In service of convergence

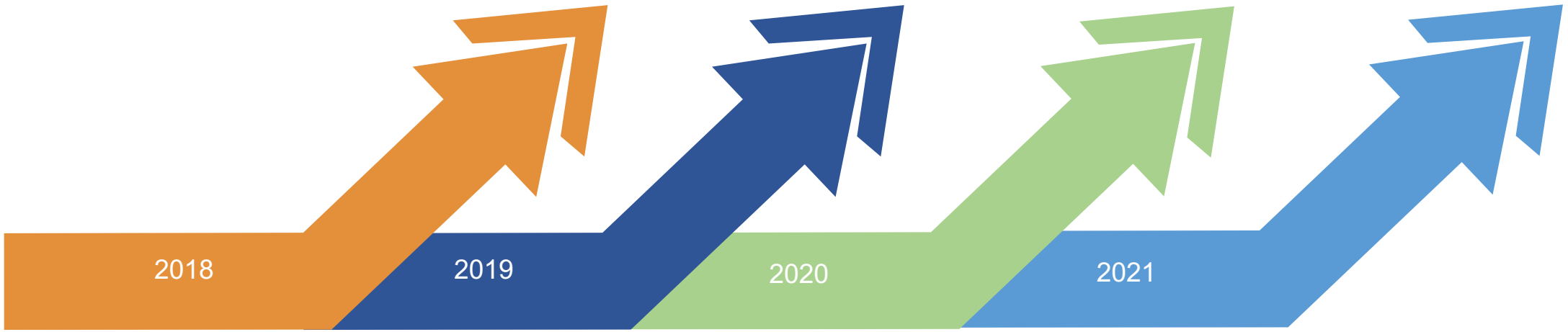
Building a multi-disciplinary community of cybernorms practitioners

June 9th, 2022

Rightscon Community Lab

IGF Internet Governance Forum

Cybersecurity in the BPFs



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

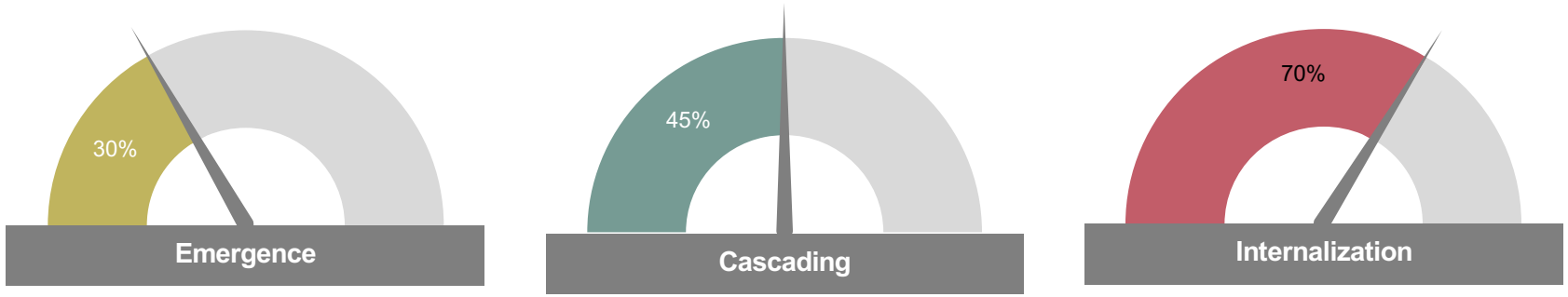
BPF on Cybersecurity

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

Cyber norms

Cyber norms

- "*Collective expectation for the proper behavior of actors with a given identity*", Katzenstein (1996)
- Identified by those who perceive a need, or when contested
- Require time to develop



Where do they originate

Stakeholder group	Example norms creating body or normative text
Government	UN Government Group of Experts, Freedom Online Coalition
Civil Society	Manila Principles (EFF et al)
Technical Community	Internet Society (Mutually Agreed Norms for Routing Security)
Private Sector	Microsoft
Multi-stakeholder	Global Commission on the Stability of Cyberspace

Examples of cyber norms

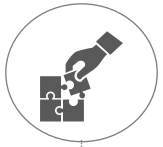
Proposer	Language	Affected party
UNGGE	*States should not conduct or knowingly support activity to harm the information systems of another state's security incident response teams and should not use their own teams for malicious international activity;*	States
GCSC	*State and non-state actors should not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites*	Everyone
Microsoft	*Global ICT Companies should issue patches to protect ICT users, regardless of the attacker and their motives*	Global ICT companies

2022 Workstreams

Agreements

Lead: John Hering and Pablo Hinojosa

Publication of research paper assessing 36 normative documents.



Events

Lead: Mallory Knodel

How would specific norms have been effective at mitigating adverse cybersecurity events?

Outreach

Lead: Sheetal Kumar and Markus Kummer

Identified and engaged new stakeholders into the BPF on Cybersecurity community.

Workstream 1: Approach and learnings

Analytical approach:

- Identified 36 agreements that met our core criteria
- Classified into multilateral, single-stakeholder and multistakeholder
- Identified trends and shared priorities

Key learnings:

- Identified cooperation and human rights as core themes, with human rights a growing portion over 2020
- Least common was ”restraint” in development of cyber capabilities
- Published a detailed analysis of 36 agreements

Workstream 1: Scoping and agreements

36 international agreements between or among stakeholders including voluntary, nonbinding cybersecurity norms

1	Draft EAC legal framework for cyberlaws
2	Shanghai Cooperation Organization's Agreement on cooperation in the field of ensuring the international information security
3	League of Arab States Convention on Combating Information Technology Offences
4	Convention on International Information Security
5	APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice
6	ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies (ICTs)
7	Southern African Development Community (SADC) Model Law
8	African Union Convention on Cyber Security and Personal Data Protection
9	Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document
10	G20 Leaders Communique
11	International code of conduct for information security
12	Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015)
13	NATO Cyber Defence Pledge
14	OSCE Confidence Building Measures (2013 and 2016)
15	The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security
16	ITU-T WTSA Resolution 50 -Cybersecurity
17	Charter for the Digitally Connected World
18	G7 declaration on responsible state behaviour in cyberspace
19	Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU
20	Charlevoix Commitment on Defending Democracy from Foreign Threats
21	Commonwealth Cyber Declaration
22	The Paris Call for Trust and Security in Cyberspace
23	Siemens Charter of Trust
24	Cybersecurity Tech Accord
25	The Council to Secure the Digital Economy International Anti-Botnet guide
26	ASEAN-United States Leaders' Statement on Cybersecurity Cooperation
27	DNS Abuse Framework
28	Contract for the Web
29	Ethics for Incident Response and Security Teams (EthicsfIRST)
30	GCSC's Six Critical Norms
31	FOC Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies
32	Organization of American States List of Confidence- and Security-Building Measures (CSBMS), Committee on Hemispheric Security
33	XII BRICS Summit Moscow Declaration
34	OEWG Consensus Report (2021)
35	Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security
36	Mutually Agreed Norms for Routing Security

Workstream 1: Norm elements

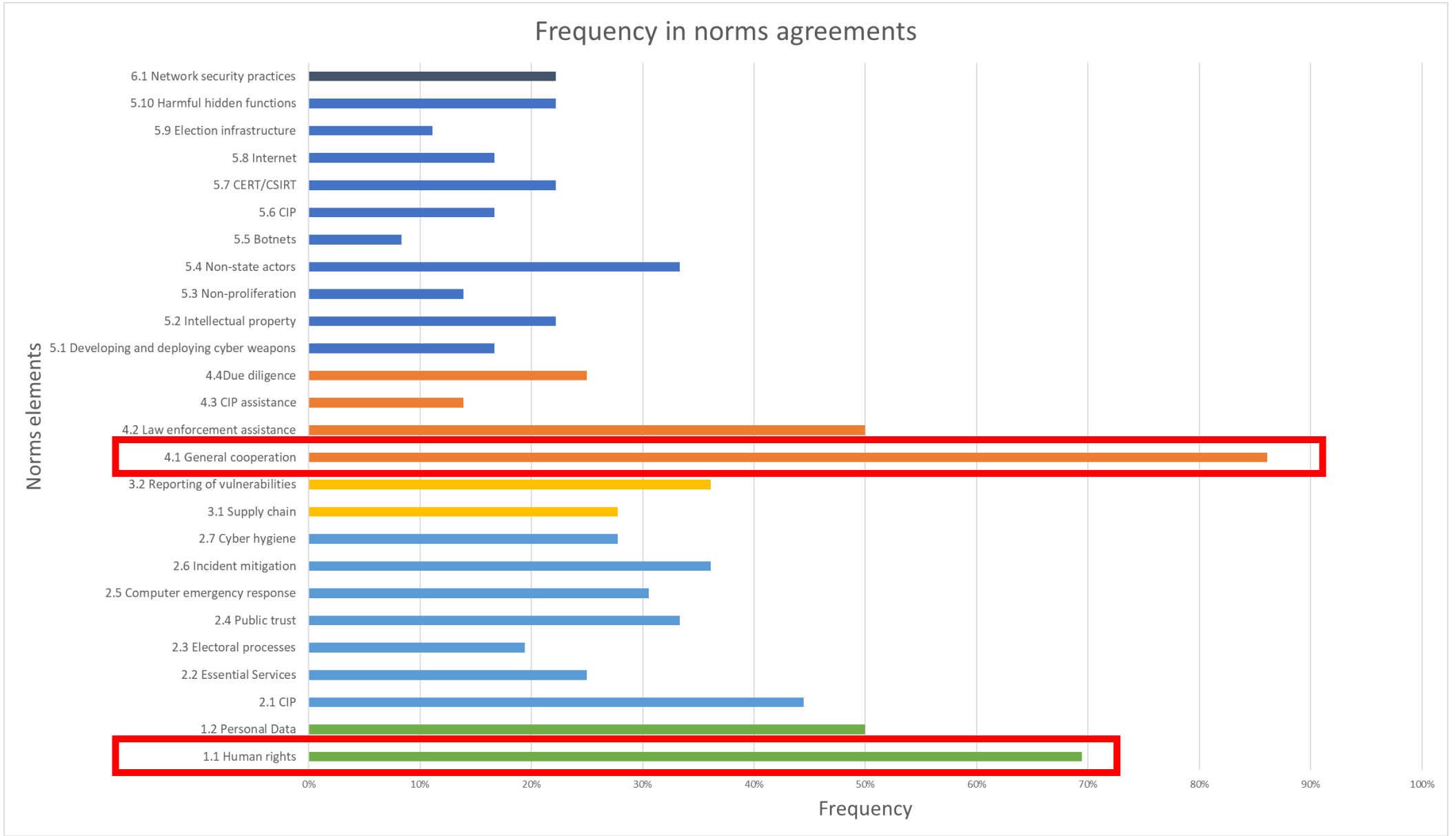
1. Rights and freedoms+A1:B26	1.1 Human rights
	1.2 Personal Data
2. Information Security and resiliance	2.1 CIP
	2.2 Essential Services
	2.3 Electoral processes
	2.4 Public trust
	2.5 Computer emergency response
	2.6 Incident mitigation
	2.7 Cyber hygiene
3. Reliability of products	3.1 Supply chain
	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

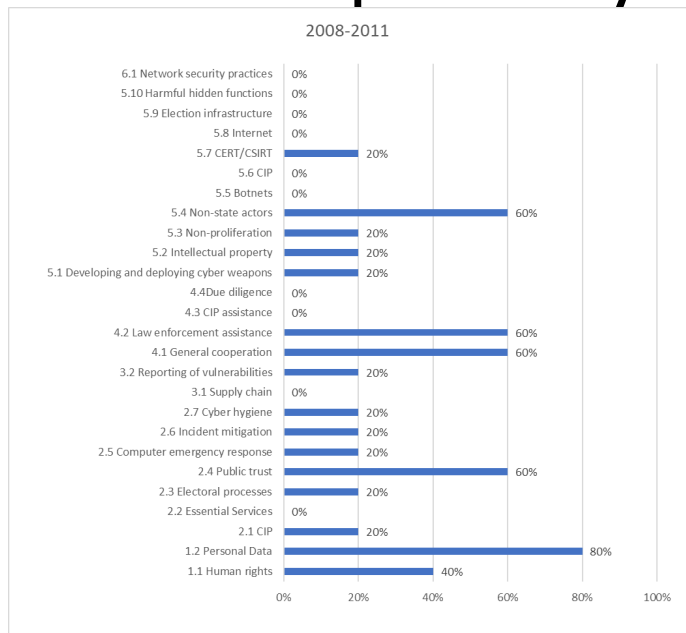
Workstream 1: Heat map

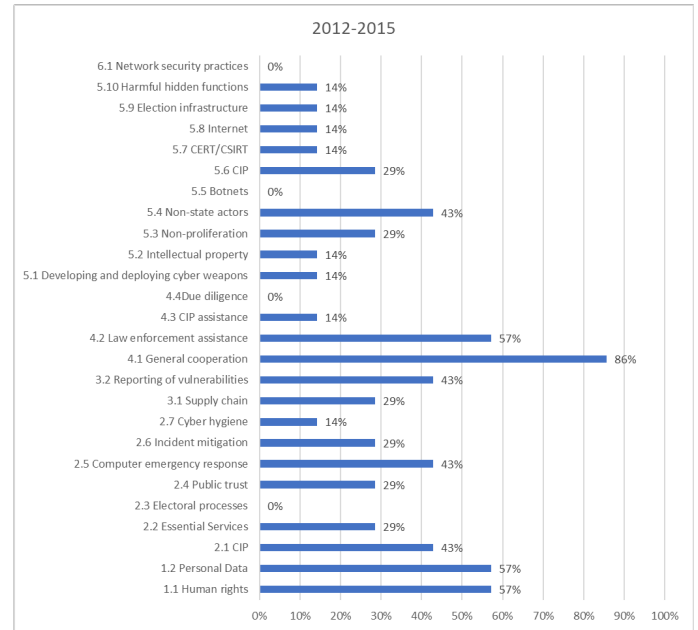
Overview			1. Rights and freedoms		2. Information Security and resilience							3. Reliability of products		4. Cooperation and assistance				5. Restraint on development and use of cyber capabilities									6. Technical/Operational
Agreement Name	Year	Stakeholders	1.1 Human rights	1.2 Personal Data	2.1 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	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																									

