BPF on Cybersecurity

Report on the BPF activities 2016-2018

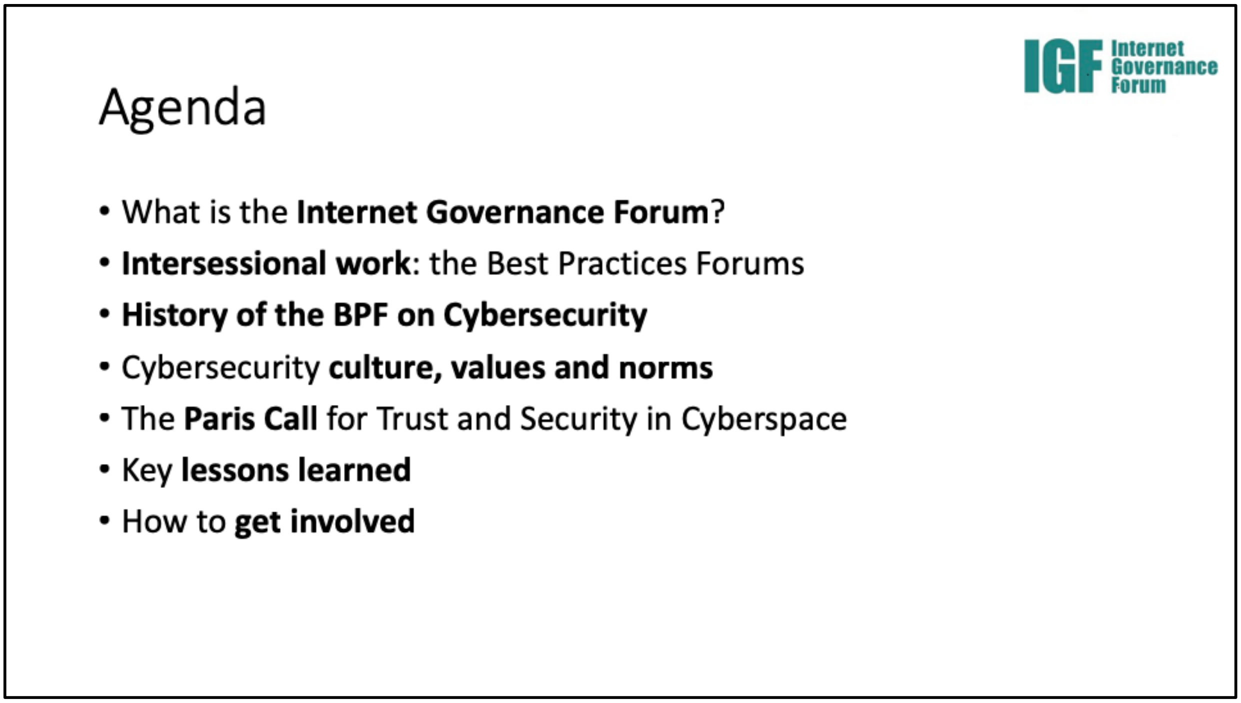
Internet Governance Forum

IGF Internet Governance Forum

The Internet of Trust

INTERNET GOVERNANCE FORUM
PARIS, 12–14 NOVEMBER 2018

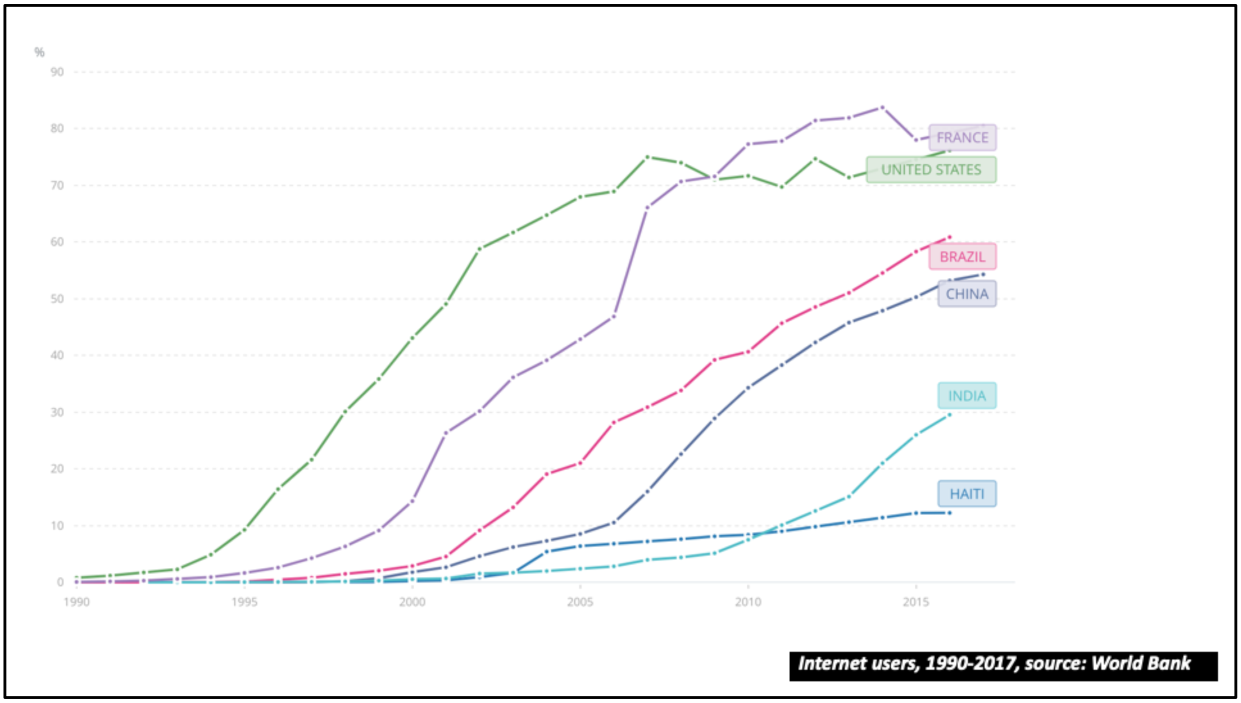
This deck introduces the Best Practices Forum on Cybersecurity, an intersessional activity of the Internet Governance Forum which has been organized since 2016.



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**

In this deck we'll cover the basics around how the IGF came to be, what the Best Practices Forums aim to achieve. We'll go into more detail on the BPF on Cybersecurity, and do a deep dive into the BPF in 2018, which focused on Cybersecurity culture, norms and values. You'll also learn how to get involved!



Internet users, 1990-2017, source: World Bank

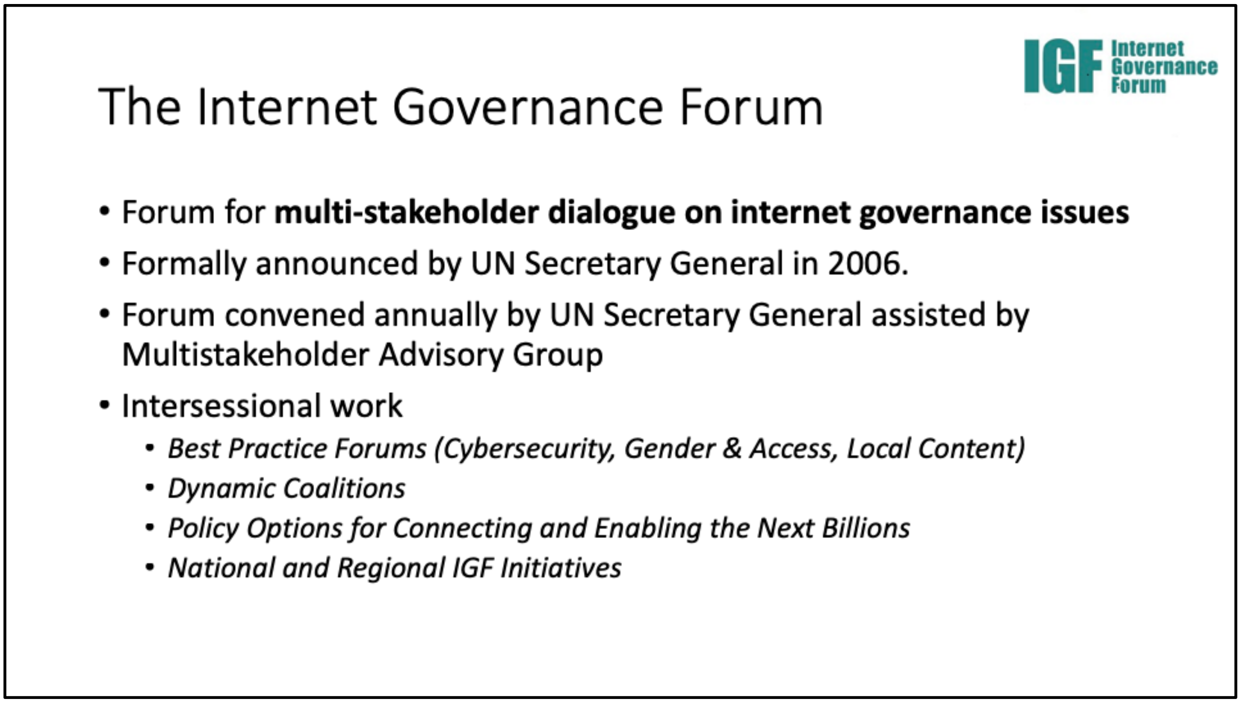
The internet has been growing rapidly.

