IGF 2021

Best Practice Forum Cybersecurity

on the use of norms to foster trust and security

Mapping and Analysis of International Cybersecurity Norms Agreements

BPF WORKSTREAM 1 DRAFT REPORT

NOVEMBER 2021

Acknowledgements

The *Best Practice Forum Cybersecurity (BPF)* is an open multistakeholder effort conducted as an intersessional activity of the *Internet Governance Forum (IGF)*. This report is the draft output of the IGF 2021 BPF on Cybersecurity Workstream 1 'Mapping and Analysis of International Cybersecurity Norms Agreements' and is the product of the collaborative work of many.

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

BPF Workstream 1 Lead:
John Hering

Key contributors in developing the paper:
Pablo Hinojosa
Eneken Tikk

Contributors to the analysis and research of the report:
Brishailah Brown
John-Michael Poon
Ying Chu Chen
Bart Hogeveen
Maarten Van Horenbeeck
Sheetal Kumar
Wim Degezelle

Disclaimer:

The views and opinions expressed herein do not necessarily reflect those of the United Nations Secretariat. The designations and terminology employed may not conform to United Nations practice and do not imply the expression of any opinion whatsoever on the part of the Organization.

Mapping and Analysis of

International Cybersecurity Norms Agreements

Table of Contents

I. Background

Recent years have witnessed a persistent escalation of sophisticated attacks in cyberspace, resulting in the rapidly emergence of a new domain of conflict. These attacks, whether conducted by criminal groups or sponsored by nation-state actors, have had damaging impacts on individuals and organizations around the world that increasingly depend on the reliability of ICT products and services. This is especially true when they threaten, damage or interrupt critical services like healthcare.

As with other domains of conflict, expectations for responsible behavior to promote stability and security have necessarily started emerging as well in the form of multilateral, regional, and bilateral agreements between states on voluntary and non-binding norms of conduct. However, distinct from other physical domains – air, land, sea, and space – the very fabric of cyberspace is largely owned and operated by private organizations, and as a fundamentally new domain of human activity it has also garnered the attention of academia and civil society groups concerned with defending rights and freedoms online. As a result, agreements on norms and expectations for responsible behavior have expanded beyond exclusively interstate agreements, to include agreements within other stakeholder groups, as well as prominent multistakeholder agreements that bring together governments, industry, academia, and civil society in common cause.

Despite the rise of these international agreements on cybersecurity norms and expectations, however, conflict in cyberspace continues to increase in both scale and sophistication, with new malicious tools and techniques rapidly proliferating across an ecosystem of bad actors at a tremendous rate. Since 2018, the Internet Governance Forum (IGF) Best Practice Forum on Cybersecurity (BPF) has focused its efforts on the evolution, implementation, and impact of international cybersecurity norms. In 2021, the BPF has continued this work via multiple workstreams.

II. Workstream 1 – Mapping agreements and exploring the intentions of norms

The BPF's Workstream 1 (WS1) is responsible for updating the BPF's list of existing cybersecurity norms agreements that were previously identified in the 2020 report, and then analyzing the norm elements that exist within the agreements to identify trends and explore their intended impact. To update the list of agreements, we hosted an open call earlier this year soliciting suggestions from the BPF community for agreements to be included in our work based on the below scoping criteria.

To be included in the scope of the BPF's analysis, agreements must reflect the following four elements:

1. Describe specific commitments or recommendations that apply to any or all signatory groups (typically governments, non-profit organization, or private sector companies).
2. The commitments or recommendations in the agreement must have a stated goal to improve the overall state of cybersecurity.
3. The agreement must be international in scope – intended to apply multiple well-known actors that either operate significant parts of internet infrastructure or are governments and therefore representing a wide constituency.
4. The agreement must include voluntary, nonbinding norms for cybersecurity, among and between different stakeholder groups.

Based on these criteria, experts participating as volunteers in the BPF were able to identify 36 international agreements on cybersecurity norms for inclusion in this report, as compared to the 22 agreements that were included in 2020 report based on similar criteria. This reflects both the establishment of new agreements in the past year – including 2 new reports adopted in UN First Committee processes – as well an expansion in the number of earlier agreements that were identified for inclusion this year. Importantly, this list of agreements does not include treaties/conventions or other legally-binding agreements between countries, as the intent of the Best Practice Forum is to remain focused on the development, evolution, and impact of voluntary and non-binding norms for cybersecurity. Agreements included in the scope of this work include political commitments to norms and principles between different parties, as well as things like draft laws or legal frameworks, and even draft conventions or guidance for responsible behavior online applicable to international stakeholders.