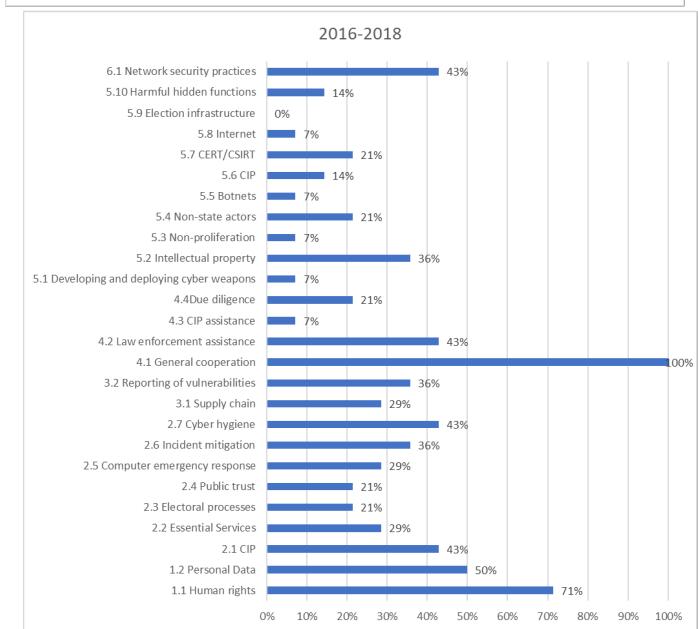
Workstream 1: Frequency

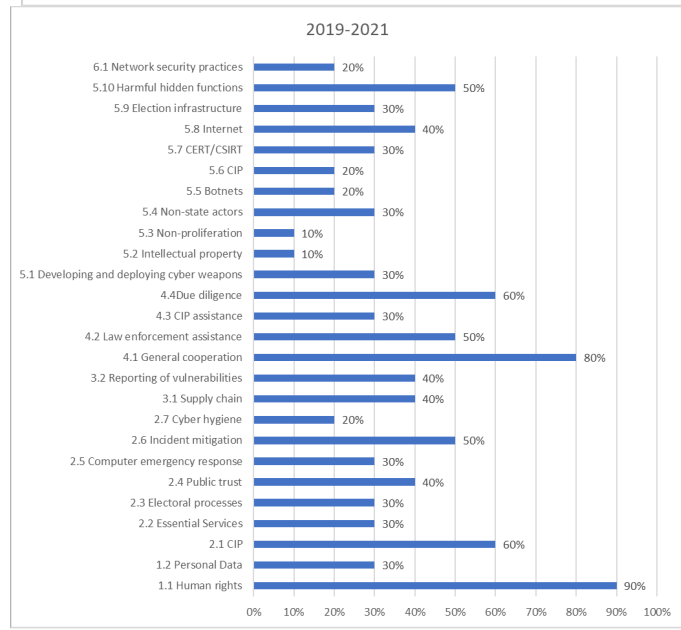


Workstream 1: Frequency over time









Workstream 2: Approach and learnings

Analytical approach:

- Identified criteria to select historical events (coverage by secondary and tertiary sources, demonstrable harm, successful mitigation)
- Analyzed events for influence of cybersecurity norms
- Expert contributor-led interviews with incident responders and victims

Key learnings:

- Existing cyber norms would have helped mitigate many cybersecurity events from the past
- Each analysis uncovered a missing nuance: e.g. GhostNet showed that cyber resilience is really a community-level concern

Workstream 2: Approach and learnings

Questions to ask

- 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?

Events for discussion

- **Pegasus**
- Stuxnet
- **Solarwinds**
- Snowden disclosures
- **Ghostnet**
- Heartbleed

- **Do you have another example to share?**

Thank you!

- **BPF on Cybersecurity conveners**
  - Markus Kummer
  - Hariniombonana Andriamampionona

- **UN Consultant:** Wim Degezelle

- Join the mailing list at https://intgovforum.org/pipermail/bpf-cybersecurity_intgovforum.org/
- More information on the BPF at https://www.intgovforum.org/multilingual/content/bpf-cybersecurity