IGF 2022

Best Practice Forum on Cybersecurity

Output document

January 2023

Acknowledgements

The *Best Practice Forum Cybersecurity (BPF)* is an open multistakeholder effort conducted as an intersessional activity of the *Internet Governance Forum (IGF)*. This report is the output of the IGF 2022 BPF on Cybersecurity and is a compilation of the work of Workstream 1 'Mapping and Analysis of International Cybersecurity Norms Agreements', Workstream 2 'Exploring Historic Cybersecurity Events', Workstream 3 'BPF Outreach and Engagement', and the ad hoc Workstream 'Mythbusting: Cybersecurity vs. Cybercrime'.

The BPF output is the product of the collaborative work of many, who participated in BPF virtual meetings (open to all), the BPF's session during the IGF 2022 in Addis Ababa, Ethiopia, or provided input on the mailing list or requests for feedback on draft outputs.

BPF Cybersecurity coordinating team

Ms Hariniombonana Andriamampionona, *MAG Co-facilitator*
Mr Markus Kummer, *BPF Co-facilitator*
Mr Maarten Van Horenbeeck, *BPF Lead expert*

Mr John Hering, *BPF Workstream I Lead*
Ms Mallory Knodel, *BPF Workstream II Lead*
Ms Sheetal Kumar, *BPF Workstream III Lead*
Mr Wim Degezelle, *BPF Consultant*

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

Table of Contents

Acknowledgements **2**

Table of Contents **3**

Executive Summary **5**

Workstream 1: Mapping International Cybersecurity Norms Agreements **8**

1. Introduction and list of agreements 8

2. Analysis of norms elements 11

Workstream 2: Exploring Historic Cybersecurity Events **18**

1. Introduction - the IGF Best Practice Forum Cybersecurity 18

2. Introduction to Workstream 2 - Exploring historic cybersecurity events 18

2.1. 2021 work and key findings 18

2.2. 2022 work plan 19

3. Storytelling …. 20

4. Developing a Framework for collecting and evaluating cybersecurity events 20

4.1. Collecting details on cybersecurity events with a focus on the voices of those most affected 21

5. Next Steps 23

Workstream 3: BPF Outreach and Engagement **25**

RightsCons Community Lab - In service of Convergence. Building a multi-disciplinary community of cybernorms practitioners 25

Input to the UN OEWG Chair's Informal Dialogue 26

Input to IGF 2022 Parliamentary Track 26

Input to the UN OEWG Informal Inter-Sessional Meetings 27

Ad Hoc Workstream: Mythbusting Cybercrime vs. Cybersecurity **28**

Introduction 28

Myth 1: They are two sides of the same coin: Cybersecurity policy is proactive and cybercrime policy is reactive. **29**

Myth 2: Considerations for human rights are equally compatible with cybercrime and cybersecurity policy. **30**

Myth 3: The security of information is a consideration for both cybercrime and cybersecurity. (It's controversial!) **31**

Myth 4: Countering cybercrime improves cybersecurity. **31**

Myth 5: Cybercrime and Cybersecurity both improve with enforcement. **31**

Conclusion **32**

References **33**

Executive Summary

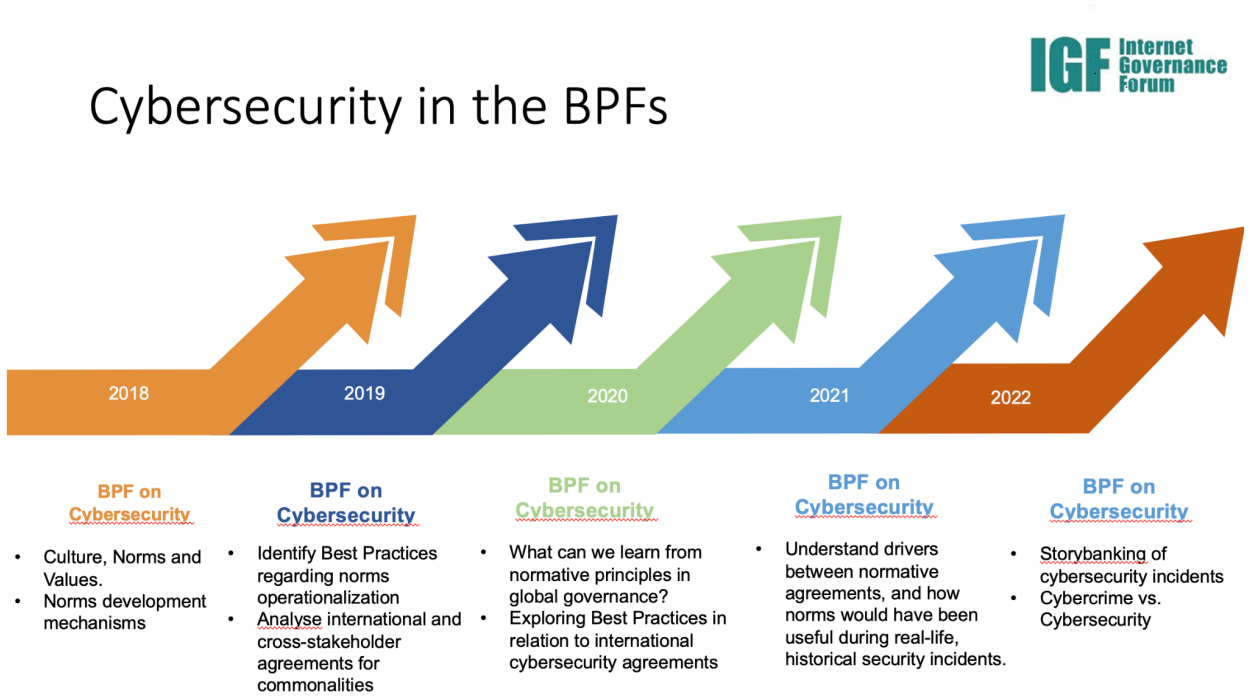
Introduction

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. Last year's BPF Cybersecurity investigated more deeply the drivers behind, and disablers of, cyber norms. A second work stream tested norms concepts against historical Internet events to understand how specific norms have or would have been effective at mitigating adverse cybersecurity events.

In 2022, the BPF Cybersecurity added new agreements to its assessment of normative cybersecurity agreements, explored the value of storybanking cybersecurity incidents, and produced an ad hoc mythbusting paper on the difference between cybercrime and cybersecurity from a policy perspective.



