BPF on Cybersecurity

Report on the BPF activities 2016-2018

Internet Governance Forum

IGF Internet Governance Forum

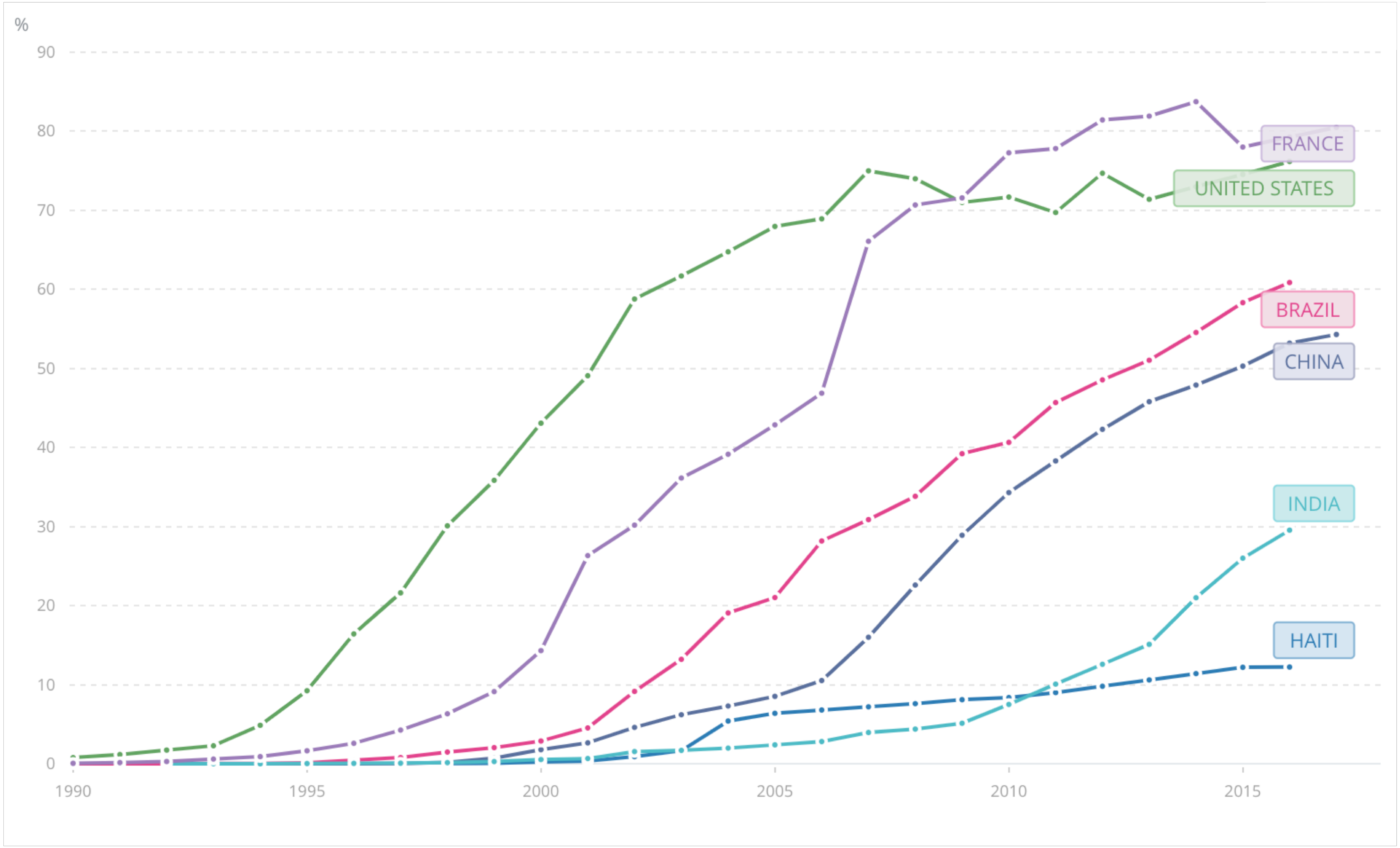
The Internet *of* Trust

INTERNET GOVERNANCE FORUM

PARIS, 12–14 NOVEMBER 2018

Agenda

- What is the **Internet Governance Forum**?
- **Intersessional work**: the Best Practices Forums
- **History of the BPF on Cybersecurity**
- Cybersecurity **culture, values and norms**
- The **Paris Call** for Trust and Security in Cyberspace
- Key **lessons learned**
- How to **get involved**