In 2005, 67% of the US population was online. In 2010, it was 71%, and today, 76%. That’s almost flat growth. If you look internationally though, in 2005, we had 15% of people online, in 2010 that was 28%, and today it is 45%. Each of those people comes from a different cultural understanding, different education perspective, and with different needs. Hence there’s a lot more misunderstanding today around what an acceptable level of cybersecurity really means.

There’s a need for spaces where people from each of these backgrounds can come together and share their existing best practices, especially from a policy perspective.

Multistakeholderism

Enter the idea of “multistakeholderism”. It was introduced as the most important principle in the Tunis Agenda for the Information Society in 2006, and is typically used to describe the cooperation of representatives in the *‘government, private sector, civil society and technical community’* as they contribute to governing a particular space, such as the internet. No single player can, or should for that matter, control all aspects of the internet, but they each have a role to play in discussing, decisionmaking and implementation of what the network looks like.



IGF Internet Governance Forum

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*

The Internet Governance Forum (IGF) is convened by the Secretary-General of the united Nations as a global forum to discuss policy issues pertaining to the Internet.

It was officially announced in 2006, and has taken place annually since. The UN Secretary General is assisted by a Multistakeholder Advisory Group (MAG), which he establishes from the IGF community.

The IGF is today a major internet conference, with over 2,000 attendees annually. During the event, workshops and meetings are organized for different stakeholder communities to connect on challenging topics of the internet, such as cybersecurity, privacy, local content, gender and access, and many more.

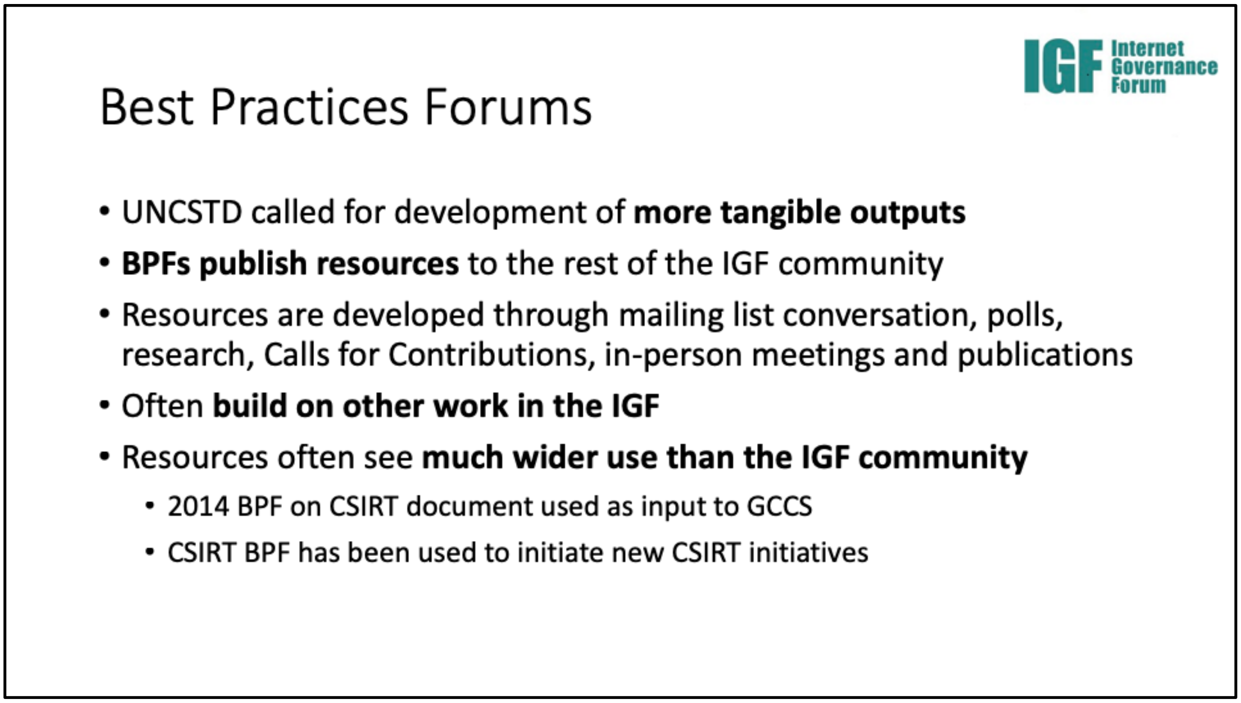
In order to continue to contribute throughout the year, rather than just during one week, the IGF also establishes intersessional work activities, which include Best Practice Forums, Dynamic Coalitions and National and Regional IGF initiatives.

Best Practice Forums, also known as BPFs offer substantive ways for the IGF community to produce more concrete outcomes. While BPF outcomes have already been useful in informing policy debates, they are also viewed as iterative materials that are not only flexible but also ‘living’ in the sense that they can be updated at any time to accommodate the pace of technological change faced by internet policymakers. BPFs have the freedom to define their own methodologies; tailored to each theme’s specific needs and requirements.

Dynamic Coalitions (DCs) are They are informal, issue-specific groups comprising members from various stakeholder communities. DCs welcome collaboration with anyone interested in contributing to their activities.

The IGF intersessional work focused on the Policy Options for Connecting and Enabling the Next Billion(s) is a community-driven process started during the IGF 2015 preparatory cycle, identifying policy options for connecting the next billion(s) of internet users – with a different focus each year. In 2018, the focus was on showing how connecting the next billion(s) helps support the Sustainable Development Goals (SDGs).

The National and Regional IGF Initiatives (NRIs) are the Internet Governance Forums organized on a national basis in different countries, or on a regional or sub-regional level, depending on the size of the geographic area, where the main criteria for identifying region is geography, but also in some cases mutual language and culture.



Best Practices Forums

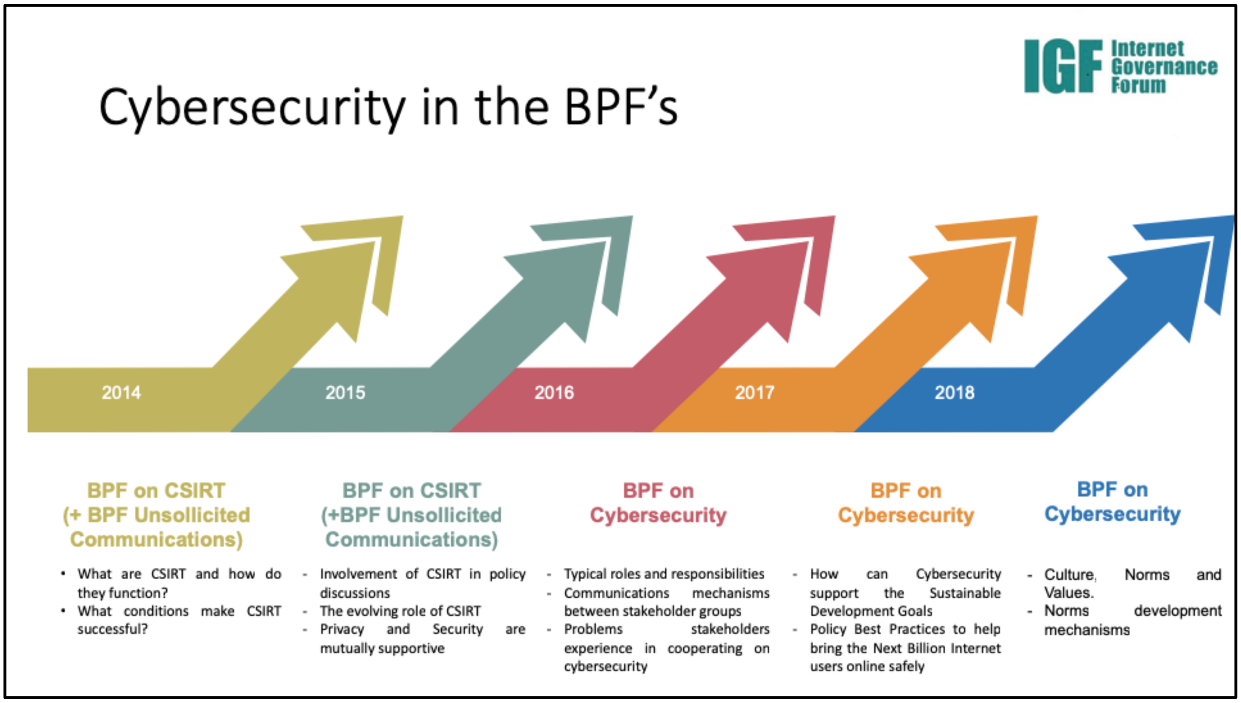
IGF Internet Governance Forum

- 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

As mentioned, the BPFs were established to help the IGF develop more tangible outputs, and they identify and collected Best Practices in various areas, publishing them to the IGF community.

They commit to their work through mailing list conversations, polls, research, Calls for Contributions, in-person meetings, on-line meetings and publications. They often also build on other work in the IGF. For instance, several BPFs have aligned with the Connecting and Enabling the Next Billion(s) intersessional activities over the years.

The resources from the BPFs are often used much more widely than the IGF community. For instance, the 2014 BPF on Computer Security Incident Response Teams (CSIRT) outcome paper was used as input reading for attendees to the Global Conference on Cyberspace in 2015. In addition, new CSIRT have used that year’s paper to help establish their work programs.