Work Stream I - Mapping International Cybersecurity Norms Agreements

The BPF added two new agreements - *the Copenhagen Pledge on Tech for Democracy* and *A Declaration for the Future of the Internet* - to its database, which now includes 38 international agreements between or among stakeholders, including voluntary, nonbinding cybersecurity norms. The analysis showed that "human rights" and "general cooperation" are the most commonly seen norms elements across the 38 agreements. Norms that relate to express restraint on what either government actors, private sector actors, or other actors will not do occur the least frequently, but have become more prominent over time. Interestingly, the new norms agreements included in the 2022 analysis have overlapping qualities as well as norms elements that set them apart. They are both led independently by foreign ministries and have emphasis on protecting democracy and on working to building democratic coalitions, of governments in one case and of broader multistakeholder actors in the other. There's a focus in both agreements on disinformation, misinformation, and influence operations related to the security of democracies. Lastly, the overall analysis of the 38 agreements showed a growing interest in combating ransomware as an action item.

Work Stream II - Exploring Historic Cybersecurity Events

Building on its work in 2021 that revealed a gap in understanding the roles of actors and stakeholders in mitigating cybersecurity incidents, the work stream 2 explored how storytelling can be an effective tool to listen and learn from the experiences of first responders and those most affected by a cybersecurity event. These insights are valuable input for those involved in cyber norm development. At the end of the day, cybersecurity norms must make a difference in the lived experiences of these people, past, present and future. The workstream 2 developed a framework for collecting stories from networks of first responders.

Work Stream III - Outreach and Engagement

Under its Outreach and Engagement work stream the BPF organised an outreach session during *RightsCon 2022* and contributed relevant findings of its work on cybersecurity norms with the *UN Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025* during the OEWG Chair's Informal Dialogue (BPF input) and Informal Inter-Sessional Meetings (BPF input).

Ad hoc paper - Mythbusting: Cybercrime versus Cybersecurity

The BPF created an ad hoc work stream to develop a paper to help stakeholders understand the key policy differences between cybersecurity and cybercrime such that their advocacy strategies can better align with a human rights centric approach to internet governance. In general the suggested strategy is to remove the policy decision making out of the criminal frameworks so as to balance the implications on human rights, while promoting cybersecurity as an incentivized, normative framework that depends on cross sector collaboration, and can be compatible with human rights. The paper is included in this report as well as available online.

Workstream 1: Mapping International Cybersecurity Norms Agreements

1. Introduction and list of agreements

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[1] and 2021[2] report, and then analyzing the norm elements that exist within the agreements to identify trends and explore their intended impact.

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.

Two new agreements *The Copenhagen Pledge on Tech for Democracy* and *A Declaration for the Future of the Internet* have been added to the database, which now includes 38 international agreements between or among stakeholders, including voluntary, nonbinding cybersecurity norms.

	Agreement Name	**Year**
1	**Draft EAC Legal Framework For Cyberlaws**	2008

[1] https://www.intgovforum.org/en/filedepot_download/10387/2397
[2] https://www.intgovforum.org/en/filedepot_download/235/20623

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
37	**Copenhagen Pledge on Tech for Democracy**	2022
38	**A Declaration for the Future of the Internet**	2022

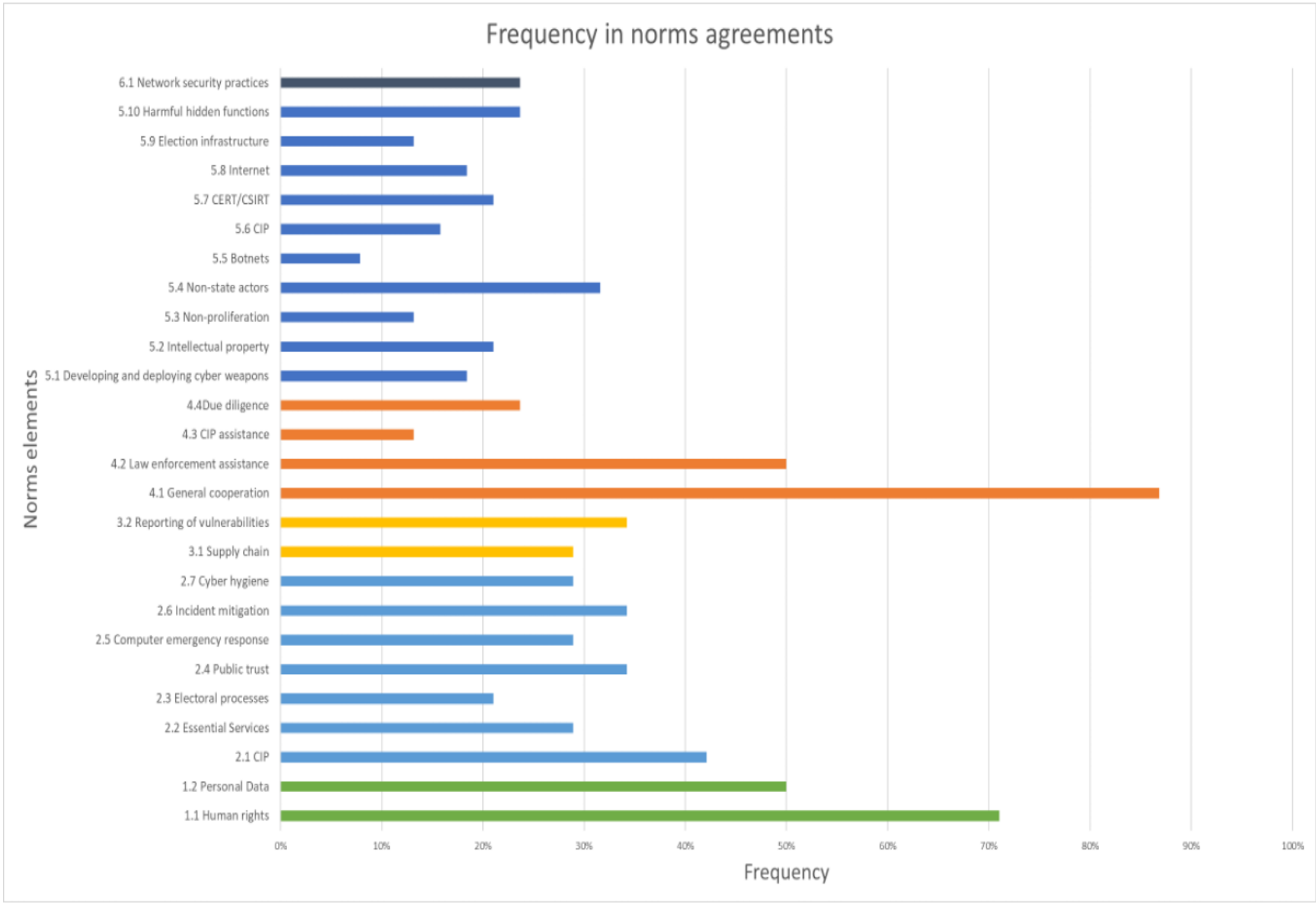
2. Analysis of norms elements

The 2022 analysis looked at the presence of different elements across the 38 cybersecurity agreements in the database.