Internet users, 1990-2017, source: World Bank

Multistakeholderism

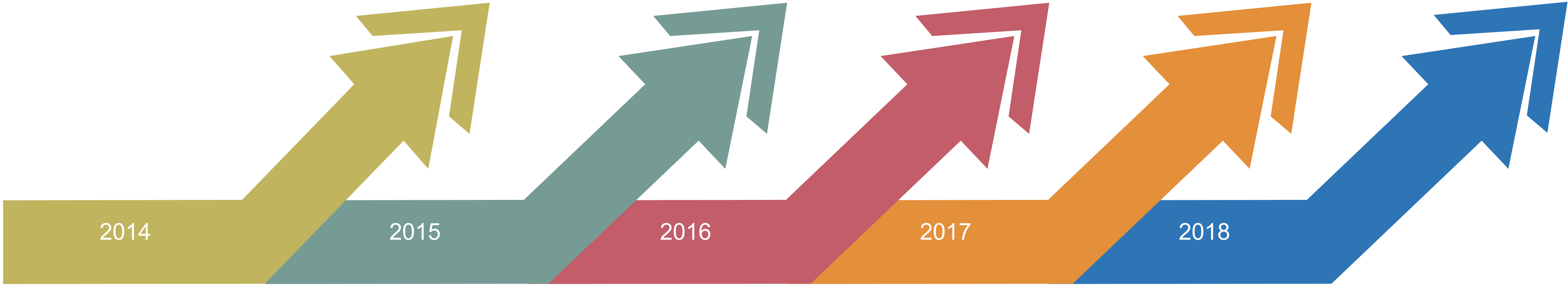
The Internet Governance Forum

- Forum for **multi-stakeholder dialogue on internet governance issues**
- Formally announced by UN Secretary General in 2006.
- Forum convened annually by UN Secretary General assisted by Multistakeholder Advisory Group
- Intersessional work
  - *Best Practice Forums (Cybersecurity, Gender & Access, Local Content)*
  - *Dynamic Coalitions*
  - *Policy Options for Connecting and Enabling the Next Billions*
  - *National and Regional IGF Initiatives*

Best Practices Forums

- UNCSTD called for development of **more tangible outputs**
- **BPFs publish resources** to the rest of the IGF community
- Resources are developed through mailing list conversation, polls, research, Calls for Contributions, in-person meetings and publications
- Often **build on other work in the IGF**
- Resources often see **much wider use than the IGF community**
  - 2014 BPF on CSIRT document used as input to GCCS
  - CSIRT BPF has been used to initiate new CSIRT initiatives

Cybersecurity in the BPF’s



2014

2015

2016

2017

2018

BPF on CSIRT (+ BPF Unsollicited Communications)

- What are CSIRT and how do they function?
- What conditions make CSIRT successful?

BPF on CSIRT (+BPF Unsollicited Communications)

- Involvement of CSIRT in policy discussions
- The evolving role of CSIRT
- Privacy and Security are mutually supportive

BPF on Cybersecurity

- Typical roles and responsibilities
- Communications mechanisms between stakeholder groups
- Problems stakeholders experience in cooperating on cybersecurity

