*IGF 2019*

*Best Practices Forum on Cybersecurity*

# Cybersecurity Agreements

*Draft BPF Output Report*

# Acknowledgements

The *Best Practice Forum Cybersecurity (BPF)* is an open multistakeholder group conducted as an intersessional activity of the *Internet Governance Forum (IGF)*. This report is the draft output of the IGF2019 BPF Cybersecurity and is the product of the collaborative work of many:

**Editor:**
Maarten Van Horenbeeck, BPF Lead Expert
Wim Degezelle, BPF Consultant

**Co-facilitators BPF Cybersecurity:**
Markus Kummer
Ben Wallis, MAG member

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

**Formal contributions to the BPF Call for contributions:**
Tech Accord, JP-CERT, Orange Group, Dalsie Baniala, Microsoft, Association for Progressive Communications

**Participants to the discussions on the BPF mailing list and virtual meetings**

**Participants to the BPF Cybersecurity sessions at the IGF2019**

DOCUMENT REVIEW & FEEDBACK
(editorial note 23 October 2019)

# The BPF Cybersecurity is inviting Community feedback on this draft report!

**How ?**

Please send your feedback to **bpf-cybersecurity-contribution@intgovforum.org**

**Format?**

Feedback can be sent in an email or as a word or pdf document attached to an email.

If a comment is on a specific section or paragraph, please indicate this clearly.

**Deadline?**

It is possible to submit feedback on this document until the last day of the IGF2019 meeting. However, we would appreciate your feedback before Friday 22 November, as this would allow us to take your feedback into account during the BPF workshop at the IGF meeting.

**Publication?**

Received feedback will be posted on the BPF webpage (link) - unless the author indicates that he/she prefers that it is not published - and feed into the final BPF output report.

# Table of Contents

# List of abbreviations and acronyms

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

# Executive Summary

[the executive summary will be added to final report]

# I. Introduction to the Best Practices Forum on Cybersecurity

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

Since 2014, the IGF has operated a Best Practices Forum focused on cybersecurity. In 2014-2015, the BPF worked on identifying Best Practice in Regulation and Mitigation of Unsolicited Communications and Establishing Incident Response Teams for Internet Security. Subsequent iterations of the BPF focused more narrowly on cybersecurity; identifying roles and responsibilities and ongoing challenges in 2016, and identifying policy best practices in 2017. BPF outputs, including for each BPF Cybersecurity, are listed on the IGF website here: https://www.intgovforum.org/multilingual/content/best-practice-forums-bpfs.

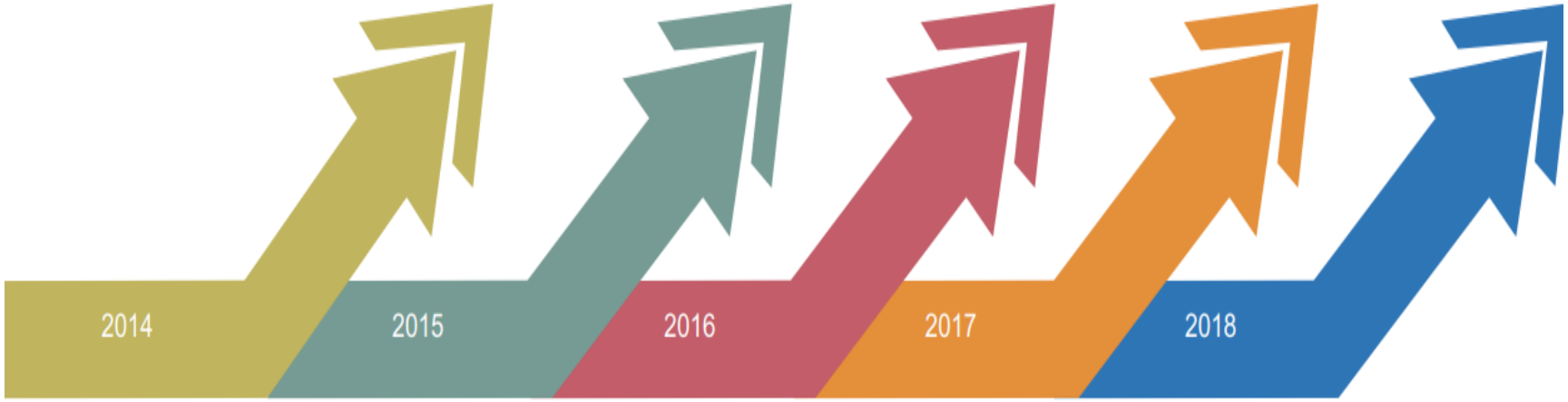
In 2018, the BPF Cybersecurity focused on the culture, norms and values in cybersecurity. We developed an action plan to address different elements:

- The BPF started the process by building on its previous work on the roles and responsibilities of the IGF stakeholder groups in cyberspace and explored what norms have developed that apply to each of these groups. Some of the questions explored related to the behaviour of the respective stakeholder groups, such as “state behaviour” or “industry behaviour”, or the civil society’s role in norms development including social norms of safe and secure online behaviour by individual users.
- The BPF identified, documented, and compared sample norms established in various forums. It did so by engaging experts, BPF contributors and the IGF’s network of National and Regional IGF initiatives (NRIs).
- The BPF leveraged the work on policy best practices done by the BPF 2017 to identify if any of the policy recommendations had seen widespread acceptance, and may have developed into a recognized “best practice”.
- The BPF 2018 aimed to understand the impact of a “digital security divide”. This concept refers to the emergence of a differentiation between digital security "haves" and "have nots" -- those that can afford the access to digitally secure devices and services; and those that can implement specific norms and safeguards to provide digital security in their country and/or business.
- In the beginning of 2018, the BPF published a Background document that was developed with support from its participants. The purpose of the document was to serve as an

introduction to a landscape of cybersecurity initiatives and norms, as well as to assist and support anyone responding to the public call for input, which was released on August 15th 2018. The Background paper and Report on the public Call for Contributions were compiled in the final 2018 BPF Cybersecurity output report, published in December 2018.

- The BPF Cybersecurity also convened a meeting during the Paris IGF, bringing in experts from the norms development community to discuss the key issues in this space.

*The BPF Cybersecurity 2014-2018 - topic and focus*



## IGF2019 Best Practice Forum Cybersecurity

In 2019, the BPF Cybersecurity continued its work by identifying best practices related to the implementation of the different elements (e.g. norms, principles, initiatives, frameworks, policy approaches) contained within a variety of international agreements and initiatives on cybersecurity.

The first phase of the work identified relevant initiatives and agreements. This included (i) identifying horizontal and/or overlapping or potential cross-cutting elements across different initiatives and (ii) initiative-specific elements (which only appear in one). This analysis resulted in a Background Paper that was published in July 2019 with the BPF call for contributions.. The BPF attempted to identify elements across the initiatives and agreements as objectively as possible. The observation that an element appears in one or several agreements does not necessarily imply that it is endorsed by the BPF.