1. Rights and freedoms	1.1 Human rights
	1.2 Personal Data
2. Information Security and resiliance	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. Reliability of products	3.1 Supply chain
	3.2 vulnerability reporting
4. Cooperation and assistance	4.1 General cooperation
	4.2 Law enforcement assistance
	4.3 CIP assistance
	4.4Due diligence
5. Restraint on development and use of cyber capabilities	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 H functions
6. Technical/Operational	6.1 Network security practices

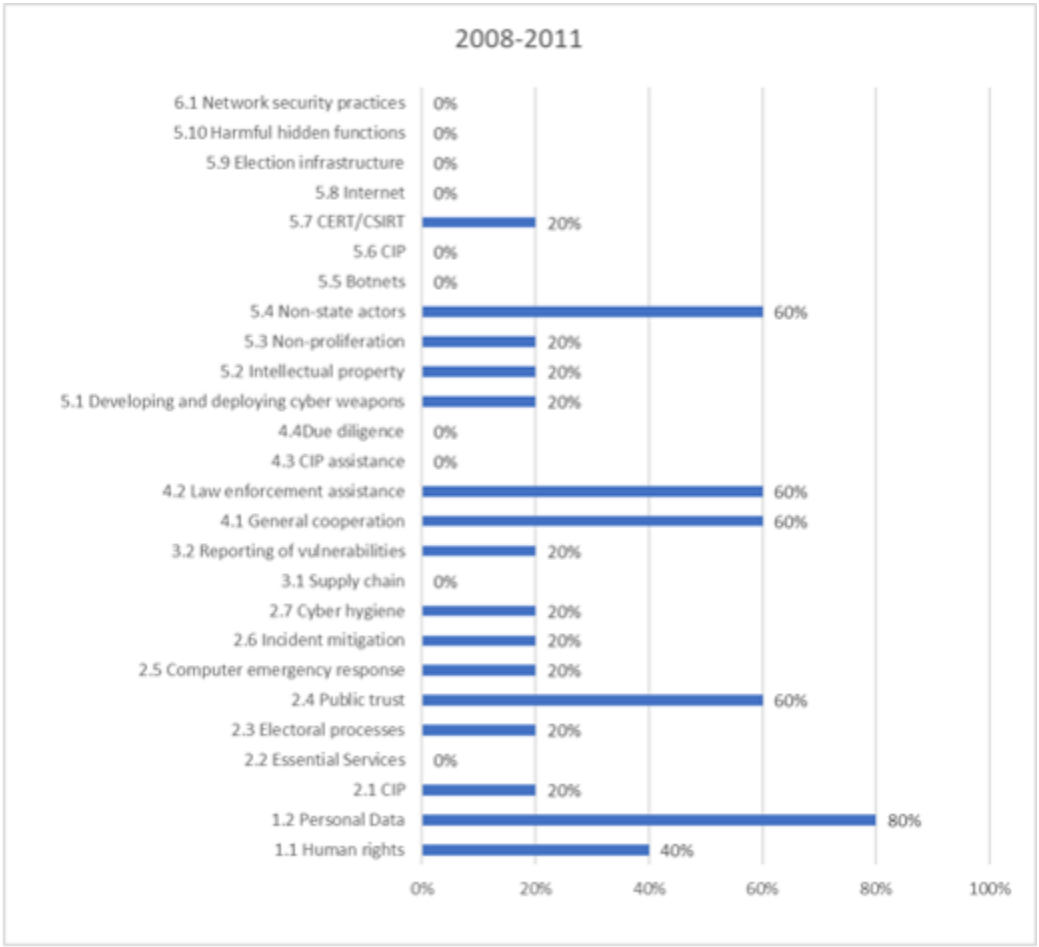
The analysis showed that **“human rights”** and **“general cooperation”** are the most commonly seen norms elements across the 38 agreements. Norms that relate to express **restraint** on what either government actors, private sector actors, or other actors will not do occur the least frequently, but have become more prominent over time.


Frequency in norms agreements
Norms elements
6.1 Network security practices
5.10 Harmful hidden functions
5.9 Election infrastructure
5.8 Internet
5.7 CERT/CSIRT
5.6 CIP
5.5 Botnets
5.4 Non-state actors
5.3 Non-proliferation
5.2 Intellectual property
5.1 Developing and deploying cyber weapons
4.4Due diligence
4.3 CIP assistance
4.2 Law enforcement assistance
4.1 General cooperation
3.2 Reporting of vulnerabilities
3.1 Supply chain
2.7 Cyber hygiene
2.6 Incident mitigation
2.5 Computer emergency response
2.4 Public trust
2.3 Electoral processes
2.2 Essential Services
2.1 CIP
1.2 Personal Data
1.1 Human rights
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Frequency

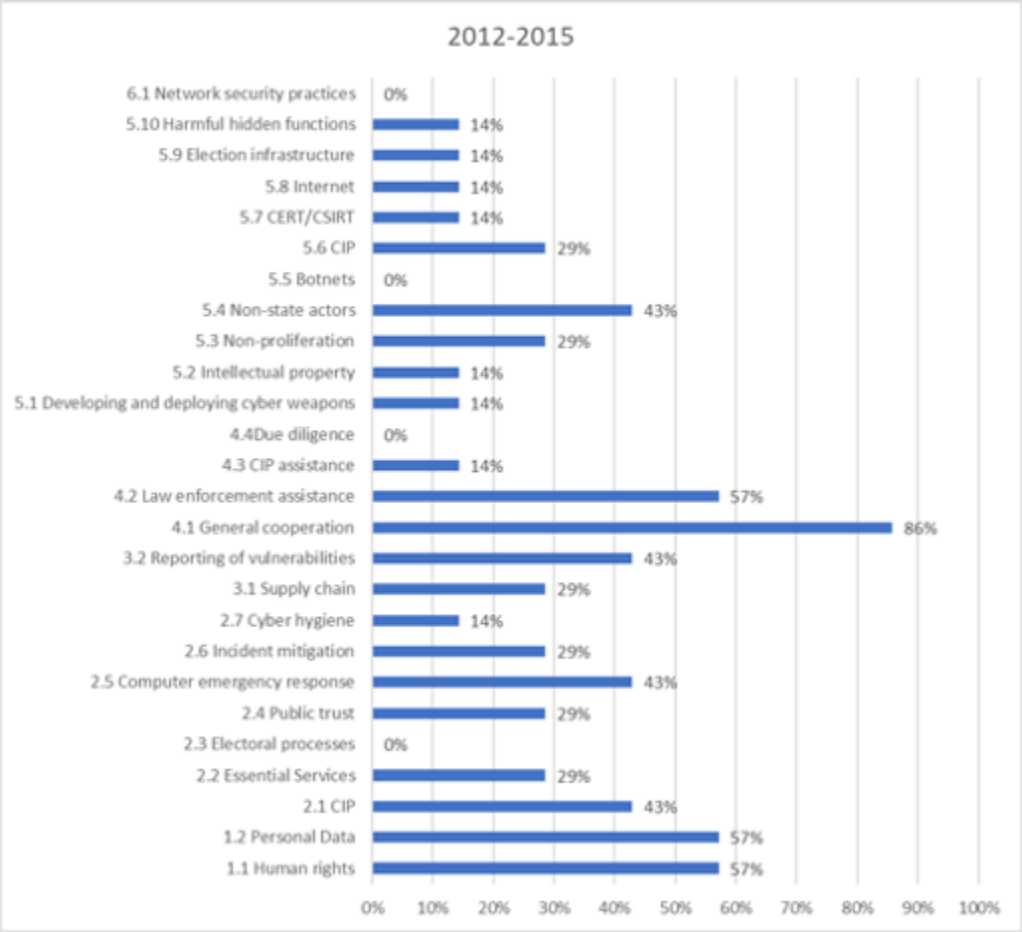
Interestingly, the new norms agreements included in the 2022 analysis have overlapping qualities as well as norms elements that set them apart. They are both led independently by foreign ministries and have emphasis on protecting democracy and on working to building democratic coalitions, of governments in one case and of broader multistakeholder actors in the other. There's a focus in both agreements on disinformation, misinformation, and influence operations related to the security of democracies.

The analysis of the frequency of norms elements over time shows a growing interest in **human rights**, **elections**, and all **restraint** norms, while **personal data** and **non-state actors** are less present. The overall analysis of the 38 agreements further shows a growing interest in **combating ransomware** as an action item.