III. List of agreements included in study

Below is the complete list of the 36 agreements included in this year's study, organized by the year they were created/finalized. A breakdown of each agreement and the norm elements identified in each is featured in section VIII.

	Agreement Name	Year
1	**Draft EAC Legal Framework For Cyberlaws**	2008
2	**SCO agreement on cooperation in the field of ensuring the international information security**	2009
3	**League of Arab States Convention on Combating Information Technology Offences**	2010
4	**Convention on International Information Security**	2011
5	**APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice**	2011
6	**ASEAN Regional Forum Work Plan on Security of and in the Use of ICTs**	2012
7	**Southern African Development Community (SADC) Model Law**	2012
8	**African Union Convention on Cyber Security and Personal Data Protection**	2014
9	**OECD Digital Security Risk Management for Economic and Social Prosperity**	2015
10	**G20 Leaders Communique**	2015
11	**International code of conduct for information security**	2015
12	**UN-GGE Final Report (2015)**	2015
13	**NATO Cyber Defence Pledge**	2016
14	**OSCE Confidence Building Measures (2013 and 2016)**	2016
15	**FOC Recommendations for Human Rights Based Approaches to Cyber security**	2016
16	**ITU-T WTSA Resolution 50 -Cybersecurity**	2016
17	**Charter for the Digitally Connected World**	2016
18	**G7 declaration on responsible state behaviour in cyberspace**	2017
19	**Joint Communication to the European Parliament and the Council**	2017
20	**Charlevoix Commitment on Defending Democracy from Foreign Threats**	2018
21	**Commonwealth Cyber Declaration**	2018
22	**The Paris Call for Trust and Security in Cyberspace**	2018
23	**Charter of Trust**	2018
24	**Cybersecurity Tech Accord**	2018

25	**The Council to Secure the Digital Economy International Anti-Botnet guide**	2018
26	**ASEAN-United States Leaders' Statement on Cybersecurity Cooperation**	2018
27	**DNS Abuse Framework**	2019
28	**Contract for the Web**	2019
29	**Ethics for Incident Response and Security Teams (EthicsfIRST)**	2019
30	**GCSC's Six Critical Norms**	2019
31	**FOC Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies**	2020
32	**OAS List of Confidence- and Security-Building Measures (CSBMS)**	2020
33	**XII BRICS Summit Moscow Declaration**	2020
34	**OEWG Final Report (2021)**	2021
35	**UN-GGE Final Report (2021)**	2021
36	**Mutually Agreed Norms for Routing Security**	2021

IV. Classifications and breakdown of agreements

The agreements included in this report can be split into three categories based on the groups they apply to:

i. *Multilateral* – agreements established by the UN. As the international institution exclusively responsible for cooperation on peace and security in cyberspace, agreements established within the auspices of the UN are the only ones that can be said to be reflective/inclusive of all its 193 member states and therefore effectively universal.
ii. *Single-Stakeholder* – 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.
iii. *Multistakeholder* – agreements across stakeholder groups. These include agreements which are led by a state actor, but which include multiple stakeholders or non-governmental actors in their elaboration and implementation.

Multilateral agreements included

Multilateral agreements are those which effectively apply to every, or nearly every, government around the world, and are distinct from regional or bilateral agreements that involve smaller subsets of governments. Given the UN's exclusive role in promoting peace and security around the world, all of the multilateral agreements included in this report are a result of the UN dialogues on cybersecurity. This includes the 2015 report of the UN Group of Governmental Experts (GGE) on information security that established the UN's 11 norms for responsible state behavior online for the first time, as well as the two reports from the recent 2021 GGE and the parallel Open-Ended Working Group (OEWG), which each respectively reaffirmed those 11 norms and provided additional interpretation/implementation guidance.

Single-stakeholder agreements included

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, ...etc), were by far the most common form of cybersecurity norms-setting agreements we encountered in compiling this list. 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 that was first launched in 2018. It currently has over 150 company signatories from around the world, the largest such commitment of its kind.
- The Freedom Online Coalition's (FOC) Recommendations for Human Rights Based Approaches to Cyber security frames cybersecurity approaches in a human rights context, and reflects a commitment of the FOC member states. In 2020, the FOC released as well a Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies, which includes a set of nonbinding recommendations to states that FOC members commit to upholding respectively.
- In the Shanghai Cooperation Organization's (SCO) 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 the 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, recognizes 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 EU 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 have now expanded to include internet exchange points, as well as cloud service providers.
- The Commonwealth Cyber Declaration, launched in 2018, is a commitment among the Commonwealth of Nations' 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."
- 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."