Cybersecurity in the BPF’s

IGF Internet Governance Forum

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

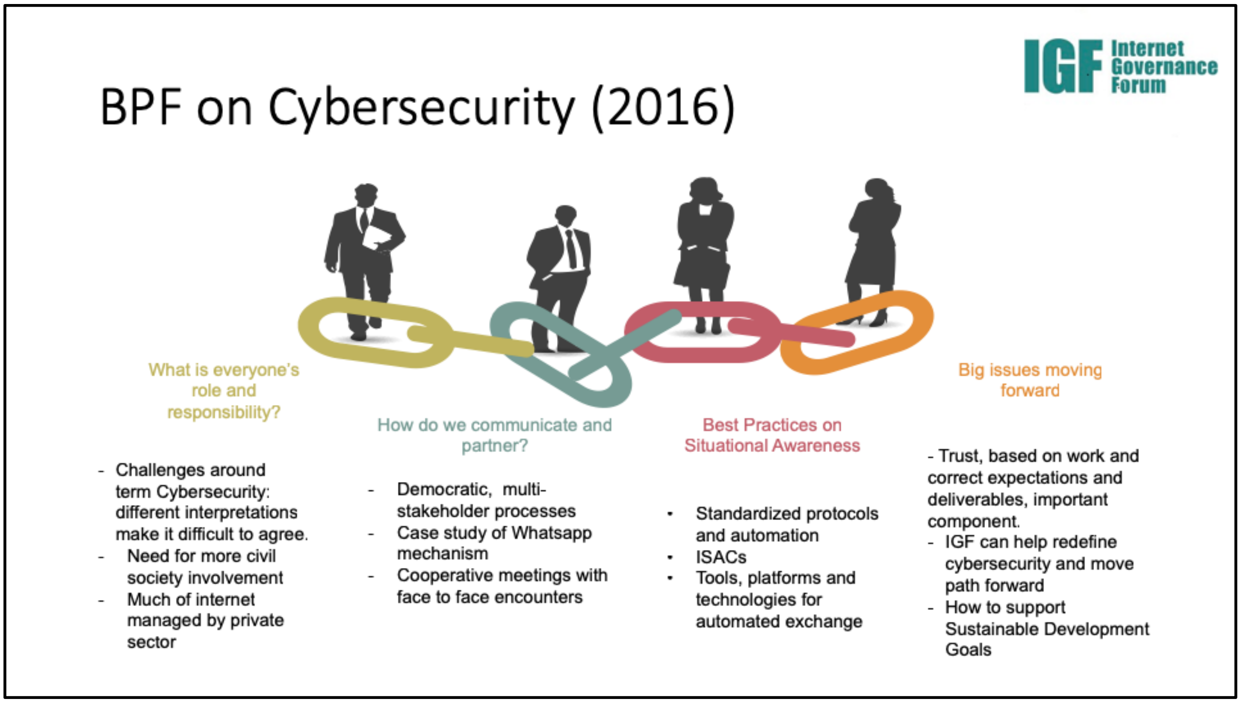
BPF on Cybersecurity

- 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

Since 2014, the IGF has operated a Best Practices Forum focused on cybersecurity. In 2014-2015, the BPF worked on identifying Best Practices in Regulation and Mitigation of Unsolicited Communications and Establishing Incident Response Teams for Internet Security. Later, the BPF has been focused on cybersecurity; identifying roles and responsibilities and ongoing challenges in 2016, and identifying policy best practices in 2017.



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

Various stakeholder communities have different definitions of ”cybersecurity”, and different understandings of who needs to get involved. A common challenge has been that the term was mostly used by governments.

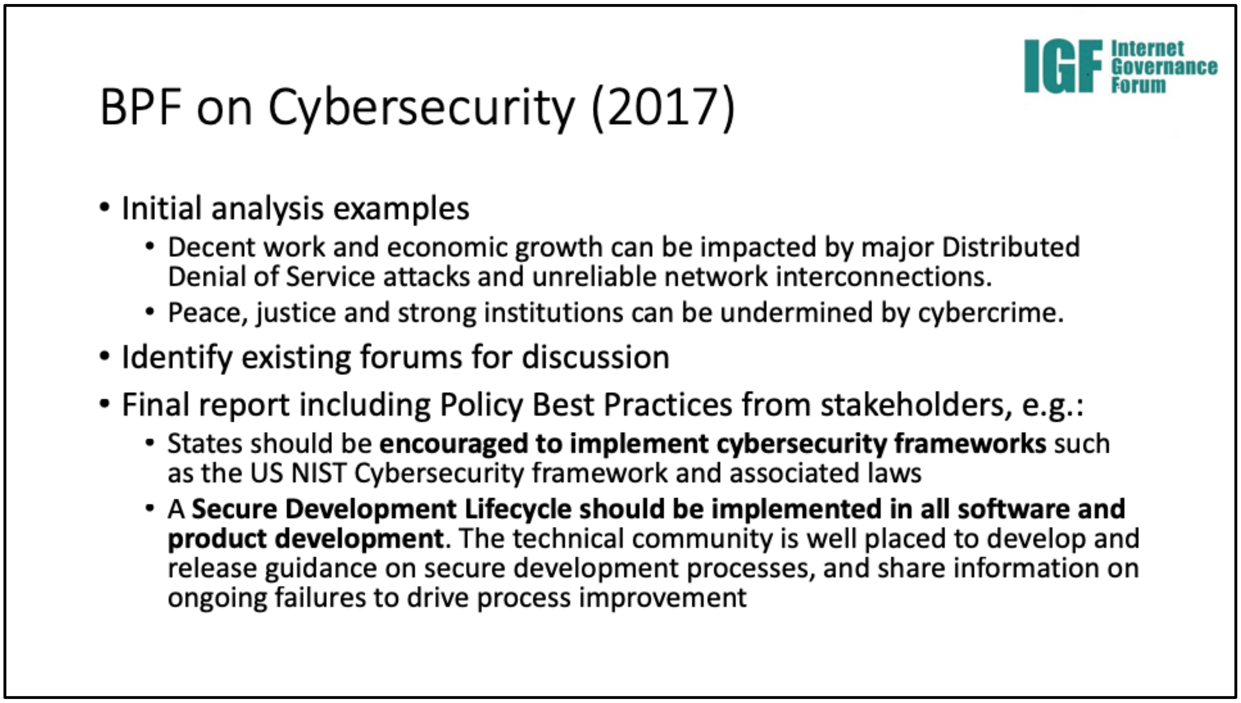
The BPF worked to address this issue by focusing on four key questions:

- What is everyone’s role and responsibility in cybersecurity?
- How do stakeholder groups communicate and partner with eachother?
- What best practices exist around the world to establish situational awareness?
- What big issues moving forward is the BPF well placed to help tackle?

BPF on Cybersecurity (2017)

IGF Internet Governance Forum
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

In 2017, the BPF worked to identify cybersecurity policy statements from around the world that could help cybersecurity contribute to the Sustainable Development Goals. As a group, we wanted to learn what policies could help establish better cybersecurity, and what would negatively affect the cybersecurity environment.



IGF Internet Governance Forum

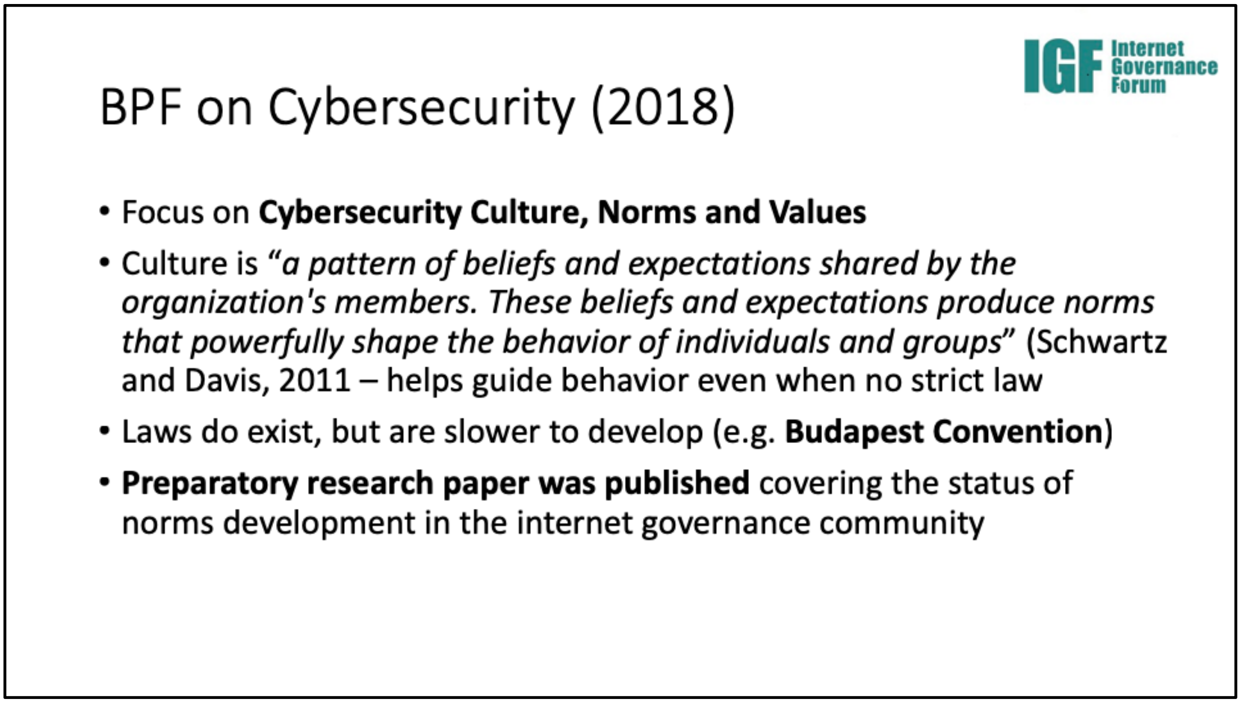
BPF on Cybersecurity (2017)

- 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

We started this effort by conducting initial analysis using two subject matter experts of the SDGs, and identify how they could be affected by various cybersecurity efforts. We also reviewed policy options identified by the CENB effort, and reviewed how cybersecurity could negatively affect the implementation of those options.