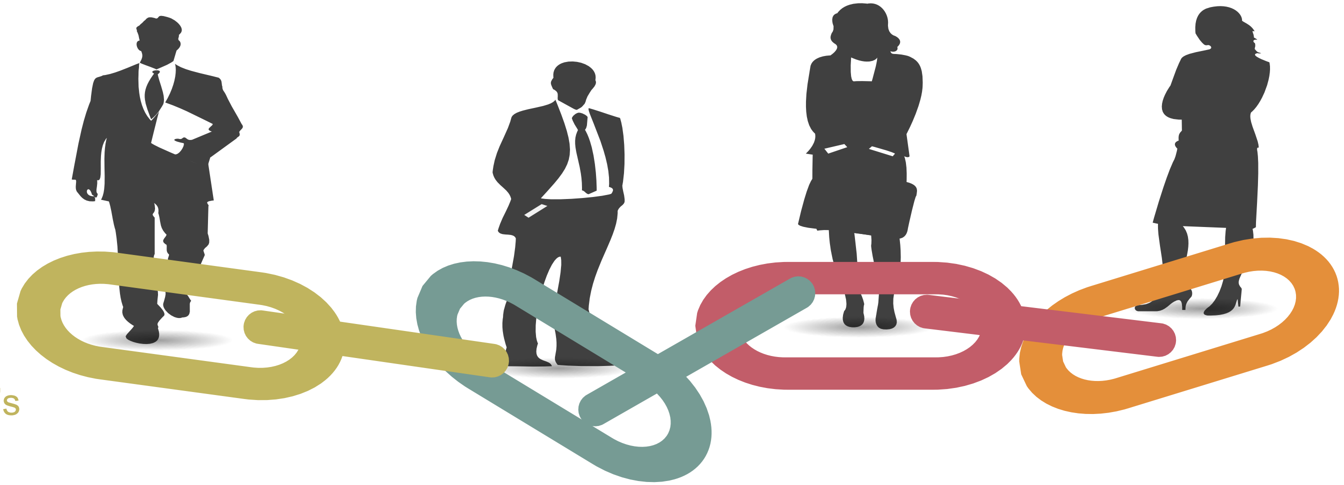
BPF on Cybersecurity

- How can Cybersecurity support the Sustainable Development Goals
- Policy Best Practices to help bring the Next Billion Internet users online safely

BPF on Cybersecurity

- Culture, Norms and Values.
- Norms development mechanisms

BPF on Cybersecurity (2016)



What is everyone's role and responsibility?

- Challenges around term Cybersecurity: different interpretations make it difficult to agree.
- Need for more civil society involvement
- Much of internet managed by private sector

How do we communicate and partner?

- Democratic, multi-stakeholder processes
- Case study of Whatsapp mechanism
- Cooperative meetings with face to face encounters

Best Practices on Situational Awareness

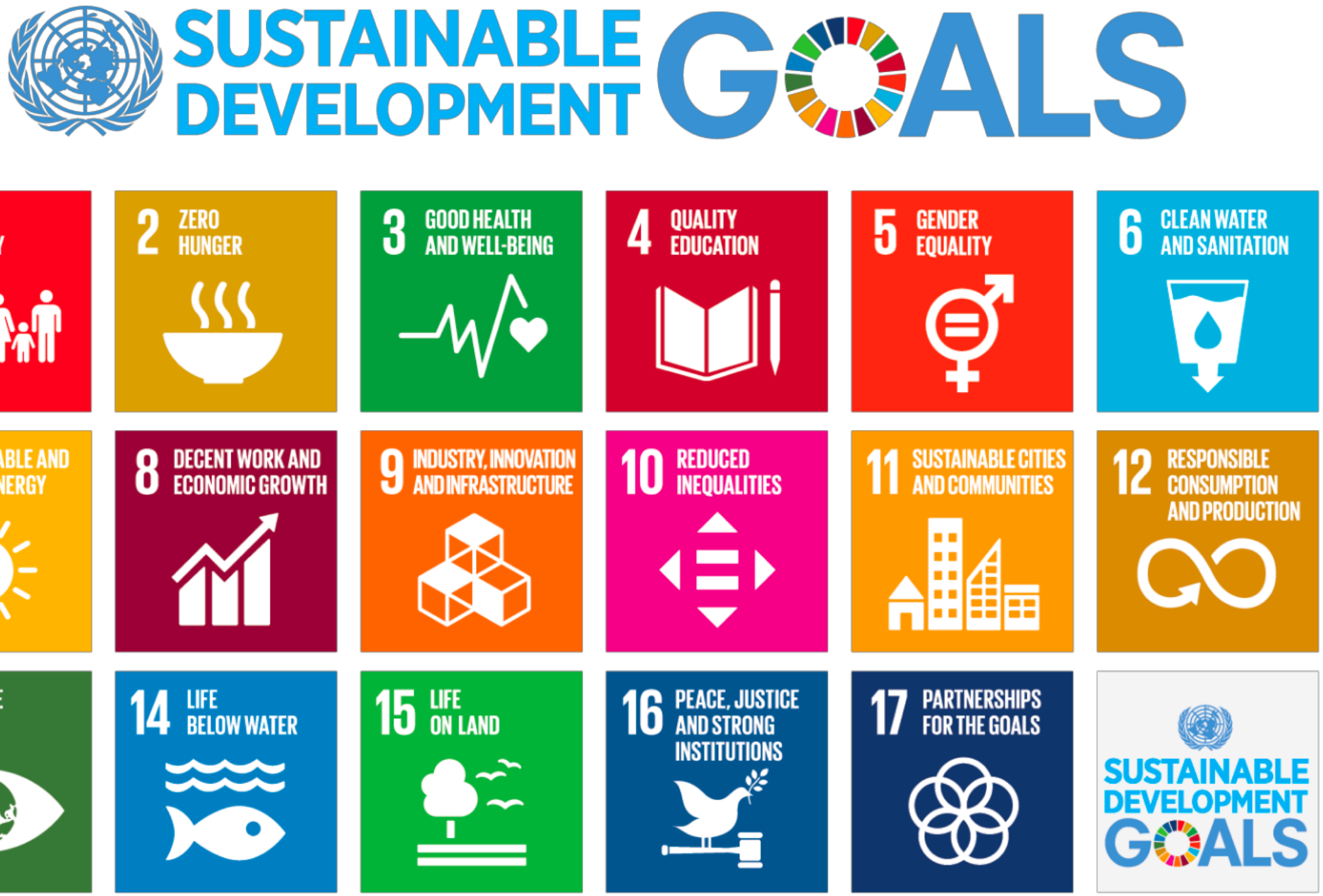
- Standardized protocols and automation
- ISACs
- Tools, platforms and technologies for automated exchange

