Confidence Building Measures

States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

International Cooperation

The 2013 report called upon the international community to work together in providing assistance to: improve the security of critical ICT infrastructure; develop technical skills and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridge the divide in the security of ICTs and their use.

International Law

The adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs and to promote an open, secure, stable, accessible and peaceful ICT environment. These obligations are central to the examination of the application of international law to the use of ICTs by States.

XVIII. Siemens' Charter of Trust

A. Date it was signed/launched: March, 2018

B. Stakeholders who are party to the agreement: Multistakeholder

C. Total number of signatories/supporters of the agreement: 13

D. Organization responsible for ongoing management of the agreement: Charter of Trust Secretariat

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs **– N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. – **N/A**
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools.—**Yes**

    "(2) Responsibility throughout the digital supply chain

    Companies – and if necessary – governments must establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity, and availability by setting baseline standards, such as identity and access management: Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them."

4. Recognizing computer emergency response teams as a protected and benign group. – **N/A**
5. Recognizing human rights online and/or right to privacy – **N/A**
6. Cooperation with states to increase stability and security in use of ICTs

    "(5).Innovation and co-creation

    Combine domain know-how and deepen a joint understanding between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage i.a. contractual Public Private Partnerships"

    "(10) Joint initiatives

    Drive joint initiatives including all relevant stakeholders in order to implement the above principles in the various parts of the digital world without undue delay."

7. States (or other stakeholders) should consider all relevant information following ICT incidents – **N/A**
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. – 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."

9. States (or other stakeholders) should protect their own critical infrastructure. – Yes.

    "(7.) Certification for critical infrastructure and solutions

    Companies – and if necessary – governments establish mandatory independent third-party certifications (based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions."

10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack." – **N/A**
11. Encourage responsible reporting of ICT vulnerabilities and share remedies. – **N/A.**

F. Additional norms included in the agreement:

1.Ownership for cyber and IT security

Anchor the responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and CISOs. Establish clear measures and targets as well as the right mindset throughout organizations – "It is everyone's task".

2.Responsibility throughout the digital supply chain

Encryption: Connected devices must ensure confidentiality for data storage and transmission purposes, wherever appropriate. Continuous protection: Companies must offer updates, upgrades, and patches throughout a reasonable lifecycle for their products, systems, and services via a secure update mechanism.

3.Security by default

Adopt the highest appropriate level of security and data protection and ensure that it is preconfigured into the design of products, functionalities, processes, technologies, operations, architectures, and business models.

4.User-centricity

Serve as a trusted partner throughout a reasonable lifecycle, providing products, systems, and services as well as guidance based on the customer's cybersecurity needs, impacts, and risks.

6.Education

Include dedicated cybersecurity courses in school curricula – as degree courses in universities, professional education, and trainings – in order to lead the transformation of skills and job profiles needed for the future.

9.Regulatory framework

Promote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of WTO; inclusion of rules for cybersecurity into Free Trade Agreements (FTAs).

XIX. Global Commission on the Stability of Cyberspace's Six Critical Norms

A. Date it was signed/launched: November, 2019

B. Stakeholders who are party to the agreement: Government, Industry, Civil Society

C. Total number of signatories/supporters of the agreement: 10

D. Organization responsible for ongoing management of the agreement: Commission on the Stability of Cyberspace (GCSC)

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs – **N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. – **Yes**

   State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.

3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. – **Yes**
   - *NORM to Avoid Tampering: State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace*
   - *NORM Against commandeering of ICT Devices into botnets: State and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes.*
4. Recognizing computer emergency response teams as a protected and benign group. – **N/A**
5. Recognizing human rights online and/or right to privacy – **Yes**.

   Not being listed in these 8 norms but listed in the principles: Respect for Human Rights: Efforts to ensure the stability of cyberspace must respect human rights and the rule of law.

6. Cooperation with states to increase stability and security in use of ICTs – **Yes**.
7. States (or other stakeholders) should consider all relevant information following ICT incidents. – **Yes.**

   Developers and producers of products and services on which the stability of cyberspace depends should (1) prioritize security and stability, (2) take reasonable steps to ensure that their products or services are free from significant vulnerabilities, and (3) take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity.