This was then followed by a Call for Contributions, and the publication of a report with Best Practices. Two examples included the recommendation that states should implement cybersecurity frameworks that make security understandable to a wide variety of audiences – and stakeholders, in particular those in the technical community should endorse and support the implementation of a Secure Development Lifecycle in software development organizations.

A much wider set of policy recommendations is included in the BPF's final output paper. During our meeting at the IGF in Geneva, these were reviewed with a wide set of experts, including representatives from the Shadowserver Foundation, the Global Commission on the Stability of Cyberspace and the Association for Progressive Communications.



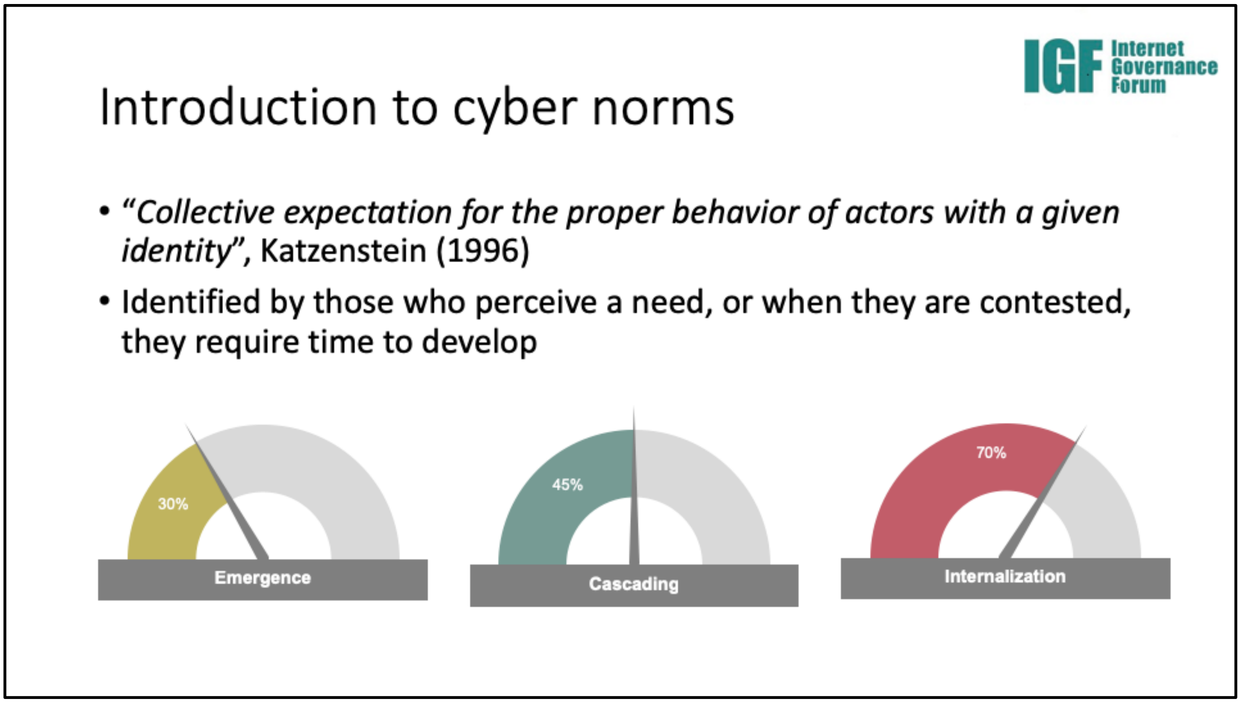
BPF on Cybersecurity (2018)

- 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

In 2018, the BPF explored the topic of "cybersecurity culture, norms and value".

As part of its work in 2017 the BPF consulted with the community on what areas would benefit from further stakeholder conversation and a possible way forward for the BPF. Two areas surfaced 'Defining and identifying a cybersecurity culture, norms and values,' and 'Identifying the risk of a potential digital security divide, between those who have and those who do not have access to cybersecurity measures'. This lead to the formulation of the proposal for a BPF on cybersecurity in 2018, which was confirmed by the IGF Multistakeholder Advisory Committee (MAG).

We started off with a study by several members in the BPF community. Together, this group drafted a paper that covered the basic ideas behind culture, how it applies to cyber, and how norms development can help create a positive culture that encourages responsible behaviors. We identified that while laws existed in cybersecurity, or at least cybercrime, such as the Budapest convention, they were slower to develop – for instance, work on the Budapest convention started in earnest in 1997, with entry into force in 2004, and national ratifications still ongoing today.

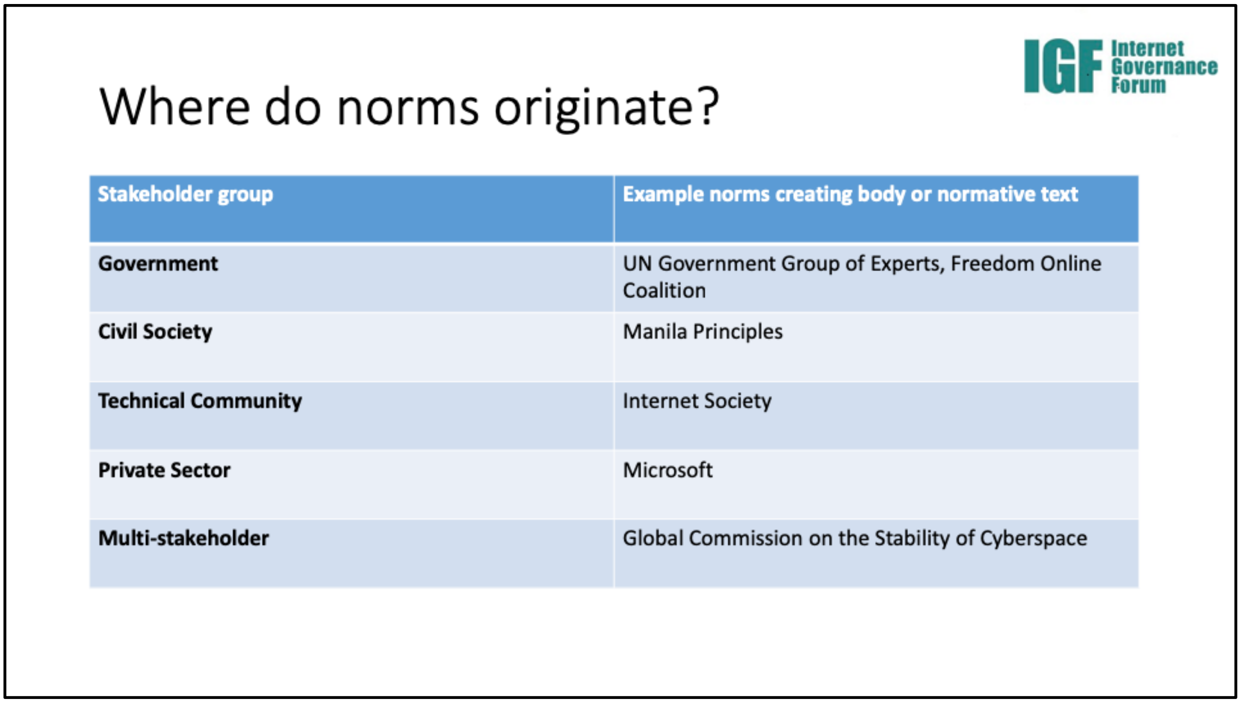


Introduction to cyber norms

- "*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

30%
Emergence
45%
Cascading
70%
Internalization

We used a social science definition of norms for our work, which originated with Katzenstein in 1996. Norms are typically identified by those who perceive a need, or when they are contested by others. In norms development, we see emergence of norms first, followed by them cascading through the system, where multiple states or other stakeholders adopt them. Finally, we see norms internalization, where states who have adopted the norm implement programs and processes to make sure they are effectively operated, and can be used to call out others who do not comply.



Where do norms originate?