Following this phase, the BPF launched a public Call for Contributions for direct stakeholders and signatories as well as for interested parties and individuals to assist in assessing particular agreement elements, and to collect and share best practices related to the implementation of the agreements. The BPF also aimed to identify existing forums and networks that are already addressing elements of cybersecurity agreements, or are well-placed to do so, and to provide an understanding of how stakeholders can participate in those existing processes.

The BPF has organised a session on its work to take place at the IGF2019 annual meeting in Berlin, and will publish a draft output report ahead of the meeting Input from the discussions in Berlin and additional feedback on the draft report will feed directly into the final BPF output report.

## Inclusive and multidisciplinary approach

In his Address to the IGF2018 in Paris, UN-Secretary General António Guterres noted the importance of the work being done in the Internet governance space and described the vast changes that have occurred in the field since the IGF was established. Moving forward, he made three recommendations: (i) a multidisciplinary approach, (ii) the development and use of shared language; (iii) efforts to draw “weak and missing voices” into the IGF’s work. The IGF2019 BPF Cybersecurity paid particular heed to the Secretary-General’s call in it’s work and discussions throughout the year.

# II. Cybersecurity Agreements

### Agreements within the BPF's scope

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

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

## a. Spaces for agreement

Agreements among and between stakeholders to address and promote cybersecurity internationally take different forms. The BPF has chosen to classify the agreements analysed under three headings:

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

### Agreements Within a Stakeholder Group

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

- The G20, in their Antalya Summit Leaders' Communiqué, "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, included a commitment to "Strengthen G7 cooperation to prevent, thwart and respond to malign interference by foreign actors aimed at undermining the democratic processes and the national interests of a G7 state."
- The Cybersecurity Tech Accord is a commitment to four foundational cybersecurity principles among global technology companies, which outlines industry responsibilities for promoting a safer online world.
- The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security frames cyber security approaches in a human rights context, and originates from a set of member governments.
- In the Shanghai Cooperation Organization's Agreement on cooperation in the field of ensuring the international information security member states of the Shanghai Cooperation Organization agree on major threats to, and major areas of cooperation in cybersecurity.
- The African Union Convention on Cyber Security and Personal Data Protection assists in harmonizing cybersecurity legislation across member states of the African Union.
- The Council to Secure the Digital Economy is a group of corporations which together published an International Anti-Botnet guide with recommendations on how to best prevent and mitigate the factors that lead to widespread botnet infections.
- The League of Arab States published a Convention on Combating Information Technology Offences which intends to strengthen cooperation between the Arab States on technology-related offenses.
- Perhaps one of the oldest documents, the Council of Europe developed and published a Convention on Cybercrime, also known as the Budapest Convention. Adopted in November 2001, it is still the primary international treaty harmonizing national laws on cybercrime.
- The East African Community (EAC) published its Draft EAC Framework for Cyberlaws in 2008, which contains a set of recommendations to its member states on how to reform national laws to facilitate electronic commerce and deter conduct that deteriorates cybersecurity.
- The Economic Community of Central African States (ECCAS) in 2016 adopted the Declaration of Brazzaville, which aims to harmonize national policies and regulations in the Central African subregion.
- The Economic Community of West African States (ECOWAS) Directive C/DIR. 1/08/11 on Fighting Cyber Crime within ECOWAS, agree with central definitions of offenses and rules of procedure for cybercrime investigations.
- The European Union in 2016 adopted, and in 2018 enabled its Directive on Security of Network and Information Systems (NIS Directive). The Directive provides legal measures

to improve cybersecurity across the EU by ensuring states are equipped with incident response and network information systems authorities, ensuring cross-border cooperation within the EU, and implement a culture of cybersecurity across vital industries.

- In December of 2018, the EU reached political agreement on a EU Cybersecurity Act, which reinforces the mandate of the EU Agency for Cybersecurity (ENISA) to better support member states. It also built in a basis for the agency to develop a new cybersecurity certification framework. In May 2019, the EU adopted and authorized the use of sanctions in response to unwanted cyber-behavior.
- The NATO Cyber Defence Pledge, launched during NATO's 2016 Warsaw summit, initiated cyberspace as a fourth operational domain within NATO, and emphasizes cooperation through multinational projects.
- In 2017, the EU Council published to all delegations its conclusions on the Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. This reinforced several existing EU mechanisms, such as the EU Cyber Security Strategy, and further recognized other instruments such as the Budapest Convention, while calling on all Member States to cooperate on cybersecurity through a number of specific proposals.
- The Mutually Agreed Norms for Routing Security (MANRS), an initiative by the Internet Society, is a voluntary set of technical good common practices to improve routing security compiled primarily by members of the network operators community.

### Agreements Between Stakeholder Groups

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

Perhaps one of the most visible examples, the Paris Call for Trust and Security in Cyberspace, launched by France at the IGF2018, currently has 564 official supporters, including 67 states.

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

The Global Commission on the Stability of Cyberspace (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.

Agreements Within the United Nations

The key United Nations agreement we investigated as part of this project is the 2015 consensus report of the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. It proposed several norms, rules and principles for the responsible behavior of States in cyberspace. A new iteration of the UNGGE was established in 2019 through resolution 73/226 of the United Nations General Assembly, which will continue to explore this topic 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 UN initiative in this space, 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. This new 2019 group will reportedly study the norms established by the 2015 UNGGE report and explore potential new ones, as well as study the application of international law, the threat landscape, confidence building measures, capacity building and institutional dialogues related to cyberspace. 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, non-governmental organizations and academia, to share input on issues within the OEWG's mandate. This meeting is scheduled to take place in December (02-04), at the UN headquarters in New York.

## b. The binding or non-binding nature of agreements

The agreements we scoped can be considered binding to differing degrees on their respective supporters/endorsers/signatories. Some documents, such as the Budapest convention, are legally binding instruments. Others, such as the African Union Convention on Cybersecurity, can become legally binding once ratified by a sufficient number of states (15, as opposed to the 4 to date).

Other agreements are normative rather than binding. They are not legally binding but seek to affect behavior by incentivizing or motivating the parties to comply. Examples include the 11 non-binding, voluntary norms included in the 2015 GGE reports, or the Mutually Agreed Norms for Routing Security (MANRS) proposed by the Internet Society. These are often codified after best practices or agreements have had some chance to settle in the international system, and where violation of these best practices is at least considered undesired by a large number of parties.