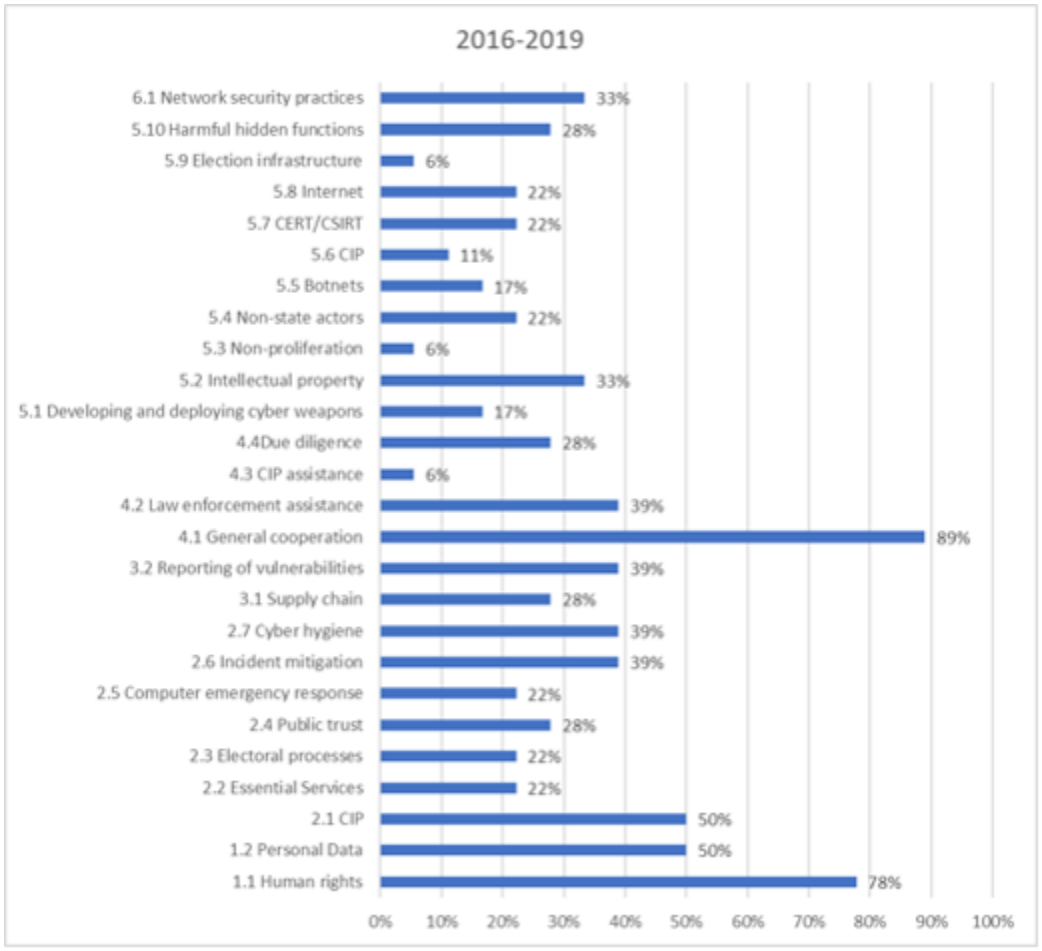
frequency of norms elements - 2008-2011



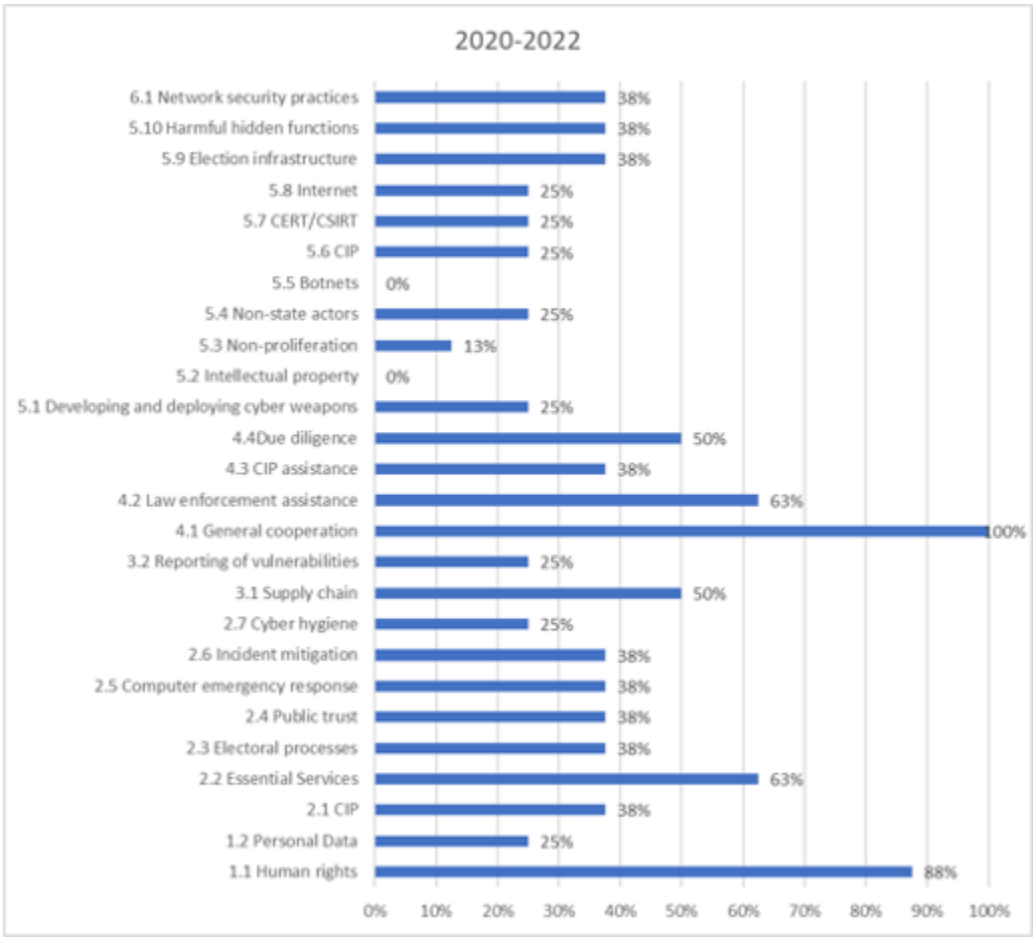
frequency of norms elements - 2012-2015



frequency of norms elements - 2016-2019



frequency of norms elements - 2020-2022



Workstream 2: Exploring Historic Cybersecurity Events

1. Introduction - the IGF Best Practice Forum Cybersecurity

The Internet Governance Forum, convened by the United Nations Secretary-General, is the global multistakeholder platform facilitating the discussions of public policy issues pertaining to the internet. As part of its mandate[3], the IGF facilitates the exchange of information and identifies best practices identified by experts and academics working on area issues.

Since 2014, IGF Best Practice Forums have focused on cybersecurity related topics as a multistakeholder group. From 2018 onwards, the BPF on Cybersecurity instigated investigations of cultures of cybersecurity, identifying the norms and values in development of these practices.

As a global initiative, the IGF BPF on Cybersecurity leverages an international and cross-stakeholder approach in their operationalization of cybernorms. The BPF recognizes the significance of powerful norm promoters and of ensuring incentives as critical in global governance. They state "norm development, even without results, creates socialization, which can be critical for further success"[4].

2. Introduction to Workstream 2 - Exploring historic cybersecurity events

2.1. 2021 work and key findings

[3] https://www.intgovforum.org/en/about
[4] IGF 2020 BPF Cybersecurity, *Exploring best practices in relation to international cybersecurity agreements.* *https://www.intgovforum.org/en/filedepot_download/10387/2397*

In 2021, the work stream 2 produced a report[5] that took a closer look at notable cybersecurity events of the past and wondered if norms would have made a difference, and whether these notable events led to changes in norms frameworks.

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.

The differential in depth of analysis between the events with desk research only versus those for which qualitative interviews were also conducted, made clear that **the voices of those most affected by cybersecurity events provide key nuance that are not present in secondary source reports or tertiary source reporting.**

Our distilled findings coalesced 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**.

2.2. 2022 work plan

The work stream 2 work plan's aim has been to build upon the 2021 report by developing a framework and workflow for similarly collecting and evaluating cybersecurity events, both past and present, with a focus on the storytelling narrative.

The purpose of this workflow is to be prepared to present first-person narratives from those most affected as victims or first responders of cybersecurity events and to connect those first responders and victims directly into the decision making processes about norms at a high level.

Our hope is that in norms development processes the Global IGF's BPF Cybersecurity can present real-world impacts as told directly by most affected voices as a way to ground in reality these high-level policy decisions.

[5] IGF 2021 BPF Cybersecurity, *The use of norms to foster trust and security.* https://www.intgovforum.org/en/filedepot_download/235/20623

3. Storytelling ….

Storytelling is an effective tool in changing minds, shifting thinking and balancing power. Sharing stories is an exercise in both telling and listening. Recounting an authentic personal experience is not only persuasive, it is an activity that rebalances power relationships between top-down governance structures and everyday lives.

Cybersecurity events make headlines. Often this is because of their sheer scale in terms of which users were affected, dollars lost, or number of consumers affected. However there are always stories to be told in how exactly a case of ransomware, data breach, hardware attack or other event ended up affecting those targeted or incidentally victimised by the incident. There are also those who are alert 24/7 in the event of such attacks that are the first to respond with a code fix, mutual aid or other interventions to victims and affected systems alike. At the end of the day, cybersecurity norms must make a difference in the lived experiences of these people, past, present and future.

Some examples of storytelling in communities that are closely related and relevant to the Internet Governance Forum and UN-level Cybersecurity Norms deliberations include:

- Global Encryption Coalition asks for testimonials from users and providers of encrypted services how encryption keeps us all safe. https://www.globalencryption.org/get-involved/tell-your-story/

4. Developing a Framework for collecting and evaluating cybersecurity events

We ask, “How would specific norms have been effective at mitigating adverse cybersecurity events?”

Last year the Cybersecurity Best Practice Forum of the Internet Governance Forum published a discussion paper that interrogates which are the core ideas behind prominent cybersecurity normative agreements that had the most continuity through various incidents.

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, aimed 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.

In all cases we point to the need to put those most affected by cybersecurity events and first responders in direct contact with policy makers designing norms and laws.

4.1. Collecting details on cybersecurity events with a focus on the voices of those most affected

The following form captures the basic details about cybersecurity events in order to continue to analyse these events against existing and developing norms, with a particular focus on the voices of those most affected by the incidents themselves. The form was developed in an iterative way by the participants in the workstream 2 effort.

Major cybersecurity events

Introduction

Thank you for participating in our survey. The information you share will be used by the IGF BPF Cybersecurity and any personally identifiable information is kept fully confidential.

How would specific norms have been effective at mitigating adverse cybersecurity events? In 2021 The Cybersecurity Best Practice Forum of the Internet Governance Forum published a discussion paper that interrogates which are the core ideas behind prominent cybersecurity normative agreements that had the most continuity through various incidents. 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, aimed 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.

In all cases we point to the need to put those most affected by cybersecurity events and first responders in direct contact with policy makers designing norms and laws.

This form captures the basic details about cybersecurity events in order to continue to analyse these events against existing and developing norms, with a particular focus on the voices of those most affected by the incidents themselves.

Read more about the IGF BPF Cybersecurity's analysis and findings on *'Testing norms concepts against cybersecurity events'* in section 2 of last year's report (p. 50-76) at https://www.intgovforum.org/en/filedepot_download/235/20623 .

More on the IGF BPF Cybersecurity at https://www.intgovforum.org/en/content/bpf-cybersecurity

Questionnaire

1. Name of the Event **(*required)**

2. Date

3. Type of Event

   - ☐ Advanced persistent threat (APT)
   - ☐ Data breach
   - ☐ Data leak
   - ☐ Denial of Service (DOS) or Distributed Denial of Service (DDOS)
   - ☐ Malware
   - ☐ Supply chain attack
   - ☐ Technique disclosure (eg Snowden Revelations)
   - ☐ Vulnerability
   - ☐ Control systems breach
   - ☐ Dual-use software
   - ☐ Disinformation campaign
   - ☐ Ransomware
   - ☐ Social engineering
   - ☐ Other

4. Country/countries (of the attack)

5. Target

6. Intent

7. Description **(*required)**

8. Outcomes/response

9. Elements of response/outcomes

    - ☐ Cybersecurity norms helped with mitigation
    - ☐ Influenced new or existing cybersecurity norms
    - ☐ Security research
    - ☐ Cross-sector cooperation
    - ☐ Cross-border cooperation
    - ☐ Political/legal/technical attribution
    - ☐ Other

10. Three secondary sources for reference (URLs)

11. Your name and contact information for follow-up questions

Consent

- ☐ If you have shared your contact information it will be kept fully confidential.

5. Next Steps

Now that our framework is in place, we hope in 2023 to begin in earnest to populate it with stories that are collected from networks of first responders. We hope that those first responders can also help connect us to the victims of past attacks.

Measures of success of this work in 2023 should be:

- Whether we are able to collect stories of emerging cybersecurity incidents in 2023,
- Whether we can use storytelling directly in the cybersecurity norms deliberations at the UN-high level in 2023.

Key Contributors to the work of the BPF Cybersecurity workstream 2: Mallory Knodel (Workstream 2 lead & Editor), Anastasiya Kazakova, Allison Wylde, Evan Summers, Wim Degezelle (IGF consultant).

Workstream 3: BPF Outreach and Engagement

The BPF's *Workstream 3 Outreach and Engagement* serves a double purpose, identifying and engaging new stakeholders into the BPF Cybersecurity community and raising awareness about the work and outputs of the BPF Cybersecurity.

Under its Outreach and Engagement work stream the BPF organised an outreach session during *RightsCon 2022,* contributed relevant findings of its work on cybersecurity norms with the *UN Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025* during the OEWG Chair's Informal Dialogue and Informal Inter-Sessional Meetings, and participated in the *IGF 2022 Parliamentary track*.

RightsCons Community Lab - In service of Convergence. Building a multi-disciplinary community of cybernorms practitioners

9 June 2022

The BPF Cybersecurity organised an outreach event at Rightscon 2022 under the title *In service of convergence. Building a multidisciplinary community of cybernorms practitioners.*

The meeting provided an overview of the BPF's research and then assessed a wider set of cyber incidents and their impact. The findings from a research report by the IGF's BPF on cybersecurity released in 2021 to the global internet governance community showed that the voices of those most affected by cybersecurity incidents provide key perspectives that are missing in cybernorms negotiations but there is a lack of clarity on whether and how cybernorms matter to those working on the frontlines to ensure a more peaceful and secure cyberspace.

The session seeked to build and expand action-oriented research on the application of cybernorms by bringing together academics, policymakers, civil society, the info-sec community and those directly impacted by cyber incidents. After the overview of the BPF's 2021 research and report, it continued with an assessment of a wider set of cyber incidents and their impact. This discussion was informed by a survey which was sent to stakeholders prior to the session to gather ideas and inputs on cyber incidents to assess and add to the portfolio of analysis. Findings of this session were fed into the IGF's BPF this year to expand the portfolio of analysis conducted. All participants were invited to contribute to the multistakeholder BPF after the session as well. Through its hands-on analysis of cybernorms and cyber incidents, the BPF

intends to strengthen bridges between different communities working to make the internet more secure for everyone.

- Session link (RightsCon registration required) https://rightscon.summit.tc/t/2022/events/in-service-of-convergence-building-a-multidisciplinary-community-of-cybernorms-practitioners-7owzhEsvLWyrrviZ8qnGWz
- Slide deck https://www.intgovforum.org/en/filedepot_download/56/24200

Input to the UN OEWG Chair's Informal Dialogue

21 July 2022

The BPF Cybersecurity provided input to the *Informal Dialogue with the Chair of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025.*

The BPF contribution highlighted how its research and in-depth analysis of international cybernoms agreements, and its investigation into what lessons can be learned from norms development outside the cyber realm, can serve as valuable resource to the OEWG as its works to build upon existing international expectations to advance a rules-based order in cyberspace based on responsible state behaviour.

- Input from the BPF Cybersecurity to the UN OEWG Chair's Informal Dialogue https://www.intgovforum.org/en/filedepot_download/56/22049

Input to IGF 2022 Parliamentary Track

30 November 2022

In recent years, IGF has sought to strengthen the participation of parliamentarians in discussions on some of the most pressing issues related to the use, evolution and governance of the Internet and related digital technologies. In 2019 and 2020, a parliamentary roundtable was held in the context of the IGF annual meeting. In 2021, an extended parliamentary track was introduced. The BPF Cybersecurity participated in the organisation of the IGF 2022 Parliamentary Track[6] that was themed *Addressing cyberthreats: National, regional and international approaches.*

The BPF presented its body of work on cybersecurity norms as a resource for parliamentarians involved and interested in related discussions and further, referring to its 2020 report, advocated for multistakestakeholder involvement when measures and policies are being

[6] https://www.intgovforum.org/en/content/igf-2022-parliamentary-track

prepared, developed and implemented. The BPF also took the opportunity to share it's *Mythbusting paper on cybercrime and cybersecurity* and is pleased that one the key messages 'that "cybersecurity" and "cybercrime" are related but distinct issues, "cybersecurity" being something that needs to be improved and "cybercrime" being something to be prevented', is reflected in the Parliamentary Track's output document[7].

Input to the UN OEWG Informal Inter-Sessional Meetings

6 December 2022

The BPF Cybersecurity provided input to the *Informal Inter-Sessional Meetings of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025.*

The BPF's contribution to the OEWG's Thematic Session on Confidence-building Measures highlighted the value of multistakeholder research and capacity building to support States to implement the UN agreed norms. The BPF shared that its research demonstrated that the success of cybersecurity norms agreements largely depends on actions by its signatories and stakeholders, and called for more research work that is focussed on understanding the interplay of cybersecurity norms and legislation including cybercrime legislation, where they overlap align or are not aligned, with an aim to introduce greater stakeholder participation in the creation, enforcement and response mitigation as outlined in cybersecurity norms.

- Input from the BPF Cybersecurity to the UN OEWG Informal Inter-Sessional Meetings https://www.intgovforum.org/en/filedepot_download/56/24093

[7] Output document from the Parliamentary Track of the 17th UN Internet Governance Forum, Addressing cyberthreats: National, Regional and international approaches, https://www.intgovforum.org/en/filedepot_download/249/24060

Ad Hoc Workstream: Mythbusting Cybercrime vs. Cybersecurity

Introduction

The Internet Governance Forum (IGF), convened by the United Nations Secretary-General, is the global multistakeholder platform facilitating the discussions of public policy issues pertaining to the internet. As part of its mandate (2015), IGF facilitates the exchange of information and identifies best practice identified by experts and academics working on area issues. Since 2014, IGF Best Practice Forums have focused on cybersecurity related topics as a multistakeholder group. From 2018 onwards, the BPF on Cybersecurity started investigating the concept of cultures of cybersecurity, identifying the norms and values in development of these practices. As a global initiative, the IGF BPF on Cybersecurity leverages an international and cross-stakeholder approach in their operationalization of cybernorms. The BPF recognizes the significance of powerful norm promoters and of ensuring incentives as critical in global governance. Its 2020 output states "norm development, even without results, creates socialization, which can be critical for further success" (IGF, 2020).

While the BPF framework is based on United Nations Group of Governmental Experts norms, recognizing the unique position of the UN in promoting international peace and security, the BPF adopted a political science definition of norms as a "collective expectation for the proper behavior of actors with a given identity" (Katzenstein, 1996). There are eleven items in the 2020 analysis of international norms agreements, from which two norms come out as the most commonly referred ones: calls for cooperation to promote stability and security in cyberspace, and recognition of human rights or privacy rights online (IGF, 2020).

As identified by the Best Practice Forum, our analysis also leverages a human rights focus in global internet governance, with a key focus on a "global" perspective as both cybersecurity and cybercrime are themselves nuanced concepts that to some extent depend on geopolitical context. The following myth busting, moreover, will disambiguate the key policy differences between cybersecurity and cybercrime so that their advocacy strategies could align. Our emphasis here will be on removing the policy decision making out of the criminal frameworks so as to balance the implications on human rights. Rather, we promote cybersecurity as an incentivized, normative framework that depends on cross sector collaboration, and, as seen in the IGF Best Practice Forum, can be compatible with human rights.

Myth 1: They are two sides of the same coin: Cybersecurity policy is proactive and cybercrime policy is reactive.

Cybersecurity is a cooperative approach which partly handles criminal law - including that which is more narrowly handled under cybercrime.

While both cybersecurity and cybercrime make references to securitization of computational systems, their approaches are not as compatible as they were made out to be. Cybersecurity defines a technical approach to securing computational systems from attacks or errors; and cybercrime is about punishing unauthorised interference with computational systems with criminal intent. Sometimes cybercrime is controversially defined to include crimes committed with digital technologies. The only commonality they have is that they are about security of computer systems, but they are not antagonistic as this myth makes them out to be. Rather, cybersecurity recognises the vulnerabilities in digital systems, whereas cybercrime aims to prevent damage to these systems through punitive means (Privacy International, 2018).

In line with our reference, we can identify good practices in both these areas. Cybersecurity strategies should be based firstly on protecting individuals, devices, and networks: centre policies and practices on people and their rights. Secondly, these cybersecurity policies should aim to establish a framework rather than an isolated law, as these should encompass complementary initiatives and approaches. Specifically, these policies should identify and prioritise critical infrastructure, establish response teams for security incidents, and maintain a proper threat assessment to help in decision-making and prioritisation of a country. The last aspect of best practice in this area would be about implementing comprehensive data protection laws, to safeguard against exploitation of personal data.

Cybercrime policy, on the other hand, considers a nation's constitution, and underpins the pertinent legislation, ideally with human rights protections and safeguards. Further, cybercrime should be narrowly interpreted, without losing its specificity to other 'offline' crimes that do not necessitate the use of a computer or other digital device. Lastly, considering the rapidly changing nature of technological interception, cybercrime policy should establish frameworks narrowed to "cyber-enabled major crimes" that complement and are consistent with existing criminal law instruments, including multilateral ones. This would refer to new ways of committing the same crime like fraud or distribution of child abuse images. If such comprehensivity is undertaken in a cybercrime framework, this would allow cross border cooperation in tackling these crimes, and prevent isolation of serious crimes under the banner of 'cybercrime'.

This multitude that is contained in the frameworks of cybersecurity and cybercrime make it necessary for cyber policy to gather input from various stakeholders, and significantly, best practice should consider civil society to play an important role in this process.

Myth 2: Considerations for human rights are equally compatible with cybercrime and cybersecurity policy.