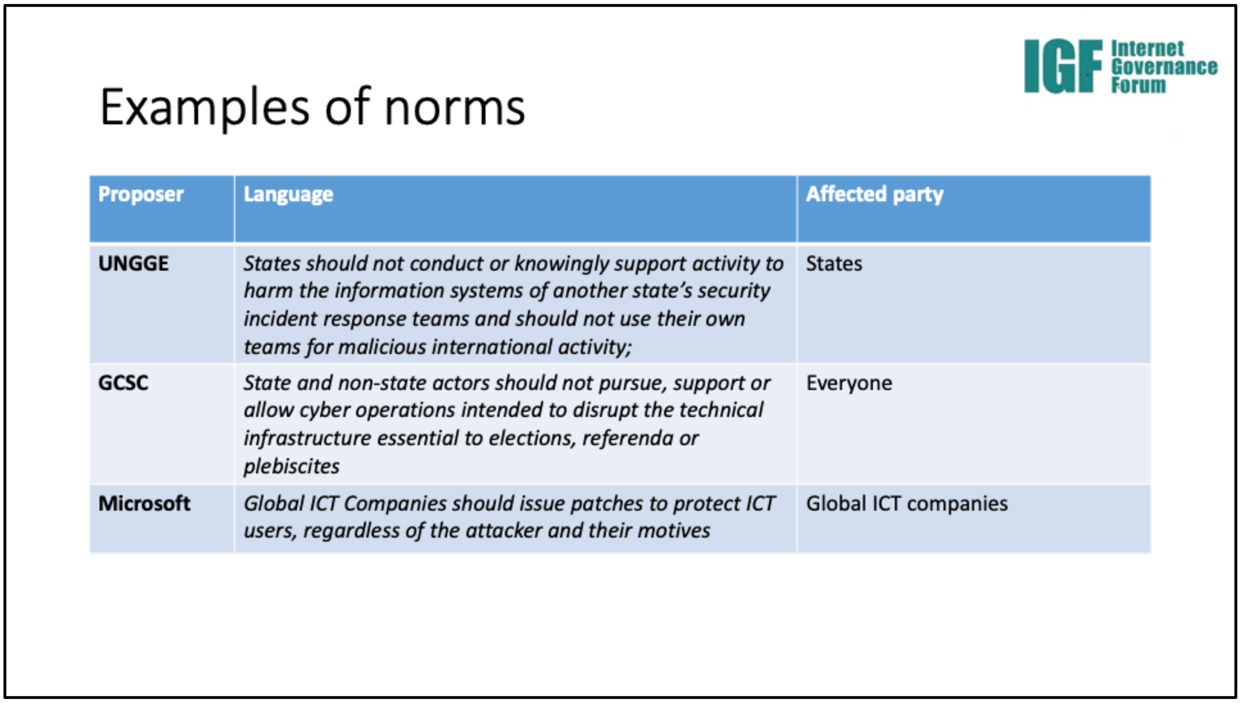
Stakeholder group	Example norms creating body or normative text
Government	UN Government Group of Experts, Freedom Online Coalition
Civil Society	Manila Principles
Technical Community	Internet Society
Private Sector	Microsoft
Multi-stakeholder	Global Commission on the Stability of Cyberspace

Norms can operate form a wide variety of stakeholder communities, and this slide lists out some examples of norms developing bodies.

the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security is a UN mandated group of experts which has been established five times since 2004. It is convened under the UN's First Committee. The GGE will meet for four one-week sessions. When consensus is reached, the group publishes an outcome report, which has happened in 2010, 2013 and 2015. In particular the 2013 and 2015 edition discussed norms development, with the 2015 report offering a proposal for voluntary cybersecurity norms. Outcomes and inputs to the UNGGE process have been echoed by other bodies, showing some level of adoption.

Global Commission on the Stability of Cyberspace (GCSC): initiated by two independent think tanks, The Hague Centre for Strategic Studies (HCSS) and the EastWest Institute (EWI), the GCSC consists of 26 prominent Commissioners from a variety of regions and stakeholder groups, and legitimacy in different aspects of cyberspace. Its aim is to help promote mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity. As a group, it has proposed a number of norms for responsible behavior in cyberspace.

The Manila Principles on Intermediary Liability were developed by several Civil Society groups including the Electronic Frontier Foundation and Article19. They are a set of standards for censorship and takedown laws.

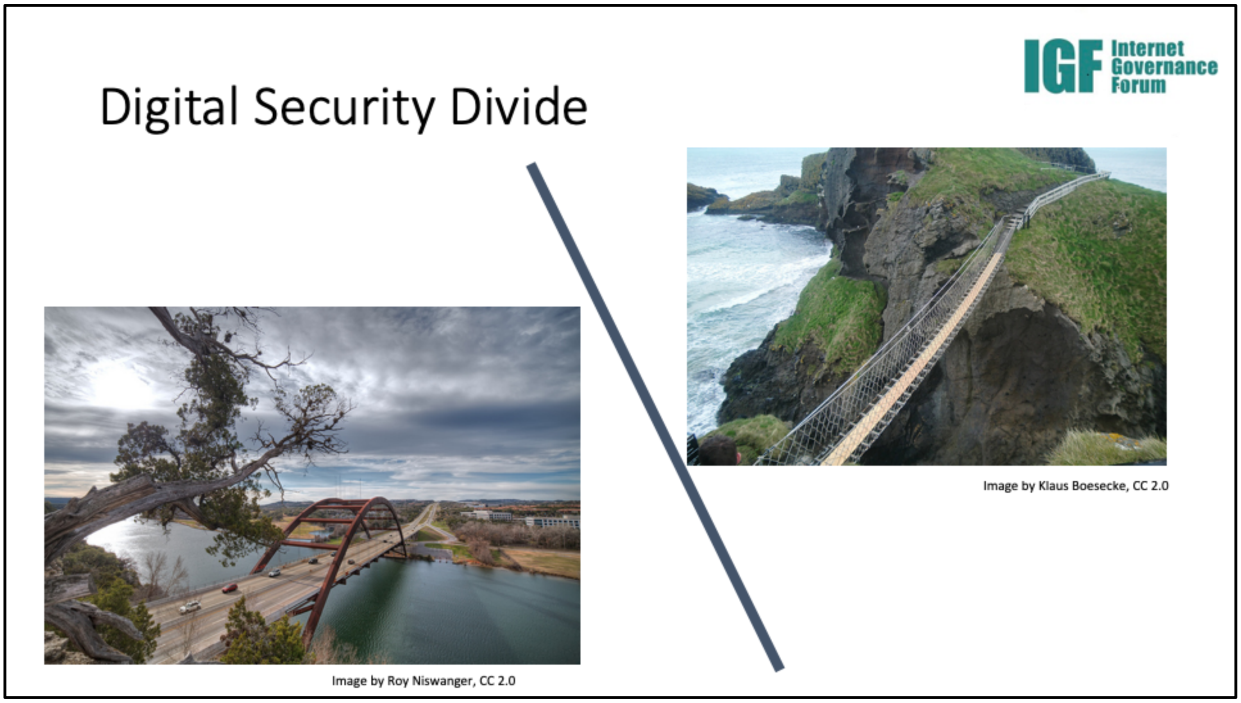


IGF Internet Governance Forum

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

These are a few examples of norms developed by these individual bodies that have either seen adoption or widespread discussion. They are only a small subset of the norms that currently exist. Our final report contains a wider variety of norms from each stakeholder community.



Digital Security Divide

IGF Internet Governance Forum

Image by Klaus Boesecke, CC 2.0

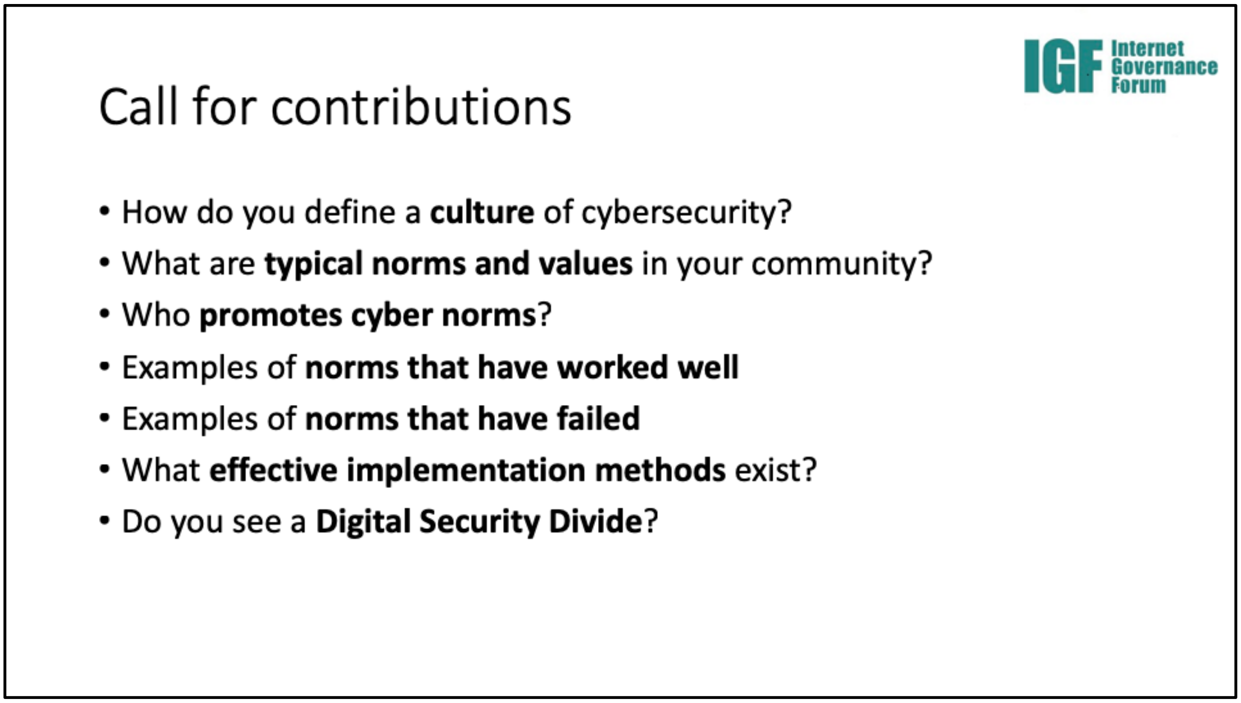
Image by Roy Niswanger, CC 2.0

We were also interested in learning more about how when or where there’s no real universal implementation of a norm, or if the implementation of a 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. We called this a “Digital Security Divide”, a concept first coined by the Internet Society.