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

## c. Key elements of agreements

### Horizontal Components

Looking at the cybersecurity agreements, and with some level of abstraction, it is possible to distinguish the following horizontal components that can be expected in cybersecurity agreements:

- **Foundational principles**: The foundational principles guide any development and implementation of cybersecurity norms, and/or binding agreements.
  For example, the commitment to multistakholderism and international law, including the UN Charter and human rights elements retained within it are by many considered critical to the success of any effort in this space as they make room for voices from all stakeholder groups to provide input, open the door to wider inclusion and cooperation, and establish meaningful progress on global cybersecurity. Other principles, such as a commitment to accountability or cooperation might also be considered as guiding foundational principles for cybersecurity agreements.
- **Definitions:** There have been numerous attempts to reach a common understanding of core terms in cybersecurity, such as cyber threats or cyber attacks. These include work within the initiatives highlighted, but also in national legislation, and in various standardization initiatives cybersecurity agreement may refer to.
- **Implementation efforts:** Implementation efforts are not as much a part of the agreements, but efforts to drive their implementation.
  For example, investments in capacity building in cyber diplomacy are critical for governments around the world to be able to participate in cybersecurity norms discussions. Similarly, it is important to increase efforts to build capacity within the technical community and civil society to work in this space. Building on that, confidence building measures (CBMs) go a step further and look to implement specific agreements to discrete proposals that serve to increase cooperation and reduce tensions in cyberspace.
- **Initiatives with broad support**: Initiatives with broad support that aim to drive positive change towards security and stability in cyberspace, for example work on vulnerability disclosure and vulnerability equities policies.

### Key Elements of Cybersecurity Agreements

Diving a little deeper and based on our review of the identified cybersecurity agreements (see section IV), we identified a number of key elements that affect more than a single agreement. In section IV we mapp these elements against the text of the agreements and note if the element is present and how it is reflected.

- **Further multi-stakeholderism:** identify or support that cybersecurity depends on the presence in debate and coordination of all stakeholder groups.
- **Responsible disclosure:** the need to coordinate disclosure of security issues between all stakeholders, including the finder, vendor and affected parties.
- **Reference to International Law:** whether the agreement mentions the importance of international law, or commits the signatories' behavior to international law.
- **Definition of Cyber threats:** whether the agreement proposes a clear or aligned definition of cyber threats.
- **Definition of Cyber-attacks:** whether the agreement proposes a clear or aligned definition of cyber attacks.
- **Reference to Capacity Building:** whether the agreement makes specific references to Capacity Building as a needed step to improve cybersecurity capability.
- **Specified CBMs:** whether the agreement describes or recommends specific Confidence Building Measures.
- **Reference to Human Rights:** whether the agreement reflects on the importance of human rights online.
- **References to content restrictions:** whether the agreement discusses the need for content restrictions online.
- **Vulnerability equities processes:** the realization that stockpiling of vulnerabilities may reduce overall cybersecurity, and processes can be implemented to help identify the appropriate course of action for a government when it identifies a vulnerability.

While nearly all of the overlapping elements identified above may be valuable to include in certain agreements, some responses brought to the BPF's attention that a successful cybersecurity agreement may not require "references to content restrictions." While discussions about what content should, and should not, be tolerated online is an important national and international dialogue, it is meaningfully different than discussions of cybersecurity, and conflating them can often limit progress on one or the other. Cybersecurity agreements should be focused on preventing the corruption and exploitation of technology products, limiting the proliferation of vulnerabilities, and improving cybersecurity capacities, as opposed to the abuse of online platforms for hate speech, extremism or other content-based concerns.

Not all the "key elements" above are present in each individual cybersecurity agreement that was reviewed by the BPF. This should not come as a surprise. Agreements have their scope, purpose, stakeholders, field of application, etc.. These context-related characteristics have an important impact on what elements are relevant and important in the context of a specific agreement.

Therefore, the BPF concluded that it should not attempt to rank key elements according to their relative importance across initiatives. All may be valuable components of cybersecurity agreements, with varying levels of importance to different agreements, and not all elements need to be present in every instance.

# III. Turning Cybersecurity Agreements into Actions

When a new cybersecurity agreement is announced, it is presented as an important milestone and a substantive contribution to improving cybersecurity. Agreements have their own scope and focus, which can be broad or more specific. Assessing the success of an agreement and its impact on cybersecurity is complex. Even where clear goals are formulated, it can be difficult to translate them into quantifiable and measurable objectives, and may be impossible to prove causal relationships. Therefore, the BPF looked into the value and outcome of cybersecurity agreements in two different ways. The BPF tried to get insight into the perceived value and outcome of a cybersecurity agreement as observed by signatories and participants to the agreement, but also by other stakeholders and outsiders. This perceived value is addressed in the next section (a). Sections (b) and (c) zoom in on what actions, programs and projects signatories and stakeholders launch to support the agreement's goals and turn their commitment into action.

## a. Perceived outcome of cybersecurity agreements

### Perceived Value and Outcome of Cybersecurity Agreements

As threats in cyberspace are becoming more commonplace and severe, cybersecurity agreements provide a valuable common footing to reduce risk and increase security and stability in cyberspace. The agreement's text, with its substantive content and goals, is a tangible and valuable document. It is the outcome of a frequently long process of co-drafting and negotiating among different parties. Both, the process of formulating the agreement as well as its product, 'the Agreement', are valuable. The process may bring stakeholders closer together and increase trust amongst them. A cybersecurity agreement may become a good basis for establishing new forms of cooperation between stakeholders, even between stakeholders who were not directly involved as signatories of negotiating parties. Additional value can lie in the announcement and communications strategy to raise awareness about the agreement. Press and media attention spread the word about the agreement, but may also spread awareness and knowledge about the cybersecurity issue(s) addressed to a wider audience of stakeholders.

The BPF identified the following perceived outcomes of cybersecurity agreements:

- **Development and reinforcement of clear expectations for responsible behavior online**

  Norms are shared beliefs held within a community which relevant actors identify with in order to generate "the pull to conform" to those norms. The inclusion of all stakeholder groups in the creation of cybersecurity agreements reinforces the shared nature of the challenge and to build agreement around the responsibilities all have to preserve the open, free and secure internet. Private industry competes in the marketplace, and nations may

have political tensions and rivalries. Cybersecurity agreements allow to focus beyond the differences and rivalries on a safe and secure online world.

- **Agreed norms are valuable as policy tools**

  By clarifying responsibilities and who should do what, agreements and norms create obligations for identifiable actors and trigger more active accountability.

- **Visibility and promotion of good cybersecurity practices**

  Cybersecurity agreements may drive a change in behaviour among their signatories. The communication about and (press) attention for the agreement can signal to the online community at large what should be acceptable and unacceptable behaviour.

- **Confidence building between stakeholders**

  Agreements operate as confidence building measures between stakeholders and as such facilitate further cooperation.

- **Development of new relationships and partnerships**

  Bringing stakeholders together and in particular allowing for multistakeholder participation in cybersecurity agreements facilitates the development of new relations and partnerships. The agreement can approach individual stakeholders and be the reason for them to initiate new or join existing projects.

