IGF Internet Governance Forum

IGF 2021 INTERNET GOVERNANCE FORUM POLAND
INTERNET UNITED

Best Practice Forum on Cybersecurity

Use of norms to foster trust and security

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.

Acknowledgments

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 output of the IGF 2021 BPF on Cybersecurity and is a compilation of the Workstream 1 output 'Mapping and Analysis of International Cybersecurity Norms Agreements' and Workstream 2 output 'Testing Norms Concepts against Cybersecurity Events'. The BPF's Workstream 3 was dedicated to 'BPF Outreach and Cooperation with other IGF Initiatives'. The BPF output is the product of the collaborative work of many.

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

BPF Cybersecurity coordinating team

Hariniombonana Andriamampionona,
MAG Co-facilitator
Markus Kummer, BPF Co-facilitator
Maarten Van Horenbeeck, BPF Lead expert
John Hering, BPF Workstream Lead
Mallory Knodel, BPF Workstream Lead
Sheetal Kumar, BPF Workstream Lead
Wim Degezelle, BPF Consultant

Key contributors

Anastasiya Kazakova, Apratim Vidyarthi, Barbara Marchiori de Assis, Bart Hogeveen, Brishailah Brown, Eneken Tikk, Evan Summers, Fred Hansen, John Hering, John-Michael Poon, Louise Marie Hurel, Maarten Van Horenbeeck, Mallory Knodel, Niamh Healy, Pablo Hinojosa, Sheetal Kumar, Wim Degezelle, Ying Chu Chen.

Executive Summary

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. Since 2014, IGF Best Practice Forums have focused on cybersecurity related topics.

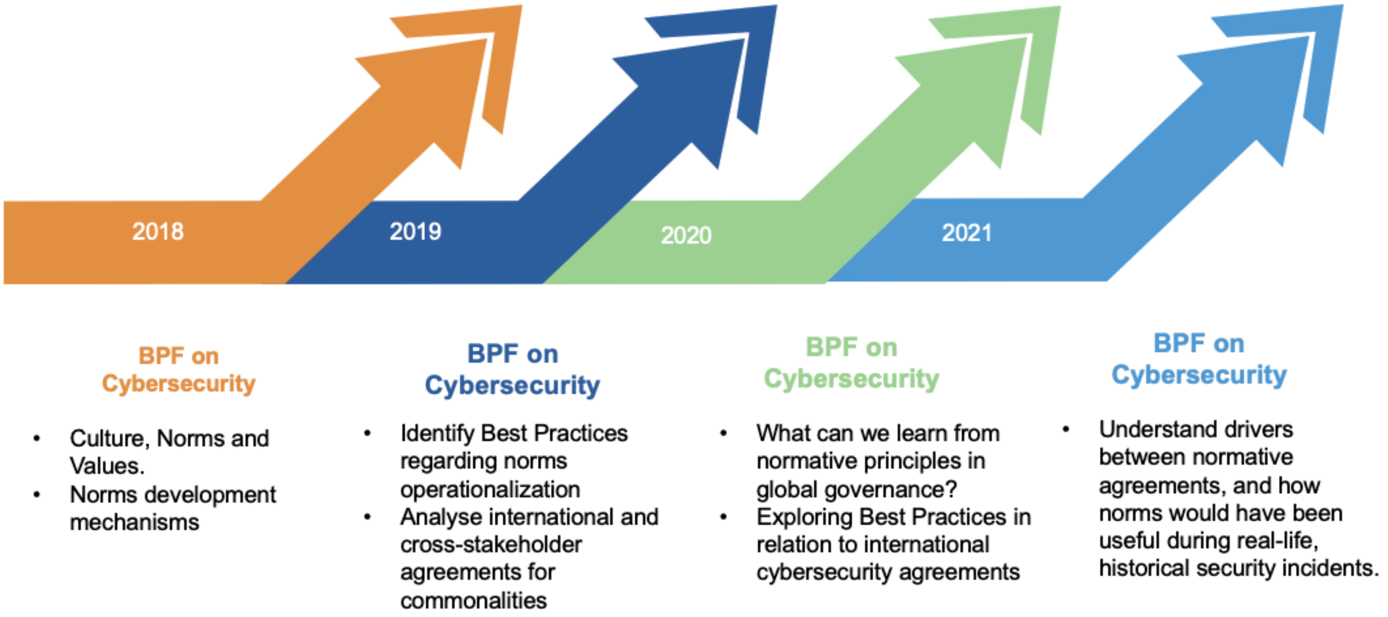
In the last four years, the BPF on Cybersecurity started investigating the concept of culture, norms and values in cybersecurity. In 2018 the BPF took a closer look at norms development mechanisms. In 2019, when the BPF ran in conjunction with the initiation of UN GGE and OEWG, the BPF looked at best practices related to the operationalization of cyber norms and started analysing international and cross-stakeholder cybersecurity initiatives for commonalities. In 2020, the BPF took a wider approach and explored what can be learned from norms processes in global governance in areas completely different than cybersecurity, and continued and further advanced the analysis of cyber norms agreements.

The 2021 BPF on Cybersecurity has continued work to support the ongoing development of cybersecurity norms in the UN and elsewhere. In our research product this year, we have worked to identify relevant cybersecurity norms agreements and investigated more deeply the drivers behind, and disablers of, cyber norms. The BPF also researched major historical cybersecurity incidents, with as goal to understand how they can help drive further norms discussions; and help us understand which norms would have been useful during their mitigation.

Mapping and Analysis of International Cybersecurity Norms Agreements

Recent years have witnessed a persistent escalation of sophisticated attacks in cyberspace, resulting in the rapid emergence of a new domain of conflict. 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. The BPF included 36 such agreements in this year's study, which each:

- Describe specific commitments or recommendations that apply to any or all signatory groups (typically governments, non-profit organization or private sector companies);
- Define commitments or recommendations in the agreement must have a stated goal to improve the overall state of cybersecurity;
- Are international in scope – intended to apply multiple well-known actors that



BPF on Cybersecurity

- Culture, Norms and Values.
- Norms development mechanisms

BPF on Cybersecurity

- Identify Best Practices regarding norms operationalization
- Analyse international and cross-stakeholder agreements for commonalities

BPF on Cybersecurity

- What can we learn from normative principles in global governance?
- Exploring Best Practices in relation to international cybersecurity agreements

BPF on Cybersecurity

- Understand drivers between normative agreements, and how norms would have been useful during real-life, historical security incidents.

either operate significant parts of internet infrastructure or are governments and therefore representing a wide constituency.

- Include voluntary, nonbinding norms for cybersecurity, among and between different stakeholder groups.

The analysis provides deeper analysis of each agreement, but specifically noted the following findings of interest regarding the focus of cyber norms:

- When it comes to the most prominent norm elements reflected across all agreements, considerations surrounding **"general cooperation"** and **"human rights"** were the most frequently included norm elements.
- 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.
- 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".

Testing norms concepts against historical internet events

The BPF's second workstream focused on understanding the answer to the question **"How would specific norms have been effective at mitigating adverse cybersecurity events?"**. This was done through a detailed review of nine major cybersecurity events, selected based on their coverage in the media, demonstrable harm, successful mitigation and their relationship to cyber norms. These events included incidents such as Ghostnet, Stuxnet, NSO Group's Pegasus and Solarwinds.

For each of these incidents, a group of expert contributors sought to answer the central research question through desk research and analysis. In each case, an assessment is provided on which cyber norms could have been helpful at mitigating impact of the incident, or preventing harm.

The investigators found that **the cyber norms we have today would have helped mitigate many of the notorious cyber events of the past.** However, each analysis uncovered a missing nuance from deeper stakeholder involvement, to application of existing legal frameworks.

For instance, the case of the GhostNet event of 2009 highlighted that cyber resilience should be a community-level concern that when addressed at the hyperlocal level, lends capacity to at-risk groups to shift into monitoring mode and can respond to the evolution of threats over time.

There is certainly more qualitative research that could be done to understand better the barriers and benefits to focussing on normative frameworks for those closest to cybersecurity incidents, past and present, in order to better mitigate future events. It is clear from the differential in depth of analysis between the events with desk research only versus those for which qualitative interviews were also conducted: **the voices of those most affected by cybersecurity events provide key nuance are not present in secondary source reports or tertiary source reporting.**

Our distilled findings coalesce around two main themes. They point to a **gap in understanding the roles of a wide variety of actors and stakeholders in mitigating cybersecurity incidents.** And they show a **persistent disclarity in the interplay of norms, policies, and laws.**

To bridge this gap, we recommend future research work that is focused on understanding the interplay of cybersecurity norms and cybercrime legislation, where they overlap, align or work in opposition, with an aim to introduce greater stakeholder participation in the creation, enforcement and response mitigation as outlined in cybersecurity norms.

Contents

1. Workstream 1 - Mapping and Analysis of International Cybersecurity Norms Agreements

Contributors to workstream 1
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

1.1 Background

Recent years have witnessed a persistent escalation of sophisticated attacks in cyberspace, resulting in the rapid 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.

1.2 Terms

CBM – Confidence Building Measures
CERT/CSIRT – Computer Emergency Response Teams/Computer Security Incident Response Teams
CIP – Critical Infrastructure Protection
CII – Critical Information Infrastructure
DNS – Domain Name System
ICT – Information Communications Technology
IOT – Internet of Things
PII – Personal Identifying Information

1.3 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.

1.4 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 1.8.

	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

1.5 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.

1.6 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).

1.7 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).

1.8 Data aggregation and visualization

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

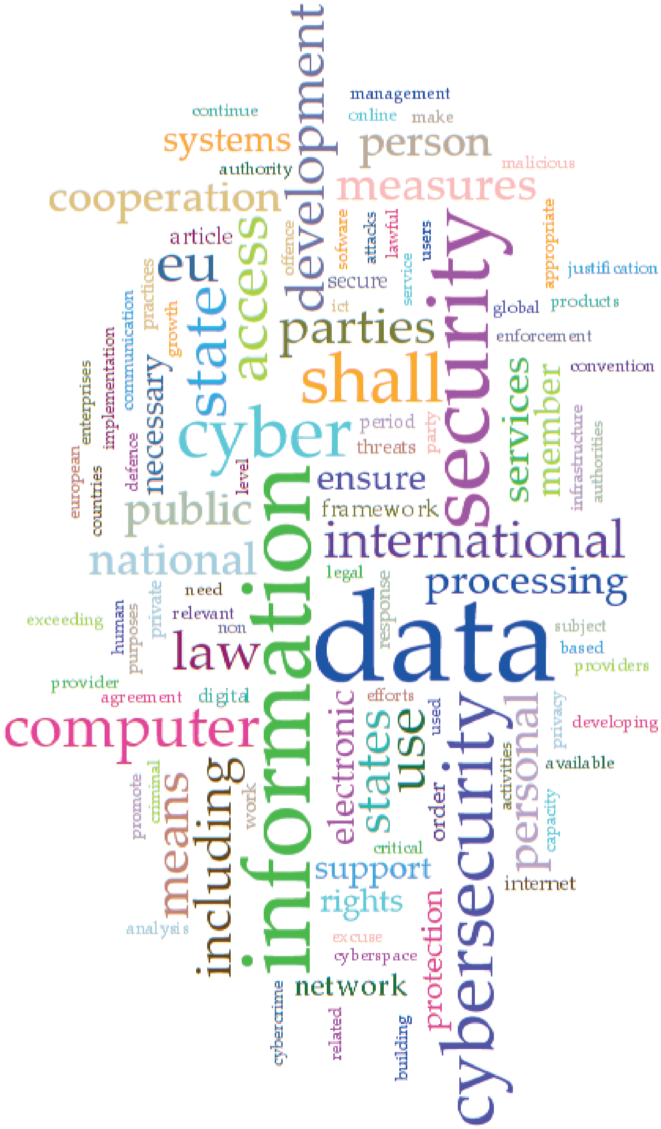
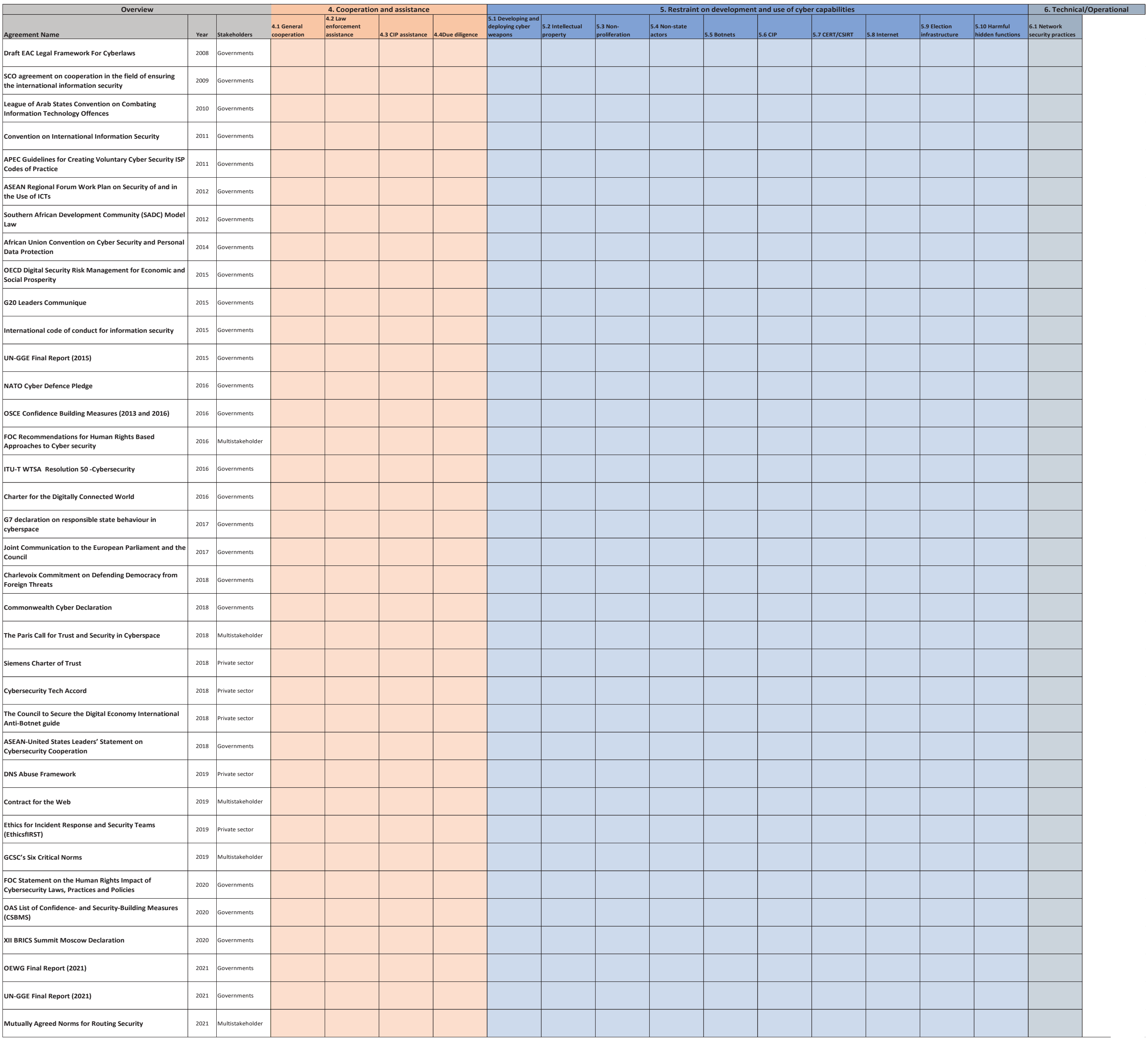


Figure II: Heatmap of norms elements identified across agreements

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 %)

