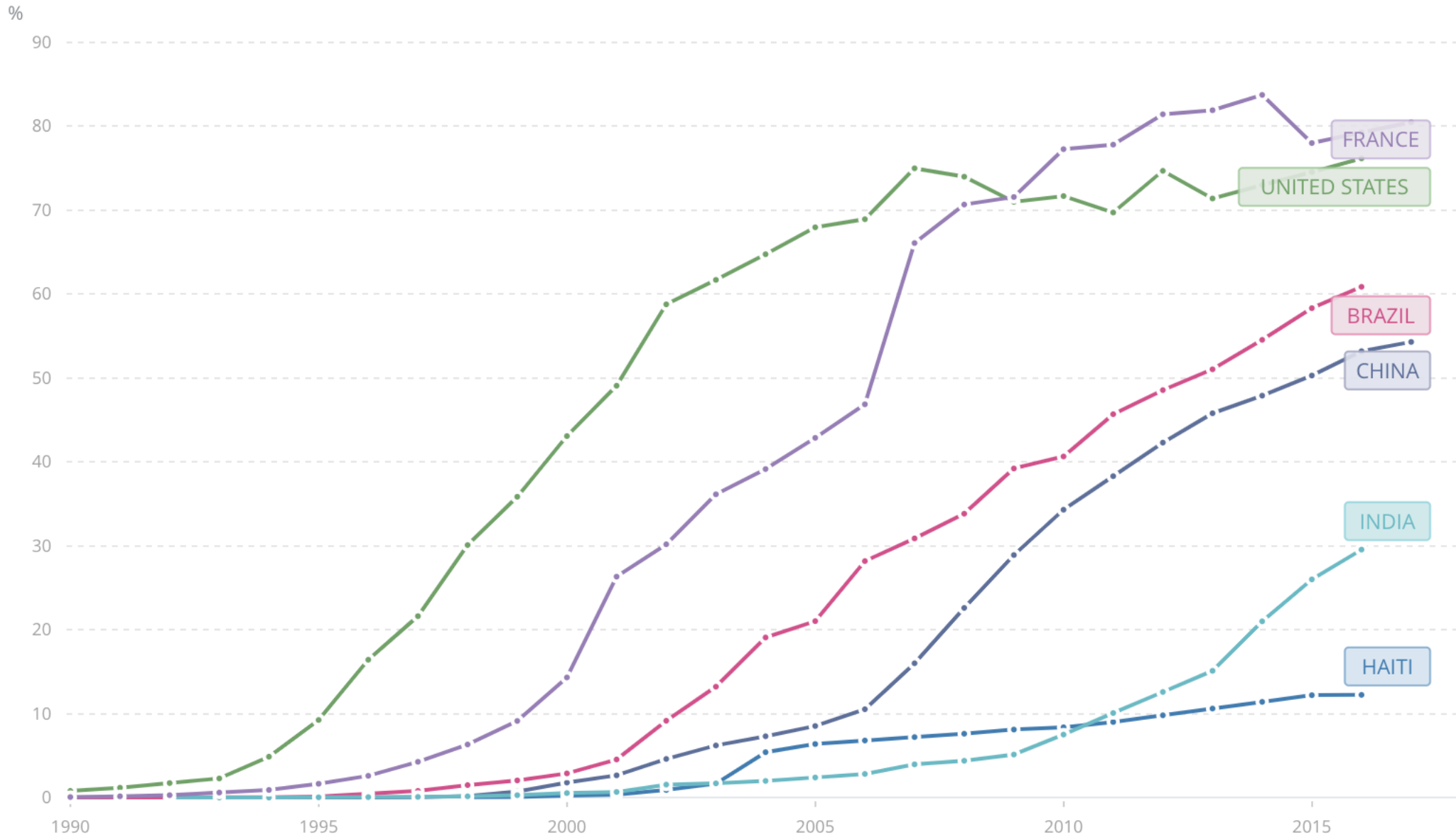# BPF on Cybersecurity

An overview as of November 2019

Internet Governance Forum

Agenda

- What is the **Internet Governance Forum**?
- **Intersessional work**: the Best Practices Forums
- **History of the BPF on Cybersecurity**
- Cybersecurity **culture, values and norms**
- How to **get involved**