8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs – **Yes**.

   States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.

9. States (or other stakeholders) should protect their own critical infrastructure – **Yes**.

   Protecting Electoral infrastructure: State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.

10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack – **N/A**
11. Encourage responsible reporting of ICT vulnerabilities and share remedies – **Yes**.

    (Same as item 8.) States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.

F. Additional norms included in the agreement:

1) State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.

2) State and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes.

3) States should enact appropriate measures, including laws, regulations, and training and capacity building, to ensure basic cyber hygiene.

4) Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.

XX. Commonwealth Cyber Declaration

A. Date it was signed/launched: 16-20 April, 2018

B. Stakeholders who are party to the agreement: Governments in the Commonwealth of Nations

C. Total number of signatories/supporters of the agreement: 54 countries

D. Organization responsible for ongoing management of the agreement: Commonwealth Secretariat

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs **– N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. **– N/A**
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. **– N/A**
4. Recognizing computer emergency response teams as a protected and benign group. **– Yes**

   Not listed in the declaration, but they listed these below:

   Highlight the importance of national cybersecurity strategic planning and establishing incident response capabilities, supported by appropriate legislation and a law enforcement and criminal justice system capable of addressing cybercrime.

5. Recognizing human rights online and/or right to privacy. – **Yes**

   Not specific about privacy, but identified human rights:

   a) Affirm that the same rights that citizens have offline must also be protected online.

   b) Recognise that access to information and digital literacy can be a powerful catalyst for economic empowerment and inclusion, and commit to take steps towards expanding digital access and digital inclusion for all communities without discrimination and regardless of gender, race, ethnicity, age, geographic location or language.

   c) *Emphasise that enhanced digital inclusion of young people in the Commonwealth can contribute in a positive way to their education, social engagement and entrepreneurship*.

6. Cooperation with states to increase stability and security in use of ICTs. – **Yes.**

   Commit to promote frameworks for cyberspace, including the applicability of international law, agreed voluntary norms of responsible state behavior, and the development and implementation of confidence building measures to encourage trust, cooperation and transparency, consistent with the 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International security (UNGGE).

7. States (or other stakeholders) should consider all relevant information following ICT incidents. **– N/A**
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. **– N/A**
9. States (or other stakeholders) should protect their own critical infrastructure. –**Yes.**

   Recognising the threats to stability in cyberspace and integrity of the critical infrastructure and affirming our shared commitment to fully abide by the principles and purposes of the Charter of the United Nations to mitigate these risks;

10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack. **– Yes**

    Commit to use national contact points and other practical measures to enable cross-border access to digital evidence through mutually agreed channels to improve international cooperation to tackle cybercrime

11. Encourage responsible reporting of ICT vulnerabilities and share remedies. **– Yes.**

> *Commit to exploring options to deepen cooperation on cybersecurity incidents and responses between Commonwealth member countries, including through the sharing of information about threats, breaches, vulnerabilities, and mitigation measures.*

F. Additional norms included in the agreement:

- *Commit to promote interoperable and global technical standards, through appropriate consultative processes involving industry, academia, governments and other relevant stakeholders, recognising that standards should be open, foster security and trust and not act as barriers to trade, competition or innovation.*
- *Highlight the importance of common standards and the strengthening of data protection and security frameworks, in order to promote public trust in the internet, confidence for trade and commerce, and the free flow of data*
- *Acknowledge the importance of tolerance, respect for diversity, and understanding in cyberspace.*
- *Affirm that the same rights that citizens have offline must also be protected online*.

XXI. A Contract for the Web

A. Date it was signed/launched: November, 2019

B. Stakeholders who are party to the agreement: Multistakeholder

C. Total number of signatories/supporters of the agreement: Over 1,000, including individuals

D. Is there an organization responsible for ongoing management of the agreement: World Wide Web Foundation

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs – **N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. **– N/A**
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. **– N/A**
4. Recognizing computer emergency response teams as a protected and benign group.
5. Recognizing human rights online and/or right to privacy – **Yes.**

   Principle 3: Respect and protect people's fundamental online privacy and data rights
6. Cooperation with states to increase stability and security in use of ICTs

   [From preamble] "*To achieve the Contract's goals, governments, companies, civil society and individuals must commit to sustained policy development, advocacy, and implementation of the Contract text."*
7. States (or other stakeholders) should consider all relevant information following ICT incidents**. – N/A**
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. **– N/A**
9. States (or other stakeholders) should protect their own critical infrastructure. **. – N/A**
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack**. – N/A**
11. Encourage responsible reporting of ICT vulnerabilities and share remedies – **Yes.**

    Principle 6-1(c) **– "***By being accountable for their work, through regular reports, including how they are… c. Assessing and addressing risks created by their technologies…"*

F. Additional norms included in the agreement:

Governments will…

1. Ensure everyone can connect to the internet
2. Keep all of the internet available, all of the time
3. Respect and protect people's fundamental online privacy and data rights

Companies will…

1. Make the internet affordable and accessible to everyone
2. Respect and protect people's privacy and personal data to build online trust
3. Develop technologies that support the best in humanity and challenge the worst

Citizens will…

1. Be creators and collaborators on the Web
2. Build strong communities that respect civil discourse and human dignity
3. Fight for the Web

XXII. EthicsfIRST

A. Date it was signed/launched: Information not available

B. Stakeholders who are party to the agreement: EthicsfIRST is designed to inspire and guide the ethical conduct of all Team members, including current and potential practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way.

C. Total number of signatories/supporters of the agreement : Information not available

D. Organization responsible for the agreement: First, Improving security Together

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. States should not allow territory be used for international wrongful acts via ICTs – **N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure **– N/A**
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. – **N/A**
4. Recognizing computer emergency response teams as a protected and benign group. – **Yes.**

   Duty to Team health

   Teams have a responsibility to continue to provide the services they have promised their constituents. This responsibility includes the physical and emotional health of the Team.

   In order to both respect as individuals the members who make up a Team and enable the longterm viability of sustaining an adequate level of service, a Team should strive to maintain a healthy, safe, and positive work environment that supports the physical and emotional health of (all) its members. In order to respond to a crisis, "normal" operations should support emotional health and stress reduction.

5. Recognizing human rights online and/or right to privacy – **Yes.**

   "Duty to respect human rights

   Team members should be aware that their actions may impact human rights of others through the sharing of information, a possible bias in their actions, or an infringement of property rights. Team members have access to a wide range of personal, sensitive, and confidential information in the course of handling incidents. This information should be handled in a way to uphold human rights.

   During incident handling, responders should not act in a biased manner and should do their utmost to eliminate bias from their processes and decision-making, either performed by responders or built into algorithms.

   For the purpose of this principle, the notion of "property" (UN Declaration of Human Rights: Article 17) includes intangibles such as intellectual property, as well as ideas and concepts in general, regardless of whether they are legally protected (e.g., patented)."

6. Cooperation with states to increase stability and security in use of ICTs **– N/A**
7. States (or other stakeholders) should consider all relevant information following ICT incidents. – **Yes.**

   Duty of coordinated vulnerability disclosure

   Team members who learn of a vulnerability should follow coordinated vulnerability disclosure by cooperating with stakeholders to remediate the security vulnerability and minimize harm associated with disclosure. Stakeholders include but are not limited to the vulnerability reporter, affected vendor(s), coordinators, defenders, and downstream customers, partners, and users.

   Data that may help other response Teams in their efforts related to other incidents should be made available to them, possibly in redacted form. Information that is confidential and proprietary should only be made available with appropriate protections.

8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. – **Yes.**

Team members should coordinate with appropriate stakeholders to agree upon clear timelines and expectations for the release of information, providing enough details to allow users to evaluate their risk and take actionable defensive measures.

9. States (or other stakeholders) should protect their own critical infrastructure **– N/A**
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack. **– N/A**
11. Encourage responsible reporting of ICT vulnerabilities and share remedies – **Yes.**

Duty to inform

Team members should consider it their duty to keep their constituents informed about current security threats and risks. When Team members have information that can either adversely affect or improve safety and security, they have a duty to inform relevant parties or others who can help, with appropriate effort, while duly considering confidentiality, privacy laws and regulations, and other obligations.

F. Additional norms included in the agreement:

- IETF RFC2119 for the definition of “SHOULD
- UN Declaration of Human Rights: Article 17