### Adverse Effects of Cybersecurity Agreements

Cybersecurity agreements may provoke unintended and adverse effects. According to the inputs received during our call for feedback, as well as the direct experiences of experts within the BPF, the following are seen as potential unintended or counterproductive effects or a cybersecurity agreement, sometimes due to causes within the agreement, sometimes due to reasons and challenges within a broader context.

- **Cybersecurity agreements can risk becoming counterproductive to furthering cybersecurity when they limit multistakeholder input.**

- **Cybersecurity agreements can risk becoming counterproductive when they fail to focus on outcomes but instead prescribe a particular course of action.**

Binding legislative agreements and standards, in particular, risk being prescriptive in their requirements for implementation. Today's technology environment develops with breakneck speed and all solutions can be used for both beneficial and nefarious purposes. An agreement that is overly prescriptive risks becoming out of date and a one-size-fits-all approach often undermines opportunities for innovation to further improve security.
As an example, legislation aimed at robust access management security could be well intentioned in mandating sufficiently complex passwords, but limit opportunities for adopting new cutting-edge multi-factor authentication techniques which offer improved security by doing away with passwords altogether.

As a rule, when establishing new legislative requirements, cybersecurity outcomes should be prioritized over respective approaches for achieving them to allow for the right balance of security and innovation.

- **Missing important players**

  Cybersecurity agreements can miss their effectiveness if important global players are not involved

- **Lack of leadership in implementation**

  Sometimes key players or powerful states who are part of these agreements (the GGE and FoC for example) flout them in practice, thereby undermining not just those specific agreements, but international agreements as a mechanism to achieve cybersecurity in the first place.

- **Direct or indirect competition with human and other rights**

  The tendency for cybersecurity agreements to either directly, or indirectly, undermine human rights, which, in turn may reduce cybersecurity. This is a result of cybersecurity frameworks focusing only on the security of the state, rather than the security of people, devices, networks and underlying infrastructure. Such narrow views of cybersecurity tend to call for disproportionate measures, like undermining encryption or criminalising speech, which may appear to strengthen national security, but in fact undermine human rights and also the security of society at large.

## b. Best Practices and experiences

Organisations can promote best practices within their own organisation and implement agreements to improve the security of the products and services they offer. They can take or

support initiatives to promote greater security for the entire ecosystem, and encourage responsible behaviour among other stakeholders .

Examples of initiatives and projects to support the different cybersecurity agreements covered by the BPF are included in the 'Review of Cybersecurity Agreements', in the next section of this report.

## c. Challenges when implementing agreements

According to the inputs received during the call for feedback, as well as the direct experiences of experts within the BPF, there are a number of key challenges faced by implementers of cybersecurity agreements.

- **Varied understandings of definitions of key terminology**

  Different signatories and stakeholders may have varied understandings or definitions of the key terminology referred to in cybersecurity agreements, for example 'what is critical infrastructure?'.

- **Vague and ambiguous language**

  Agreements are made in the past and might contain some ambiguity, which leaves room for interpretation. In most cases this is inevitable and in some cases even necessary in the process to allow various actors to come to an agreement overcoming their different situations, interests, opinions, and beliefs.

  For example, although the UNGGE Consensus Report from 2015 includes important items such as the prohibition of attacks against CERTs, some parts in the agreement are left ambiguous, and require clarification through further international discussions.

- **Varied levels of knowledge of the existence of the agreement**

  States and other stakeholders may have varied levels of knowledge of the existence of the agreements, as well as a varied capacity to implement them.

- **Overly prescriptive regarding the implementation**

  Many of the agreements included in this review have been invaluable in outlining the norms and rules that should guide responsible behavior online. It has also been helpful for them to be less prescriptive when it comes to how respective organizations should go about implementing various provisions, especially when they are creating legally binding standards for private entities. Even within one stakeholder group, there needs to be a level

of flexibility that allows for different business models and approaches to best meet their responsibilities.
Efforts to protect critical infrastructure, strengthen cyber hygiene, responsibly handle vulnerabilities or implement the many other principles included in these agreements will likely look very different in the context of a large technology company as compared to a financial services firm, a civil society organization, or any number of other multistakeholder entities. Having flexibility in the implementation of especially binding agreements is a strength, as it lets each entity pursue approaches that make the most sense in its respective context.

- **Lack of knowledge or understanding how to implement**

  While there is clear benefit in avoiding being too prescriptive regarding implementation and allowing for differentiated approaches in adhering to these cybersecurity agreements, such flexibility can also result in organizations not understanding how best to implement the provisions of agreements they have joined – or are subject to. For organisations, including government organisations, it can be difficult to understand their obligations and translate these into actionable points and projects.

  Agreements should strive to provide a sufficient enough balance in guidance on how to implement the agreement and clarity on the respective roles and responsibilities required. In addition, it is important that organisations are given the opportunity to share how they are approaching these commitments and their implementation to allow for others to learn from peers and identify good practices they too would like to adopt.

- **Lack of institutional capacity**

  Challenges in monitoring compliance and implementation because of a lack of institutional capacity and mechanisms that can do the monitoring.

- **Need for greater accountability**

  There is a particular need for greater accountability when it comes to norms for responsible behavior by government actors in cyberspace – as identified in the UNGGE consensus reports and the Paris Call, among other agreements included in this study. Despite the clear call for, and enumeration of, responsible behavior online, we do not necessarily see a reduction in cyberattacks emanating from either state or non-state actors. This underscores the importance now in pivoting in these international discussions to focus on strengthening the recognition of these norms and to pursue ways to make them more binding for governments in particular to avoid unnecessary harm to civilians and the further proliferation of cyberweapons. There is no excuse for ignorance on the part of

governments about what the norms and expectations are for responsible behavior in cyberspace.

- **Lack of leadership in implementation**

  The flouting of norms and agreements by influential states that called for them acts as a disincentive for others to support or comply with them.

- **Lack of continuity**

  Often interaction and broader consultation processes stop once the agreement has been reached or published.

