IGF 2022 Best Practice Forum

on Cybersecurity

Mythbusting: cybercrime versus cybersecurity - *Feedback on draft Paper*

On 30 August 2022, the BPF Cybersecurity published a draft paper “Mythbusting: cybercrime versus cybersecurity”.

The goal of the paper is to help stakeholders understand the key policy differences between cybersecurity and cybercrime such that their advocacy strategies can better align with a human rights centric approach to internet governance.

This document compiles the feedback on the draft paper and will feed in BPF Cybersecurity session at the IGF meeting in Addis Ababa and online (BPF CS session, 6:30-8:00 am UTC). The final version of the paper will be published after the IGF.

Myth 1: They are two sides of the same coin: Cybersecurity policy is proactive and cybercrime policy is reactive.

Feedback

- Para 2: "cybercrime is about punishing unauthorised access to such systems with criminal intent". Better to say "...punishing unauthorised interference with such systems..." as many cybercrime laws now include denial of service, data corruption, etc.

- Yes, I agree cybersecurity policy and cybercrime are two sides of the same coin. But the definition of Cybercrime is not only for unauthorized access to the computer or internet systems. That is only one of the criminal behaviors. Cybercrime can also be people who use the internet to do criminal behaviors. Suppose we need international cooperation to eliminate the harm of cybercrime. In that case, we need to make the definition of cybercrime align with the regulation and law enforcement at the national and local levels. That also helps to make the cybersecurity policy at the national level. Perhaps broad the references from the government side. For example, the Budapest convention probably is a good reference to know what is the attitude of the government side.

- Cybercrime policy is by nature and means imperative, as coercive to bring offenders to justice and to ensure victims have the support they need to rebuild their lives.

Myth 2: Considerations for human rights are equally compatible with cybercrime and cybersecurity policy.

Feedback

- “Are distinctions made between deserving and undeserving” — I would argue that in cybersecurity the answer to this is now yes, because corporate defenders completely differentiate between their employees, internal customers, and partners/third parties in terms of protections applied. The answer to that should be “maybe”, not “no”.

- Agree with the people or human rights center of the cybersecurity or cybercrime policy design. I think cybersecurity policy prevents something that will happen again in the future. And cybercrime is to punish someone or some people who do harmful behaviors to invade property, human rights, safety, or even national security with the internet. I don’t think the UN GGE will agree with this opinion. But I think people should consider this.

- The paper draft defines in a clear mode, that "The punitive, remedial, carceral and securitisation framing of cybercrime means that human rights must be balanced" It is not mandatory for a cybersecurity framework to be punitive (as it was in the Web 1.0 model) nor carceral. In fact, and in the IGF scenario: There is no individual versus national interests in investigations in countries where Common Law does not apply (which , in our times ar the prevalent, including advanced corporations as the EU). Cybrecrime investigations may harm human rights in a ny case the indivisual is subject to an interest. In these countries, human rights may well be violated by the investigative procedures involved. This is because of a very basic issue that should be pointed out that under Roman law, which applies for example in EU, it the victim who must demonstrate the crimes. