BPF on Cybersecurity

Work Stream 1
Norms Agreements

Draft output

December 2022

WS1: Norms Agreements

Workstream 1: Scoping and agreements

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

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
	4.4 Due 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	4.4 Due 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																										
Copenhagen Pledge on Tech for Democracy	2021	Multistakeholder																										
A Declaration for the Future of the Internet	2022	Governments		1																								

Workstream 1: Frequency

Frequency in norms agreements

Highlights

- Most frequent are "Human rights and "general cooperation" norms

- Least frequent are "restraint" norms

2008-2011

2012-2015

2016-2019

2020-2022

Workstream 1:
Frequency over time
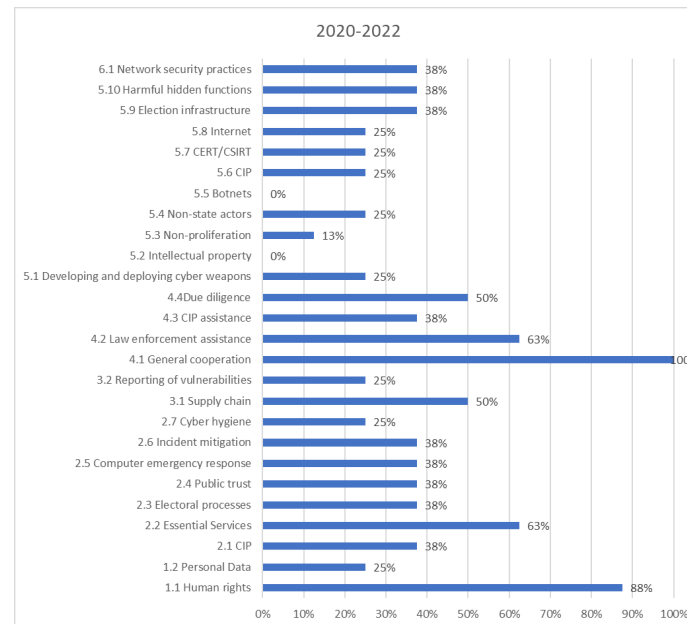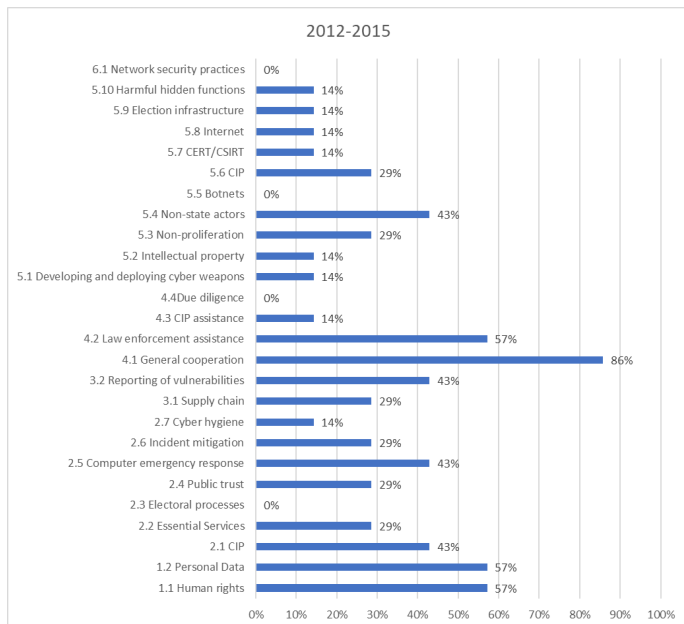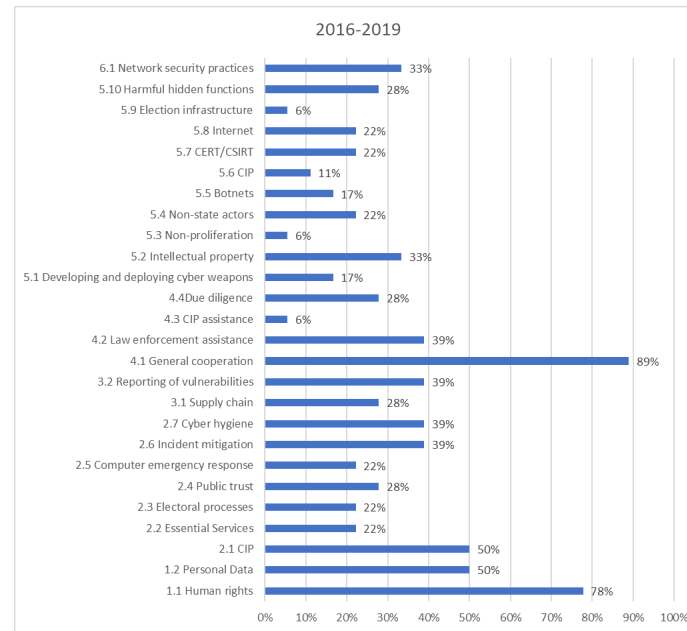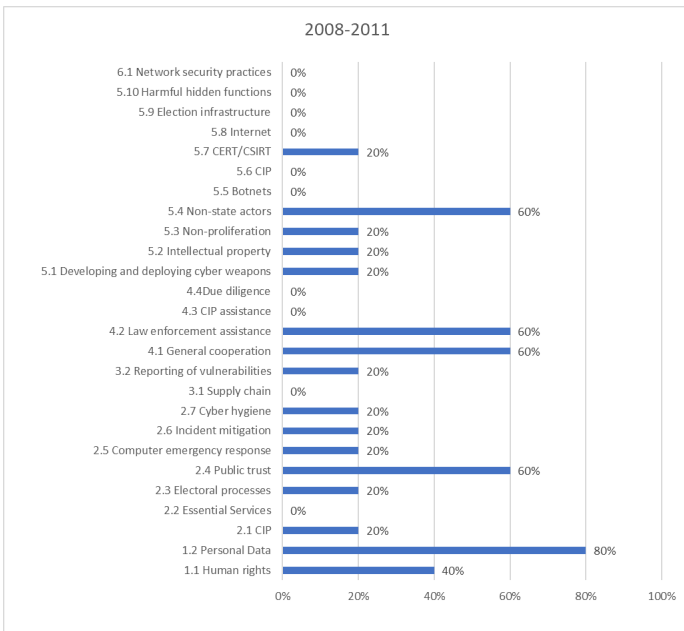
Trends

Rising norms:
- Human rights
- Elections
- All "restraint" norms

Declining norms:
- Personal data
- Non-state actors

Workstream 1: New agreements/priorities

- Two new norms agreements since IGF 2021
  - Copenhagen Pledge on Tech for Democracy (Nov. 2021)
  - A Declaration for the Future of the Internet (Apr. 2022)

- Overlapping qualities and norms elements
  - Independently led by foreign ministries (US/DK)
  - A focus on protecting "democracy" and building democratic coalitions
  - A focus on "disinformation" and influence operations

- In addition, combatting ransomware has emerged as a priority
  - Reflected in the Declaration for the Future of the Internet and the collaborative efforts under the Paris Call for Trust and Security in Cyberspace