- In 2016, the Permanent Council of the Organization for Security and Co-operation in Europe (OSCE) adopted Decision no. 1202: OSCE Confidence-Building Measures To Reduce The Risks Of Conflict Stemming From The Use Of Information And Communication Technologies. The agreement builds on earlier work of the OSCE in 2013 to adopt confidence-building measures (CBMs) across its participating states and in support of the UN's encouragement of CBMs for cyberspace. Taken together, the 2013 and 2016 agreements highlight 16 different CBMs.
- The draft Convention On International Information Security, was introduced as a proposed international convention on cybersecurity by the Russian Federation in 2011. As it was never adopted, it technically does not have any specific supporters but is nevertheless directed at governments.
- The Asia-Pacific Economic Cooperation (APEC) group in 2012 released the APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice in order to support countries adopting effective "ISP security codes of practice" on a voluntary basis.
- The DNS Abuse Framework is an agreement for domain name registrars/registries that was first launched in 2019 to provide a set of voluntary principles for these organizations to adopt to make the DNS system more secure.
- In 2015, the Association of South-East Asian Nations (ASEAN) launched the ASEAN Regional Forum Work Plan On Security Of And In The Use Of Information And Communications Technologies, including a set of suggested activities for the ASEAN member states intended to "promote a peaceful, secure, open and cooperative ICT environment and to prevent conflict and crises by developing trust and confidence between states in the ARF region…".
- The Southern African Development Community (SADC) Model Law on computer crime and cybercrime was developed in 2012 by the SADC in order to promote harmonized legal expectations across the southern African region in an effort to better cooperate in law enforcement.
- In a letter to the UN Secretary General in 2015, Six governments – China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan – put forward an International code of conduct for information security. While only six governments signed the letter, support was open to all states on a voluntary basis as a way to "identify the rights and responsibilities of States in the information space, promote constructive and responsible behaviour on their part and enhance their cooperation in addressing common threats and challenges in the information space…".
- The International Telecommunication Union's (ITU) Resolution 50 - Cybersecurity is a product of the World Telecommunication Standardization Assembly in 2016, with recommendations for ITU study groups and encouraging cooperation from member states.
- The Organization of American States (OAS) List Of Confidence- And Security-Building Measures (CSBMS), released in 2020, includes a total of 31 "traditional" and "non-traditional" CSBMS that OAS member states are encouraged to adopt on a voluntary basis, many of which are focused specifically on promoting greater cooperation in cybersecurity.
- The Charter for the Digitally Connected World is a 2016 commitment from the G7 to help improve quality of life via digital connectivity, with a subsection expressly focused on cybersecurity cooperation.

- The 2020 XII BRICS Summit Moscow Declaration, as with earlier such declarations, covers a range of areas where BRICS nations (Brazil, Russia, India, China, South Africa) will seek to cooperate, including on information security.
- The ASEAN-United States Leaders' Statement on Cybersecurity Cooperation is a 2018 statement reflecting a joint commitment between ASEAN member states and the United States, including a reaffirmation of the 2015 UN GGE norms for responsible state behavior online.
- The Organization for Economic Cooperation and Development's (OECD) Digital Security Risk Management for Economic and Social Prosperity was released in 2015 and provides recommendations for national strategies to better manage cyber risk for OECD members, as well as non-members, to adopt on a voluntary basis.

Multistakeholder agreements

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 are 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 1,200 official supporters, including 80 national governments, with various working groups tasked with promoting multistakeholder cooperation to advance its principles.
- 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) was a multi-stakeholder group of commissioners which together developed international cybersecurity norms related initiatives. Their final publication, *Advancing Cyberstability*, was released in 2019 and sets out eight 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 at the Internet Governance Forum 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.

V. Analysis process for norms agreements and limitations

For every agreement included in this year's report, an expert from the BPF reviewed the agreement to determine which norm elements it reflected to identify trends and shared priorities across agreements. In the 2020 analysis last year, this process was limited to considering whether and to what degree the norms agreements aligned with or reflected the 11 norms established by the 2015 UN First Committee Group of Governmental Experts (GGE) on information security. This year, the 2021 report has expanded this analysis considerably to include a wider range of norm elements across six categories, including elements focused on i) rights and freedoms, ii) information security and resilience, iii) reliability of products, iv) cooperation and assistance v) restraint on the development and use of cyber capabilities, and vi) technical/operational elements. Within these six categories there are then 26 specific norm elements that experts looked for evidence of across the 36 agreements.