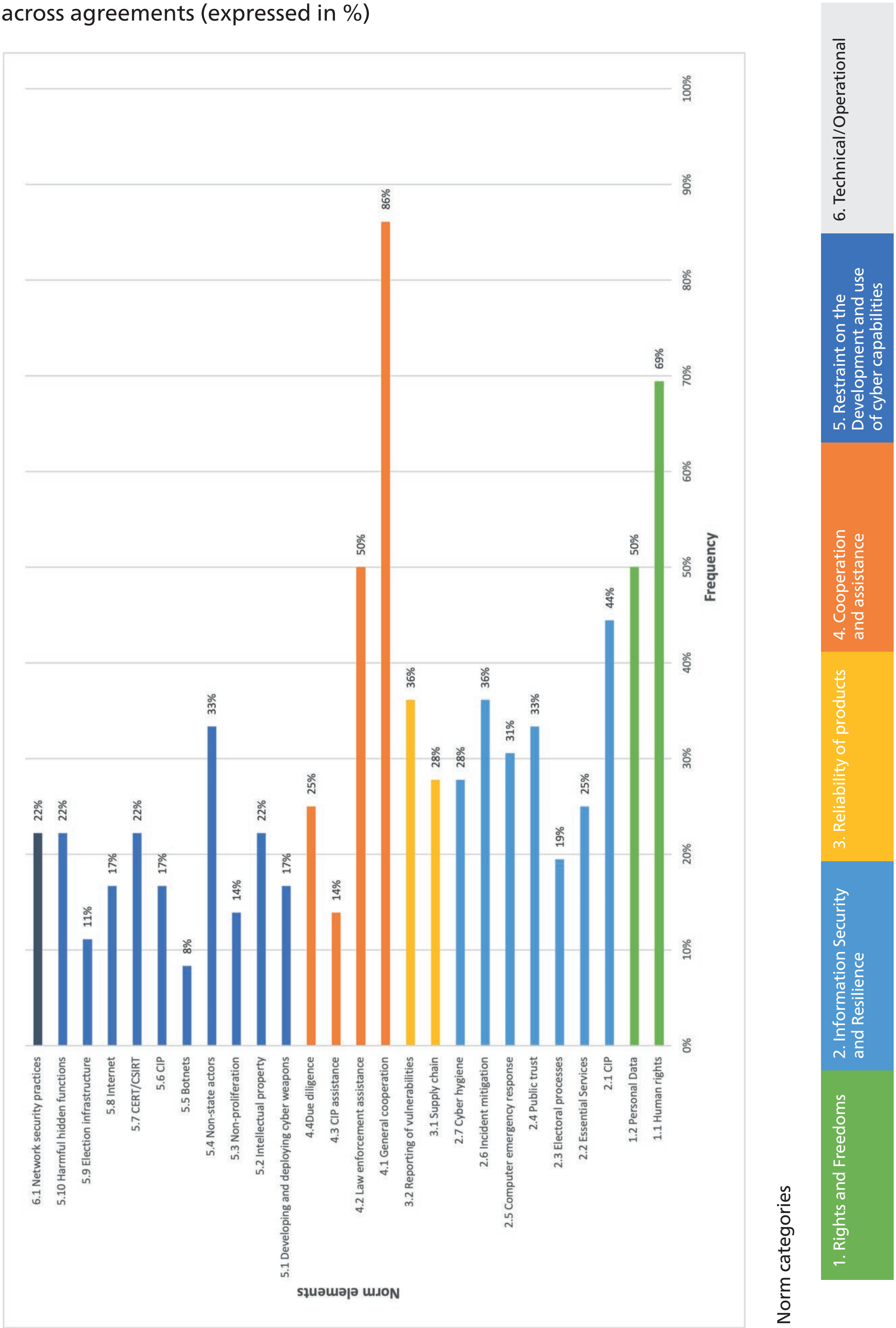
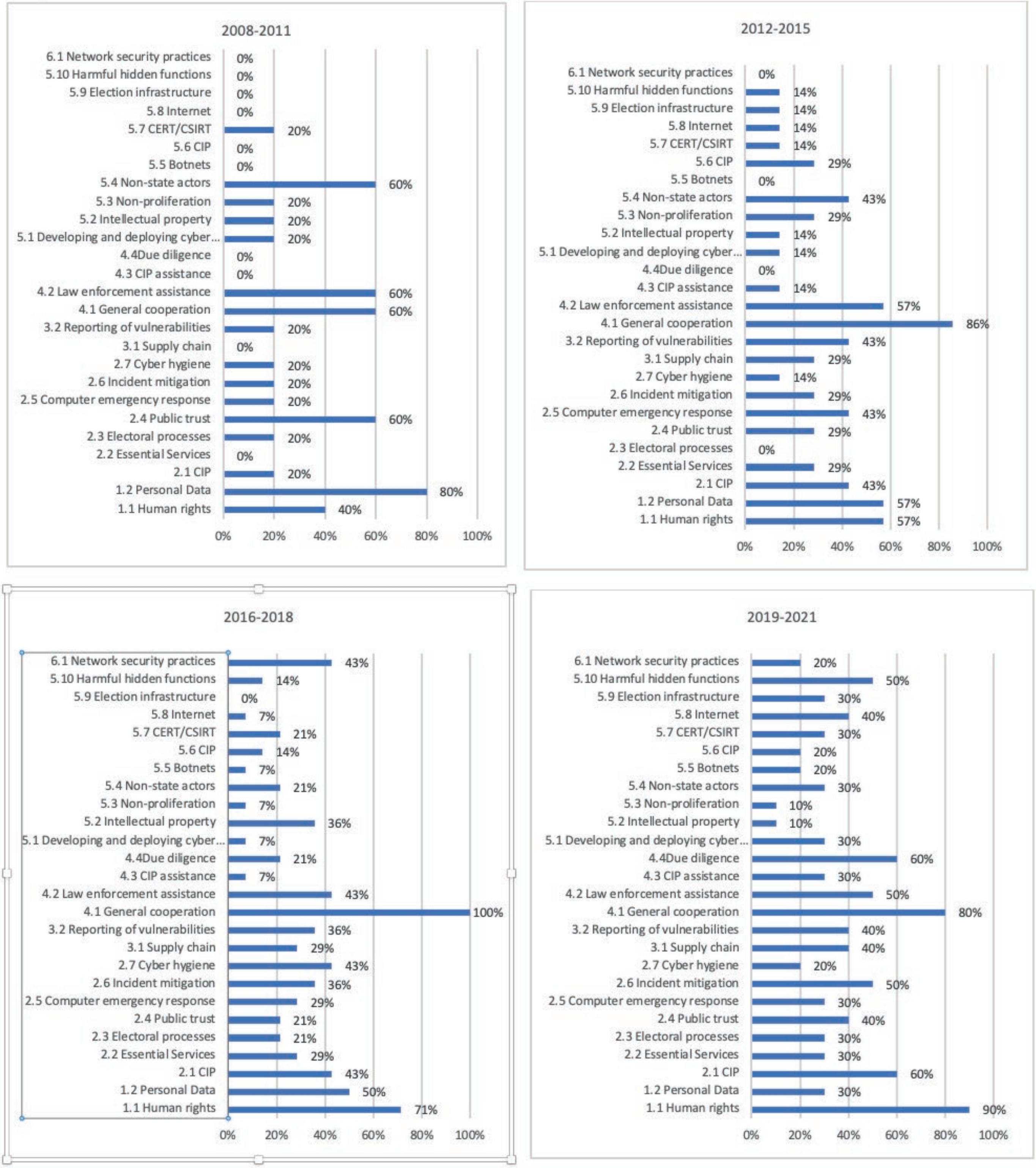


Figure IV: Norm elements reflected over time (expressed in %)



2008-2011

2012-2015

2016-2018

2019-2021

Figure V: Norm categories reflected in all agreements over time

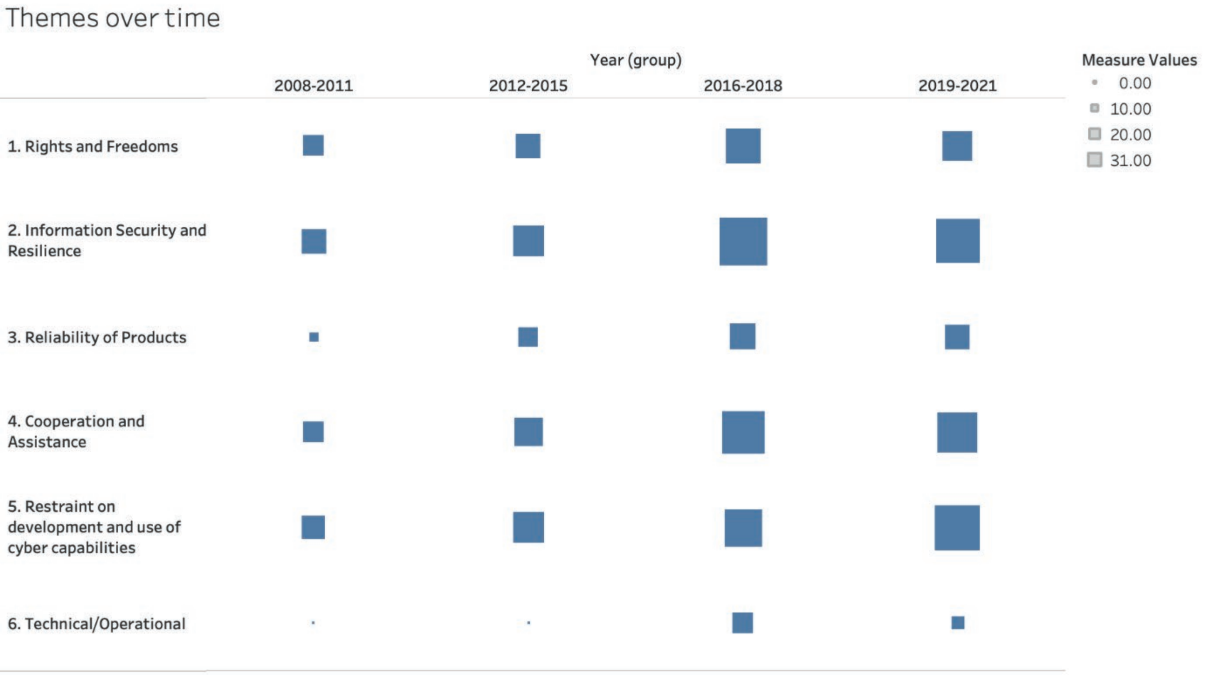
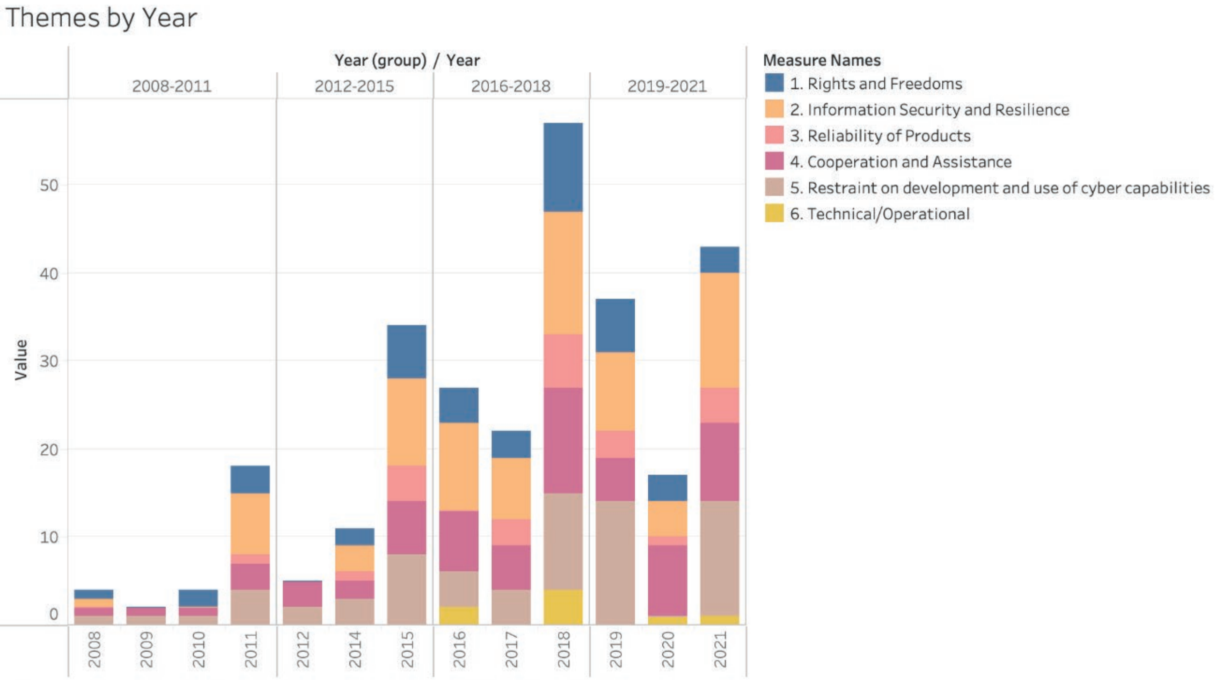
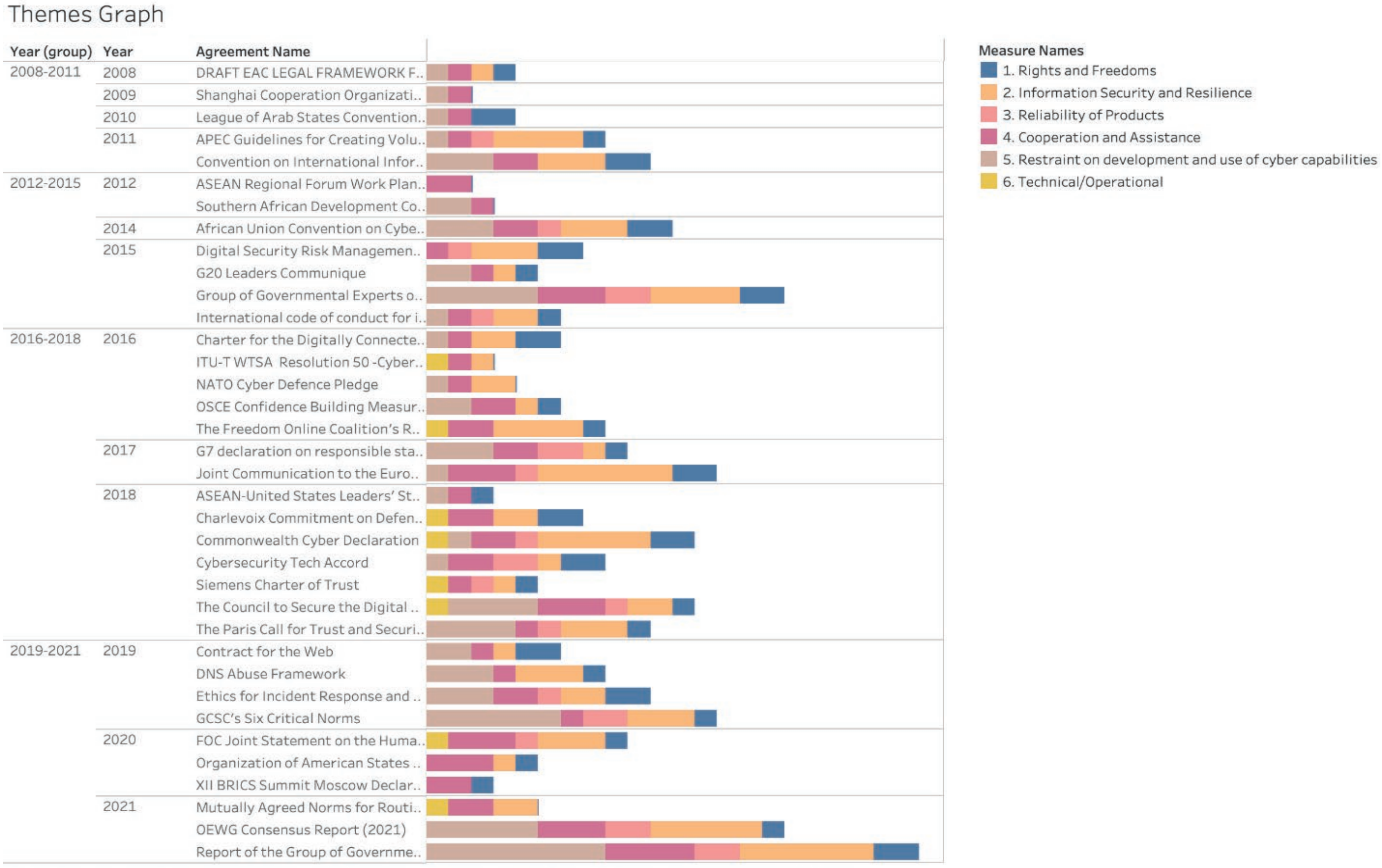


Figure VI: Norm categories reflected in agreements by year



1. Rights and Freedoms, 2. Information Security and Resilience, 3. Reliability of Products, 4. Cooperation and Assistance, 5. Restraint on development and use of cyber capabilities and 6. Technical/Operational for each Year broken down by Year (group). Color shows details about 1. Rights and Freedoms, 2. Information Security and Resilience, 3. Reliability of Products, 4. Cooperation and Assistance, 5. Restraint on development and use of cyber capabilities and 6. Technical/Operational. Details are shown for 1. Rights and Freedoms, 2. Information Security and Resilience, 3. Reliability of Products, 4. Cooperation and Assistance, 5. Restraint on development and use of cyber capabilities and 6. Technical/Operational.

Figure VII: Norm categories reflected in all cyber norms agreements



1. Rights and Freedoms, 2. Information Security and Resilience, 3. Reliability of Products, 4. Cooperation and Assistance, 5. Restraint on development and use of cyber capabilities and 6. Technical/Operational (color) and 1. Rights and Freedoms, 2. Information Security and Resilience, 3. Reliability of Products, 4. Cooperation and Assistance, 5. Restraint on development and use of cyber capabilities and 6. Technical/Operational (size) broken down by Year (group), Year and Agreement Name.

1.9 Evidence of norm elements across agreements

This chapter summarizes the qualitative findings across normative instruments analyzed in the study. It contains comparative accounts of normative themes across stakeholders: the UN GGE and the OEWG, multilateral and regional organizations, technical communities, and multi-stakeholder groups. Each topical summary concludes with brief observations about the depth and breadth of shared understanding across the various groups. Norms elements and categories that were addressed in less than 20% of the normative instruments analyzed have been excluded from this summary.

- Human Rights (1.1)
- Personal Data Protection and privacy (1.2)
- Critical Infrastructure Protection (2.1, 2.2, 5.6)
- Electoral Processes and Relevant Infrastructure (2.3, 5.9)
- Public Trust (2.4)
- Computer Emergency Response Mechanisms (2.5, 5.7)
- Cyber Hygiene (2.7)
- Supply Chain Security, Reporting of Vulnerabilities and Harmful hidden Functions (3.1, 3.2, 5.10)
- General Cooperation (4.1)
- Law Enforcement Assistance (4.2)
- Due Diligence (4.4)
- Intellectual Property Protection (5.2)
- Network Security Practices (6.1)

1.9.1 Human Rights (1.1)

According to norm 13 (e) of the 2015 UN GGE report, states should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

The UN GGE 2021 report explains that this norm reminds States to respect and protect human rights and fundamental freedoms, both online and offline in accordance with their respective obligations.[1]

In the 2021 UN Open Ended Working Group (OEWG) report, states concluded that they are increasingly concerned about the implications of the malicious use of ICTs for human rights and development. Increasing connectivity and reliance on ICTs without accompanying measures to ensure ICT security can bring unintended risks, making societies more vulnerable to malicious ICT activities. Despite the invaluable benefits of ICTs for humanity, their malicious use can have significant and far-reaching negative impacts.[2]

The G7 has reaffirmed that the same rights that people have offline must also be protected online, making reference to the Human Rights resolutions mentioned by the UN GGE.[3] The G7 has further encouraged states to share lessons learned and best practices in collaboration with governments, civil society and the private sector that are developing related initiatives including those that promote free,

[1] Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, para 36.

[2] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021), para 15.

[3] G7 declaration on responsible state behaviour in cyberspace, page 2.

independent and pluralistic media; fact-based information; and freedom of expression.[4]

Several multilateral instruments address human rights. BRICS states have emphasized the need of a comprehensive and balanced approach to ICTs development and security, including technical advancement, business development, of safeguarding the security of States and public interests, and of respecting the right to privacy of individuals.[5] The Commonwealth Cyber Declaration states that the implementation of the Declaration is based on the shared Commonwealth values of human rights, tolerance, respect and understanding, freedom of expression, rule of law, good governance, sustainable development and gender equality.[6]

Several instruments address human rights in their preambles. The African Union has reaffirmed the commitment of Member States to fundamental freedoms and human and peoples' rights contained in the declarations, conventions and other instruments adopted within the framework of the African Union and the United Nations.[7] The Arab Convention on Combating IT offences mandates adhering to the relevant Arab and international treaties and charters on human rights, and guaranteeing, respecting and protecting them.[8] The EU states that a comprehensive approach to cybersecurity requires respect for human rights, and the EU will continue to uphold its core values globally, building on the EU's Human Rights Guidelines on online freedom.[9] The OAS calls for exchange of information related to adopting and adapting provisions under domestic laws that govern processes for obtaining data and information, and exchange experiences involving government, service providers, end users and others, regarding the prevention, management of, and protection against cyber threats, with a view to sustained mutual cooperation to prevent, address, and investigate criminal activities that threaten security and to ensure an open, interoperable, secure and reliable internet, while respecting obligations and commitments under international law and international human rights law in particular.[10] OECD notes that all stakeholders should manage digital security risk in a transparent manner and consistently with human rights and fundamental values.[11]

Under the Convention on Information Security, each State Party guarantees freedom of speech and expression in its information space, as well as protection against illegal interference into the private lives of citizens. Further, each State Party aims to maintain a balance between fundamental human rights and the effective counteraction of terrorist use of the information space.[12]

The US and ASEAN have also reaffirmed that, as stated in UNGA resolution 71/199, the same rights that people have offline must also be protected online.[13] The same affirmation has been made by the Paris Call for Trust and Security in Cyberspace.[14]

The Global Commission's norms are accompanied by four principles, one of which is human rights.[15] The Freedom Online Coalition reminds that states

[4] Charlevoix Commitment on Defending Democracy from Foreign Threats, Art. 4.

[5] XII BRICS Summit Moscow Declaration, para 39.

[6] Commonwealth Cyber Declaration, preamble.

[7] African Union Convention on Cyber Security and Personal Data Protection, preamble.

[8] Arab Convention on Combating Information Technology Offences, preamble.

[9] Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, page 18.

[10] Organization of American States List of Confidence and Security-Building Measures (CSBMS), Committee on Hemispheric Security, para 25.

[11] Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document, 1.3., page 9.

[12] Convention on International Information Security, Art. 5.

[13] ASEAN-United States Leaders' Statement on Cybersecurity Cooperation, para 11.

[14] The Paris Call for Trust and Security in Cyberspace, para 4.

[15] GCSC's Six Critical Norms

need to comply with their obligations under international human rights law when considering, developing and applying national cybersecurity policies and legislation.[16] Contract for the Web invites respect and protect people's fundamental online privacy and data rights, so everyone can use the internet freely, safely, and without fear.[17] According to FIRST, team members should be aware that their actions may impact human rights of others, by sharing information, possible bias in their actions, or by infringing property rights.[18] The Freedom Online Coalition upholds human rights in several recommendations, including:

- Cybersecurity policies and decision-making processes should protect and respect human rights.
- The development of cybersecurity-related laws, policies, and practices should from their inception be human rights respecting by design.
- Cybersecurity-related laws, policies and practices should not be used as a pretext to violate human rights, especially free expression, association, assembly, and privacy.
- Cybersecurity-related laws, policies and practices should reflect the key role of encryption and anonymity in enabling the exercise of human rights, especially free expression, association, assembly, and privacy.
- Cybersecurity-related laws, policies and practices should not impede technological developments that contribute to the protection of human rights.[19]

1.9.2 Personal Data Protection and privacy (1.2)

Apart from more general commitments to uphold and respect their human rights obligations, the right to privacy and personal data protection has been singled out as a shared concern among international cybersecurity stakeholders.

The UN GGE 2015 report's commitment to human rights singles out General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age as an auxiliary dimension of how international cybersecurity is to be achieved.[20] The OEWG also refers to privacy in the context of the integrity, stability and security of the supply chain. To prevent the development and proliferation of malicious ICT tools and techniques and the use of harmful hidden functions, including backdoors, States can consider putting in place at the national level legislative and other safeguards that enhance the protection of data and privacy.[21] The G7 governments, concerned with defending democracy from foreign threats, commit to engagements with internet service providers and social media platforms regarding malicious misuse of information technology by foreign actors, with a particular focus on improving transparency regarding the use and seeking to prevent the illegal use of personal data and breaches of privacy.[22] The G7 also draws attention to the intertwinement of the right to privacy and secrecy of digital communications:

> …all states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications.[23]

The 2021 UN GGE report stresses that states, when putting in place critical infrastructure

[16] FOC Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies, para 14.

[17] Contract for the Web, principle 3.

[18] Ethics for Incident Response and Security Teams (EthicsfIRST), page 3.

[19] The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security.

[20] UN GGE (2015), 13 e; also G7 declaration on responsible state behaviour in cyberspace, norm 7.

[21] OEWG (2021), para 58 b,.

[22] Charlevoix Commitment on Defending Democracy from Foreign Threats, art. 5

[23] G20 Leaders Communique, para 26

protection frameworks, should make sure that relevant legislative and other safeguards enhance the protection of data and privacy.[24] States are invited to exchange information on national laws and policies for the protection of data and ICT-enabled infrastructure. [25]

Several regional frameworks emphasize the need for personal data protection in the context of cybersecurity. The African Union's Convention on Cyber Security and Personal Data Protection requires establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and to punish any violation of privacy without prejudice to the principle of free flow of personal data.[26] The Arab Convention on Combating Information Technology Offences contains offences against privacy by means of information technology.[27]APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice contains a reminder that when collecting and distributing information from networks, regulations and legislation pertaining to privacy should be taken into account.[28] The Commonwealth Cyber Declaration highlights the importance of common standards and the strengthening of data protection and security frameworks, in order to promote public trust in the internet, confidence for trade and commerce, and the free flow of data.[29] The Convention on International Information Security mentions right to a private life and the protection of personal data in the preamble.[30]OECD warns that digital security risk management should be implemented in a manner that is consistent with the confidentiality of information and communication and the protection of privacy and personal data.[31] The Draft EAC Legal Framework for Cyberlaws acknowledges the critical importance of data protection and privacy and recommends that further work needs to carried out on this issue, to ensure that (a) the privacy of citizens is not eroded through the Internet; (b) that legislation providing for access to official information is appropriately taken into account; (c) the institutional implications of such reforms and (d) to take into account fully international best practice in the area.[32] The right to privacy and protection of personal data have been flagged as core values of the EU.[33]

The Freedom Online Coalition explains that the human dimension of cybersecurity invites attention to the right to be free from arbitrary or unlawful interference with privacy.[34] FOC draws attention to the need to protect privacy in the context of cybersecurity-related laws, policies and practices: regulation should not be used as a pretext to violate human rights, especially free expression, association, assembly, and privacy.[35]

Several other stakeholders have flagged the issue. According to the Contract for the Web, respecting and protecting people's privacy, personal data, and other online data rights is essential for building online trust.[36]

[24] Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, para 58

[25] Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, para 58

[26] African Union Convention on Cyber Security and Personal Data Protection, art. 8.

[27] Arab Convention on Combating Information Technology Offences, art. 14

[28] APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice, page 10, sec 2.

[29] Commonwealth Cyber Declaration, sec 3.

[30] Convention on International Information Security, preamble

[31] Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document, sec 1.3

[32] Draft EAC Legal Framework for Cyberlaws, page 18

[33] Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, page 18

[34] FOC Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies, para 20

[35] The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security, rec 5.

[36] Contract for the Web, principle 5.

The first response community notes that data collection is necessary for incident response, but also emphasizes that balance should be struck between the goal of incident response and respecting the data stakeholders: while progressing through an incident, team members should adjust what they are collecting as the need changes."[37] The Siemens Charter of Trust commits the industry to adopting the highest appropriate level of security and data protection and ensuring that privacy is preconfigured into the design of products, functionalities, processes, technologies, operations, architectures and business models.[38]One of the baseline principles of combatting botnets flags personal data considerations in the process:

> Device manufacturers may provide notice to the consumer about security support policy and how the device is supported with updates during and what to expect after the support period. Where possible, the device should support network asset management by enabling the ability to identify and audit the device logically and physically and with proper access control. After the support period, consumers should have the ability to, and be informed about, how to "decommission" the device. Decommissioning should allow a consumer to return the product to factory defaults and remove any Personally Identifiable Information (PII).[39]

Widely acknowledged and referenced, the relationship between cybersecurity and privacy remains subject to further discussion, as is evidenced by the parallel processes in the UN setting. For the time being, the balance between personal data protection and cybersecurity is to be struck at national level, while further guidance can be expected from the UN Human Rights Commission as well as the General Assembly. While half of the instruments analyzed contain emphasis points with regard to privacy and personal data protection, there is hardly a coherent understanding among the stakeholders about the scope and the adequate level of such protections.

1.9.3 Critical Infrastructure Protection (2.1, 2.2, 5.6)

National mechanisms of critical infrastructure protection constitute another widely acknowledged measure of national and international cybersecurity. The OEWG noted the wide consensus on the need to protect all critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public. [40]

Like in the case of computer emergency response mechanisms, critical infrastructure protection enjoys support from regional cybersecurity instruments. The Organization of American States regards establishing national points of contact regarding natural disaster response, environmental security, transportation security, and critical infrastructure protection a confidence-enhancing measure.[41]The African Union requires State Parties to adopt such legislative and/or regulatory measures as they deem necessary to identify the sectors regarded as sensitive for their national security and well-being of the economy, as well as the information and communication technology systems designed to function in these sectors as elements of critical information infrastructure and… measures to improve vigilance, security and management.[42] SADC defines critical infrastructure as computer systems, devices, networks, computer programs, computer data, so vital to the country that the incapacity or destruction of or interference with such systems and assets would

[37] Ethics for Incident Response and Security Teams (EthicsfIRST), page 3

[38] Siemens Charter of Trust, page 3.

[39] The Council to Secure the Digital Economy International Anti-Botnet guide, page 28.

[40] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021), para 26

[41] Organization of American States List of Confidence and Security-Building Measures (CSBMS), Committee on Hemispheric Security, para 24

[42] African Union Convention on Cyber Security and Personal Data Protection, 25.4

have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.[43] The Commonwealth has recognised the integrity of the critical infrastructure the need to mitigate respective risks.[44] OSCE Participating States have agreed to develop crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure and to improve the security of national and transnational ICT-enabled critical infrastructure including their integrity at the regional and subregional levels.[45]

Further stakeholders, under the Paris Call for Trust and Security in Cyberspace, have stressed the need to prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure.[46] The Global Commission has noted that:

> Certain IT products and services are essential to the stability of cyberspace due to their use within the core technical infrastructure, such as in core name resolution or routing, because of their widespread facilitation of the user Internet experience, or their criticality to the functioning of critical infrastructures such as election systems or power generation. Those creating products and services must commit to a reasonable level of diligence in the designing, developing, and delivering of products and services that prioritizes security and in turn reduces the likelihood, frequency, exploitability and severity of vulnerabilities.[47]

The 2010 UN GGE report, noting that the growing use of ICTs in critical infrastructures creates new vulnerabilities and opportunities for disruption[48], called for further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure.[49] The next GGE, in the 2015 report, addressed the issue of critical infrastructure protection in length, agreeing that states 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.[50] This commitment was reiterated by the OEWG.[51] The 2015 report also pointed out that the most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a State. The experts considered the risk of harmful ICT attacks against critical infrastructure is both real and serious.[52]

The 2015 UN GGE also agreed that States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.[53]Furthermore, states should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory,

[43] Southern African Development Community (SADC) Model Law, page 1

[44] Commonwealth Cyber Declaration, preamble

[45] OSCE Confidence Building Measures (2016)

[46] The Paris Call, principle 1

[47] GCSC's Six Critical Norms

[48] UN GGE (2010), para 9

[49] UN GGE (2010), para 9, 18 i.

[50] UN GGE (2015), para 13 f; Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021), para 31

[51] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021), para 26

[52] UN GGE (2015), para 5.

[53] UN GGE (2015), para 13 g. This recommendation has been endorsed by the G7 (G7 declaration on responsible state behaviour in cyberspace, 7) and the OEWG.

taking into account due regard for sovereignty.[54] The Group guided states to strengthen measures to protect of all critical infrastructure from ICT threats, and increase exchanges on best practices with regard to critical infrastructure protection."[55]

To enhance trust and cooperation and reduce the risk of conflict, the GGE has also formulated critical infrastructure related confidence-building measures. States could exchange national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include repositories of national laws and policies for the protection of data and ICT-enabled infrastructure the development of bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure.[56]

The 2021 GGE report regards malicious ICT activity affecting critical information infrastructure, infrastructure providing essential services to the public, the technical infrastructure essential to the general availability or integrity of the Internet and health sector entities as "of specific concern."[57] Experts stressed that to implement their guidance, states need to determine which infrastructures or sectors they deem critical within their respective jurisdictions, in accordance with national priorities and methods of categorization of critical infrastructure.[58] Experts highlighted heightened awareness of the critical importance of protecting health care and medical infrastructure and facilities deriving from the COVID-19 pandemic experience. Other examples of critical infrastructure sectors that provide essential services to the public can include energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes. Critical infrastructure may also refer to those infrastructures that provide services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet.[59]

The Siemens Charter of Trust offers examples of how the private sector can be engaged in critical infrastructure protection. It suggests that companies and – if necessary – governments could establish mandatory independent third-party certifications for critical infrastructure as well as critical IoT solutions. Companies are also encouraged to share new insights, information on incidents and report incidents beyond today's practice which is focusing on critical infrastructure.[60]

The DNS Abuse Framework encourages states to think of the DNS as critical infrastructure:

> The Domain Name System (DNS) serves as a crucial but largely unheralded system underpinning the Internet's ability to connect its users and devices. The safe and secure operation of the DNS has provided a firm foundation for the growth of the Internet as a global public resource, but much like the Internet as a whole, it is not immune to abuse. For the good of the Internet and everything it enhances, the undersigned domain name registrars and registries aim to reinforce the safety and security of the DNS by highlighting shared practices toward disrupting abuse of the DNS (DNS Abuse).[61]

[54] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – Final Report (2015), 13 h.

[55] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021), para 26

[56] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – Final Report (2015), 13, 16

[57] UN GGE (2021), para 10

[58] UN GGE (2021), para 44-45

[59] UN GGE (2021), para 44-45

[60] Siemens Charter of Trust, para 7-8.

[61] DNS Abuse Framework, page 1

Acknowledged in nearly half of all the normative instruments analyzed, the need for national mechanisms for critical infrastructure protection is another basic premise of international cybersecurity. Broadly, the current normative guidance indicates general consensus on the issue between various stakeholders. More specific guidance on this critical infrastructure protection is available in numerous specialized instruments.[62]

1.9.4 Electoral Processes and relevant infrastructure (2.3, 5.9)

Electoral processes have been singled out as an area of concern when it comes to prioritizing and adequately directing information security and resilience measures.

The G7 has stressed the need to respond to foreign threats, both together and individually, in order to meet the challenges facing our democracies.[63] The UN GGE has acknowledged the issue in the 2021 report:

> Malicious ICT activities against CI and CII that undermine trust and confidence in political and electoral processes, public institutions, or that impact the general availability or integrity of the Internet, are a real and growing concern. Such infrastructure may be owned, managed or operated by the private sector, may be shared or networked with another State or operated across different States. As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability.[64]

The UN Experts have also listed electoral processes as an example of critical infrastructure sectors that provide essential services to the public.[65]

At the regional level, the issue has been directly addressed by the EU, who has stressed the need for further awareness-raising and sharing of experience, both at national and European levels, in relation to online disinformation campaigns and fake news on social media specifically aimed at undermining democratic processes and European values.[66]

Perhaps the clearest formulation of the aspired commitment comes from the Global Commission: State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.[67] The Paris Call for Trust and Security in Cyberspace, however, regards the commitment as one of additional resilience, rather than restraint, urging stakeholders to strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.[68]

Only addressed in the international cybersecurity more recently, the question of the protection of electoral processes remains an unresolved question in the context of international law. The G7 considers undermining of electoral processes a challenge to democracy and the rules-based international order and defiance of international norms.[69] Russia, however, may regard elections interference as being covered by international law of non-interference into the internal affairs

[62] For instance, A/RES/57/239 (2003)Creation of a global culture of cybersecurity, A/RES/5/199 (2004) Creation of a global culture of cybersecurity and the protection of critical information infrastructures, A/RES/64/211 (2010) Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

[63] G7 Charlevoix Commitment on Defending Democracy from Foreign Threats, art. 1.

[64] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021), para 18.

[65] Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, para 43

[66] Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, page 12.

[67] GCSC's Six Critical Norms, art 2

[68] The Paris Call for Trust and Security in Cyberspace, principle 3

[69] G7 Charlevoix Commitment on Defending Democracy from Foreign Threats, preface.

of other States, and of respect for the sovereignty of States, based on its proposed Convention on International Information Security.[70]

1.9.5 Public Trust (2.4)

Public trust is seen both as a premise and as a widely shared objective of international cybersecurity. Most normative instruments analyzed associate the notion of trust with the confidence that the population and various groups (users, consumers, data subjects) have towards ICTs and the information society. The OEWG notes that malicious ICT activities against CI and CII undermine trust and are also a real and growing concern.[71]

Curiously, the two leading instruments that include trust in their titles, The Paris Call for Trust and Security in Cyberspace and the Siemens Charter of Trust, do not operationalize the term in their substantive commitments, leading one to conclude that all measures included in the Paris Call and the Siemens Charter are perceived by their signatories as trust measures.

The UN GGE has addressed the question of trust primarily in the 2021 report's implementation guidance. According to the Experts, end-user trust in an ICT environment that is open, secure, stable, accessible and peaceful is increased by responsible reporting of ICT vulnerabilities.[72] Experts further conclude that harm to emergency response teams can undermine trust.[73] The GGE has also highlighted CBMs and the implementation of norms of responsible State behaviour as measures to foster trust and ensure greater clarity, predictability and stability in the use of ICTs by States.[74]

ASEAN and the United States have addressed the question of trust in their bilateral relations, committing to encouraging economic growth through policies that build trust in the digital economy.

Such policies could include frameworks that strengthen consumer protection, intellectual property rights and cybersecurity, and promote effective personal data protection across jurisdictions, as well as policies in areas such as education and technology competency.[75]

The Commonwealth notes that common standards and the strengthening of data protection and security frameworks help promote public trust in the internet, confidence for trade and commerce.[76] “The East African Community Task Force on Cyber Laws associates trust with consumer protection: rules in a cyberspace environment should facilitate eCommerce by engendering trust among consumers and thereby encouraging them to enter into online transactions.[77] The EU believes that trust can be achieved through a “duty of care” principle: reducing product/software vulnerabilities by applying a range of methods from design to testing and verification, including formal verification where applicable, long term maintenance, and the use of secure development lifecycle processes, as well as developing updates and patches to address previously undiscovered vulnerabilities and fast update and repair would increase consumers' trust in digital products.[78]

> When a cyber-attack takes place, a fast and effective response can mitigate its impact. This can also demonstrate that public authorities

[70] Convention on International Information Security, art 5

[71] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021), para 18

[72] UN GGE (2021), para 60.

[73] UN GGE (2021), para 65

[74] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021), para 41

[75] ASEAN-United States Leaders' Statement on Cybersecurity Cooperation, para 8.

[76] Commonwealth Cyber Declaration, sec 3.

[77] Draft Eac Legal Framework for Cyberlaws, page 16.

[78] Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, page 5.

> are not powerless in the face of cyber-attacks, and contribute to building trust.[79]

The Contract for the Web regards respect for people's privacy, protection of personal data, and other online data rights to build online trust.[80] The Freedom Online Coalition associates trust with the protection of online users and promoting trust-worthy technologies.[81] FOC also calls upon states to uphold human rights in order to build mutual trust between all stakeholders.[82]

More specialized instruments suggest the importance of trust in epistemic communities and provide examples of technical measures to increase and express trust:

> Registered ISPs that achieve the requirements set out in the code may also display a Trustmark to indicate their compliance with the code of practice on their website and in emails to their customers. The Trustmark could provide an online link to information about the code of practice to further increase consumer awareness of the provisions of the code.83

The DNS Abuse Framework centers on trust as it concludes that bettering the DNS means making it a more trusted space.[84]

The Draft Convention of International Information Security authored by the Russian Federation acknowledges that trust and security when using information and communication technologies is a fundamental basis of the information society.[85] It also notes that national strategies for the management of digital security risk should foster trust and confidence in the digital environment.[86] The SCO's Agreement on cooperation in the field of ensuring the international information security tabled jointly by Russia, China and a number of CIS countries, regards "developing and implementing joint measures of trust conducive to ensuring international information security" as one of key areas of international cooperation.[87]

Appearing in about a third of normative instruments analyzed, the notion of trust is valued by diverse communities and a wide number of stakeholders. However, the concept remains too vague for consensus at this point and its relationship with international cybersecurity is still to be clarified.

1.9.6 Computer emergency response mechanisms (2.5 and 5.7)

Ensuring the establishment of computer incident response capability is a widely acknowledged essential step towards cybersecurity. The OEWG recognized the existence of, and support to, Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) as an example of "concrete, action-oriented" capacity-building.[88] The UN GGE has consistently emphasized the role of first responders in confidence-building as mechanisms for increasing transparency and cooperation.[89] The 2015 UN GGE report

[79] Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

[80] Contract for the Web, principle 5.

[81] FOC Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies, para 4

[82] FOC Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies, para 17

[83] APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice, page 5.

[84] DNS Abuse Framework, pg 5

[85] Convention on International Information Security, preamble.

[86] Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document, sec 2A.

[87] Shanghai Cooperation Organization's Agreement on cooperation in the field of ensuring the international information security, art 3 (areas od coop=

[88] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021), para 61.

[89] UN GGE (2013), para 26 d

guides states to establish a national computer emergency response team and/or cybersecurity incident response team or to officially designate an organization to fulfil this role. Experts further note that states should support and facilitate the functioning of and cooperation among such national response teams and other authorized bodies.[90] The OEWG agrees, stating that the prior existence as well as the building of national Computer Emergency Response Teams (CERTs), is essential to ensuring that CBMs serve their intended purpose.[91]

The OSCE Participating States have committed to providing contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts.[92]

Acknowledgment of the central role of CERTs and CSIRTs in cybersecurity can also be found in several regional agreements. The Commonwealth Cyber Declaration underscores the importance of national cybersecurity strategic planning and establishing incident response capabilities, supported by appropriate legislation.[93] The African Union calls member states to establish appropriate institutions to ensure monitoring and a response to incidents and alerts, national and cross-border coordination of cyber security problems, as well as global cooperation.[94] OECD has called for ensuring the establishment of one or more Computer Security Incident Response Team (CSIRT), also known as Computer Emergency Response Team (CERT), at national level.[95] APEC also concludes that Computer Emergency Response Teams (CERTs) are essential stakeholders in managing cyber security.[96]

Experts and states have also emphasized the potential of involving established first response mechanisms in international cybersecurity cooperation. The EU has stressed the essence of Computer security incident response teams in creating situational awareness.[97] OECD also encourages cross-border cooperation between CERTs and CSIRTs.[98] The 2015 UN GGE report encouraged states to expand and support practices in computer emergency response team and cybersecurity incident response team cooperation. Examples of such cooperation could include information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organizing exercises, supporting the handling of ICT-related incidents and enhancing regional and sector-based cooperation.[99] Keeping in mind that such additional functions may expose CERTs and CSIRTs to additional political risk, the UN GGE experts have also committed to protect the independence and functionality of first response:

> States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or

[90] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – Final Report (2015), para 17 c

[91] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021), para 46.

[92] OSCE Confidence Building Measures (2013 and 2016), 2013: 8

[93] Commonwealth Cyber Declaration, sec. 2.

[94] African Union Convention on Cyber Security and Personal Data Protection, Art. 27 (2).

[95] Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document, 2 B.1.

[96] APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice, page 3.

[97] Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2.21

[98] Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document, 2 B.1.

[99] UN GGE (2015), para 17 d

> cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.[100]

The 2021 UN GGE report explains that this commitment reflects that CERTs/CSIRTs or other authorized response bodies have unique responsibilities and functions in managing and resolving ICT incidents, and thereby play an important role in contributing to the maintenance of international peace and security. They are essential to effectively detecting and mitigating the immediate and long-term negative effects of ICT incidents. Harm to emergency response teams can undermine trust and hinder their ability to carry out their functions and can have wider, often unforeseen consequences across sectors and potentially for international peace and security.[101] Experts call states to abstain from politicizing CERTs/CSIRTs and respecting the independent character of their functions.[102] The Freedom Online Coalition underscores that responses to cyber incidents should not violate human rights.[103]

The GGE has further suggested that states may wish to consider CERTs and CSIRTs within their definition of critical infrastructure.[104] More specialized guidance on the functioning of and expectations towards computer emergency response mechanisms can be found in the guidelines issued by FIRST and CSDE.[105]

Although the establishment of and support to computer emergency response mechanisms is only addressed in less than a third of analyzed normative instruments, these measures enjoy strong consensus among stakeholders and constitute one of the basic premises of international cybersecurity.

1.9.7 Cyber hygiene (2.7)

Cyber hygiene has emerged as a theme of normative guidance in several multilateral instruments. The European Union has stressed that people need to develop cyber hygiene habits and businesses and organizations must adopt appropriate risk-based cybersecurity programs and update them regularly to reflect the evolving risk landscape.[106] NATO has seen the need to enhance skills and awareness, among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences.[107] The Commonwealth has encouraged investment in cybersecurity and cyber hygiene skills, and to develop skills in the workforce, particularly for women and girls, and public awareness to help the public adopt secure online behaviours and protect themselves from cybercrime."[108]

The African Union suggests that as part of the promotion of the culture of cyber security, states may develop programmes and initiatives for sensitization on security for systems and network users; encourage the development of a cyber-security culture in enterprises and launch a comprehensive and detailed national sensitization programme for Internet users, small business, schools and children.[109]

[100] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – Final Report (2015), para 13 k.

[101] Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, para 65.

[102] Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, para 65.

[103] The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security, para 6.

[104] UN GGE (2015), para 17 d

[105] Ethics for Incident Response and Security Teams (EthicsfIRST), The Council to Secure the Digital Economy International Anti-Botnet guide.

[106] Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, page 11, para 2.7

[107] The NATO Cyber Defence Pledge, sec 5.V.

[108] Commonwealth Cyber Declaration, sec. 4.

[109] African Union Convention on Cyber Security and Personal Data Protection, Art. 26 (1).

APEC addresses the need to educate consumers:

> ISPs who have agreed to comply with a cyber security code should be encouraged to raise the cyber security awareness of their customers. ISPs are best placed to distribute this information as they have a direct relationship with their customers and are in regular contact through network updates and billing.110

The Freedom Online Coalition is explicit about states encouraging private sector actors to promote and practice good cyber hygiene.[111] Stakeholders should promote education, digital literacy, and technical and legal training as a means for improving cybersecurity and the realization of human rights.[112] The Global Commission invites states to enact laws and regulations to ensure basic cyber hygiene.[113] The Paris Call for Trust and Security in Cyberspace concurs, recommending efforts to strengthen an advanced cyber hygiene for all actors.[114]

1.9.8 Supply chain security, reporting of vulnerabilities and harmful hidden functions (3.1, 3.2 and 5.10)

The UN GGE first addressed the issue of vulnerability reporting, supply chain security and harmful hidden functions in their 2015 report. Experts stated that States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.[115] They called states to 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.[116] Voluntary sharing of national views and information on vulnerabilities and identified harmful hidden functions in ICT products was also seen as practice for enhancing confidence between states.[117] Experts also noted that states should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders.[118]

The OEWG confirmed the importance of the issue and relevance of the UN GGE guidance:

> States, reaffirming General Assembly resolution 70/237 and acknowledging General Assembly resolution 73/27, should: take reasonable steps to ensure the integrity of the supply chain, including through the development of objective cooperative measures, so that end users can have confidence in the security of ICT products; seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions; and encourage the responsible reporting of vulnerabilities.119

The 2021 GGE report provided the

[110] APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice, page 5.

[111] FOC Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies, page 6, para 24.

[112] The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security, para 11.

[113] GCSC's Six Critical Norms, Art. 7.

[114] The Paris Call for Trust and Security in Cyberspace, principle 7.

[115] UN GGE (2015), 13 (i).

[116] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – Final Report (2015); para 13 (j).

[117] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – Final Report (2015); para 16 (c).

[118] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – Final Report (2015); para 16 (d).

[119] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021), para 28.

following implementation guidance:

> Norm 13 (i) recognizes the need to promote end user confidence and trust in an ICT environment that is open, secure, stable, accessible and peaceful. Ensuring the integrity of the ICT supply chain and the security of ICT products, and preventing the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions are increasingly critical in that regard, as well as to international security, and digital and broader economic development.120
>
> Norm 13 (j) reminds States of the importance of ensuring that ICT vulnerabilities are addressed quickly in order to reduce the possibility of exploitation by malicious actors. Timely discovery and responsible disclosure and reporting of ICT vulnerabilities can prevent harmful or threatening practices, increase trust and confidence, and reduce related threats to international security and stability.121
>
> To prevent the development and proliferation of malicious ICT tools and techniques and the use of harmful hidden functions, including backdoors, States were encouraged to introduce, at the national level, measures that prohibit the introduction of harmful hidden functions and the exploitation of vulnerabilities in ICT products that may compromise the confidentiality, integrity and availability of systems and networks, including in critical infrastructure.122

The G7 concurs that 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.[123]

Several regional instruments have offered guidance on this issue as well. The AU Convention on Cyber Security and Personal Data Protection requires member states to take the necessary legislative and/or regulatory measures to make it a criminal offence to unlawfully produce, sell, import, possess, disseminate, offer, cede or make available computer equipment, program, or any device or data designed or specially adapted to commit offences, or unlawfully generate or produce a password, an access code, or similar computerized data allowing access to part or all of a computer system."[124] The Commonwealth Cyber Declaration commits states to exploring options to deepen cooperation on cybersecurity incidents and responses between Commonwealth member countries, including through the sharing of information about threats, breaches, vulnerabilities, and mitigation measures.[125] OECD regards encouraging the responsible discovery, reporting and/or correction of digital security vulnerabilities by all stakeholders an essential aspect of digital security risk management.[126] The East African Community Task Force on Cyber Laws has guided states to criminalize misuse of devices, including the supply or possession of tools such as password cracking or virus writing software. [127]

More specialized guidance is provided in the APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice :

[120] UN GGE (2021), pära 56.

[121] Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (2021), page 11, para 56.

[122] Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (2021), page 11, para 58.

[123] G7 declaration on responsible state behaviour in cyberspace, norm 9.

[124] African Union Convention on Cyber Security and Personal Data Protection, art. 29.

[125] Commonwealth Cyber Declaration, sec. 1.

[126] Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document, Sec. 2.B.3

[127] East African Community Task Force on Cyber Laws, page 14, sec 2.3.1.

> When a compromised connection exists on an ISP's network, it is of benefit to the ISP to provide assistance to affected users and therefore restore the integrity of its networks. For a cyber security code of practice to function efficiently, ISPs need to be sufficiently engaged in managing their networks, notifying affected users and assisting in their recovery.128

Vulnerability disclosure is also considered ethical in the work of first response and in botnet mitigation:

> Team members who learn of a vulnerability should follow coordinated vulnerability disclosure by cooperating with stakeholders to remediate the security vulnerability and minimize harm associated with disclosure. Stakeholders include but are not limited to the vulnerability reporter, affected vendor(s), coordinators, defenders, and downstream customers, partners and users.129
>
> Providers should create a security vulnerability policy and process to identify, mitigate, and where appropriate disclose known security vulnerabilities in their products.130

Other stakeholders have advised that states should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.[131] While regarding it duty of all actors to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity, the Global Commission regards the responsibility for vulnerability disclosure as a divided task between governments, developers and producers:

> Developers and producers of products and services on which the stability of cyberspace depends should (1) prioritize security and stability, (2) take reasonable steps to ensure that their products or services are free from significant vulnerabilities, and (3) take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process.132

The Commission has offered a formulation, whereby state and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace. [133]

The Paris Call for Trust and Security in Cyberspace posits that stakeholders need to develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm[134] and to strengthen the security of digital processes, products and services, throughout their lifecycle and supply chains.[135] The Freedom Online Coalition acknowledges that the risks that some technologies and practices pose to the enjoyment of human rights can be exacerbated when governments seek to compel the suppliers of such technologies to cooperate with their security and intelligence agencies without any democratic or independent checks or balances on these authorities.[136]

Siemens Charter of Trust, in turn, emphasizes responsibility throughout the digital supply chain:

[128] APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice, page 8, sec. 1.

[129] Ethics for Incident Response and Security Teams (EthicsfIRST), page 2.

[130] The Council to Secure the Digital Economy International Anti-Botnet guide, page 28.

[131] GCSC's Six Critical Norms, para 39.

[132] GCSC's Six Critical Norms, para 39.

[133] GCSC's Six Critical Norms, Art. 3.

[134] The Paris Call for Trust and Security in Cyberspace, page 3, Principle 5.

[135] The Paris Call for Trust and Security in Cyberspace, principle 6.

[136] FOC Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies, page 4, para 12

> Companies and - if necessary - governments must establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity and availability by setting baseline standards, such as:
>
> - Identity and access management: Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them.
> - Encryption: Connected devices must ensure confidentiality for data storage and transmission purposes wherever appropriate.
> - Continuous protection: Companies must offer updates, upgrades and patches throughout a reasonable lifecycle for their products, systems and services via a secure update mechanism.137
> - Differences remain as to the depth of the states' implementation modalities in their commitment to engage in vulnerability disclosure. It is generally acknowledged that relevant responsibility is remains divided between governments and non-government stakeholder groups.

1.9.9 General Cooperation (4.1)

The 2015 UN GGE report includes a recommendation, whereby:

> (a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.138

The UN GGE 2021 report further suggests that States consider approaching cooperation in ICT security and capacity-building in a manner that is multidisciplinary, multistakeholder, modular and measurable.[139] The OEWG notes that ensuring an open, secure, stable, accessible and peaceful ICT environment requires effective cooperation among States to reduce risks to international peace and security.[140]

The G7 reiterates that consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.[141] The cooperation encouraged by the G7 is 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 G7 Rapid Response Mechanism is intended to strengthen coordination to identify and respond to diverse and evolving threats to our democracies, including through sharing information and analysis, and identifying opportunities for coordinated response.[142]

Under the African Union Convention, states are required to make use of existing means for international cooperation with a view to responding to cyber threats, improving cyber security and stimulating dialogue between stakeholders. These means may be international, intergovernmental or regional, or based on public-private partnerships.[143] APEC strongly encourages close collaboration with the private sector and with other international

[137] Siemens Charter of Trust, page 6, para 2.

[138] UN GGE (2015), para 13 (a).

[139] UN GGE (2021), para 92, page 18.

[140] OEWG (2021), para 55.

[141] G7 declaration on responsible state behaviour in cyberspace, norm 1.

[142] Charlevoix Commitment on Defending Democracy from Foreign Threats, Art. 2 and 3.

[143] African Union Convention on Cyber Security and Personal Data Protection, para 28 (4).

organizations.[144] Commonwealth countries commit to exploring options to deepen cooperation on cybersecurity incidents and responses between them, including through the sharing of information about threats, breaches, vulnerabilities, and mitigation measures.[145] The OECD calls on governments and public and private organizations to work together to empower individuals and small and medium enterprises to collaboratively manage digital security risk.[146] The EU states that implementing the measures under the Communication on Deterrence and Defence will provide a clear demonstration that the EU and the Member States will work together to put in place a standard of cybersecurity equal to the ever-growing challenges faced by Europe.[147] NATO countries have emphasized NATO's role in facilitating co-operation on cyber defense, including through multinational projects, education, training, exercises and information exchange, in support of national cyber defence efforts and have pledged to reinforce the interaction amongst respective national cyber defense stakeholders to deepen cooperation and the exchange of best practices.[148] The OAS expects to foster cooperation and exchange of best practices on cyber diplomacy, cybersecurity and cyberspace, through, for example, the establishment of working groups, other dialogue mechanisms, and the signing of agreements among states.[149] The OSCE Participating States will "voluntarily facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs".[150]

BRICS underscores the importance of establishing legal frameworks of cooperation among BRICS States on ensuring security in the use of ICTs, noting the proposal for a BRICS intergovernmental agreement on cooperation on ensuring security in the use of ICTs and on bilateral agreements among BRICS countries.[151]

Under the International Information Security Convention, states, to avoid conflict, are expected to ensure international information security to maintain world peace and security and to contribute to global economic stability and progress, general welfare of the peoples of the world and discrimination-free international cooperation.[152] The Shanghai Cooperation Organization identifies several major areas of cooperation:

1) defining, coordinating and implementing necessary joint measures in the field of ensuring international information security;

2) creating of a system of joint monitoring and response to emerging threats in this area;

3) elaborating joint measures for the development of the provisions of the international law limiting the spread and use of information weapons threatening defense capacity, national security and public safety;

4) countering threats related to the use of information and communication technologies for terrorist purposes;

5) combating cybercrime;

6) conducting expertise, research and evaluation in the field of information security t;

[144] APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice, section 5.4, page 14.

[145] Commonwealth Cyber Declaration, Sec. 1.

[146] Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document, page 7.

[147] Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, sec 5, page 20.

[148] The NATO Cyber Defence Pledge, 5. IV.

[149] Organization of American States List of Confidence and Security-Building Measures (CSBMS), Committee on Hemispheric Security, para 31.

[150] OSCE Confidence Building Measures (2013)

[151] XII BRICS Summit Moscow Declaration, para 40.

[152] Convention on International Information Security, chapter 2.

7) promoting secure, stable operation and governance internationalization of the global Internet network;

8) ensuring information security of the critically significant structures;

9) developing and implementing joint measures of trust conducive to ensuring international information security;

10) developing and implementing coherent policies and organizational and technical procedures for the implementation of digital signature and data protection in the cross-border exchange of information;

11) exchanging information on the legislation of the Parties on issues of information security;

12) improving the international legal framework and practical mechanisms of cooperation of the Parties in ensuring international information security;

13) creating conditions for cooperation between the competent authorities of the Parties;

14) interacting within international organizations and fora on issues of international information security;

15) exchanging experience, training of specialists, holding working meetings, conferences, seminars and other forums of authorized representatives and experts of the Parties in the field of information security;

16) exchanging information on issues related to the cooperation.[153]

The Freedom Online Coalition emphasizes the need for cooperation in the context of regulation:

> Cybersecurity-related laws, policies, and practices at national, regional and international levels should be developed through open, inclusive, and transparent approaches that involve all stakeholders.154

General cooperation is one of the most frequently mentioned themes in the analyzed normative instruments. However, its scope and focus remains difficult to establish.

1.9.10 Law enforcement assistance (4.2)

In the UN GGE 2015 report, experts called states to consider additional confidence-building measures that would strengthen cooperation on a bilateral, subregional, regional and multilateral basis. These could include voluntary agreements by States to cooperate, in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.[155] Norm 13 (d) guided states to consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats.[156]

The 2021 UN GGE report noted that observance of this norm implies the existence of national policies, legislation, structures and mechanisms that facilitate cooperation across borders on technical, law enforcement, legal and diplomatic matters relevant to addressing criminal and terrorist use of ICTs."[157]The G7

[153] Shanghai Cooperation Organization's Agreement on cooperation in the field of ensuring the international information security, Art. 3.

[154] The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security, Recommendation 10.

[155] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – Final Report (2015), para 17 (e).

[156] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – Final Report (2015), para 13 (d).

[157] Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, page 7, para 32.

has reiterated the UN GGE 2015 report's recommendation in para 13 (d).[158]

Law enforcement cooperation and assistance has been prioritized in numerous other multilateral and regional instruments. According to the African Union, states that do not have agreements on mutual legal assistance in cyber-crime shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal liability.[159] The EAC Task Force recommends the adoption of common criminal procedures within the EAC.[160] The Arab Convention on Combating IT Offences has provided a set of offences for instances where no cooperation and mutual assistance treaty or convention exists between the State Parties requesting assistance and those from which assistance is requested.[161]

The ASEAN Regional Forum has called for measures to promote cooperation among ARF Participating Countries against criminal and terrorist use of ICTs including, inter alia, cooperation between law enforcement agencies and legal practitioners, possible joint task force between countries, crime prevention and information sharing on possible regional cooperation mechanism.[162] The Commonwealth has highlighted the importance of national cybersecurity strategic planning, supported by appropriate legislation and a law enforcement and criminal justice system capable of addressing cybercrime. Under this declaration, states have committed to the establishment and use of national contact points and other practical measures to enable cross-border access to digital evidence through mutually agreed channels to improve international cooperation to tackle cybercrime.[163]

Similarly, the OAS requires states to identify a national point of contact at the policy level able to discuss the implications of hemispheric cyber threats. The work of these national points of contact may be distinct from, yet supplement the ongoing work of law enforcement and other technical experts in combating cybercrime and responding to cyber incidents of concern."[164] OSCE adds that states should have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to counter terrorist or criminal use of ICTs.[165]

The Russian Convention on International Information Security requires states to take legislative or other steps which may be necessary to empower the law enforcement authorities of the State to collect or record information by means of technology in its territory as well as to demand similar action from service providers carried out continuously and in cooperation with the law enforcement authorities of the States.[166] The European Union notes that Europol has become a key actor in supporting Member States' multijurisdictional investigations and should become a centre of expertise for Member States' law enforcement on online investigations and cyber forensics.[167]

[158] G7 declaration on responsible state behaviour in cyberspace, norm 4.

[159] African Union Convention on Cyber Security and Personal Data Protection, art. 28.2.

[160] Draft EAC Legal Framework for Cyberlaws, 16 (Sec 2.3.2)

[161] Arab Convention on Combating Information Technology Offences, art. 34.

[162] ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies (ICTs), Sec.2 (viii)

[163] Commonwealth Cyber Declaration, sec 1.

[164] Organization of American States List of Confidence and Security-Building Measures (CSBMS), Committee on Hemispheric Security, para 27.

[165] OSCE Confidence Building Measures (2013 and 2016)

[166] Convention on International Information Security, chapter 4.

[167] Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, page 13, sec. 3.1.

According to the Southern African Development Community (SADC) Model Law:

> If a [law enforcement] [police] officer that is undertaking a search based on Sec. 25 (1) has grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, he shall be able to expeditiously extend the search or similar accessing to the other system.
>
> Any person, who is not a suspect of a crime or otherwise excluded from an obligation to follow such order, but who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein that is the subject of a search under section 26 must permit, and assist if reasonably required and requested by the person authorized to make the search...168

BRICS have expressed concern over the rising level and complexity of criminal misuse of ICTs as well as the absence of a multilateral framework to counter the use of ICTs for criminal purposes, yet recommends considering the need to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes under the auspices of the UN and note the establishment of an openended ad hoc intergovernmental committee of experts under the auspices of the UN in accordance with UNGA Resolution 74/247 of 27 December 2019.[169]

Expert communities regard cooperation with law enforcement as baseline practice in countering botnets:

> Providers should maintain an easy-to-find list of points of contact for law enforcement and security researchers. Providers should also have a well-defined policy describing how they can and cannot support law enforcement efforts. Advanced Capabilities: Generally, industry leaders will have more procedures and technologies with which to support law enforcement. They will also have defined policies and legal positions on specific law enforcement tactics. They may conduct global risk assessment to account for global legal requirements. In addition to cooperating with law enforcement, providers may have processes for collaborating with competitors during exceptional events.170

The Freedom Online Coalition flags the considerations of human rights in the context of law enforcement cooperation:

> While State authorities are responsible for protecting the human rights of those in their territory and law enforcement should be enabled to assist victims of harmful cyber activities, the FOC is deeply concerned about the practices by some States of asserting excessive control over the Internet under the pretence of ensuring national security while disregarding international human rights law and the principles of an open, free, secure, interoperable and reliable Internet. In particular, the FOC is alarmed at the growing number of restrictions placed on the exercise of the right to freedom of opinion and expression online, including where States have manipulated or suppressed online expression in violation of international law, including through discriminatory or politically motivated Internet censorship or Internet shutdowns, unlawful or arbitrary monitoring, and the arrest and intimidation of online activists for exercising their human rights.171

Almost half of all the instruments analyzed made reference to the necessity of effective law enforcement cooperation and offered

[168] Southern African Development Community (SADC) Model Law, page 15.

[169] XII BRICS Summit Moscow Declaration, para 41.

[170] The Council to Secure the Digital Economy International Anti-Botnet guide, page 22.

[171] FOC Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies, page 4, para. 11

advice and guidance on the matter. However, some stakeholders still hold the view that the existing frameworks and regimes are insufficient and that further international agreement needs to be built on the issue.

1.9.11 Due Diligence (4.4)

The voluntary and non-binding commitment to due diligence, regarded as a legally binding obligation by some states, was first expressed in the UN 2015 report. The experts guided states to not knowingly allow their territory to be used for internationally wrongful acts using ICTs.[172] The G7 has endorsed this commitment.[173]

The 2021 UN GGE report explains that the norm on due diligence:

> …reflects an expectation that if a State is aware of or is notified in good faith that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory it will take all appropriate and reasonably available and feasible steps to detect, investigate and address the situation. It conveys an understanding that a State should not permit another State or non-State actor to use ICTs within its territory to commit internationally wrongful acts.174

At the regional level, due diligence has been addressed by the EU: on a bilateral level, cyber dialogues will be further developed and complemented by efforts to facilitate cooperation with third countries to reinforce principles of due diligence and state responsibility in cyberspace.[175]

While due diligence has been addressed between states as a term of art in international law, it has been emphasized also in ither contexts. In Ethics for Incident Response and Security Teams, it has been suggested that:

> Teams should operate on the basis of verifiable facts. When sharing information, such as indicators of compromise (IOCs) or incident descriptions, Team members should provide evidence and scope transparently. If this is not possible, the reasons for not sharing this evidence and scope should be given with the information.176

The FOC has noted the challenges posed to business and government alike by the scarcity of domestic laws, international best practice, and private sector awareness of human rights abuses linked to the export of items with surveillance capabilities and tools to support efforts to conduct human rights due diligence to mitigate the risk of potential adverse human rights impacts.[177]

1.9.12 Intellectual Property Protection (5.2)

The relationship between international cybersecurity and intellectual property protection, while acknowledged, has not been thoroughly examined. Both the G20 and G7 have noted 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.[178]

Noting this commitment, ASEAN-US Leaders have pledged to encourage economic growth through policies that build trust and confidence in the digital economy, such as but not limited to

[172] UN GGE (2015), para 13 (c).

[173] G7 declaration on responsible state behaviour in cyberspace

[174] Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, para 29, page 6.

[175] Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, para 4.1, page 18.

[176] Ethics for Incident Response and Security Teams (EthicsfIRST), page 4.

[177] FOC Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies, para 12, page 4.

[178] G20 Leaders Communique, para 26., G7 declaration on responsible state behaviour in cyberspace, norm 12.

frameworks that strengthen consumer protection, intellectual property rights and cybersecurity, and promote effective personal data protection across jurisdictions, as well as policies in areas such as education and technology competency.[179]

Russia and China have also put emphasis on the need for intellectual property protection, associating it with the implementation of national legislation. According to the Convention on International Information Security, each State Party will, within the limits of its means, ensure that intellectual property laws, including patents, technologies, commercial secrets, brands, and copyrights, are adhered to in its information space.[180] The SCO agreement regards violating legal rights and freedoms of citizens in the field of information, including intellectual property rights and privacy as acts that need to be criminalized.[181]

Technical communities have also drawn attention to the need to acknowledge the rights of users. In the context of first response, it has been advised that:

> Team members should be aware that their actions may impact human rights of others, by sharing information, possible bias in their actions, or by infringing property rights. Team members have access to a wide range of personal, sensitive and confidential information in the course of handling incidents. This information should be handled in a way to uphold human rights.182

In the context of the fight against botnets, enterprises of all sizes have been encouraged to take their own proactive steps to mitigate ecosystem risk through, for example, implementing appropriate identity and access management techniques and discontinuing the use of legacy and pirated products and software that do not receive updates, among other things. Steps like these can help enterprises protect sensitive data and intellectual property on their networks, in addition to helping to protect the ecosystem at large by reducing the attack surface for DDoS and other distributed attacks.[183]

Multistakeholder processes have also stressed the need to prevent ICT-enabled theft of intellectual property, anchoring it in the above-mentioned G20 and G7 statements.[184] While not a primary theme in international cyber norms discussion, intellectual property protection remains a consideration for states and enterprises alike. In the context of economic espionage, states have made commitments to not conduct or support ICT-enabled theft of intellectual property, while the industry has taken note of the intersection between network security practices and intellectual property rights.

1.9.13 Network Security practices (6.1)

International cyber policy instruments also contain references to network security practices, either by pointing out some of the good practices or explaining the relationship between policy guidance and network security.

The G7 Charlevoix Commitment on Defending Democracy from Foreign Threats calls states to engage directly with internet service providers and social media platforms regarding malicious misuse of information technology by foreign actors, with a particular focus on improving transparency regarding the use and seeking to prevent the illegal use of personal data and breaches of privacy."[185]

[179] ASEAN-United States Leaders' Statement on Cybersecurity Cooperation

[180] Convention on International Information Security, art. 5

[181] Shanghai Cooperation Organization's Agreement on cooperation in the field of ensuring the international information security, Annex 1.

[182] Ethics for Incident Response and Security Teams (EthicsfIRST), page 3.

[183] The Council to Secure the Digital Economy International Anti-Botnet guide, page 33.

[184] The Paris Call for Trust and Security in Cyberspace, page 3, principle 4.

[185] Charlevoix Commitment on Defending Democracy from Foreign Threats, art 5,

The Commonwealth Cyber Declaration, underscoring shared interest in protecting the security of networks, security of data, the people that use them, and the services that run on them invites to limit the circumstances in which communication networks may be intentionally disrupted, consistent with applicable international and domestic law.[186]

ITU-T WTSA Resolution on Cybersecurity emphasizes the need to raise awareness, within ITU-T mandate and competencies, of the need to harden and defend information and telecommunication systems from cyberthreats and cyberattacks, and continue to promote cooperation among appropriate international and regional organizations in order to enhance exchange of technical information in the field of information and telecommunication network security.[187]

In the context of routing security, network operators are encouraged to implement a system that enables source address validation for their own infrastructure and end users, and for any Single-Homed Stub Customer Networks. This should include anti-spoofing filtering to prevent packets with an incorrect source IP address from entering or leaving the network.[188]

Siemens prioritizes the sense of ownership of cyber and IT security. The responsibility for cybersecurity should be anchored at the highest governmental and business levels by designating specific ministries and CISOs. Cybersecurity is everyone’s task, therefore presuming clear measures and targets as well as the right mindset throughout organizations. Siemens supports security by default, advising enterprises to adopt the highest appropriate level of security and data protection and ensure that it’s preconfigured into the design of products, functionalities, processes, technologies, operations, architectures and business models. Without user-centricity, cybersecurity would fail: companies should serve as a trusted partner throughout a reasonable lifecycle, providing products, systems and services as well as guidance based on the customer’s cybersecurity needs, impacts and risks.[189]

The Freedom Online Coalition sees a gap between international policy community and the private sector practices: States should encourage private sector actors to adhere to the UN Guiding Principles on Business and Human Rights, to improve their accountability and to share best practices in this respect and help to share lessons learned.[190] FOC states that cybersecurity policies and practices should be rights-respecting by design.[191]

Clear connections between policy-level guidance and practical cybersecurity are still to be made. Only some 20% of the reviewed instruments addressed practical cybersecurity, most of these instruments drafted by and within technical communities or corporate stakeholders. Bridging the gap between policies and practices would help determining the roles of the private sector in international cybersecurity, and perhaps also provide feasibility assessments to policy-level guidance.

[186] Commonwealth Cyber Declaration

[187] ITU-T WTSA Resolution 50 - Cybersecurity, page 4, para 3.

[188] Mutually Agreed Norms for Routing Security, page 5.

[189] Siemens Charter of Trust, page 6, paras 1, 3 and 4.

[190] FOC Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies, page 6, para 22.

[191] The Freedom Online Coalition’s Recommendations for Human Rights Based Approaches to Cyber security, sec 1.

2. Workstream 2 - Testing norms concepts against cybersecurity events

How would specific norms have been effective at mitigating adverse cybersecurity events? The following is a discussion paper that interrogates which are the core ideas behind prominent cybersecurity normative agreements that had the most continuity through various incidents. 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, by writing background briefs for historical cybersecurity events, the authors' review, evaluation and analysis take into consideration the Best Practice Forum on Cybersecurity's prior reports, as well as other published research and reports, to conclude whether and how cyber norms have been successful at mitigating the adverse effects of these events. In some cases we conclude that important cybersecurity events may have supported norms implementation, or expanded the scope of an existing norm.

Editor: Mallory Knodel <mknodel@cdt.org>

Authors: Anastasiya Kazakova, Niamh Healy, Allison Wylde, Barbara Marchiori de Assis, Fred Hansen, Evan Summers, Louise Marie Hurel, Ying Chu Chen, Mallory Knodel, Apratim Vidyarthi

BPF consultant: Wim Degezelle

2.1 Introduction

The Best Practice Forum on Cybersecurity of the Internet Governance Forum has set out to test cybersecurity norms concepts against significant historical internet events in order to answer the central question: How would specific norms have been effective at mitigating adverse cybersecurity events?

In a discussion paper, expert contributors bring forward past analyses from the BPF Cybersecurity that connect the core ideas behind cybersecurity normative agreements, and present details of the actual risks, told through the voices of those most affected, to cybersecurity and human rights from incidents around the world of data leaks, vulnerability disclosures, malware and others.

First we identified criteria to select major historical cybersecurity events (including adverse events such as incidents) that are representative of cybersecurity issues, and that in some cases may have informed cyber norms development. Second we analysed a subset of those significant events, especially those that were or might have been impacted by or influenced the creation of global cybersecurity norms. Lastly we conducted qualitative research to include the voices of those affected by cybersecurity events through expert contributor-led interviews with incident responders and victims of historical cybersecurity events to determine first-hand perception of the research question, "how would specific norms have been effective at mitigating adverse cybersecurity events?"

Building on the past work of the BPF Cybersecurity, a group of expert contributors sought to answer our central research question through desk research and analysis of nine significant cybersecurity events.

For four of those events, researchers additionally identified both victims of the attacks and those who helped mitigate them, and interviewed them for an additional deep dive into the research question through qualitative methods. In describing the events, and in four cases those most affected by the events, researchers analysed through summative evaluation of present-day proposed norms that would have had influence or impact, and identify any proposed cyber norms that have resulted from the incidents. Our findings, where possible, are supported through qualitative interviews with those most affected.

The nine chosen cyber incidents had the minimum elements of: coverage by secondary sources (media, academia) and at least three primary sources; demonstrable harm at scale (number affected, impacted community); successful mitigation (was it attributed? fixed?); relationship to cybernorms. We ensured that our analysis was complete by mapping events that were distributed over time; from a variety of stakeholder groups; demonstrating the gamut of incident types, and with geography diversity.

For interviews, we ensured baseline consistency in interrogating our research question with the following loose script:

- Describe the incident and your role.
- What do cyber norms mean to you?
- What cyber norms do you think apply in this case?
- What cyber norms do you think have been, or would have been, helpful in this case?
- What cyber norms did you, or might you hope to, see arising from this case?

2.2 Analysing cybersecurity events

The table on the following page captures and highlights the main qualities of each of the events that our group of expert contributors analysed against mitigations that included or impacted cybersecurity norms.

For each of these events we present the basic narrative of who, what, where, when and why supported with secondary source citations. What happened after the incident, or its mitigation, is then analysed to present how it was responded to and if cybersecurity norms played a role or were influenced as a result of the event. Lastly we present known information about the victims of the attack and their direct views on how norms did or could have shaped the incident and its outcomes.

For events marked with a * researchers conducted qualitative analysis to understand directly from those most affected by the incident their views on the relationship to mitigating the incident and cyber norms.

2.2.1 CIH virus (1999)

CIH malware, also known as Chernobyl or Spacefiller, is a very dangerous malware which targeted Microsoft Windows and specifically infected Windows 95, 98 and ME[192]. The name for the malware came from the alleged author, Chen Ing-hau. The malware is also sometimes referred to as Spacefiller, highlighting its ability to take up file space on computers and prevent anti-virus software from running. It is believed to be the first malware known to have the power to damage computer hardware. First detected as early as 1998, some sources state that its payload was triggered in April 16, 1999 which was the 13th anniversary of the disaster at the Chernobyl nuclear reactor[193].

Chen claimed to have written the malware as a challenge against bold claims of antivirus software developers about their products' efficiency. So he created the original virus to challenge those products. The spread of the malware began locally, and then spread globally quickly. The CIH-infected file is executed on a system and the virus becomes resident, infecting every executable accessed within empty, unused spaces in the file. Next, it breaks itself up into smaller pieces and inserts its code into these unused spaces. The virus only works on Windows 9X and ME OS. It cannot work on Windows NT or later Windows versions. Because the virus broke the BIOS, many producers made hardware modifications to prevent the damage.

It should also be noted that a virus seldom causes hardware failure, but the CIH virus disrupted the work of any infected system by deleting the data in the Flash BIOS[194], thus making it impossible to even boot the computer and in most cases the cost of the repair exceeded the cost of a new laptop (the drive, video card and other hardware are also affected as a consequence), resulting in damaged computers being simply thrown away.

[192] https://www.f-secure.com/v-descs/cih.shtml

[193] http://virus.wikidot.com/cih

[194] https://encyclopedia.kaspersky.com/knowledge/damage-caused-by-malware/

Date	Type	Countries	Event	Target	Attribution
Apr 2007	DDoS	Estonia	Estonian DDoS attacks	Estonia	Public policy protest
Mar 2009	APT	Tibet	Ghostnet*	Tibetan institutions	Undetermined. Attack servers predominantly based in China
Jun 2010	APT, malware, Control systems breach	Iran	Stuxnet	Iran's nuclear program	Israel
Jun 2013	Technique disclosure	Global	Snowden disclosures	Global mass surveillance	US, Canada, UK, Australia, New Zealand
Apr 2014	Vulnerability	Global	Heartbleed*	None	None
Jan 2018	APT	Mexico, Canada, Saudi Arabia, Palestine, Bahrain, Kazakhstan, Morocco, UAE	NSO Group's Pegasus*	Human rights defenders, journalists	Governments using NSO Group commercial software
Jan 2018	Breach	India	Aadhar data breach	Indian citizens	[Sale of data]
Dec 2020	Supply chain	US/ global	Solarwinds*	Compromise of government agencies and private companies (18,000+) followed by targeted espionage	APT29 / Organised cyber criminals

What Cyber Norms Could Have Been Helpful?

> Secure software development and trustworthy computing: In 2002 following the incident, the CEO of Microsoft Bill Gates sent[195] the internal memo informing the colleagues about this nascent normative framework[196] perhaps in part because the CIH virus has been among the most devastating malware targeting Windows machines, but its spread has increased the industry's awareness of a necessity to invest more into secure software development and trustworthy computing practices.

2.2.2 Estonian DDoS attacks (2007)

In April of 2007, there were a series of cyberattacks which targeted websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters. The series of cyberattacks lasted almost for 22 days[197]. The internet services from the government

[195] https://www.wired.com/2002/01/bill-gates-trustworthy-computing/

[196] https://docs.microsoft.com/en-us/previous-versions/ms995349(v=msdn.10)?redirectedfrom=MSDN

[197] https://stratcomcoe.org/cuploads/

nearly collapsed, at a time when Estonia depended fully on internet connectivity to deliver critical government services. The email services, online banking, web-based government services have been largely hit, impacting many citizens in Estonia (a population of about 1.3 million people).

In the chain of those attacks, there were in particular three DDoS attacks and a few more complex attempts to hack into systems, for example using SQL injection. Some of these attacks were successful at non-critical sites[198]. At the same time it was reported that the 2007 attacks did not damage much[199] of the Estonian IT infrastructure because they were not sophisticated, and also because the limited size of the country allowed it to quickly respond to incidents and mitigate the impact for national networks. However, these attacks were a wake-up call for the country and other NATO members, highlighting a new attack vector and vulnerability.

The Estonia government thought the attacks were from Russia because of political issues at that time. But the Russian government denied the accusation. As a member of NATO, Estonia requested emergency assistance, however, the lack of timely response revealed that NATO did not have a 'coherent cyber doctrine and a comprehensive cyber strategy'[200].

What Cyber Norms Could Have Been Helpful?

- Requesting for assistance: the norm H in the 2015 UN GGE report[201] which says that 'states should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts.'
- The majority of norms, including on the protection of critical infrastructure, which emerged together with the 2015 UN GGE report could have been helpful at the event of these cyberattacks. Their possible existence in 2007 could have already greatly systematized possible options which Estonia as a victim state might have to defend itself as well as how it could have cooperated better with its allies for investigation, remediation and attribution.
- Together with these norms, greater clarity on the application of international law to cyberspace could have also served Estonia as a victim state with a better understanding on how to qualify and react to these cyberattacks. Some countries, including Estonia, have since pushed for such clarity.

What Cyber Norms Have Arisen As a Result?

- The direct result of the cyberattacks was the launch by NATO of internal assessment of its cybersecurity and infrastructure defenses, and further greater awareness and work on a coherent cybersecurity strategy within NATO. The internal assessment led to the report issued to the allied defense ministers in October 2017 and helped to create an intergovernmental cyber defense policy as well as the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia.[202]
- The Tallinn Manual,[203] as a consequence after these attacks, has become an influential resource for legal advisers and policy experts dealing with cyber issues. This report outlined international laws which are considered applicable to the cyber realm. The manual provided a total of ninety-five rules addressing cyber conflicts and most likely informed the work of governmental experts at the UN which later in 2013 and 2015 agreed on the set of eleven non-binding cyber norms.

pfiles/cyber_attacks_estonia.pdf

[198] https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[199] https://www.files.ethz.ch/isn/143191/rp_76.pdf

[200] R. Hughes, NATO and Cyberdefence, Mission Accomplished?, April 2009, No 1/4.

[201] https://undocs.org/A/70/174

[202] https://ccdcoe.org

[203] https://ccdcoe.org/research/tallinn-manual/

2.2.3 GhostNet (2009)

GhostNet was a large-scale cyber espionage campaign discovered in March 2009, following a ten-month investigation by the Information Warfare Monitor (IWM).[204] In this campaign, attackers used social engineering to distribute malware to targeted machines. The investigation of the attack began at the request of the Office of His Holiness the Dalai Lama, and Tibetan government and civil society organisations were extensively affected. The investigation by the IWM however revealed a much larger network of high-value, compromised computers, consisting of 1,295 computers in 103 countries.[205] Particularly notable about this attack was the public documentation of the campaign through the published report by IWM and the method of attack that used highly personalised social engineering to infect the campaign's targets.

This case study was completed using analysis of publicly available written documents, including newspaper reporting and technical publications about the campaign, and interviews with individuals directly involved in responding to the campaign: Dr Shishir Nagaraja and Lobsang Gyatso Sither.

There had been historical allegations of cyber attacks against the Tibetan community in the years prior to the discovery of GhostNet.[206] Investigation of GhostNet by IWM began following a specific request by the Office of His Holiness the Dalai Lama (OHHDL).[207] The IWM team consisted of researchers from the SecDev Group, a think-tank based in Ottawa, Canada, and the Munk Centre for International Studies, University of Toronto.[208] An initial investigation by the research team discovered malware on computers within the OHHDL, other Tibetan government institutions, and Tibetan non-governmental organisations (NGOs).[209] Through an analysis of this malware, the researchers identified servers associated with the attack and mapped out a wider network of control servers and compromised computers. The attack was investigated in 2008 and 2009, with the report by IWM published in March 2009.

The malware was spread through a phishing attack where victims of the attack were targeted through fraudulent emails containing either a malicious link or file attachment.[210] The link or file would then direct infected computers to connect to a control server and await further instructions, while the user would be left unaware of the infection.[211] The attack was particularly innovative in how it was spread: specifically targeting the psychology and sociology of affected users.[212] For example, some malicious emails used content stolen from previously-infected computers to imitate legitimate communications when targeting new users to enhance the apparent legitimacy of the communication.[213]

Infected computers were directed to download gh0st RAT or similar Trojan malware, which allowed the attackers to take full control of infected computers, search for and download files, and open attached devices such as microphones and webcams.[214]

[204] http://news.bbc.co.uk/1/hi/world/americas/7970471.stm; https://www.nytimes.com/2009/03/29/technology/29spy.html; https://www.theguardian.com/world/2009/mar/30/china-dalai-lama-spying-computers

[205] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 5

[206] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 13

[207] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf

[208] http://news.bbc.co.uk/1/hi/world/americas/7970471.stm

[209] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf

[210] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 18

[211] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 18

[212] Author interview.

[213] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 18

[214] https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, p 18

The GhostNet campaign was one of the first publicly-reported targeted cyberattacks.[215] After the publication of the GhostNet report, more targeted cyberattacks began to be publicly reported and documented.

During the course of the investigation, the IWM researchers identified the command and control servers used in the attacks, which in turn revealed a much larger network of affected computers.[216] The IWM researchers identified over 1,295 affected computers in 103 countries, including networks belonging to foreign ministries and regional organizations like ASEAN and NATO. Interview participants observed that prior to the discovery of the attack, there was awareness of cyber-attacks and cybersecurity within the community.[217] However, there was no concrete knowledge of the extent of targeted attacks against certain groups or clear evidence of attacks.[218] The publication of the IWM report helped identify the extent of cybersecurity risks faced, how cyber-attacks were being carried out, and what the impact of cyber-attacks were, underscoring the importance of cybersecurity. [219] The discovery of GhostNet highlighted the significance of cybersecurity for organisations involved in advocacy and campaigns work, and for individuals. [220] Particularly notable about GhostNet was how widespread the attack was. Before the attack, there had been an assumption that attacks were limited, directed only towards The discovery of GhostNet disrupted this assumption and suggested that cybersecurity was a community-level concern.[221]

The discovery of the GhostNet campaign, led awareness raising and institutional capacity development on cybersecurity. A hyperlocal data-driven approach was adopted. Through work with partners like Citizen Lab, a monitoring on how threats evolved over time was conducted.[222] Cybersecurity training was adjusted as threats changed over time: for example, material initially focused on being careful with email attachments changed to focus on the risks associated with Google Drive links, in response to changing attacker behaviour.[223] In 2018, local Computer Emergency Readiness Team was founded.[224] Its key aim of the was to enable information-sharing using a shared Traffic Light Protocol (TLP).[225]

What Cyber Norms Could Have Been Helpful?

- Participants observed that norm J (report vulnerabilities and remedies) was well practiced in this case.[226] The Tibetan Central Administration's request for assistance from the IWM and their admittance of researchers into their facilities and networks permitted a thorough and publicly documented investigation of the GhostNet campaign.

- While the eleven norms agreed in the 2015 GGE report are directed at states, future international efforts to develop norms of responsible behaviour in cyberspace might consider what norms are applicable to non-state actors such as non-governmental organisations like the Central Tibetan Administration and the Tibetan civil society organisations affected by the campaign.

- As this attack was not conclusively attributed, norm C (states should not knowingly allow their territory to be used for intentionally wrongful acts using ICTs) of the 2015 UN GGE report may have been of relevance and utility.

- Some interview participants understood the targets affected by the campaign as

[215] Author interview.

[216] Author interview.

[217] Author interview.

[218] Author interview.

[219] Author interview.

[220] Author interview.

[221] Author interview.

[222] Author interview.

[223] Author interview.

[224] Author interview.

[225] Author interview.

[226] 2015 UN GGE report https://undocs.org/A/70/174; author interview.

critical infrastructure, which means norms F and G of the 2015 UN GGE report may be considered relevant to this campaign. Norm F indicates that states should not conduct or knowingly support activity that intentionally damages critical infrastructure while norm G indicates that states should take appropriate measures to protect their critical infrastructure from ICT threats. Future efforts to develop and operationalise norms should offer greater clarity and specification on what constitutes critical infrastructure.

- In this case, non-state actors played a significant response role in investigating, documenting and responding to this campaign. As discussed in the section on the Heartbleed bug, norms to promote the neutrality of the technical community, incident responders and vulnerability analysts can help ensure effective and timely incident response and vulnerability mitigation.
- Some participants thought the norms would be of limited use in mitigating the campaign's effects on non-governmental organisations. Future efforts might contemplate whether states have special responsibilities to assist non-governmental organisations in cybersecurity-related matters or have particular responsibility to avoid adversely affecting the security of non-governmental organisations.

What Cyber Norms Have Arisen As a Result?

- The level of public reporting of the GhostNet campaign was uncommon at the time of the discovery of the campaign. Since the publication of the GhostNet report, thorough and *public* documentation of cyber espionage campaigns and other significant cybersecurity incidents is much more commonplace.

2.2.4 Stuxnet (2010)

A control systems breach was discovered at the Natanz Nuclear Complex in Natanz, Iran. Different from other malware that hijacked computers or stole information from them, the Stuxnet worm caused the destruction of the physical equipment controlled by infected industrial control systems. Specifically, the attackers designed a malware that could manipulate the Siemens's WinCC/PCS 7 Supervisory Control and Data Acquisition (SCADA) control software responsible for monitoring and controlling the centrifuges' speed. Siemens' WinCC/PCS 7 was the SCADA model used in the Natanz Nuclear Complex, in Iran, the target of the Stuxnet attack. Although most infections of the malware were found in Iran, the Stuxnet worm spread around the globe.

Highly complex, the Stuxnet worm combined several components, such as "zero-day exploits [unknown vulnerabilities], a Windows rootkit, the first ever PLC rootkit [programmable logic controller], antivirus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command-and-control interface."[227] Interestingly, the worm only allowed each infected computer to infect up to three other devices and was designed to self-destruct. Simply put, Stuxnet was designed to reach a specific target.[228]

Given that the computers were not directly connected to the Internet, it was not possible to launch the attack remotely; therefore, the attack was designed to be launched through USB flash drives. To reach Natanz Nuclear Complex, the attackers targeted five other organizations in Iran that would help get them to their final target, making these five organizations the attack's "patient zero." Four of these organizations have been identified.[229] These four organizations

[227] Falliere, N.; Murchu, L.O.; & Chien, E. (February 2011). "W32. Stuxnet Dossier." Symantec, p. 1-2. https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

[228] Singer, P. W. (2015). Stuxnet and its hidden lessons on the ethics of cyberweapons. Case W. Res. J. Int'l L., 47, 79.

[229] The companies identified were Foolad Technic, Behpajooh, Neda Industrial Group, and CGJ, believed to be Control Gostar Jahed. Zetter, K. (March 2014). "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." In Wired. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

were contractors of the Natanz nuclear power plant, providing a gateway through which contractors' devices infected with Stuxnet could reach the attackers' final target.

The worm was probably damaging the centrifuges at the Natanz plant, in Iran, for about a year when discovered in July 2010. The attacks against the five Iranian organizations took place in June and July 2009, and later in March, April, and May 2010.[230] Notably, one year before, the nuclear power plants had already been attacked by an early version of the malware, which manipulated the valves on the centrifuges to increase the pressure inside them. Such an increase in pressure damaged not only the equipment but also the uranium enrichment process. The Stuxnet attack was unleashed as the nuclear power plant was recovering from the effects of this previous attack.

Although no country has taken responsibility for the Stuxnet attack, it is widely acknowledged that the attack was the result of a collaboration between the United States and Israel through the so-called "Operation Olympic Games."[231] Started during the Bush Administration, the "Operation Olympic Games" aimed to slow down the Iranian Nuclear Program to buy time for sanctions and diplomacy with Iran to take effect.

It has been presumed that the cyber-attack goal was to sabotage Natanz nuclear facility by reprogramming the PLCs to operate according to the attackers' instructions. Ultimately, the goal was to hamper Iran's nuclear bomb-making program. Although the attack targeted the Natanz nuclear facility, the Stuxnet worm spread around the world and infected other industrial control systems indiscriminately.

Stuxnet was considered the world's first digital weapon and raised the concern of the destructive impact of cyber weapons.[232]

What Cyber Norms Could Have Been Helpful?

- The global consequences of the Stuxnet attack brought cyber warfare and digital weapons discussions into the forefront. While the impact of previous attacks was limited to the digital realm, the Stuxnet worm caused physical damage and could be considered an "armed attack" by international law standards.[233] Despite avoiding the expansion of the Iranian nuclear program,[234] Stuxnet was neither in response to an armed attack nor self-defense, potentially violating the prohibition on the use of force set forth in Article 2(4) of the UN Charter.

- Although the 2013 Tallinn Manual's International Group of Experts were divided on whether the Stuxnet attack reached the "armed attack" threshold, all members agreed that a cyber-attack alone could potentially cross such a threshold.[235] Tallinn Manual 2.0 International Group of Experts were also divided on whether the Stuxnet attack reached the armed attack threshold, but all agreed

[230] Zetter, K. (November 2011). "Report: Stuxnet Hit 5 Gateway Targets on Its Way to Iranian Plant." In Wired. https://www.wired.com/2011/02/stuxnet-five-main-target/

[231] Sanger, D. E. (June 2012). "Obama Order Speed Up Wave of Cyberattacks against Iran." In The New York Times. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[232] Lucas, G. R. (2014). Permissible preventive cyberwar: Restricting cyber conflict to justified military targets. In The Ethics of Information Warfare (pp. 73-83). Springer, Cham; Singer, P. W. (2015). Stuxnet and its hidden lessons on the ethics of cyberweapons. Case W. Res. J. Int'l L., 47, 79; Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. Broadway books.

[233] United Nations Institute for Disarmament Research – UNIDIR (2013). The Cyber Index: International Security Trends and Realities, p. xi. https://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf;

[234] In 2010, the International Atomic Energy Agency (IAEA) reports suggested problems with Iran's nuclear efforts, albeit being denied by Iranian authorities. https://www.nytimes.com/2010/11/24/world/middleeast/24nuke.html?_r=0

[235] Schmitt, M. N. (Ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press, p. 58, 83-84.

that the attack consisted of a use of force.[236] For the Group of Experts, whether the Stuxnet attack could be considered an international armed conflict remained unclear due to the challenges of attributing it to a State.[237] Some called the Stuxnet attack a "Pyrrhic victory;" that is, although the attack delayed the Iranian Nuclear Program, Stuxnet also revealed a blueprint for cyberweapons and opened the path for cyber armed attacks against countries' infrastructure.[238] Determining the threshold of "armed attack" for cyber operations is quite challenging.[239] For instance, the Heads of State and Government of NATO Allies have reaffirmed that the invocation of the Collective Defense in case of a cyber-attack against one Ally, set forth in Article 5 of the NATO Treaty, "would be taken by the North Atlantic Council on a case-by-case basis."[240]

- Given that Stuxnet was launched miles away from its target, and even months before infecting its final target, it is possible to consider Stuxnet "the first truly autonomous weapon."[241] Plus, despite acknowledging the participation of Israel and US in the attack, Stuxnet traced back to servers in Denmark and Malaysia, highlighting the challenge of determining the origin of the attack and attribution.[242] Aside from Stuxnet automated nature, the worm also engendered important ethical discussions regarding proportionality and discrimination in warfare. Although the Stuxnet attack caused less damage than traditional weapons, it also enabled a preemptive attack that impacted not only its target but also other industrial control systems around the world.[243] In other words, while the attack seemed to be in consonance with the proportionality principle in terms of the physical impact caused, it violated the discrimination principle by infecting other computers beyond the SCADA systems of Natanz nuclear power facilities.

- Despite infecting other computers, the Stuxnet attack had some elements that revealed the attackers concern to avoid its indiscriminate spread, particularly civilian incidental damage. As mentioned, the Stuxnet worm was designed to infect up to three computers and self-destruct afterwards. When formulating its Rule 54 about the need to choose the means or methods to prevent or at least mitigate civilian collateral damage in the case of a cyber-attack, the 2013 Tallinn Manual's International Group of Experts believed that the Stuxnet attack seemed to "have been planned with this Rule in mind" since it "seek out a specific type of industrial process-control systems."[244] Indeed, to lessen the collateral damage beyond the Natanz facilities and ensure its effectiveness against the Iran Nuclear Program, it is believed that Stuxnet was tested first in Israel to better understand how the worm would affect the industrial control systems.[245]

[236] Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, p. 342.

[237] Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, p. 384.

[238] Clayton, M. (September 2011). "From the man who discovered Stuxnet, dire warnings one year later." In CSMonitor. https://www.csmonitor.com/USA/2011/0922/From-the-man-who-discovered-Stuxnet-dire-warnings-one-year-later

[239] Schmitt, M. N., & Vihul, L. (2016). The nature of international law cyber norms. In Osula, A. M., & Rõigas, H. (Eds.). International cyber norms: Legal, policy & industry perspectives. NATO Cooperative Cyber Defence Centre of Excellence, p. 44.

[240] Brussels Summit Communiqué (June 14, 2021); Wales Summit Declaration (September 5, 2014)

[241] Singer, P. W. (2015). Stuxnet and its hidden lessons on the ethics of cyberweapons. Case W. Res. J. Int'l L., 47, 79, p. 83

[242] Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. Broadway books.

[243] Singer, P. W. (2015). Stuxnet and its hidden lessons on the ethics of cyberweapons. Case W. Res. J. Int'l L., 47, 79, p. 85.

[244] Schmitt, M. N. (Ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press, p. 168-170.

[245] Broad, W. J. et al (January 2011). "Israeli Test on

- Some authors have argued that post-incident forensic analysis could help determine whether an automated cyber-attack was indiscriminate in nature and whether the attack was in accordance with the legal principles of distinction and discrimination. In the case of the Stuxnet worm, studies revealed that: the attackers collected painstaking information about Natanz Nuclear Complex to ensure that the attack vector would access the specific networks and systems employed in the Natanz facility; despite spreading beyond its initial targets, Stuxnet did not damage other systems as it was designed to harm a system with the specific configurations identified at Natanz.[246]

What Cyber Norms Have Arisen As a Result?

- The 2015 and 2021 reports of the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (UN GGE) stressed the application of the UN Charter and other international law to the use of information and communications technologies (ICT) by States, urging them to refrain from using force against other States in consonance with such norms. The UN GGE also underscored the principles of proportionality and distinction, and that the international humanitarian law only applies in cases of armed conflict. Notably, the 2021 UN GGE report also pointed out "the need for further study on how and when these principles apply to the use of ICTs by States."[247]
- The impact of the Stuxnet attack pushed Iranian authorities to the negotiation table, and ultimately resulted in the "Joint Comprehensive Plan of Action," an agreement signed between Iran and the United States, France, Germany, the United Kingdom, Russia, and China in July 2015. Through the JCPOA, Iran started providing the International Atomic Energy Agency (IAEA) information related to nuclear activities in the country.[248]

2.2.5 Snowden disclosures (2013)

In June 2013 two Western media outlets -- the US's Washington Post[249] and the UK's Guardian[250]-- released reports of top secret documents that were leaked from the US federal government by intelligence contractor Edward Snowden inculpating the US, Canada, UK, Australia and New Zealand in operating a global surveillance network.