The punitive, remedial, carceral and securitisation framing of cybercrime means that human rights must be balanced, e.g. individual privacy versus national security interests in investigating crimes. However, with cybersecurity, human rights can be more aligned with and compatible when people are placed at the centre of the security of cyberspace (FOC, 2016). In cybersecurity policy making, where human rights advocates push back against the geopoliticized use of vulnerabilities and other "cyber capabilities" as tools that manipulate power in cyberspace, that tactic and others are part and parcel of sovereign states' strategies to fight cybercrime.

In the activist toolkit "So is this Actually an Abolitionist Proposal or Strategy?" the following questions may help define a human rights approach through contrast. The approach taken by cybercrime versus cybersecurity might be considered as such, and explained below:

Question	**Cybercrime**	**Cybersecurity**
Do policy solutions expand the carceral system?	Yes	No
Do policy solutions benefit prisons and policing?	Yes	No
Will human rights advocates need to remain vigilant against the effects of the policy solution?	Yes	Yes
Does the solution reinforce existing State or economic power?	Yes	Yes
Are distinctions made between deserving and undeserving populations?	Maybe; Criminals may be denied access to online services.	No; Distinctions between employees, partners, customers are not inequitable.
Does the policy solution undermine popular resistance to its effects?	Maybe; Some forms of protest may be considered criminal.	No

Myth 3: The security of information is a consideration for both cybercrime and cybersecurity. (It's controversial!)

It may be common for "information security" to be used by technical practitioners within the context of an organization as an engineering practice, but in some parts of the world it's used as a term covering many other problems of the information space - for instance cultural and political stability. Directly speaking, in these contexts information security can sometimes mean that information itself is a security threat. From a human rights perspective, because of the needed balance with free expression, the term cybersecurity largely steers clear of addressing these often content driven issues.

In cybercrime this same issue is harder to avoid due to explicit issues such as those related to copyright law, however advocates should minimise or advocate to eliminate the presence of intellectual property in cybercrime legislation because it can easily introduce content considerations in cybercrime, which unchecked as a matter of State security is at greater risk of infringing on human rights of free expression than cybercrime.

Myth 4: Countering cybercrime improves cybersecurity.

One would think that in most cases, work to counter cybercrime improves cybersecurity. However, entrenched cybercrime laws, such as outlawing security research or development of exploit code, has been shown to negatively impact the ability of defenders to improve cybersecurity overall. When cybercrime laws are being developed, they should thoughtfully consider the impact on defenders, who often rely on the same techniques to validate and protect systems, but have no criminal or malicious intent.

Myth 5: Cybercrime and Cybersecurity both improve with enforcement.

In the cybercrime world, we often speak of enforcement of laws. Cybersecurity has its equivalent – compliance. However, that is only one part of building healthy cybersecurity.

A second portion is culture. Cybersecurity is so rapidly evolving that we can't prescribe to everyone how to act online. There are some basic steps individuals and organizations can take to protect themselves, and where the goal of cybersecurity is to achieve maximum compliance. However, in the face of rapid change, cybersecurity also requires education, awareness and norms, which cannot be governed in such a way and need to be grown to create aware and knowledgeable citizens.

Relatedly, one aspect of this elaboration on the norms in cybersecurity would be considering the linkages between cybersecurity frameworks and gender equality frameworks. Understanding how gender structurally operates within cybersecurity spaces is a crucial step in achieving a healthy system of cybersecurity. UNIDIR proposes a framework based on the design, defence, and response of cybersecurity activities so as to better identify how such gendered practices are part of the normative structure of this space, and to implement systems to mitigate gender inequality (Millar et al., 2021).

This reinforces the view that addressing cybersecurity and cybercrime from the points of view of communities most affected by power imbalance is critical for human rights as well as achieving success.

Conclusion

Prevention of cybercrime, and improving cybersecurity, are worthwhile efforts that are deserving of attention and development of expertise. However, in this document we hope we clarified the approaches to solving both will by definition be different, and an approach that is functional in one area, will not be functional in the other without serious adaptation and rethinking.

Today, cybersecurity and cybercrime policy practitioners are often asked to "stretch" between both domains. This poses risks in terms of approaches that may not cleanly translate from one to the other. Taking into account these five myths will help us understand where a solution may be the right fit for one, but not the other.

The authors of this paper recommend:

- **All stakeholders** put the principles of safety, human rights and frameworks front and centre when developing cybersecurity policy, and take a narrower lens when developing and advocating for cybercrime laws.
- **States** to avoid developing cybercrime laws that may negatively affect the work of cybersecurity defenders, by outlawing or criminalising their defensive activities, even though they may look like what a cybercrime law typically outlaws. They should do so by inviting other stakeholders to their conversations and enable an ongoing learning activity between these communities.
- **States** to develop proactive contributions to solving cybersecurity with other stakeholder groups and push accountable frameworks.
- **States** to actively narrow the range of issues covered in cybercrime to comprise "major crimes" and entirely exclude content-layer discussions.
- **States** to identify rights-respecting frameworks for accessing data by LEAs across borders given the necessary and proportionate principles.
- **Corporations** to invest in appropriate cybersecurity programs and policies to avoid some of the outcomes that may require law enforcement to react.
- **Civil society** to participate, and where possible, invite themselves to both cybercrime and cybersecurity discussions; and educate themselves on the different approaches each field

requires. Start with these 5 myths and work your way into guidance as published by specialized organizations, as listed in the references.

References

Millar, Katharine; Shires, James; and Tropina, Tatiana. 2021. Gender Approaches to Cybersecurity: Design, Defence and Response. Geneva, Switzerland: United Nations Institute for Disarmament Research. https://doi.org/10.37559/GEN/21/01

United Nations Internet Governance Forum (IGF), About the Internet Governance Forum, 2015.

United Nations Internet Governance Forum (IGF), Cybersecurity Culture, Norms and Values, Best Practice Forum Cybersecurity, 2018.

United Nations Internet Governance Forum (IGF), Exploring Best Practices in Relation to International Cybersecurity Initiatives, Best Practice Forum Cybersecurity, 2020.

Peter J. Katzenstein, ed., The Culture of National Security: Norms and Identity in World Politics, New York: Columbia University Press, 1996, 5.

Privacy International, Understanding the Difference between Cyber Security and Cyber Crime, 2018.

Key Contributors to the Mythbusting paper: Mallory Knodel, Sheetal Kumar, Maarten van Horenbeeck, Wim Degezelle. Thank you to all who provided feedback on the draft paper.

A copy of the BPF paper "Mythbusting: cybercrime versus cybersecurity" is available at https://www.intgovforum.org/en/filedepot_download/56/24126