This methodology used to collect and analyze the various agreements is not without its limitations, which should be noted. Analysis of any particular agreement contains a degree of subjectivity on the part of the evaluator. Each BPF volunteer was responsible for analyzing approximately 4-5 of the agreements included, and while each received common guidance and level-setting regarding how to conduct this evaluation, and there was a centralized review of the findings, there are inevitably still some discrepancies between what one individual would recognize as evidence of a norms element in an agreement as compared to what another might determine. As a result, the findings are not intended to be authoritative for each individual agreement, but rather indicative of broader trends when considered together. Moreover, when a norm element was not able to be identified in a particular agreement, it is recorded as "N/A," which does not mean that it doesn't exist in the agreement, but simply that the BPF volunteer was unable to find evidence of it.

Finally, when it comes to placing and comparing agreements on a timeline, it should be noted that the BPF worked to include the most up-to-date version of each agreement and gave each agreement the date associated with its most recent approval/release. This slightly inflates the number of recent agreements when comparing along a timeline, and so for the purposes of this report the agreements are split into four time-periods for comparison, where the first two reflect four years (2008-2011 and 2012-2015), and the second two each reflect three (2016-2018 and 2019-2021) to provide more balance (see Figure IV).

While this report is still in draft form, we welcome contributions from others in the IGF community, in particular from the organizations responsible for the respective agreements, to provide feedback and suggested edits to better reflect the contents of the agreements in each case. Feedback can be submitted to bpf-cybersecurity-info@intgovforum.org until Friday 10 December 2021.

VI. Trends and key findings

This section includes an overview of the findings of the BPF Workstream 1 analysis, comparing the 36 agreements and capturing how norm elements/categories have been reflected over time across the agreements. This information is captured in subsequent figures and charts in the next section (VII) – including a heat map (Figure II) that shows for each agreement where evidence of the different norm elements could be identified, as well as an overall frequency graph (see Figure III) comparing which norm elements and categories were most commonly reflected across all agreements. Finally, a series of frequency charts show how the focus on different norm elements in cybersecurity agreements has evolved over time by grouping the 36 agreements into time-bands based on the years they were established (Figure IV).

When it comes to the most prominent norm elements reflected across all agreements, considerations surrounding (4.1) "general cooperation" and (1.1) "human rights" were the most frequently included norm elements – with evidence of these elements found in 86% and 69% of agreements included in the report, respectively (see Figure III). This prioritization was consistent with the findings in the 2020 BPF report as well. As it relates to "general cooperation," the emphasis is perhaps unsurprising as most international agreements can be understood to be promoting some form of international cooperation, especially when it comes to cybersecurity, where support for capacity building and collaboration for implementing expectations is of paramount importance. Cooperation is also prioritized in the context of law enforcement, assistance in case of serious cyber incidents and exchanges on threats and ways to mitigate them.

Meanwhile, the emphasis on human rights across agreements is especially notable because not only is it the second most frequently recognized norm element, but also because this recognition has been consistently and noticeably growing over time. Only 40% of agreements the BPF reviewed between 2008-2011 included human rights considerations, as compared to 57% of agreements established between 2012-2015, and 71% of the agreements between 2016-2018. In the most recent agreements, between 2019-2021, evidence of human rights considerations was identified in 90% (see Figure IV) of the agreements included. This quantitative analysis highlights areas where further engagement and discussion among stakeholders is feasible and necessary – these themes reflect shared and growing priorities and hold potential for further agreement and joint implementation (such as human rights), or are expected to be detailed and deconflicted (for instance, supply chain security).

On the other end of the spectrum, the two least frequently cited norm elements across all agreements included were both in the fifth norm category: "Restraint on the development and use of cyber capabilities." Within this category, considerations of restraint related to (5.5) "botnets" and (5.9) "election infrastructure" were identified in only 8% and 11% of the agreements included in this report (see Figure III). While these are perhaps more niche elements when compared to things like "human rights" or "critical infrastructure," it is worth noting that this category as a whole – emphasizing restraint on what actors can and can't do – is also the least frequently reflected category overall across the agreements included in this report.

Each of the norm elements under the "restraint" category are reflected in less than 25% of the agreements included in the analysis, with the exception of restraints on "non-state actors" which appears in 33% of agreements. And the comparatively greater focus on restraining non-state actors

is perhaps an understandable outlier as the majority of the agreements included are between governments that may be more willing to limit the activities of other actors than they would be to curb their own capabilities voluntarily. Nevertheless, it is interesting to note that while these restraint elements were indeed found to be the least frequently included in cybersecurity agreements, their presence in these agreements has also distinctly and significantly grown in the time period captured since 2008 (see Figure IV).