Much like other infrastructure, such as bridges, unequal development can lead to specific users being more or less affected by security issues.

Stakeholder groups often have the ability to mitigate or increase these gaps through coordinated action. For example, if a state implements data protection laws and has competent data protection authorities in place, people will be exposed to less risk irrespective of their own skills and knowledge. Governments can also contribute to digital insecurity of individuals by requiring them to provide their biometric data in order to gain access to critical public service, and not managing this data in a secure manner.

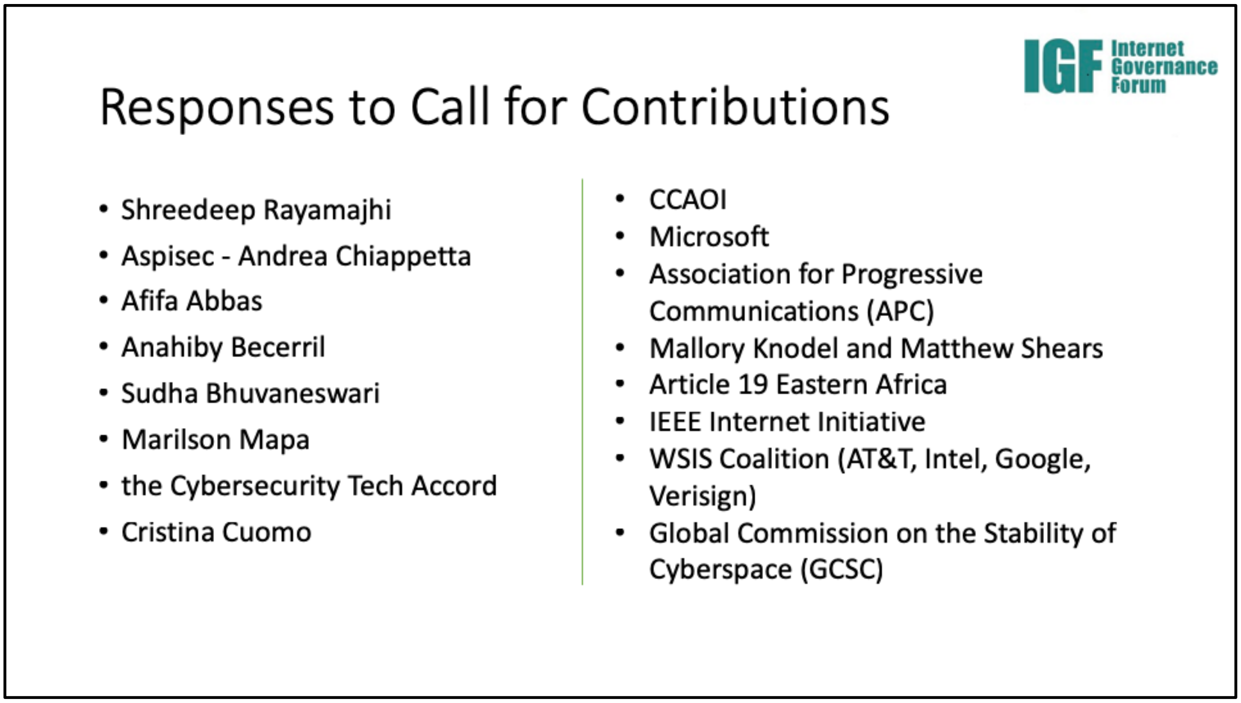
Our group also determined that other issues, such as the lack of protection for minorities, can be a large instigator, which can be exacerbated when a norm is only implemented for a partial set of users.



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**?

Our Call for Contributions was focused along the lines of these key questions. We were hoping to understand, from the perspective of each stakeholder community, how they see development of norms, whether they have best practices around implementation processes, and where those failed and succeeded. We were also looking to understand their view on the concept of the Digital Security Divide.

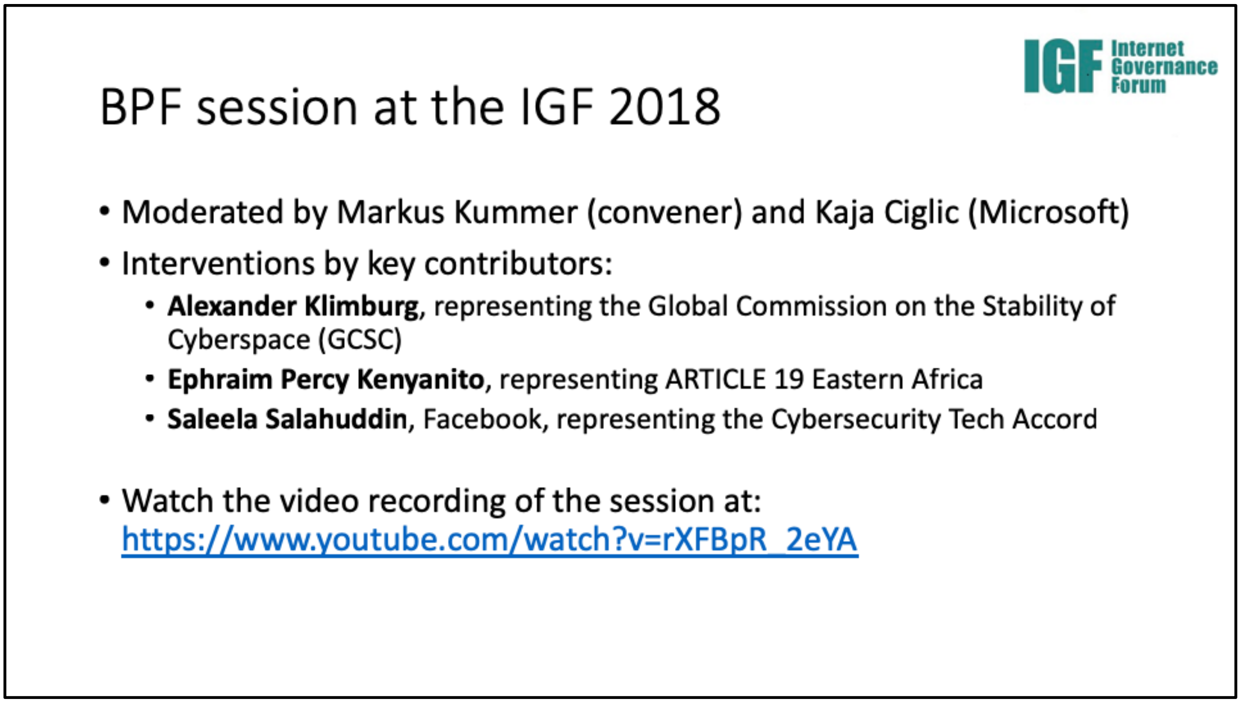


Responses to Call for Contributions

- 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)

We received 16 responses to our Call for Contributions, with a wide variety of respondents across civil society, the technical community and private sector. We did not see significant submissions from governments in this year.