Now known as "the Snowden Disclosures", most major outlets across the five countries covered the disclosures in significant detail during 2013 and in the eight years afterwards, including The New York Times, the Canadian Broadcasting Corporation, the Australian Broadcasting Corporation, Der Spiegel, O globo, Le Monde, and L'espresso. Around 1.7 million US intelligence files,[251] 58,000 British

Worm Crucial in Iran Nuclear Delay." In The New York Times. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

[246] Kaminska, M., Broeders, D., & Cristiano, F. (2021, May). Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone. In Kaminska, M., Broeders D., and Cristiano, F.(2021)." Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone", 13th International Conference on Cyber Conflict:'Going Viral (pp. 59-72). https://ccdcoe.org/uploads/2021/05/CyCon_2021_Kaminska_Broeders_Cristiano.pdf

[247] UN GGE (2021). A/76/135 Report of the Group of Governmental

[248] https://www.armscontrol.org/factsheets/JCPOA-at-a-glance

[249] Barton Gellman, Aaron Blake & Greg Miller, Edward Snowden comes forward as a source of NSA leaks, Wash. Post. (June 9, 2013), https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html

[250] Glen Greenwald, Ewen MacAskill & Laura Poitras, Edward Snowden: the whistleblower behind the NSA surveillance revelations, The Guardian (June 11, 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance .

[251] Chris Strohm & Del Quentin Wilber, Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers, Bloomberg News (Jan. 9, 2014), http://www.bloomberg.com/news/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.html .

intelligence files,[252] and 20,000 Australian intelligence files[253] were shared with journalists. It is unclear whether all the files shared with journalists have been disclosed to the public.

The files and subsequent reporting showed the existence of a broad global surveillance network implemented through treaties that enabled intelligence sharing between the five countries and other partners, including Sweden, Germany, Denmark, France, the Netherlands, Italy, Norway, Spain, Switzerland, Singapore, and Israel. The disclosures laid out the mechanisms by which these intelligence agencies gathered information broadly and deeply, including through the NSA's ability to access phone calls and emails of foreigners and US citizens, through a program developed by the NSA to record a foreign country's telephone calls, and through the use of XKeyscore, a program, to penetrate internet traffic and monitor targets in Europe and Africa.[254] The revelations also showed that private sector companies like Verizon complied with the NSA's data collection,[255] while others like Microsoft, Google, Yahoo, and Facebook complied with requests for cooperation with the NSA and GCHQ to weaken commercial encryption.[256]

The Snowden revelations had significant impacts globally, and for Snowden himself. In the US, various groups filed suit against the NSA[257] and have voiced support for Edward Snowden.[258] The public in the affected countries categorically disapproved of US surveillance.[259] The revelations also prompted governmental reviews of surveillance systems across the accused countries,[260] including President Obama's creation of an intelligence and communications technology review.[261] Simultaneously, the U.S. government charged Snowden with espionage and revoked his passport,[262] and multiple lawmakers across the Executive[263] and Congress[264] have called for his prosecution.

[252] David Miranda row: Seized files 'endanger agents', BBC (Aug. 30, 2013), https://www.bbc.com/news/uk-23898580 .

[253] Cameron Stewart & Paul Maley, Edward Snowden stole up to 20,000 Aussie files, The Australian (Dec. 5, 2013), https://www.theaustralian.com.au/national-affairs/foreign-affairs/edward-snowden-stole-up-to-20000-aussie-files/news-story/5c082d0996d2435a412aa603fefa60ae .

[254] See generally Snowden Revelations, Lawfare (Oct. 30, 2021), https://www.lawfareblog.com/snowden-revelations .

[255] Glenn Greenwald, NSA collecting phone records of millions of Verizon customers daily, The Guardian (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order .

[256] See, e.g., Jeff Larson, Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security, ProPublica (Sept. 5, 2013), https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption .

[257] See, e.g., Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013); ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).

[258] See, e.g., US: Statement on Protection of Whistleblowers in Security Sector, Human Rights Watch (June 18, 2013), https://www.hrw.org/news/2013/06/18/us-statement-protection-whistleblowers-security-sector# .

[259] Global Opinions of U.S. Surveillance, Pew Research Center (July 14, 2014), https://www.pewresearch.org/global/interactives/global-opinions-of-u-s-surveillance/ .

[260] See, e.g., Nick Hopkins, Patrick Wintour, Rowena Mason & Matthew Taylor, Extent of spy agencies' surveillance to be investigated by parliamentary body, The Guardian (Oct. 17, 2013), https://www.theguardian.com/uk-news/2013/oct/17/uk-gchq-nsa-surveillance-inquiry-snowden .

[261] See, e.g., Ewen MacAskill, White House insists James Clapper will not lead NSA surveillance review, The Guardian (Aug. 13, 2013), https://www.theguardian.com/world/2013/aug/13/white-house-james-clapper-nsa-surveillance-review .

[262] Peter Finn & Sari Horwitz, U.S. charges Snowden with espionage, Wash. Post (June 21, 2013), https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html .

[263] Aaron Blake, Clapper: Leaks are 'literally gut-wrenching,' leaker being sought, Wash. Post (Aug. 8, 2013), https://www.washingtonpost.com/news/post-politics/wp/2013/06/09/clapper-leaks-are-literally-gut-wrenching-leaker-being-sought/ .

[264] Edward Snowden: Ex-CIA leaker drops out of sight, faces legal battle, Chicago Tribune (June 10, 2013), https://www.chicagotribune.com/news/ct-xpm-2013-06-10-chi-edward-snowden-nsa-leaks-20130610-story.html .

What Cyber Norms Apply?

- Deterrence: the Snowden revelations gave credibility to US cyberdefense and cyberwarfare capabilities, giving the US a stronger hand in bargaining with other states that engage in cyberattacks.[265]

What Cyber Norms Could Have Been Helpful?

- Enable journalists to coordinate with incident responders to prevent details about vulnerabilities in commonly-used software being shared with the public, since that information could be misused by malicious actors. Similarly, creating direct channels of communication to prevent the sharing or spread of software that could facilitate hacking or other types of cyberattacks.

- Cyber norms for reporters and whistleblowers alike on what kind of information could be shared without endangering at-risk populations under authoritarian regimes implicated in intelligence operations might have been helpful.

What Cyber Norms Have Arisen As a Result?

- While norms deliberations rarely cite the Snowden Disclosures in plain terms because of the political difficulties that would create if any U.S. government representative was part of the body, many trends in norms setting post-Snowden can be inferred:

  - Somewhat strengthened oversight on data sharing and the breadth of surveillance programs.

  - More scrutiny over private-public cooperation in surveillance. After the disclosures, President Obama moved to split the NSA and US Cyber Command under different leaders. The NSA continued its activities under Title 50, whereas the US Cyber Command had Title 10 authority to conduct offensive cyber operations against adversaries.

  - Storage of metadata is now in the hands of telecom companies, rather than with the NSA at Fort Meade. The NSA now needs to obtain a warrant to access specific files that are relevant to any investigation.

  - Stronger collaboration, including notice to allies, when US cyber operations encroach on allies' territories.

2.2.6 Heartbleed (2014) [266]

The Heartbleed Bug is a serious vulnerability in the widely used popular OpenSSL cryptographic software library which was inadvertently introduced in April 2014. It was created after Robin Seggelmann, a programmer based in Germany, submitted an update code at 11:59 pm on New Year's Eve 2011. His update enabled the TLS extension "Heartbeat," but an error in his update code led to major ramifications, accidentally creating the "Heartbleed" vulnerability, as reported by the Guardian in 2014.[267]

The vulnerability was independently discovered

[265] Henry Farrell, The political science of cybersecurity IV: how Edward Snowden helps U.S. deterrence, Wash. Post (Apr. 12, 2014), https://www.washingtonpost.com/news/monkey-cage/wp/2014/03/12/the-political-science-of-cybersecurity-iv-how-edward-snowden-helps-u-s-deterrence/ ; see also Matthew Waxman, Snowden Disclosures and Norms of Cyber-Attacks, Lawfare (Mar. 20, 2014), https://www.lawfareblog.com/snowden-disclosures-and-norms-cyber-attacks .

[266] Through interviews with Rauli Kaksonen, who worked at Codenomicon at the time of the discovery of the Heartbleed vulnerability and who is now a senior security specialist at the University of Oulu in Finland; Igor Kumagin, a cybersecurity expert at Kaspersky with more than 11 years of experience and work in Kaspersky Research and Development (RnD). Igor was the person responsible for vulnerability mitigation at Kaspersky and later building the company's vulnerability management and disclosure processes; Art Manion, a senior member of the Vulnerability Analysis team in the CERT Program at the Software Engineering Institute (SEI), Carnegie Mellon University. At the time of the discovery of the Heartbleed vulnerability, Art was a key expert coordinating the vulnerability notification from CERT/CC to its vendors and community.

[267] https://www.theguardian.com/technology/2014/apr/11/heartbleed-developer-error-regrets-oversight

by a team of security engineers at Codenomicon and a security researcher from Google Security, who first reported it to the OpenSSL team. Regarding its exploitation it is unknown if the vulnerability was abused in the wild. There are still discussions that, based on examinations of audit logs by researchers, it may have been exploited by attackers at least five months before discovery, announcement and mitigation. Later Codenomicon created the website heartbleed.com[268] to raise awareness about the vulnerability to both the wider public and those operating impacted websites and services.

The impact of the vulnerability was global and risks from exploitation were significant. Due to the popularity of OpenSSL many applications were impacted which enabled attacks that obtain a huge amount of sensitive data. It is not a design flaw in the SSL/TLS protocol specification, but an implementation problem, i.e. programming mistake in the popular OpenSSL library that provides SSL/TLS cryptographic resources to applications and services. This compromised the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content, as well as allowed attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users. This weakness allowed stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.[269]

Discussing the response to this vulnerability, it should be noted that immediately after the discovery of the bug, NCSC-FI took up the task of verifying it, analyzing it further and reaching out to the authors of OpenSSL, and to software, operating system and appliance vendors, which were potentially affected. Later, however, the vulnerability had been found by others and the mitigation was completed by several researchers. Particularly, Bodo Möller and Adam Langley of Google prepared the fix for Heartbleed, while the resulting patch was added to Red Hat's issue tracker on 21 March 2014. Stephen N. Henson applied the fix to OpenSSL's version control system on 7 April 2014, and the first fixed version, 1.0.1g, was released on the same day. The Heartbleed vulnerability was a classic example of a coordination failure: two organizations Codenomicon and Google, both discovered the vulnerability around the same time, but when the vulnerability was reported a second time to the OpenSSL team, they assumed a possible leak and the vulnerability was quickly disclosed publicly. "A more coordinated response may have allowed further remediation to be available immediately at disclosure time", said[270] Garret Wassermann, Vulnerability Analyst at CERT/CC.

What Cyber Norms Apply?

- Responsible reporting of vulnerabilities (Norm J of the UN 2015 GGE report[271]): the Heartbleed vulnerability triggered higher awareness of the industry and policy-makers of significant vulnerabilities and thus led to continuous improvement and development of vulnerability management and vulnerability disclosure best practices across public and private sectors.

What Cyber Norms Could Have Been Helpful?

- Norm on vulnerability exchange and coordination between states as well as non-state actors (including private sector, technical community, academia). We have heard from experts that still today not all technical experts can freely exchange vulnerability information with companies or CERTs located in not like-minded or allied countries, which create security and safety risks for all. Therefore, cyber norms promoting neutral status of technical community, incident responders, vulnerability analysts and researchers as well as CERTs are important to ensure the effective and timely incident response and vulnerability mitigation.

[268] https://heartbleed.com/

[269] https://us-cert.cisa.gov/ncas/alerts/TA14-098A

[270] https://insights.sei.cmu.edu/blog/cvd-series-principles-of-coordinated-vulnerability-disclosure-part-2-of-9/

[271] https://dig.watch/un-gge-report-2015-a70174

- Norm on greater transparency in vulnerability handling by both the public and private sector to shed light on vulnerabilities, once they are discovered. In the ideal case and ideal world, all vulnerabilities should be reported (as a next step after discovery) to code owners and vendors responsible for development of vulnerability mitigation. In a real world, if vulnerabilities are retained and kept private, the global community needs greater transparency into why, under which criteria such vulnerabilities could be retained and who has access to this information to ensure the security and confidentiality of actors involved in vulnerability handling. The Global Commission on the Stability of Cyberspace (CSCS) already suggested the norm[272] for States to create a vulnerabilities equities process, and this could be taken as a basis for promoting further the norm across both public and private actors.

What Cyber Norms Have Arisen As a Result?

- Industry and technical community has matured and advanced vulnerability management and coordinated vulnerability disclosure processes and guidelines (especially since the Heartbleed vulnerability has become a case of uncoordinated efforts taken by independent researchers). The Heartbleed vulnerability led to greater cross-industry collaboration on vulnerability analysis, management and disclosure, and for instance FIRST (Forum of Incident Response and Security Teams) called[273] in 2015 for members, security and IT vendor communities to join forces and participate in a new Special Interest Group (SIG) on Vulnerability Coordination which later produced the fundamental Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure (updated in May 2020)[274].

- Greater awareness of precarity of open source software (OSS) and the necessity to standardize secure software development given its widespread use even in proprietary software. The Heartbleed vulnerability highlighted the existing lack of security practices for OSS and, particularly, the incident led to the establishment of the Core Infrastructure Initiative (CII), a project of the Linux Foundation to support free and open-source software projects that are critical to the functioning of the Internet and other major systems. The CII funds specific tasks such as providing compensation to developers to work full-time on an open-source software project, conducting reviews and security audits, deploying test infrastructure, and facilitating travel and face-to-face meetings among developers. The CII has been replaced by the Open Source Security Foundation (OpenSSF)[275]. Thus the goal was to change failed 'software economics' where multiple developers create a highly complex code for open-source software which is not properly tested.

- Greater awareness across the industry to responsible vulnerability discovery and analysis. The Heartbleed vulnerability also led to the establishment of Google's Project Zero which is tasked with finding zero-day vulnerabilities to help secure the Web and society.

2.2.7 Aadhar data breach (2018)

In early 2018 the largest Indian personal identification database, Aadhar, was reported to be leaking information on every registered Indian citizen (around 1.2 billion citizens which is almost 89% of India's population in 2018), including names, bank details and sensitive personal data such as biometrics.[276]

[272] https://cyberstability.org/norms/#toggle-id-6

[273] https://www.first.org/newsroom/releases/20150325

[274] https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination.pdf

[275] https://openssf.org/

[276] https://www.google.com/url?q=https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/&sa=D&source=docs&ust=1637598921355000&usg=AOvVaw2rIGLXgGu-DErFYotbAyNO

The 'Aadhaar Card' collects citizens' fingerprints, retina scans, and face photos. That information is connected to the users' banking system. A journalist found that anyone can buy the Aadhaar card details from an anonymous group on WhatsApp at a very low price. The journalist bought the package and used the information to access the database for individual information easily. The data leak was first revealed after anonymous sellers over Whatsapp provided unrestricted access to the Aadhar database for nominal costs. As a result Indian citizens may face personal identity forgery or privacy exposure.

The Unique Identification Authority of India (UIDAI) refused the media report claiming there were no data leaks. They claimed there were no internal or external risks to the database, and the database is constitutional. There were also reports that this was not an actual leak, and attempted to make an arbitrary distinction that instead it was just a security mistake on the part of the government.

What Cyber Norms Apply?

- The necessity to ensure the protection of personal data, including sensitive personal data.

What Cyber Norms Have Arisen As a Result?

- In 2019 the Indian government also proposed the Personal Data Protection Bill to introduce a legal framework for protection of personal data of Indian citizens.

2.2.8 Solarwinds (2020)

The SolarWinds breach occurred as part of a routine update for its Orion IT software. As with other client software, Orion was designed to download updates. A custom-made backdoor program then enabled attackers to gain access to the SAML and add malicious payload.

The breach, named Sunburst, was installed during routine updates, initiating the compromise. The program was hidden in legitimate software to appear as though it was a telemetry sending program. The program did not execute immediately. It was designed to evade antivirus (AV) protection and sandboxes. It tried to identify what monitoring or management software was running or blocking.

Sunburst was designed to provide the attackers with information about the entity through sending encoded DNS requests to the C&C server. The initial attack targeted more than 18,000 users with the attackers carefully selecting 100 entities for a deeper second stage attack. This deeper exploitation involved installing additional malware and/ or persistence mechanisms that allowed the exfiltration of data. The sophistication and targeted nature of the attack suggests extensively resourced, likely state supported attackers. The threat actor modified an Orion platform plug-in called SolarWinds.Orion.Core.BusinessLayer.dll. The sophisticated attack changed specific code in memory to avoid detection in the build process.[277]

"The malware masquerades its network traffic as the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds activity. The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers."[278]At first there appeared to be no obvious connections to any previously observed tactics, techniques or procedures (TTP). The unknown attacker named UNC2452 or Dark Halo, appears to be a variant of the .NET module.

The actual time line was found to have started with secondary attacks in April 2020. The breach targeted confidential information belonging to multiple government agencies, organizations including the financial sector, universities

[277] https://www.msn.com/en-us/news/politics/solarwinds-update-server-could-be-accessed-in-2019-using-password-solarwinds123-report/ar-BB1bXgXC

[278] https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

and medical institutions, and cybersecurity companies. Victims included 425 of the US Fortune 500, the top ten US telecommunications companies, the top five US accounting firms, all branches of the US Military, the Pentagon, the State Department, as well as hundreds of universities and colleges worldwide. The second stage attack carefully extracted further targeted material. The sensitivity of the breach may mean that the full extent of this breach may never be publicly released and may be restricted to the international intelligence community.

Espionage and data theft are some of the motives behind the SolarWinds Hack, albeit the size and scope of the incident suggest that the threat acts might have had broader reasons, including the possibility of using the intelligence gathered to launch a cyber-attack. By injecting a hidden code into the SolarWinds' Orion software updates, the hackers could remotely access the networks and systems of SolarWinds' customers who downloaded the compromised software updates. This 'backdoor' gave the threat actors access to the systems of several thousand public and private organizations in the US and around the globe that use SolarWinds' products. Given that SolarWinds is widely employed by US federal government agencies and other key organizations worldwide, this incident appears to be an intelligence reconnaissance operation that offered threat actors a unique opportunity to spy on these organizations' systems and networks. For this reason, the SolarWinds attack is considered one of the most sophisticated cyber-attacks.

What Cyber Norms Apply?

- The most important norm violations are 1., the non interference of the public core of the internet and 8., offensive cyber operations by non-state actors.[279]

What Cyber Norms Could Have Been Helpful?