VII. Data aggregation and visualization

Figure I: Word cloud of top 100 unique words used across all 36 agreements

Developed via Voyant Tools

Figure II: Heatmap of norms elements identified across agreements

Overview			1. Rights and freedoms		2. Information Security and resilience							3. Reliability of products	
Agreement Name	Year	Stakeholders	1.1 Human rights	1.2 Personal Data	2.1 CIP	2.2 Essential Services	2.3 Electoral processes	2.4 Public trust	2.5 Computer emergency response	2.6 Incident mitigation	2.7 Cyber hygiene	3.1 Supply chain	3.2 Reporting of vulnerabilities
Draft EAC Legal Framework For Cyberlaws	2008	Governments	○	●	○	○	○	●	○	○	○	○	○
SCO agreement on cooperation in the field of ensuring the international information security	2009	Governments	○	○	○	○	○	○	○	○	○	○	○
League of Arab States Convention on Combating Information Technology Offences	2010	Governments	●	●	○	○	○	○	○	○	○	○	○
Convention on International Information Security	2011	Governments	●	●	●	○	●	●	○	○	○	○	○
APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice	2011	Governments	○	●	○	○	○	●	●	●	●	○	●
ASEAN Regional Forum Work Plan on Security of and in the Use of ICTs	2012	Governments	○	○	○	○	○	○	○	○	○	○	○
Southern African Development Community (SADC) Model Law	2012	Governments	○	○	○	○	○	○	○	○	○	○	○
African Union Convention on Cyber Security and Personal Data Protection	2014	Governments	●	●	●	○	○	○	●	○	●	○	●
OECD Digital Security Risk Management for Economic and Social Prosperity	2015	Governments	●	●	○	○	○	●	●	●	○	○	●
G20 Leaders Communique	2015	Governments	○	●	○	○	○	●	○	○	○	○	○
International code of conduct for information security	2015	Governments	●	○	●	●	○	○	○	○	○	●	○
UN-GGE Final Report (2015)	2015	Governments	●	●	●	●	○	○	●	●	○	●	●
NATO Cyber Defence Pledge	2016	Governments	○	○	○	●	○	○	○	○	●	○	○
OSCE Confidence Building Measures (2013 and 2016)	2016	Governments	●	○	○	○	○	○	●	○	○	○	○
FOC Recommendations for Human Rights Based Approaches to Cyber security	2016	Multistakeholder	●	○	●	●	○	○	●	○	●	○	○
ITU-T WTSA Resolution 50 -Cybersecurity	2016	Governments	○	○	○	○	○	○	○	●	○	○	○
Charter for the Digitally Connected World	2016	Governments	●	●	●	●	○	○	○	○	○	○	○
G7 declaration on responsible state behaviour in cyberspace	2017	Governments	●	○	○	○	○	○	○	●	○	●	●
Joint Communication to the European Parliament and the Council	2017	Governments	●	●	○	●	●	●	●	●	●	○	●
Charlevoix Commitment on Defending Democracy from Foreign Threats	2018	Governments	●	●	○	○	●	●	○	○	○	○	○
Commonwealth Cyber Declaration	2018	Governments	●	●	●	○	○	●	●	●	●	○	●
The Paris Call for Trust and Security in Cyberspace	2018	Multistakeholder	●	○	●	○	●	○	○	○	●	●	○
Siemens Charter of Trust	2018	Private sector	○	●	●	○	○	○	○	○	○	●	○
Cybersecurity Tech Accord	2018	Private sector	●	●	○	○	○	○	○	○	●	●	●
The Council to Secure the Digital Economy International Anti-Botnet guide	2018	Private sector	○	●	●	○	○	○	○	●	○	○	●
ASEAN-United States Leaders' Statement on Cybersecurity Cooperation	2018	Governments	●	○	○	○	○	○	○	○	○	○	○
DNS Abuse Framework	2019	Private sector	●	○	●	○	○	●	○	●	○	○	○
Contract for the Web	2019	Multistakeholder	●	●	○	○	○	●	○	○	○	○	○
Ethics for Incident Response and Security Teams (EthicsfIRST)	2019	Private sector	●	●	●	○	○	○	○	●	○	○	●
GCSC's Six Critical Norms	2019	Multistakeholder	●	○	●	○	●	○	○	○	●	●	●
FOC Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies	2020	Governments	●	○	○	●	○	●	○	○	●	●	○
OAS List of Confidence- and Security-Building Measures (CSBMS)	2020	Governments	●	○	●	○	○	○	○	○	○	○	○
XII BRICS Summit Moscow Declaration	2020	Governments	●	○	○	○	○	○	○	○	○	○	○
OEWG Final Report (2021)	2021	Governments	●	○	●	●	●	○	●	●	○	●	●
UN-GGE Final Report (2021)	2021	Governments	●	●	●	●	●	●	●	●	○	●	●
Mutually Agreed Norms for Routing Security	2021	Multistakeholder	○	○	○	○	○	○	●	●	○	○	○