Big issues moving forward

- Trust, based on work and correct expectations and deliverables, important component.
- IGF can help redefine cybersecurity and move path forward
- How to support Sustainable Development Goals

IGF Internet Governance Forum

BPF on Cybersecurity (2017)


SUSTAINABLE DEVELOPMENT GOALS
1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS
SUSTAINABLE DEVELOPMENT GOALS

BPF on Cybersecurity (2017)

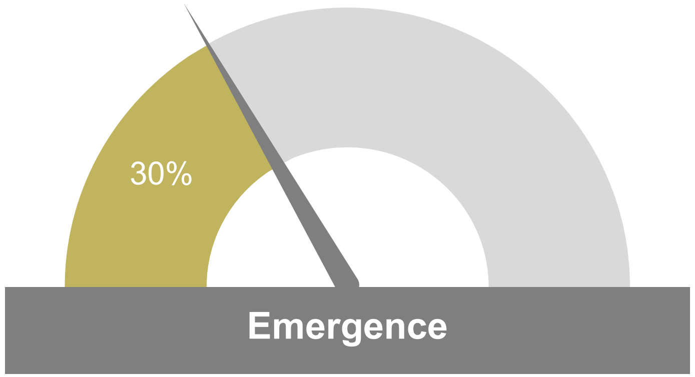
- Initial analysis examples
  - Decent work and economic growth can be impacted by major Distributed Denial of Service attacks and unreliable network interconnections.
  - Peace, justice and strong institutions can be undermined by cybercrime.
- Identify existing forums for discussion
- Final report including Policy Best Practices from stakeholders, e.g.:
  - States should be **encouraged to implement cybersecurity frameworks** such as the US NIST Cybersecurity framework and associated laws
  - A **Secure Development Lifecycle should be implemented in all software and product development**. The technical community is well placed to develop and release guidance on secure development processes, and share information on ongoing failures to drive process improvement

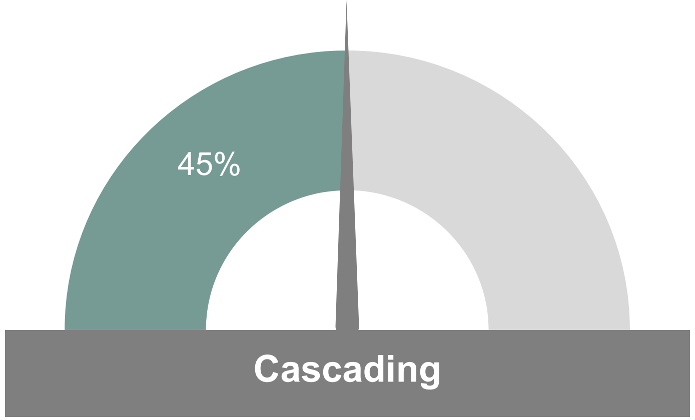
BPF on Cybersecurity (2018)

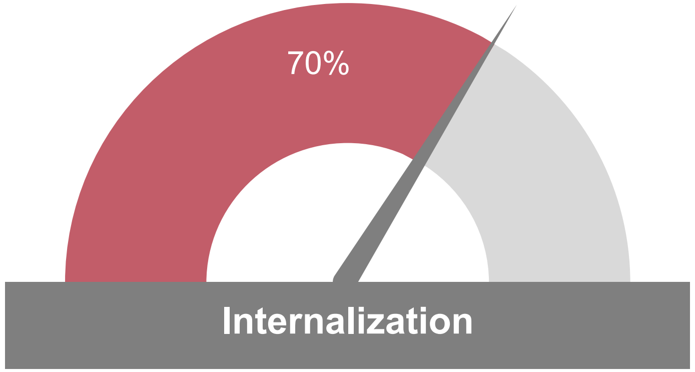
- Focus on **Cybersecurity Culture, Norms and Values**
- Culture is "*a pattern of beliefs and expectations shared by the organization's members. These beliefs and expectations produce norms that powerfully shape the behavior of individuals and groups*" (Schwartz and Davis, 2011 – helps guide behavior even when no strict law
- Laws do exist, but are slower to develop (e.g. **Budapest Convention**)
- **Preparatory research paper was published** covering the status of norms development in the internet governance community

Introduction to 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 they are contested, they require time to develop







Where do norms originate?