# IV. Review of Cybersecurity Agreements

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

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

Agreements were identified and reviewed by experts participating in the Best Practices Forum. This chapter contains a review of the following agreements:

- African Union Convention on Cyber Security and Personal Data Protection
- Southern African Development Community Model Laws on Cybercrime
- Paris Call for Trust & Security in Cyberspace
- UNGGE Consensus Report of 2015
- Cybersecurity Tech Accord
- Siemens Charter of Trust
- GCSC Six Critical Norms
- Freedom Online Coalition Recommendations for Human Rights Based Approaches to Cybersecurity
- Shanghai Cooperation Organization Agreement on Cooperation in the Field of Ensuring the International Information Security
- Mutual Agreed Norms for Routing Security (MANRS)
- Brazzaville Declaration
- Budapest Convention
- EU Cybersecurity Act
- EU NIS Directive
- Draft EAC Framework for Cyber Laws
- ECOWAS Directive C/DIR. 1/08/11
- NATO Cyber Defence Pledge
- EU Joint Communication: Resilience, Deterrence and Defence
- CSDE Anti-botnet Guide
- OAS - Organization of American States

Other initiatives and agreements suggested to the BPF but not included in this review:

- The work of the UN High Level Panel on Digital Cooperation
- The efforts by the World Wide Web Foundation on A Contract for the Web
- The ongoing work by the Global Forum on Cybersecurity Expertise

## African Union Convention on Cyber Security and Personal Data Protection

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

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

### Southern African Development Community Model Laws on Cybercrime

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

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

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

Paris Call for Trust & Security in Cyberspace

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

The Paris Call for Trust and Security in Cyberspace was launched at the IGF in Paris on November 12th, 2018. It includes today over 550 endorsements from governments, the private sector and civil society, and is the largest multistakeholder commitment to cybersecurity principles. While many of its principles are derivative of norms previously established in other agreements, the Paris Call is unique in its expansive, multistakeholder nature and some of the more original elements including:

- Signatories commit to preventing activity that "intentionally and substantially damages the general availability or integrity of the public core of the internet";
- Take steps to prevent non-state actors from hacking back;
- Promote international norms of responsible behavior;
- The principle on foreign electoral interference (e.g., malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities") was a major contribution, although a version of it appeared earlier in 2018 in a G7 Ministers' Declaration.
- It acknowledges the Budapest convention as a key tool in preventing cyber criminality.

**Stakeholder initiatives supporting the implementation**

- Microsoft utilizes and has published its coordinated vulnerability disclosure policy, which ensures that any known vulnerabilities in our products are reported and remediated in a timely and systematic fashion that puts customer security first. This is also in keeping with a recently-announced Cybersecurity Tech Accord commitment to have all company signatories adopt vulnerability disclosure policies by the end of 2019.
  *(Cybersecurity Tech Accord principle 1, Paris Call principle 1, GCSC norm 5)*
- Microsoft uses its Security Development Lifecycle (SDL) and Operational Security Assurance (OSA) programs to improve the security and resiliency of our products and services. SDL is focused on building trustworthy software by focusing on secure design, threat modeling, secure coding, security testing, and privacy best practices. OSA minimizes risk by ensuring that ongoing operational activities follow rigorous security guidelines and by validating that guidelines are being followed effectively. This helps make Microsoft cloud-based services' infrastructure more resilient to attack and decreases the amount of time needed to detect, contain, and respond to threats. *(Cybersecurity Tech Accord principle 1, Paris Call principle 1, GCSC norm 5)*
- *In developing its products and services, Microsoft is dedicated to promoting user awareness and customer control of their security environment with the most advanced tools. This includes many innovative initiatives, including the promotion of password-less security options and distributed digital identity. (Cybersecurity Tech Accord principle 3, Paris Call principle 7)*
- Microsoftleveragesitspositionoperatingandmaintainingoneofthelargestcloudenvironmentsin the world to scale its security responses and capabilities to protect users everywhere. This has included blocking over 5 billion malicious and suspicious phishing mails in 2018 alone, analyzing over 6.5 trillion signals each day, and investing over a billion dollars each year in security. *(Cybersecurity Tech Accord principle 1, Paris Call principle 1)*
- Microsoft has hosted webinars on cloud security and an upcoming webinar on IoT security as part of the Cybersecurity Tech Accord's series of webinars that is now a growing library of free resources meant to improve the cybersecurity capacities of governments and organizations around the world. *(Cybersecurity Tech Accord principle 3, Paris Call principles 1 and 7)*
- Microsoft's cybersecurity policy team regularly partners with the United States Telecommunications Training Institute (USTTI) to provide guidance and support to policymakers from across the world looking to establish informed policies on cloud security and other topics. *(Cybersecurity Tech Accord principle 3, Paris Call principle 7)*
- As part of the Cybersecurity Tech Accord, Microsoft joins a monthly meeting of company signatories to address progress and identify new initiatives aligned with the four principles of the agreement. Work products that Microsoft has contributed to have included blogs, whitepapers, policy guidance, workshops and industry consultations on cybersecurity. The collective work products of the organization are available for review on the Cybersecurity Tech Accord website. *(Cybersecurity Tech Accord principle 4, Paris Call principle 1)*
- Microsoft has established the Defending Democracy Program to focus on protecting elections and democratic institutions and processes. This program has developed several new initiatives over the past year:
  - Amplified threat monitoring for campaigns and democratic institutions through AccountGuard, a free resource for qualifying customers, along with awareness-raising and training workshops for practitioners in this space;
  - Security optimization for campaigns using Microsoft software via M365 for Campaigns;
  - An open source software development kit (SDK), leveraging homomorphic cryptography to secure voting systems via ElectionGuard; and

- Instantaneous verification of news sources to combat disinformation online via a partnership in launching the NewsGuard app.

*(Paris Call principle 3)*

- Microsoft contributes to the development of national and international standards by leveraging our own best practices and participating in collaborative working groups and initiatives. For example, we have shared our experiences using SDL (see above) through SAFECode and as a part of an international standard for secure software development (ISO 27034). We also participate in working groups hosted by the National Institute of Standards and Technology (NIST) and the European Union Agency for Cybersecurity (ENISA) to develop approaches and best practices for addressing a range of emerging cybersecurity challenges, including IoT device security and post-quantum cryptography.
  *(Cybersecurity Tech Accord principle 4, Paris Call principles 1, 2, 6, 7)*
- Through the Cybersecurity TechAccord, Microsoft has joined with others in industry in encouraging policies that promote greater stability in cyberspace and discouraging those that promote instability. This has included advocacy on the importance of vulnerabilities equities processes for governments, discouraging policies that would undermine encryption, and supporting an open letter to the G7 on not undermining the security of technology products. *(Cybersecurity Tech Accord principle 2, Paris Call principle 1)*
- Microsoft has contributed as an active partner to the work of deliberative bodies that are seeking to draw attention to the dangers of escalating cyber conflict and limit irresponsible actions by governments in cyberspace. This has included contributing to the deliberations of the UN High Level Panel on Digital Cooperation which recently released its final report, and A Contract for the Web which recently released its first draft of commitments for comment.
  *(Cybersecurity Tech Accord principle 2, Paris Call principle 1 and 9, GCSC norm 7)*
- In 2017, Microsoft President Brad Smith issued a call for the establishment of a Digital Geneva Convention, a binding commitment to protect civilians from nation-state cyberattacks in peacetime. *(Cybersecurity Tech Accord principle 2, Paris Call principles 1, 2, 5, 9, GCSC norm 7)*

UNGGE Consensus Report of 2015

| Agreement element | Present? | Notes |
|---|---|---|
| Further multi-stakeholderism | Yes | There are three references to the role of non-government stakeholders. They focus on the role of these stakeholders in international cooperation, implementation of ICT security awareness and capacity building initiatives. |
| Vulnerability equities processes | No | |
| Responsible disclosure | Yes | The GGE report comprises norm on vulnerabilities behaviour: 13 (j) 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 |
| Reference to International Law | Yes | |
| Definition of Cyber threats | No | Discussion of threats that use ICTs to target infrastructure, but no express definition is written. |
| Definition of Cyberattacks | No | |
| Reference to Capacity Building | Yes | |
| Specified CBMs' | Yes | The UNGGE report lists out specific CBM's in section IV. |
| Reference to Human Rights | Yes | The Report makes reference to the UN Charter, as well as to the need for states to comply with their obligations under international law to respect and protect human rights and fundamental freedoms, and to the norm on respecting human rights council resolutions on FoE and privacy. |
| References to content restrictions | | |

Unique elements of the GGE norms include that states should not conduct or knowingly support activity to harm the information systems of the authorized Computer Emergency Response Teams of another state, as well as that they "*should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public*".