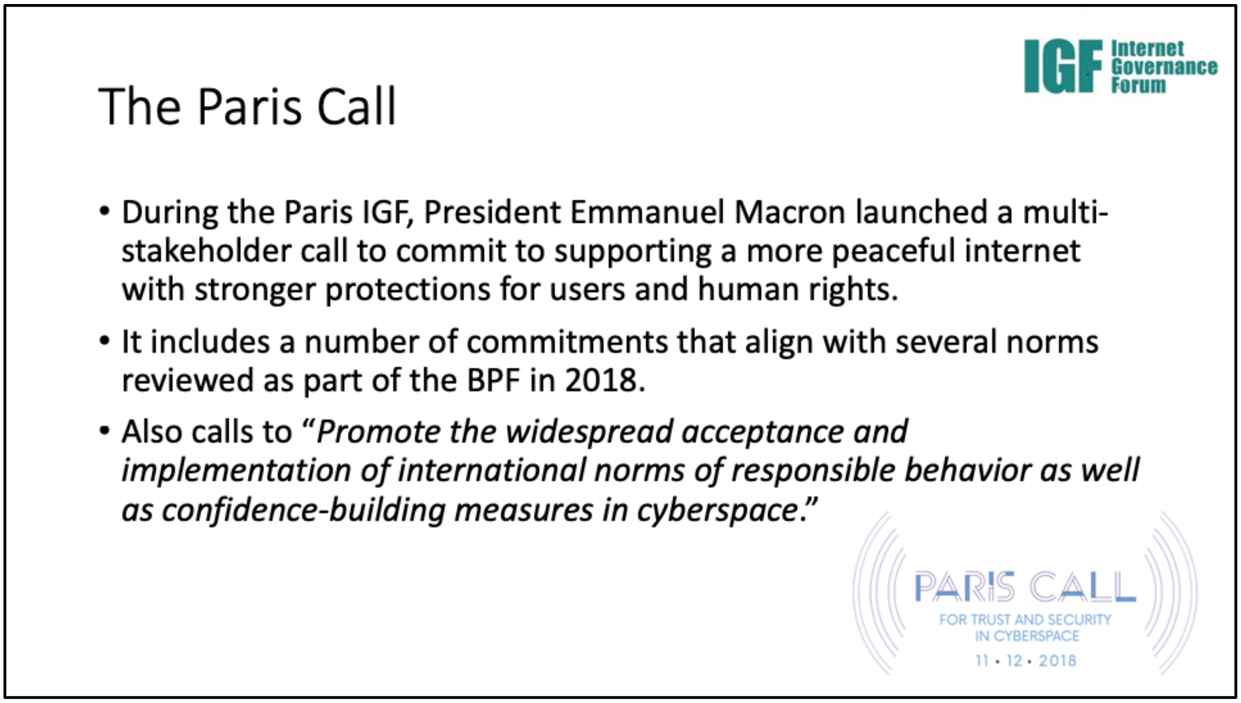


BPF session at the IGF 2018

- 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 BPF met in person at the IGF in Paris, with interventions by representatives from the Global Commission on the Stability of Cyberspace (GCSC), a multi-stakeholder norms development body. In addition, Ephraim Percy Kenyanito represented civil society, in particular ARTICLE 19 from Eastern Africa, and Saleela Salahuddin represented the Cybersecurity Tech Accord. Each of these participants introduced their submission to the BPF, and how it represented their stakeholder community.

A video of the session is available on YouTube at https://www.youtube.com/watch?v=rXFBpR_2eYA.



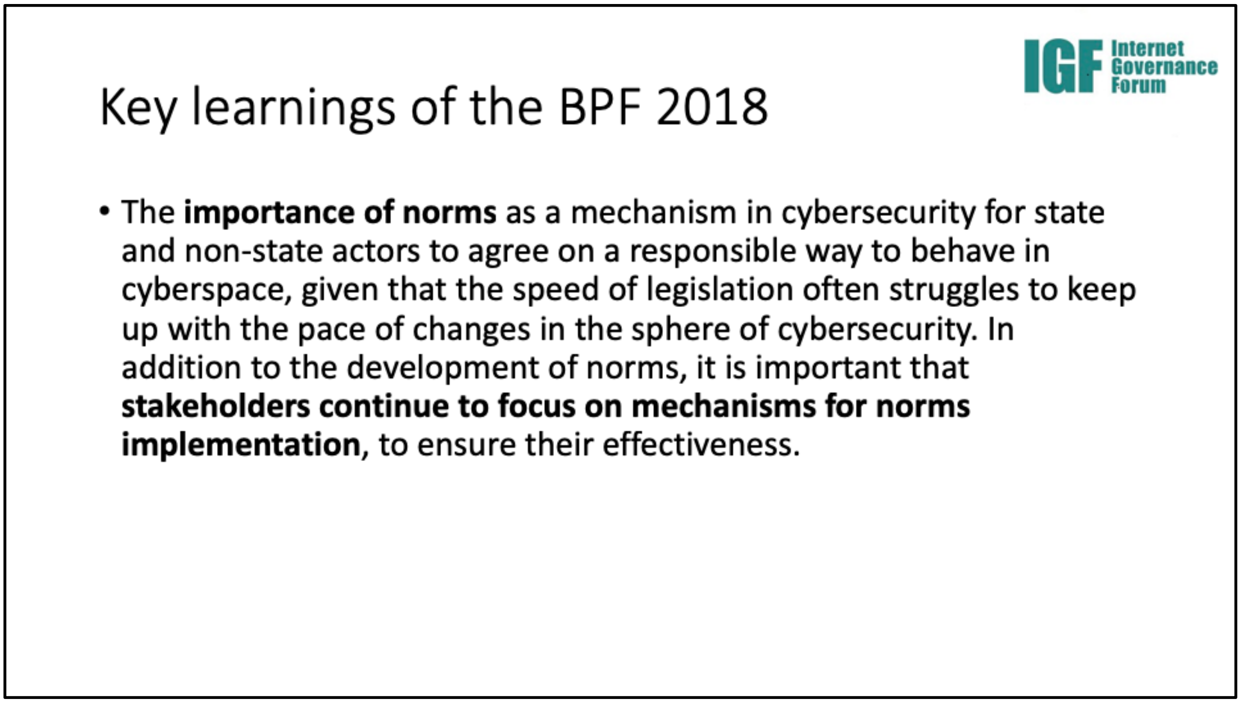
The Paris Call

- 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

During the IGF, President Emmanuel Macron launched the Paris Call, a multi-stakeholder call to commit to supporting a more peaceful internet with stronger protections for users and human rights. Its participants commit to working together to:

- increase prevention against and resilience to malicious online activity;
- protect the accessibility and integrity of the Internet;
- cooperate in order to prevent interference in electoral processes;
- work together to combat intellectual property violations via the Internet;
- prevent the proliferation of malicious online programmes and techniques;
- improve the security of digital products and services as well as everybody’s “cyber hygiene”;
- clamp down on online mercenary activities and offensive action by non-state actors;
- work together to strengthen the relevant international standards.



IGF Internet Governance Forum

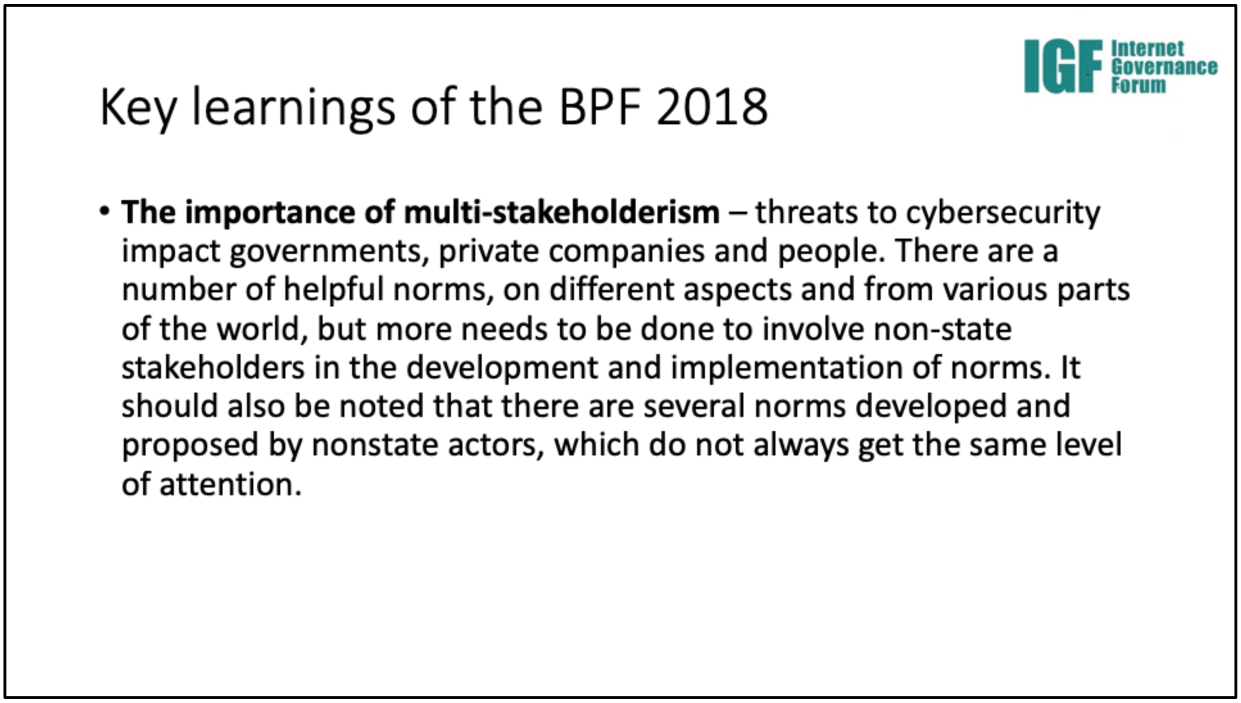
Key learnings of the BPF 2018

- 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.

At the conclusion of the 2018 process, we identified three key learnings. More detailed learnings are included in the output document, which consists of our research paper, our Call for Contributions, and notes from the session at the IGF in Paris.