Stakeholder group	Example norms creating body or normative text
Government	UN Government Group of Experts, Freedom Online Coalition
Civil Society	Manila Principles
Technical Community	Internet Society
Private Sector	Microsoft
Multi-stakeholder	Global Commission on the Stability of Cyberspace

Examples of 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

Digital Security Divide

Image by Roy Niswanger, CC 2.0

Image by Klaus Boesecke, CC 2.0

Call for contributions

- How do you define a **culture** of cybersecurity?
- What are **typical norms and values** in your community?
- Who **promotes cyber norms**?
- Examples of **norms that have worked well**
- Examples of **norms that have failed**
- What **effective implementation methods** exist?
- Do you see a **Digital Security Divide**?

Responses to Call for Contributions

- Shreedeep Rayamajhi
- Aspisec - Andrea Chiappetta
- Afifa Abbas
- Anahiby Becerril
- Sudha Bhuvaneswari
- Marilson Mapa
- the Cybersecurity Tech Accord
- Cristina Cuomo

- CCAOI
- Microsoft
- Association for Progressive Communications (APC)
- Mallory Knodel and Matthew Shears
- Article 19 Eastern Africa
- IEEE Internet Initiative
- WSIS Coalition (AT&T, Intel, Google, Verisign)
- Global Commission on the Stability of Cyberspace (GCSC)

BPF session at the IGF 2018

- Moderated by Markus Kummer (convener) and Kaja Ciglic (Microsoft)
- Interventions by key contributors:
  - **Alexander Klimburg**, representing the Global Commission on the Stability of Cyberspace (GCSC)
  - **Ephraim Percy Kenyanito**, representing ARTICLE 19 Eastern Africa
  - **Saleela Salahuddin**, Facebook, representing the Cybersecurity Tech Accord

- Watch the video recording of the session at: https://www.youtube.com/watch?v=rXFBpR_2eYA

The Paris Call

- During the Paris IGF, President Emmanuel Macron launched a multi-stakeholder call to commit to supporting a more peaceful internet with stronger protections for users and human rights.
- It includes a number of commitments that align with several norms reviewed as part of the BPF in 2018.
- Also calls to "*Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.*"

PARIS CALL
FOR TRUST AND SECURITY
IN CYBERSPACE
11 • 12 • 2018

Key learnings of the BPF 2018

- The **importance of norms** as a mechanism in cybersecurity for state and non-state actors to agree on a responsible way to behave in cyberspace, given that the speed of legislation often struggles to keep up with the pace of changes in the sphere of cybersecurity. In addition to the development of norms, it is important that **stakeholders continue to focus on mechanisms for norms implementation**, to ensure their effectiveness.

Key learnings of the BPF 2018

- **The importance of multi-stakeholderism** – threats to cybersecurity impact governments, private companies and people. There are a number of helpful norms, on different aspects and from various parts of the world, but more needs to be done to involve non-state stakeholders in the development and implementation of norms. It should also be noted that there are several norms developed and proposed by nonstate actors, which do not always get the same level of attention.

Key learnings of the BPF 2018

- **Cybersecurity norms and laws should be respectful of human rights**, and not stray into areas such as freedom of expression and control of content online. It is important to separate the security of the infrastructure, which this BPF is focused on, from questions of content shared online.

How to contribute

- **Read the BPF on Cybersecurity final output at:**
  - https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-1
- **Share your thoughts** on our mailing list for public discussion at https://intgovforum.org/mailman/listinfo/bpf-cybersecurity_intgovforum.org
- If the BPF is renewed for 2019, the mailing list will be the right place to learn about the new topic, and contribute.

Contact us

- **BPF on Cybersecurity 2018 conveners**
  - Markus Kummer, kummer.markus@gmail.com
  - Ben Wallis, bewallis@microsoft.com
- **UN Consultant:** Wim Degezelle, wdegezelle@drmv.be
- **BPF Lead Expert:** Maarten Van Horenbeeck, maarten@first.org