**Stakeholder initiatives supporting the implementation**

- The country submissions of Australia and the United Kingdom ahead of the UN OEWG first meeting in September 2019 address how the respective countries have pursued implementing the norms included in the 2015 UNGGE report:
    - Australian Paper - Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, September 2019, https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf

- Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015, https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/uk-un-norms-non-paper-oewg-submission-final.pdf

Cybersecurity Tech Accord

| Agreement element | Present? | Notes |
|---|---|---|
| Further multi-stakeholderism | Yes | The fourth principle of the agreement is expressly about working collaboratively on cybersecurity challenges with like-minded entities within the technology industry and beyond. |
| Vulnerability equities processes | No | Not in the agreement itself, but the Cybersecurity Tech Accord has published statements to this effect. |
| Responsible disclosure | Yes | The group has also committed to having all signatories adopt vulnerability disclosure policies. |
| Reference to International Law | No | |
| Definition of Cyber threats | No | No definitions in the agreement itself, but the group has issued a call for comment on cybersecurity definitions previously. |
| Definition of Cyberattacks | No | |
| Reference to Capacity Building | Yes | A core mandate for the Cybersecurity Tech Accord is focused on empowering technology users everywhere, and much of their ongoing work focuses on raising awareness and promoting greater capacities across the cybersecurity ecosystem. |
| Specified CBMs' | No | |
| Reference to Human Rights | No | |
| References to content restrictions | No | |

The Cybersecurity Tech Accord contains several product development norms and operational norms, such as "opposing cyberattacks on users from anywhere", which are less relevant to some of the inter-state norms but carve out a clear and distinct set of priorities and responsibilities for the technology industry in this issue space. The document also proposes joint initiatives between different stakeholders to uphold these principles.

**Stakeholder initiatives supporting the implementation**

- The Cybersecurity Tech Accord signatories have tackled substantial work during its first year and a half of existence, work on definitions, commitment to multistakeholder approaches, dedication to vulnerability disclosure policies and capacity building, as well as recommendations issued on vulnerability equities processes and confidence building measures.
- Microsoft utilizes and has published its coordinated vulnerability disclosure policy, which ensures that any known vulnerabilities in our products are reported and remediated in a timely and systematic fashion that puts customer security first. This is also in keeping with a recently-announced Cybersecurity Tech Accord commitment to have all company signatories adopt vulnerability disclosure policies by the end of the year.
  *(Cybersecurity Tech Accord principle 1, Paris Call principle 1, GCSC norm 5)*
- Microsoft uses its Security Development Lifecycle (SDL) and Operational Security Assurance (OSA) programs to improve the security and resiliency of our products and services. SDL is focused on building trustworthy software by focusing on secure design, threat modeling, secure coding, security testing, and privacy best practices. OSA minimizes risk by ensuring that ongoing operational activities follow rigorous security guidelines and by validating that guidelines are being followed effectively. This helps make Microsoft cloud-based services' infrastructure more resilient to attack and decreases the amount of time needed to detect, contain, and respond to threats. *(Cybersecurity Tech Accord principle 1, Paris Call principle 1, GCSC norm 5)*
- In developing its products and services, Microsoft is dedicated to promoting user awareness and customer control of their security environment with the most advanced tools. This includes many innovative initiatives, including the promotion of password-less security options and distributed digital identity. *(Cybersecurity Tech Accord principle 3, Paris Call principle 7)*
- Microsoft leverages its position operating and maintaining one of the largest cloud environments in the world to scale its security responses and capabilities to protect users everywhere. This has included blocking over 5 billion malicious and suspicious phishing mails in 2018 alone, analyzing over 6.5 trillion signals each day, and investing over a billion dollars each year in security. *(Cybersecurity Tech Accord principle 1, Paris Call principle 1)*
- Microsoft has hosted webinars on cloud security and an upcoming webinar on IoT security as part of the Cybersecurity Tech Accord's series of webinars that is now a growing library of free resources meant to improve the cybersecurity capacities of governments and organizations around the world.
  *(Cybersecurity Tech Accord principle 3, Paris Call principles 1 and 7)*
- Microsoft's cybersecurity policy team regularly partners with the United States Telecommunications Training Institute (USTTI) to provide guidance and support to policymakers from across the world looking to establish informed policies on cloud security and other topics.
  *(Cybersecurity Tech Accord principle 3, Paris Call principle 7)*
- As part of the Cybersecurity Tech Accord, Microsoft joins a monthly meeting of company signatories to address progress and identify new initiatives aligned with the four principles of the agreement. Work products that Microsoft has contributed to have included blogs, whitepapers, policy guidance, workshops and industry consultations on cybersecurity. The collective work products of the organization are available for review on the Cybersecurity Tech Accord website.
  *(Cybersecurity Tech Accord principle 4, Paris Call principle 1)*
- Microsoft contributes to the development of national and international standards by leveraging our own best practices and participating in collaborative working groups and initiatives. For example, we have shared our experiences using SDL (see above) through SAFECode and as a part of an international standard for secure software development (ISO 27034). We also participate in working

groups hosted by the National Institute of Standards and Technology (NIST) and the European Union Agency for Cybersecurity (ENISA) to develop approaches and best practices for addressing a range of emerging cybersecurity challenges, including IoT device security and post-quantum cryptography.
*(Cybersecurity Tech Accord principle 4, Paris Call principles 1, 2, 6, 7)*

- Through the Cybersecurity TechAccord, Microsoft has joined with others in industry in encouraging policies that promote greater stability in cyberspace and discouraging those that promote instability. This has included advocacy on the importance of vulnerabilities equities processes for governments, discouraging policies that would undermine encryption, and supporting an open letter to the G7 on not undermining the security of technology products. *(Cybersecurity Tech Accord principle 2, Paris Call principle 1)*
- Microsoft has contributed as an active partner to the work of deliberative bodies that are seeking to draw attention to the dangers of escalating cyber conflict and limit irresponsible actions by governments in cyberspace. This has included contributing to the deliberations of the UN High Level Panel on Digital Cooperation which recently released its final report, and A Contract for the Web which recently released its first draft of commitments for comment.
*(Cybersecurity Tech Accord principle 2, Paris Call principle 1 and 9, GCSC norm 7)*
- In 2017, Microsoft President Brad Smith issued a call for the establishment of a Digital Geneva Convention, a binding commitment to protect civilians from nation-state cyberattacks in peacetime.
*(Cybersecurity Tech Accord principle 2, Paris Call principles 1, 2, 5, 9, GCSC norm 7)*