- Attribution. State level attribution followed rapidly. In January 2021, the US Biden administration attributed the hacking campaign to Russia's Foreign Intelligence Service (SVR). US Agencies, the FBI, CISA, ODNI, and the NSA characterized the SolarWinds incident as "an intelligence gathering effort" by "an Advanced Persistent Threat (APT) actor, likely Russian in origin"[280] The Washington Post attributed the attack to APT29(Cozy Bear).[281] After further investigation, the cybersecurity firm FireEye[282] also officially attributed the incident to Russian state affiliated actors. The full attribution came in April 2021, when the Biden Administration and the UK Government formally named Russia's Foreign Intelligence Service (SVR)– also known as APT29, Cozy Bear, and the Dukes – as the perpetrator of the SolarWinds cyber-attack[283]. Further investigation centered on the attackers' code Sunburst and its similarity to Casure, in its ability to calculate a unique victim ID. The nature of the signature was found to be connected to the APT29 and Zebra C campaigns, DLL and more recently as NOBELIUM.[284] Arguably, with numerous articles blaming cyber criminals, the initial attribution may not be quite so clear cut. Our interview with Kaspersky provided an important guide, suggesting that what is needed is a Geneva Convention for cyber security norms. In addition, as a supply chain attack, the breach's success was helped by its complexity.

- Financial sanctions. In the aftermath of the SolarWinds hack, the Biden Administration

[279] https://cyberstability.org/norms/#toggle-id-8

[280] https://www.justsecurity.org/75779/solarwinds-accountability-attribution-and-advancing-the-ball

[281] https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html

[282] How FireEye attributed the SolarWinds hacking campaign to Russian spies (cyberscoop.com)

[283] https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

[284] https://thestack.technology/microsoft-customer-support-hacked-nobelium-apt29-solarwinds/

signed the 'Executive Order Targeting the Harmful Foreign Activities of the Russian Government' in April 2021. The Executive Order aims to hold Russia accountable for the SolarWinds cyber-attack and signal that the US will impose costs on Russia if it keeps facilitating malicious activities in cyberspace against the US and its allies. As a result, the US Department of Treasury issued a directive prohibiting US financial institutions from purchasing bonds from Russia's Central Bank, National Wealth Fund, or the Ministry of Finance, and from lending funds to these institutions. Notably, the Executive Order also mentioned that the US Government might expand the sanctions on Russian sovereign debt as appropriate.

- Company and personnel sanctions. Additionally, the US Government would sanction six Russian technology companies that supported Russian SVR and 32 individuals involved in Russia's attempts to influence the 2020 US presidential election and other disinformation campaigns. Ten personnel from the Russian diplomatic mission in Washington, DC, were also expelled from the US. In retaliation, Russia asked 10 US diplomats to leave the country.

- Implementing training. Alongside the US Government's formal attribution of the SolarWinds hack to Russia, the US National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) jointly published a Cybersecurity Advisory. This document described tactics and techniques used by the Russian SVR to exploit five publicly known vulnerabilities to target US and allied networks. Moreover, the US will promote the so-called "framework of responsible state behaviour in cyberspace" by offering a course to equip policymakers worldwide with "policy and technical aspects of publicly attributing cyber incidents". This course's first edition will take place this year at the George C. Marshall Centre, in Germany.

- Implementing enhanced cybersecurity. The SolarWinds attack also prompted President Biden to sign the "Executive Order on Improving the Nation's Cybersecurity" on May 12, 2021. This order: eliminates obstacles for private sector organizations to share cyber incident information with the government, requires the Federal Government to set the example, and implement robust cybersecurity standards (e.g., zero-trust architecture, encryption, multi factor authentication, and cloud security); enhances software supply chain security; creates a Cybersecurity Safety Board with representatives from the public and private sectors; creates a playbook for the Federal Government to respond to cyber incidents; aims to improve detection of cyber threats on Federal Government networks, and improves Federal Government investigation capability by requiring IT service providers of federal departments and agencies to collect and maintain information from network and system logs to facilitate the investigation of cyber incidents.

- Implementing increased collaboration and policy at the level of nation states. At the international level, following the US announcements about Russia's involvement in the SolarWinds hack, the European Union and its Member States and the North Atlantic Treaty Organization (NATO) stood in solidarity with the US. The EU and its Member States reinforced the importance of international efforts to establish a Programme of Action to Advance Responsible State Behaviour in Cyberspace within the United Nations (through the UN Group of Governmental Experts and Open-Ended Working Group). NATO also affirmed that Russia's actions threatened Euro-Atlantic security and urged the country to cease its disrupting behaviour. This outcome of collaboration links closely with the immediate responses in implementing training and cyber security initiatives as above.

In conclusion, the effects of the Biden Administration's decision to formally attribute the SolarWinds attack to the Russian Government and impose sanctions will be closely watched. Yet, on balance sanctions may not be enough to discourage cyber criminal gangs from carrying out similar attacks in the future.

The US Government signalled that it could adopt more sanctions in the future. Commentators suggest that escalating tension between countries, particularly considering that cyber espionage is common among countries, including the US and its allies. In this context, the threshold of acceptable and unacceptable espionage practices in cyberspace is yet to be clarified. Many experts believe that the retaliations against the SolarWinds incidents was a proportionate response; both countries left the door open for dialogue. The first face-to-face summit between President Biden and President Putin took place in Geneva, Switzerland, in June 2021. Both countries showed interest in re-establishing US-Russian relationships and bringing ambassadors back to their posts in Moscow and Washington.

At the same time, rapid responses in policy development and implementation, including preventative training and improved cybersecurity together with increased collaboration among nation states and organizations point to a promising alternative avenue to punitive measures.

2.2.9 NSO Group’s Pegasus (2016 -)

Since 2016 nation-state attackers have depended upon a privately-developed spyware called Pegasus to infect and monitor the devices of journalists, human rights defenders, politicians, activists and a range of others.[285] Pegasus was developed by NSO Group, an Israeli based company that is perhaps the most well-known of many in the private surveillance tech/ spyware industry. Their success has led to a proliferation of sophisticated spyware and a “democratization” of access[286] - making such surveillance technology that was once available only to a few elite intelligence agencies now procurable by essentially any government with the desire to surveill.

While, according to NSO Group, Pegasus was built and sold as a tool for governments to help stop threats such as terrorism, and crime, including human trafficking,[287] it has been clear for some time that Pegasus has been used without respect for human rights and sold to non rights-respecting states. Reporting in the summer of 2021 by a consortium of investigative journalists revealed the scope of Pegasus’ sale to nation states and the wide-ranging use of the tool.[288] Pegasus was sold to nation states including the UAE, Mexico, Saudi Arabia, Bahrain, Morocco, Hungary, Togo, Rwanda, India, Azerbaijan, Kazakhstan, and presumably others, and has targeted hundreds of people.[289]

Pegasus is noteworthy not only because it is a privately developed spyware exported and sold to nation-states for conducting surveillance (often unlawfully), but also because of its technical sophistication. The spyware allows for “zero click” exploits, a term referring to attacks that need no action on the part of the victim to succeed.[290] According to a security researcher we interviewed, the “development in exploitation technology and the way (these technologies) are being weaponized does not allow for any ability to challenge them.” According to that same researcher, “while in the past you could still address (vulnerabilities) at least on an operational security level….that is no longer possible, especially with the advent

[285] https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/

[286] https://www.occrp.org/en/the-pegasus-project/where-nso-group-came-from-and-why-its-just-the-tip-of-the-iceberg

[287] https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments

[288] https://forbiddenstories.org/case/the-pegasus-project/

[289] https://docs.google.com/spreadsheets/d/1lUv-hoQWGZagZi-8DbX9bLiC_WUWpL-o3f7NRyZmA04/edit#gid=0

[290] https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/

of these so-called ‘zero click’ vulnerabilities where there is literally nothing visible and nothing you’ve done wrong.” As the researcher stated, “it’s a completely asymmetric power imbalance, one that until very recently wasn’t even conceived in people’s minds as possible, especially on the side of those being targeted.”[291]

What Cyber Norms Apply?

- Two key norms from the UN 2015 GGE report aimed at promoting an open, secure, stable, accessible and peaceful ICT environment most clearly apply to this case. Those norms include recognizing the promotion, protection and enjoyment of human rights on the Internet (Norm E[292]), encouraging the responsible reporting of ICT vulnerabilities and sharing associated information on available remedies (Norm J[293]). In addition, the Global Commission on the Stability of Cyberspace’s proposed norm against offensive cyber operations by non-state actors is quite relevant - particularly given the role of private entities such as NSO Group in the spyware industry. According to this norm, “non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.”[294]

While potentially relevant, it would appear that these norms have as of now done very little to limit the presence and impact of Pegasus in particular, and targeted surveillance technologies more generally. Such is certainly true of the regulatory space as well. As the former UN Special Rapporteur on Freedom of Opinion and Expression David Kaye has noted: “It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists. While human rights law provides definite restrictions on the use of surveillance tools, States conduct unlawful surveillance without fear of legal consequence. The human rights law framework is in place, but a framework to enforce limitations is not.”[295]

What Cyber Norms Could Have Been Helpful?

- Enhance the norms for states to respect human rights, and expand this norm to apply to the private sector. Even before the most recent, explosive revelations about Pegasus, it was clear to the now former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, that the private spyware industry was operating without much oversight or guidance, particularly when it came to human rights concerns. Kaye wrote in July 2019 that private surveillance companies had a responsibility “to respect freedom of expression, privacy and related human rights, and integrate human rights due diligence processes from the earliest stages of product development and throughout their operations.”[296] More recently, Kaye has called for “genuine implementation of the UN Guiding Principles (on Business and Human Rights) and Human rights policies baked into company practice.”[297] While expanding the norm on respecting human rights to the private sector could have been helpful, so too would an enhanced norm around respecting human rights for states. Ultimately, Pegasus was procured from the NSO group by states - some of whom participated in the 2015 UN GGE process that developed this norm. According to the former Special Rapporteur, “States that purchase or use surveillance technologies should ensure that domestic laws permit their use only in accordance with the human rights standards of legality, necessity and legitimacy of objectives, and establish oversight mechanisms.”[298]

[291] Author interview, October 26th, 2021.

[292] https://undocs.org/A/70/174

[293] https://undocs.org/A/70/174

[294] https://cyberstability.org/norms/#toggle-id-8

[295] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report: Surveillance and Human Rights, 28 May 2019, UN Doc. A/HRC/41/35, para. 46

[296] https://undocs.org/A/HRC/41/35

[297] https://www.youtube.com/watch?v=yrP9vEH63HA

[298] https://undocs.org/A/HRC/41/35

- Norms related to spyware exports and licensings. According to a security researcher who studied the impact of Pegasus, one of the most significant normative gaps relates to a lack of export and license controls. According to this researcher, prior efforts at license and export control[299] "have been a useful stepping stone, but evidently not sufficient to curb what has been a pretty wild industry".[300] In response to this issue, various actors have made concrete normative (and policy-based) recommendations. Civil society organizations have made strong calls for action in this space[301]. Former Special Rapporteur David Kaye has argued for normative enhancements, stating that "states that export or permit the export of surveillance technologies should ensure a transparent process that solicits public input, and exporting states should join the Wassenaar Arrangement, which should be updated to be consistent with human rights standards."[302] Kaye also argued in that same report that such states participating in Wassenaar should "develop a framework by which the licensing of any technology would be conditional upon a national human rights review and companies' compliance with the Guiding Principles on Business and Human Rights."[303]

- Expand and strengthen norms around vulnerability disclosure to the private sector. According to multiple security researchers and journalists interviewed, expanding Norm J of the UN 2015 GGE related to vulnerability disclosure to include technology companies such as device and operating system developers, if done responsibly and with proper considerations to the risks such disclosures can raise, could be very helpful.[304]

- Norm around investment in rapid mitigation. According to one security researcher, one area of focus should be "raising the costs of exploiting the vulnerabilities successfully and introducing mitigations wherever possible. That's where I'd like to see more concrete investment, and ownership and responsibility. [New mitigations] should not be sacrificed for economic or business reasons, which unfortunately tends to be the case in some situations. From a technical standpoint, (it's important) to push companies to embrace the latest available mitigations even if that's an economic cost that doesn't seem favorable to a large customer base, but is vital to a small user base that are nevertheless customers of theirs… facing sophisticated threats from the likes of governments and corporates."[305] Perhaps a sign that this type of investment is starting to grow, Apple - whose iOS devices were among those targeted by Pegasus spyware - recently announced a pledge of at least $10 million dollars to support cybersecurity researchers. As part of that same announcement, Ivan Krstić, head of Apple Security Engineering and Architecture, emphasized the company's commitment to "analyze new threats, rapidly patch vulnerabilities, and develop industry-leading new protections in our software and silicon."[306]

- Norm around legal accountability for companies for misuse of their products. A lack of legal accountability, according to the aforementioned security researcher, is another limiting factor: "If there would be legal accountability for misuse of their (spyware developers') products that would be a deterrent for uncontrolled proliferation of this sort of (technology)." Despite some examples of past legal action against spyware company executives[307], legal accountability has been far from a norm.

[299] https://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/

[300] Author interview, October 26th, 2021.

[301] https://www.hrw.org/news/2021/09/08/eu-robustly-implement-new-export-rules-surveillance-tech#

[302] https://undocs.org/A/HRC/41/35

[303] https://undocs.org/A/HRC/41/35

[304] Author interview, October 19th, 2021.

[305] Author interview, October 26th, 2021.

[306] https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

[307] https://www.technologyreview.com/2021/06/22/1026777/france-spyware-amesys-nexa-crimes-against-humanity-libya-egypt/

What Cyber Norms Have Arisen As a Result?

- A few concrete actions have taken place from both state and non-state actors in response to the significant Pegasus revelations since the recent revelations in the summer of 2021, as well as to the use of private spyware stretching back years prior. While perhaps too regulatory in nature or too specific to be called norms, these actions offer a glimpse into what normative responses might develop in the future in response to Pegasus and the broader private spyware industry:

    - The United States recently blacklisted NSO Group and, as a result, American companies are prohibited from selling technology to it or its subsidiaries.[308] Such a step is by far the strongest ever taken by one of the world's most impactful economic actors against a private spyware firm.

    - Private companies including Apple and WhatsApp filed lawsuits against NSO Group. Both lawsuits focus on NSO Group's misuse of the plaintiffs' platforms and resources, in some cases explicitly against terms of service, to cause a wide range of damages in violation of US law (given that both companies are based in the United States.)[309] In the case of Apple's lawsuit, they seek "redress for Defendants' multiple violations of federal and state law arising out of their egregious, deliberate, and concerted efforts in 2021 to target and attack Apple customers, Apple products and servers and Apple through dangerous malware and spyware."[310] It is important to note that Apple's lawsuit emphasizes that while NSO Group did not breach data contained on Apple's servers, the abuse of Apple services and servers to perpetrate attacks on Apple's users and data stored on users' devices still constitutes a breach of law.[311] According to Ivan Krstić, head of Apple Security Engineering and Architecture, Apple's decision to bring this lawsuit "will send a clear message: In a free society, it is unacceptable to weaponize powerful state-sponsored spyware against those who seek to make the world a better place."[312]

    - The Supreme Court of India ordered an inquiry into the Indian government's alleged use of Pegasus spyware against journalists and political opposition.[313] This is one of the first examples of potential domestic legal oversight and transparency related to the recent Pegasus revelations in a country that has been accused of using the spyware itself.

    - Private entities have adopted strategic divestment from states revealed to have used Pegasus spyware for human rights abuses, as was the case with Cambridge University halting a 400 million Euro deal with the UAE.[314]

- It is also important to note that even before 2021, the existence of the private spyware industry has drawn considerable attention and led to many recommendations for global norms and regulations related to the industry. Perhaps the most succinct are those listed in the afore referenced 2019 report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on Surveillance and

[308] https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html

[309] https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf

[310] https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf

[311] https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf

[312] https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

[313] https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware

[314] https://www.theguardian.com/education/2021/oct/14/cambridge-university-halts-400m-deal-with-uae-over-pegasus-spyware-claims

Human Rights.[315] While recommendations such as these are still being debated and are not yet widely recognized or adopted, the revelations of 2021 have given them new attention and focus on the global stage.

2.3 Conclusions

In many ways, the cyber norms we have today would have helped mitigate many of the notorious cyber events of the past. However each analysis uncovers a missing nuance from deeper stakeholder involvement to application of existing legal frameworks.

2.3.1 Our findings

- The shocking DDoS attacks against the nation state of Estonia in 2007 led to intergovernmental action in order to 1) clarify the application of existing international law to cyberspace in the Tallinn Manual as well as 2) provide a coherent cybersecurity strategy and intergovernmental cyber defense policy among NATO members.

- Similarly the use of NSO Group's Pegasus by nation states begs stronger application of existing international human rights law in addition to an expansion to include private sector responsibility.

- The GhostNet event of 2009 highlighted that cyber resilience should be a community-level concern that when addressed at the hyperlocal level, lends capacity to at-risk groups to shift into monitoring mode and can respond to the evolution of threats over time.

- The technical details of the Stuxnet worm mattered a great deal in debates about how to mitigate it and future "digital weapons". How it worked (without internet), what it did (hardware target), whether it was indiscriminate in its damage, as well as attribution questions all inform whether or not it fell in accordance with the legal principles of distinction and discrimination.

- Both the Snowden Disclosures and Heartbleed events highlight the need to ensure that the roles of journalist and whistleblower are directly considered in norm development to avoid inadvertent revelations of software vulnerabilities and to enable responsible oversight of intelligence operations.

- Heartbleed and the NSO Group's Pegasus events illustrate that cyber norms must promote a neutral status of and specific role for the technical community, incident responders, vulnerability analysts and independent security researchers as well as CERTs in identifying and mitigating cybersecurity events.

- NSO Group's Pegasus shows what can go right when the private sector, in this case Apple, takes action against the misuse of its hardware and software, demonstrating investment, and ownership and responsibility over its users, no matter how targeted or at-risk of attack.

- The SolarWinds breach resulted in increased levels of collaboration and the implementation of training and new cybersecurity initiatives by Governments and the UN; approaching what many stakeholders have formally and informally called for as an approximate "Geneva Convention for cyberspace."

- SolarWinds indicated additional outcomes on attribution and financial sanctions that may prove controversial and therefore require additional and thorough interrogation before fully fleshed adoption in norms packages.

- The Estonian DDoS attacks and the Aadhar data breach both targeted digital, nation state infrastructure designed to provide domestic social services, though they occurred 11 years apart. In the first case norms development at the intergovernmental level was sparked and systems redesigned. In the latter case only a domestic data protection policy appears to have been a direct result.

[315] https://undocs.org/A/HRC/41/35

2.3.2 Future work

There is certainly more qualitative research that could be done to understand better the barriers and benefits to focussing on normative frameworks for those closest to cybersecurity incidents, past and present, in order to better mitigate future events. It is clear from the differential in depth of analysis between the events with desk research only versus those for which qualitative interviews were also conducted: the voices of those most affected by cybersecurity events provide key nuance are not present in secondary source reports or tertiary source reporting.

Our distilled findings coalesce around two main themes. They point to a gap in understanding the roles of a wide variety of actors and stakeholders in mitigating cybersecurity incidents. And they show a persistent disclarity in the interplay of norms, policies, and laws.

To bridge this gap, we recommend future research work that is focussed on understanding the interplay of cybersecurity norms and cybercrime legislation, where they overlap, align or work in opposition, with an aim to introduce greater stakeholder participation in the creation, enforcement and response mitigation as outlined in cybersecurity norms.