The three key takeaways are:

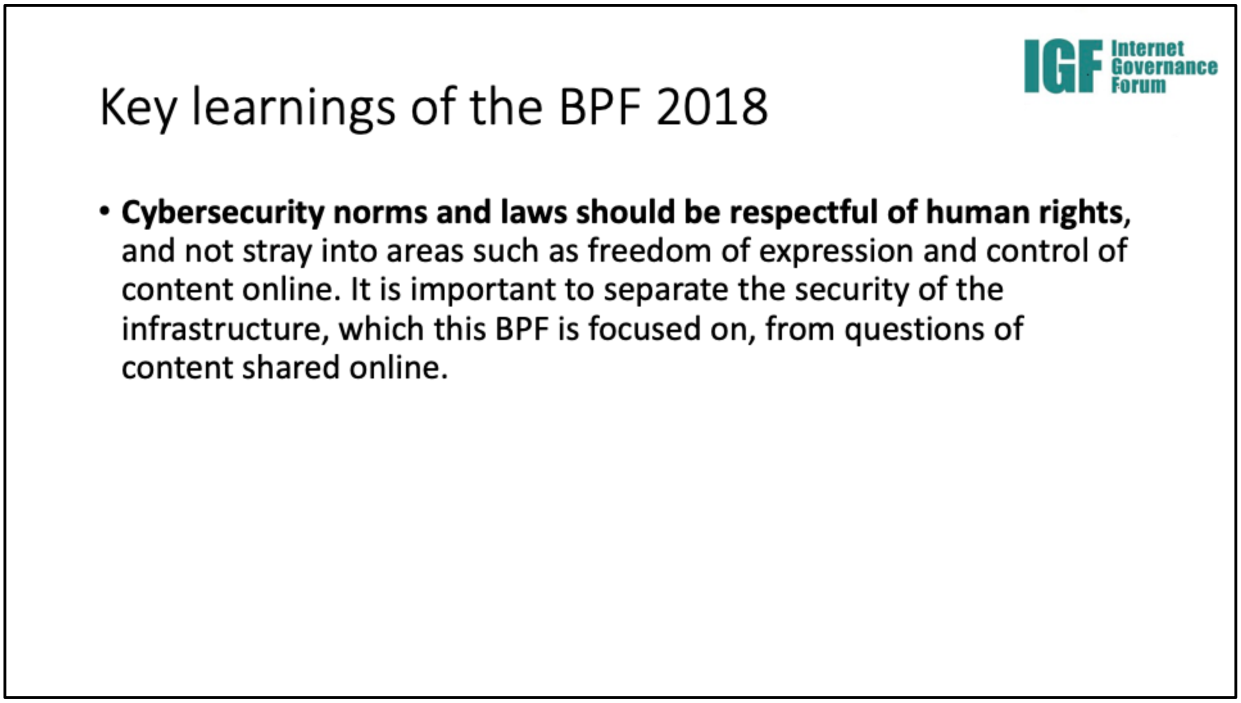
- That norms are an important part of getting state and non-state actors to agree on responsible ways of behavioar in cyberspace. They often fill a gap when “hard law” which be slow to innovate. In addition, norms cannot simply “exist”, they must be implemented and promoted, an area that is still nascent in its development, but important to ensure the norms see widespread adoption.



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.

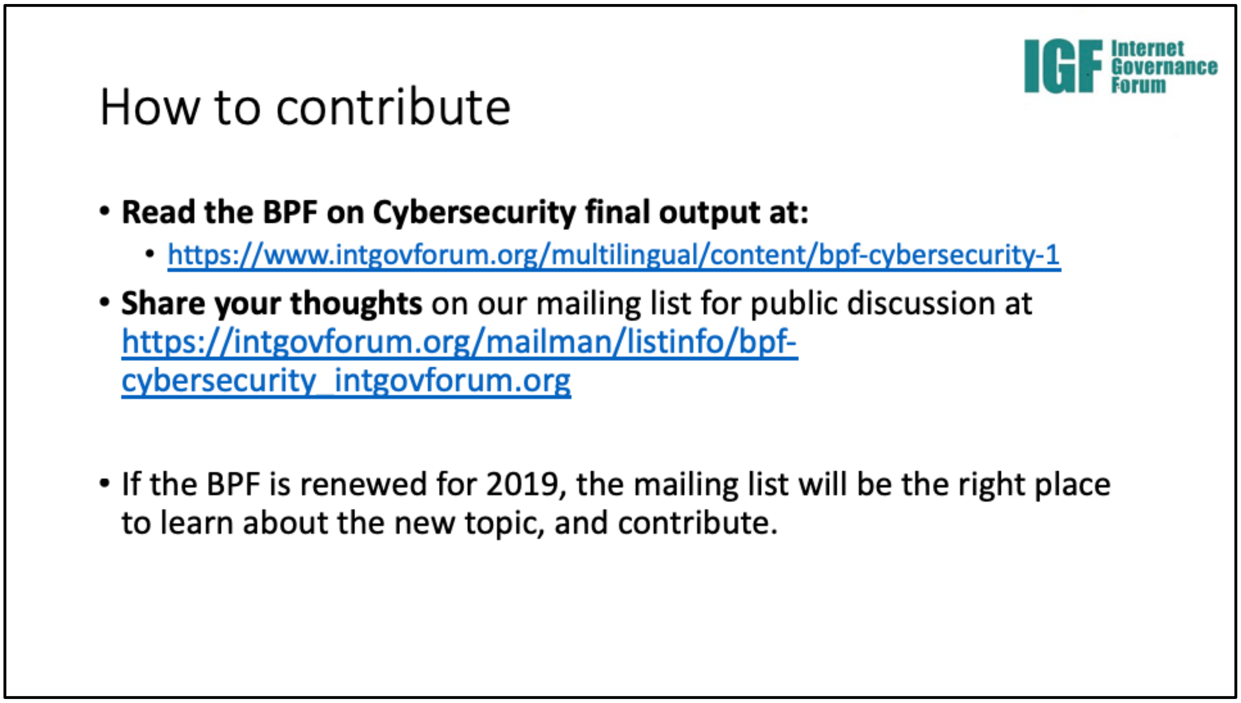
- Second, the multi-stakeholder model is important in norms development as well as internet governance. There are a wide variety of stakeholders, including the technical community (MANRS – Mutually Agreed Upon Norms for Routing Security) and civil society (the Manila Principles on Intermediary Liability) which propose and implement norms, and it’s important to recognize this is not just a state activity. These other actors often don’t get the same level of attention. There are also multi-stakeholder norms development bodies, such as the Global Commission on the Stability of Cyberspace (GCSC).



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.

- Finally, cybersecurity norms should be respectful of human rights, and be careful not to stray into freedom of expression, and controlling content online. The distinction between protecting infrastructure, and questions of content shared online, is important and should be carefully maintained and considered.

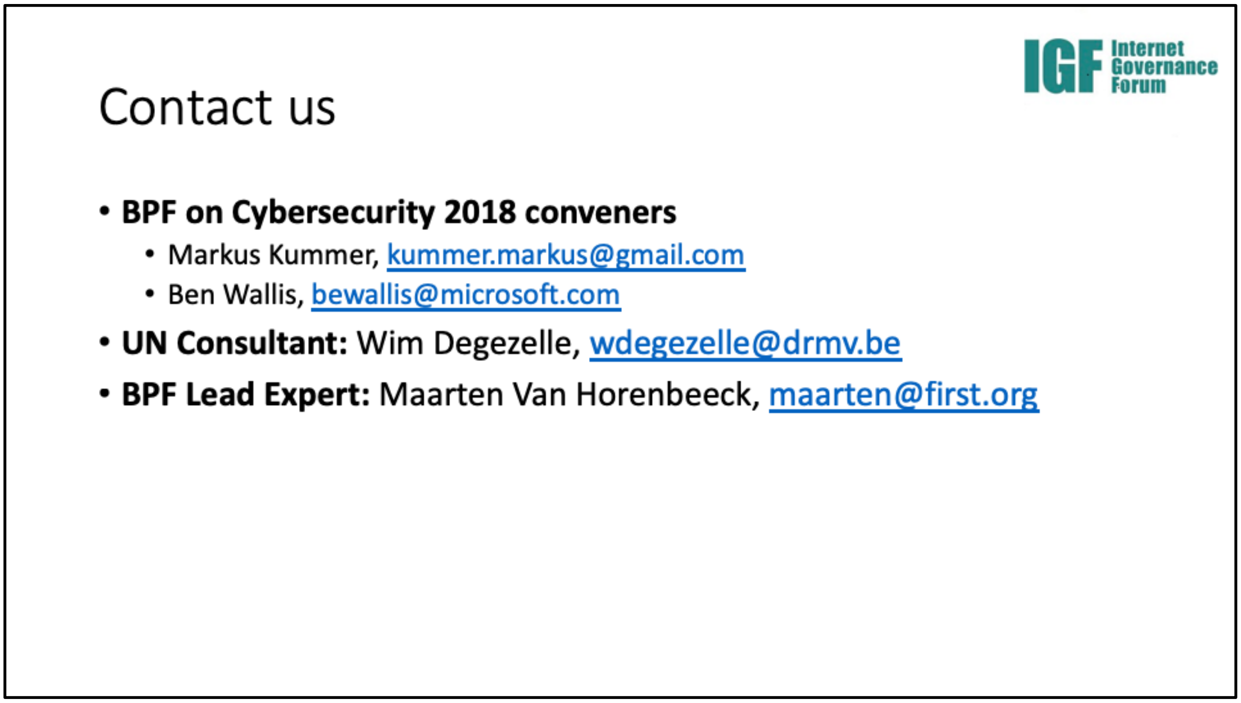


How to contribute

IGF Internet Governance Forum

- **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.

Individuals can still contribute to the BPF by reviewing our output materials, and sharing their thoughts on the mailing list. While the 2018 outcome documents won't changed, your input is still very welcome in the community. In addition, those thoughts may be taken into account if the Best Practices Forum is extended into 2019 and a new area of focus is decided.



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

If you have any further questions, feel free to contact the organizers and conveners of this year’s Best Practices Forum on Cybersecurity.