### Siemens Charter of Trust

| Agreement element | Present? | Notes |
|---|---|---|
| Further multi-stakeholderism | Yes | "In this document, the undersigned outline the key principles for a secure digital world – principles that they're actively pursuing in collaboration with civil society, government, business partners and customers." |
| Vulnerability equities processes | No | |
| Responsible disclosure | Yes | "8. Transparency and response: Participate in an industrial cybersecurity network in order to share new insights, information on incidents et al.; report incidents beyond today's practice which is focusing on critical infrastructure." |
| Reference to International Law | No | |
| Definition of Cyber threats | No | |
| Definition of Cyberattacks | No | |
| Reference to Capacity Building | Yes | Focus on education. |
| Specified CBMs' | No | |
| Reference to Human Rights | No | |

| | | |
|---|---|---|
| References to content restrictions | No | |

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

## GCSC Critical Norms

| Agreement element | Present? | Notes |
|---|---|---|
| Further multi-stakeholderism | Yes | |
| Vulnerability equities processes | Yes | |
| Responsible disclosure | Yes | |
| Reference to International Law | Yes | "Despite these difficulties, it should be recalled that state sovereignty is the cornerstone of the rules-based international system of peace and security. States have a monopoly on the legitimate use of force, strictly bound by international law. If states permit such action, they may therefore be held responsible under international law" |
| Definition of Cyber threats | No | |
| Definition of Cyber Attacks | No | |
| Reference to Capacity Building | Indirect | "states should work towards compatible and predictable processes" |
| Specified CBMs' | Indirect | Compatible and predictable VEP |
| Reference to Human Rights | No | |
| References to content restrictions | No | |

At the time of writing, the six critical norms are still in draft, and published for public input (the so-called Singapore Package). They are the result of a multistakeholder group developing cybersecurity norms and sharing them with the wider community through consultation sessions for input. The GCSC has informed the BPF that it will publish its final report in November 2019.

The six specific norms consist of:

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

Prior to the release the Singapore Package, the GCSC also released

- Norm to Protect the Public Core of the Internet, "*Without prejudice to their rights and obligations, state and non-state actors should not conduct or 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"*

- Norm to protect Electoral Infrastructure: "*State and non-state actors should not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites*."

**Stakeholder initiatives supporting the implementation**

- Microsoft utilizes and has published its coordinated vulnerability disclosure policy, which ensures that any known vulnerabilities in our products are reported and remediated in a timely and systematic fashion that puts customer security first. This is also in keeping with a recently-announced Cybersecurity Tech Accord commitment to have all company signatories adopt vulnerability disclosure policies by the end of the year.
  *(Cybersecurity Tech Accord principle 1, Paris Call principle 1, GCSC norm 5)*
- Microsoft uses its Security Development Lifecycle (SDL) and Operational Security Assurance (OSA) programs to improve the security and resiliency of our products and services. SDL is focused on building trustworthy software by focusing on secure design, threat modeling, secure coding, security testing, and privacy best practices. OSA minimizes risk by ensuring that ongoing operational activities follow rigorous security guidelines and by validating that guidelines are being followed effectively. This helps make Microsoft cloud-based services' infrastructure more resilient to attack and decreases the amount of time needed to detect, contain, and respond to threats. *(Cybersecurity Tech Accord principle 1, Paris Call principle 1, GCSC norm 5)*
- Microsoft has contributed as an active partner to the work of deliberative bodies that are seeking to draw attention to the dangers of escalating cyber conflict and limit irresponsible actions by governments in cyberspace. This has included contributing to the deliberations of the UN High Level Panel on Digital Cooperation which recently released its final report, and A Contract for the Web which recently released its first draft of commitments for comment.
  *(Cybersecurity Tech Accord principle 2, Paris Call principle 1 and 9, GCSC norm 7)*
- In 2017, Microsoft President Brad Smith issued a call for the establishment of a Digital Geneva Convention, a binding commitment to protect civilians from nation-state cyberattacks in peacetime. *(Cybersecurity Tech Accord principle 2, Paris Call principles 1, 2, 5, 9, GCSC norm 7)*

## Freedom Online Coalition Recommendations for Human Rights Based Approaches to Cybersecurity

| Agreement element | Present? | Notes |
|---|---|---|
| Further multi-stakeholderism | Yes | |
| Vulnerability equities processes | No | |
| Responsible disclosure | No | |
| Reference to International Law | Indirect | |
| Definition of Cyber threats | No | |
| Definition of Cyberattacks | Indirect | The FOC WG1 definition of cybersecurity is "Cybersecurity is the preservation – through policy, technology, and education – of the availability*, confidentiality* and integrity* of information and its underlying infrastructure so as to enhance the security of persons both online and offline". However, there is no explicit definition of an attack. |
| Reference to Capacity Building | Yes | |
| Specified CBMs' | Yes | |
| Reference to Human Rights | Yes | Multiple references (see recommendations 1, 2, 4, 5,6, 8, 9, 11, 12, 13) |
| References to content restrictions | | |

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

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

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

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

## Mutual Agreed Norms for Routing Security (MANRS)

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

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

### Stakeholder initiatives supporting the implementation

- **Orange Group** is working on integrating each of its affiliates - both Europe and EMEA, in the MANRS initiative. Orange Group launched a program in order to encourage and accompany affiliates to enhancing the lever of security of their networks (e.g., IP routing security policy, IP anti-spoofing policy. Currently, three Orange Group affiliates are involved inside the MANRS initiative and six other affiliates are working to be compliant with MANRS initiative requirements.