FRANCE

UNITED STATES

BRAZIL

CHINA

INDIA

HAITI

90

80

70

60

50

40

30

20

10

0

%

1990   1995   2000   2005   2010   2015

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 | 2019
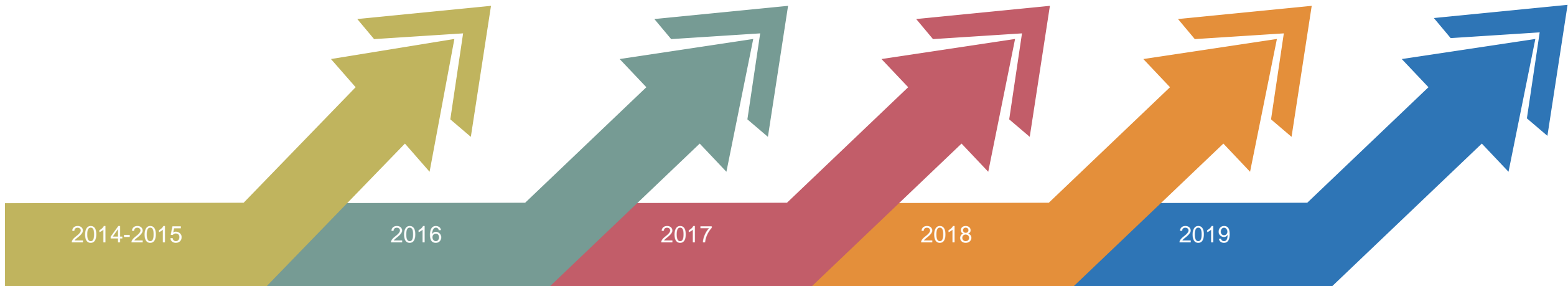
BPF on CSIRT (+ BPF Unsolicited Communications)

- What are CSIRT?
- What conditions make CSIRT successful?
- Involvement of CSIRT in policy discussions
- The evolving role of CSIRT

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
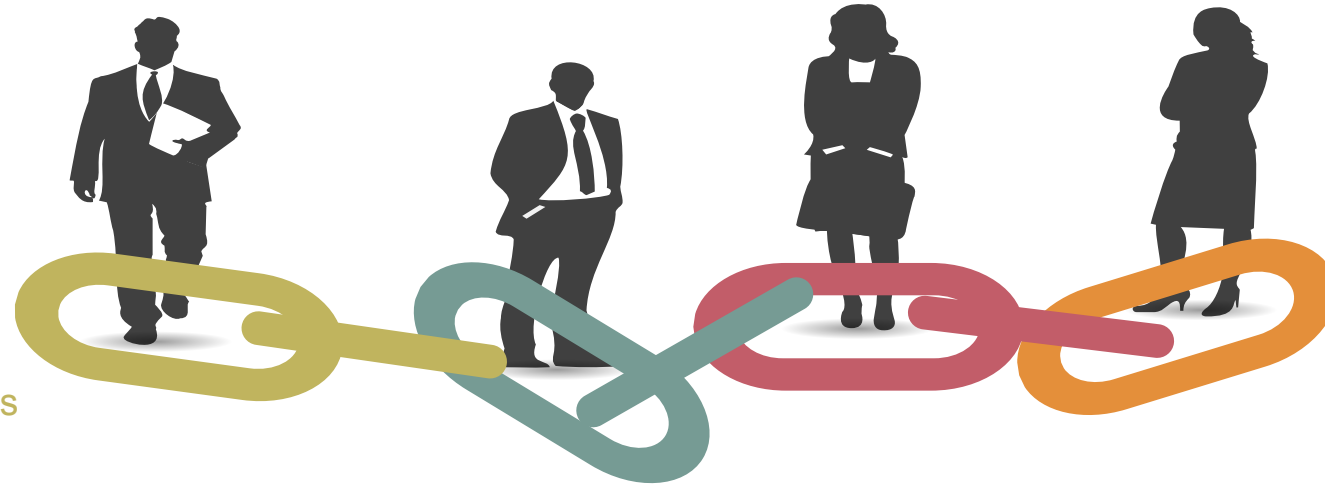- Policy Best Practices to help bring the Next Billion Internet users online safely

BPF on Cybersecurity

- Culture, Norms and Values.
- Norms development mechanisms

BPF on Cybersecurity

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

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)

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
  - 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** 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
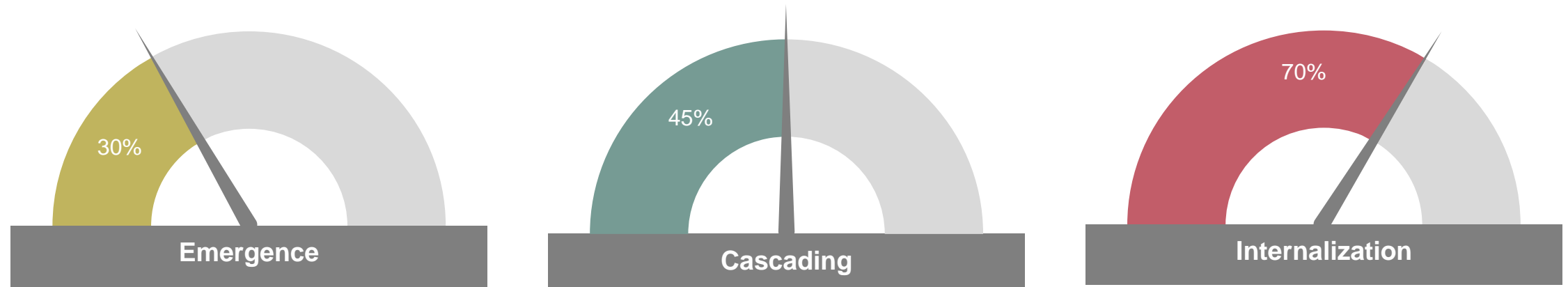
Where do norms originate?

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

When or where there's **no real universal implementation of a norm**, or if the **implementation of the norm has unintended consequences**, or has different impacts in a different context (e.g. those with and those without effective rule of law), it may result in a group of "haves" and "have nots" in terms of the protection the norms offer. Security controls will be sufficient or meaningful in some parts of the world, and not in others.

BPF on Cybersecurity (2019)

- Focus on **identifying best practices related to implementation of the different elements** of cyber norms, agreements and initiatives.

- The BPF published a **research paper** covering 19 agreements, including the UNGGE Consensus Norms, Paris Call, MANRS and others.

- Two phases of work:
  1. **Identifying relevant initiatives and agreements**, determining whether they were legally binding or not, and identify commonalities.
  2. **Call for examples of Best Practices** related to implementation of the agreements.

How to contribute

- **Read our preparatory paper**
  - https://www.intgovforum.org/multilingual/content/bpf-cybersecurity

- **Review our Call for Contributions**
  - https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-2019-contributions

- Call for Contributions is closed, but **share your thoughts** on our mailing list for public discussion at https://intgovforum.org/mailman/listinfo/bpf-cybersecurity_intgovforum.org

Join our BPF session @IGF2019

Best Practice Forum on Cybersecurity – session @IGF2019

Wednesday 27 November, 2019

15:00 – 16:30 UTC+1

- Join in person @IGF2019 in Berlin, Estrel Saal C
  https://igf2019.sched.com/event/SU3p

- Participate Remotely
  [check the IGF website closer to the meeting for Remote Participation details]

Questions and answers

- **BPF on Cybersecurity conveners**
  - Markus Kummer
  - Ben Wallis
- **UN Consultant:** Wim Degezelle
- **BPF Lead Expert:** Maarten Van Horenbeeck, maarten@first.org