Figure II: Heatmap of norms elements identified across agreements (cont'd)

Overview			4. Cooperation and assistance				5. Restraint on development and use of cyber capabilities										6. Technical/Operational
Agreement Name	Year	Stakeholders	4.1 General cooperation	4.2 Law enforcement assistance	4.3 CIP assistance	4.4Due diligence	5.1 Developing and deploying cyber weapons	5.2 Intellectual property	5.3 Non-proliferation	5.4 Non-state actors	5.5 Botnets	5.6 CIP	5.7 CERT/CSIRT	5.8 Internet	5.9 Election infrastructure	5.10 Harmful hidden functions	6.1 Network security practices
Draft EAC Legal Framework For Cyberlaws	2008	Governments	○	●	○	○	○	○	○	●	○	○	○	○	○	○	○
SCO agreement on cooperation in the field of ensuring the international information security	2009	Governments	●	○	○	○	●	○	○	○	○	○	○	○	○	○	○
League of Arab States Convention on Combating Information Technology Offences	2010	Governments	○	●	○	○	○	○	○	●	○	○	○	○	○	○	○
Convention on International Information Security	2011	Governments	●	●	○	○	○	●	●	●	○	○	○	○	○	○	○
APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice	2011	Governments	●	○	○	○	○	○	○	○	○	○	●	○	○	○	○
ASEAN Regional Forum Work Plan on Security of and in the Use of ICTs	2012	Governments	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
Southern African Development Community (SADC) Model Law	2012	Governments	○	●	○	○	○	○	○	○	○	●	○	●	○	○	○
African Union Convention on Cyber Security and Personal Data Protection	2014	Governments	●	●	○	○	○	○	●	●	○	○	○	○	○	●	○
OECD Digital Security Risk Management for Economic and Social Prosperity	2015	Governments	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
G20 Leaders Communique	2015	Governments	●	○	○	○	○	●	○	●	○	○	○	○	○	○	○
International code of conduct for information security	2015	Governments	●	○	○	○	○	○	○	○	○	○	○	○	●	○	○
UN-GGE Final Report (2015)	2015	Governments	●	●	●	○	●	○	●	●	○	●	●	○	○	○	
NATO Cyber Defence Pledge	2016	Governments	●	○	○	○	○	○	○	●	○	○	○	○	○	○	○
OSCE Confidence Building Measures (2013 and 2016)	2016	Governments	●	●	○	○	○	○	○	●	○	●	○	○	○	○	○
FOC Recommendations for Human Rights Based Approaches to Cyber security	2016	Multistakeholder	●	○	○	●	○	○	○	○	○	○	○	○	○	○	●
ITU-T WTSA Resolution 50 -Cybersecurity	2016	Governments	●	○	○	○	○	○	○	○	○	○	○	○	○	○	●
Charter for the Digitally Connected World	2016	Governments	●	○	○	○	○	●	○	○	○	○	○	○	○	○	○
G7 declaration on responsible state behaviour in cyberspace	2017	Governments	●	●	○	○	●	●	○	○	○	○	●	○	○	○	○
Joint Communication to the European Parliament and the Council	2017	Governments	●	●	○	●	○	○	●	○	○	○	○	○	○	○	○
Charlevoix Commitment on Defending Democracy from Foreign Threats	2018	Governments	●	●	○	○	○	○	○	○	○	○	○	○	○	○	●
Commonwealth Cyber Declaration	2018	Governments	●	●	○	○	○	○	○	○	○	○	●	○	○	○	●
The Paris Call for Trust and Security in Cyberspace	2018	Multistakeholder	●	○	○	○	○	●	○	●	○	○	○	●	○	●	○
Siemens Charter of Trust	2018	Private sector	●	○	○	○	○	○	○	○	○	○	○	○	○	○	●
Cybersecurity Tech Accord	2018	Private sector	●	○	○	●	○	○	○	○	○	○	○	○	○	●	○
The Council to Secure the Digital Economy International Anti-Botnet guide	2018	Private sector	●	●	●	○	○	●	○	○	●	●	●	○	○	○	●
ASEAN-United States Leaders' Statement on Cybersecurity Cooperation	2018	Governments	●	○	○	○	○	●	○	○	○	○	○	○	○	○	○
DNS Abuse Framework	2019	Private sector	●	○	○	○	○	○	○	○	●	○	○	●	○	●	○
Contract for the Web	2019	Multistakeholder	○	○	○	●	●	○	○	○	○	○	○	●	○	○	○
Ethics for Incident Response and Security Teams (EthicsfIRST)	2019	Private sector	●	○	○	●	○	●	○	○	○	○	●	○	○	●	○
GCSC's Six Critical Norms	2019	Multistakeholder	○	●	○	○	●	○	○	●	●	○	○	●	●	●	○
FOC Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies	2020	Governments	●	●	○	●	○	○	○	○	○	○	○	○	○	○	●
OAS List of Confidence- and Security-Building Measures (CSBMS)	2020	Governments	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○
XII BRICS Summit Moscow Declaration	2020	Governments	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○
OEWG Final Report (2021)	2021	Governments	●	○	●	●	○	○	○	●	○	●	●	○	●	●	○
UN-GGE Final Report (2021)	2021	Governments	●	●	●	●	●	○	●	●	○	●	●	●	●	●	○
Mutually Agreed Norms for Routing Security	2021	Multistakeholder	●	○	○	●	○	○	○	○	○	○	○	○	○	○	●