### Brazzaville Declaration

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

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

## Budapest Convention

| Agreement element | Present? | Notes |
|---|---|---|
| Further multi-stakeholderism | Yes | Chapter III talks about International co-operation. It however nor specifically talking about multistakeholder in the true sense although such cooperation will require Government and Private sector cooperation but this excludes civil society etc<br>Chapter II covers<br>Article 23 – General principles relating to international co-operation<br>Article 24 – Extradition<br>Article 25 – General principles relating to mutual assistance<br>Article 26 – Spontaneous information<br>Article 27 – Procedures pertaining to mutual assistance requests in the absence of<br>applicable international agreements<br>Article 28 – Confidentiality and limitation on use<br>Article 29 – Expedited preservation of stored computer data<br>Article 30 – Expedited disclosure of preserved traffic data<br>Article 31 – Mutual assistance regarding accessing of stored computer data<br>Article 32 – Trans-border access to stored computer data with consent or where<br>publicly available<br>Article 33 – Mutual assistance regarding the real-time collection of traffic data |
| Vulnerability equities processes | No | |
| Responsible disclosure | Yes | |
| Reference to International Law | Yes | |
| Definition of Cyber threats | Indirectly | The convention is more focused on cybercrime and as such has an extensive range of definitions for such activities deemed as criminal. Indirectly threats and cyberattacks can make use of some of these categories which are considered cybercrime. |
| Definition of Cyberattacks | Indirectly | |
| Reference to Capacity Building | No | |
| Specified CBMs' | No | |
| Reference to Human Rights | Yes | |
| References to content restrictions | Yes | Article 9 – Offences related to child pornography |

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

### EU Cybersecurity Act

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

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

### EU NIS Directive

| Agreement element | Present? | Notes |
|---|---|---|
| Further multi-stakeholderism | Yes | |
| Vulnerability equities processes | No | |
| Responsible disclosure | Indirectly | |
| Reference to International Law | No | |
| Definition of Cyber threats | No | |
| Definition of Cyberattacks | No | |
| Reference to Capacity Building | Indirectly | The NIS Directive created an NIS cooperation group and CSIRT cooperation group. These groups develop guidelines to create sectoral security standards |
| Specified CBMs' | Yes | Member states established a national point of contact to share information with European member states on breaches. |
| Reference to Human Rights | No | Mentions the Charter of Fundamental Rights of the European Union |
| References to content restrictions | No | |

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

## Draft EAC Framework for Cyber Laws

| Agreement element | Present? | Notes |
|---|---|---|
| Further multi-stakeholderism | Yes | The document is a Framework with the goal to promote harmonisation of legal responses by issues created by the increased use of ICT and cyberspace. It is primarily providing recommendations.<br><br>It involves the participation of states which may exclude private sector and Civil society, and as such is multilateral rather than multistakeholder.<br><br>However, the document does refer to enabling “private sector participation” and the need for a strong private sector to allow for a co-regulatory approach and as such it contains some limited elements to encourage partnerships across two stakeholder groups. |
| Vulnerability equities processes | No | |
| Responsible disclosure | No | |
| Reference to International Law | Yes | |
| Definition of Cyber threats | Indirectly | |
| Definition of Cyberattacks | No | |
| Reference to Capacity Building | No | |
| Specified CBMs’ | No | |
| Reference to Human Rights | Yes | |
| References to content restrictions | Indirectly | “Where illegal content is made accessible over the Internet in contravention of applicable national rules, states will often require a Internet service provider (ISP) to hand over any details which may establish the real-world identity of the content provider. “ |

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

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

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

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

## NATO Cyber Defence Pledge

| Agreement element | Present? | Notes |
|---|---|---|
| Further multi-stakeholderism | Indirect | Some reference to the value of educational institutions and defence stakeholders. |
| Vulnerability equities processes | No | |
| Responsible disclosure | No | |
| Reference to International Law | Yes | International law and norms: “We reaffirm the applicability of international law in cyberspace and acknowledge the work done in relevant international organisations, including on voluntary norms of responsible state behaviour and confidence-building measures in cyberspace.” |
| Definition of Cyber threats | No | |
| Definition of Cyberattacks | No | |
| Reference to Capacity Building | Yes | “Enhance skills and awareness, among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences;” |
| Specified CBMs’ | Yes | See number 5 of the document. |
| Reference to Human Rights | No | |
| References to content restrictions | No | |

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

### EU Joint Communication: Resilience, Deterrence and Defence

| Agreement element | Present? | Notes |
|---|---|---|
| Further multi-stakeholderism | Yes | |
| Vulnerability equities processes | No | |
| Responsible disclosure | Yes | |
| Reference to International Law | Yes | |
| Definition of Cyber threats | No | |
| Definition of Cyberattacks | Indirect | Refers to third agreement for definition of criminal behavior |
| Reference to Capacity Building | Yes | |
| Specified CBMs' | Yes | |
| Reference to Human Rights | Yes | "A comprehensive approach to cybersecurity requires respect for human rights, and the EU will continue to uphold its core values globally, building on the EU's Human Rights " |
| References to content restrictions | No | |

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

CSDE Anti-botnet Guide

| Agreement element | Present? | Notes |
|---|---|---|
| Further multi-stakeholderism | Yes | “Security relies on mutually beneficial teamwork and partnership among governments, suppliers, providers, researchers, enterprises, and consumers, built on a framework that takes collective action against bad actors and rewards the contributions of responsible actors.” |
| Vulnerability equities processes | No | |
| Responsible disclosure | Yes | “Coordinate with customers and peers” |
| Reference to International Law | Indirect | There is mention to domestic law enforcement coordination, but not directly to international law: “Coordination with law enforcement during address domain seizure and takedown.” |
| Definition of Cyber threats | Yes | The paper addresses Botnets and provides a description for them. |
| Definition of Cyberattacks | No | |
| Reference to Capacity Building | Yes | “While the industry leaders who have developed this Guide recognize that no combination of measures can guarantee the elimination of all threats and risks, they believe these practices, both baseline and advanced, present a valuable framework for ICT stakeholders to reference in identifying and choosing practices of their own to mitigate the threats of automated, distributed attacks. “ |
| Specified CBMs’ | Yes | Signature Analysis and Packet Sampling best practices, amongst others. While not directly CBMs, when universally applied they could be considered confidence building. |
| Reference to Human Rights | No | |
| References to content restrictions | Yes | Mostly describes techniques: blackholing, sinkholing, scrubbing and filtering and not categories of content. |

The CSDE Anti-botnet guide is an industry driven document that focuses more on technical elements than the other documents we reviewed. Its primary purpose is to highlight voluntary

practices that each segment of the ICT sector (e.g. infrastructure, software development, devices and device systems, home and small business systems installation, and enterprises) could implement, according to their circumstances, to mitigate the impact of botnet infections.

### OAS - Organization of American States

| Agreement element | Present? | Notes |
|---|---|---|
| Further multi-stakeholderism | Yes | |
| Vulnerability equities processes | Yes | |
| Responsible disclosure | Yes | |
| Reference to International Law | Yes | |
| Definition of Cyber threats | Yes | |
| Definition of Cyberattacks | Yes | |
| Reference to Capacity Building | Yes | |
| Specified CBMs´ | Yes | 10. The importance of promoting cooperation in the public sector with the private and academic sectors to strengthen the protection and protection of said infrastructure. |
| Reference to Human Rights | Yes | |
| Reference to content restrictions | Yes | |

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

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

# Further resources

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

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

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

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

https://cyberpolicyportal.org/en/

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

https://cybilportal.org

Members of the international cyber capacity building (CCB) community can find and share expertise to support the design and delivery of programs and projects.

_____ *End of document* _____