Figure III: Frequency of norm elements across agreements (expressed in %)

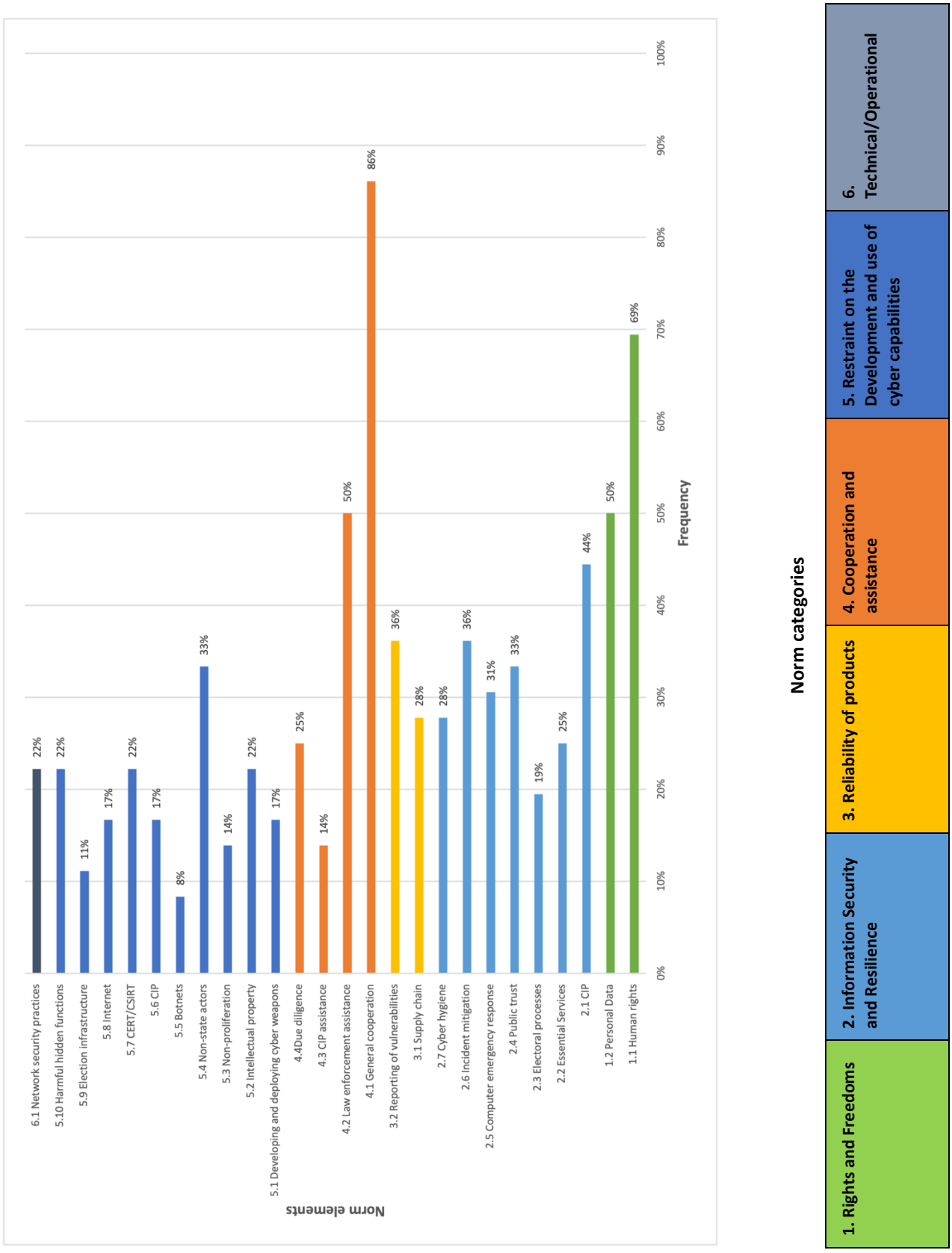
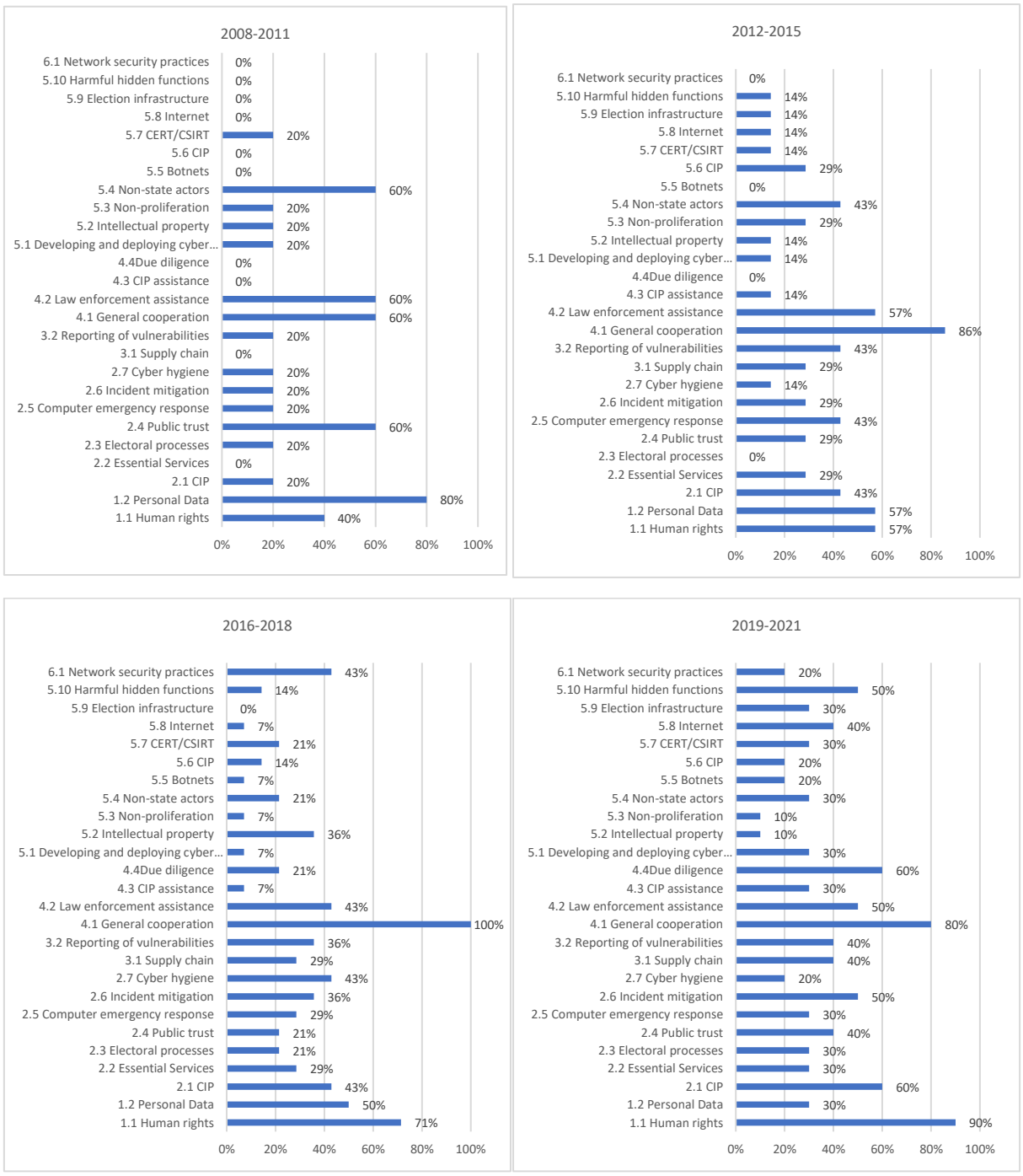


Figure IV: Norm elements reflected over time (expressed in %)



VIII. Evidence of norm elements across agreements

The references are compiled in a separate document available at https://www.intgovforum.org/en/filedepot_download/235/19830 .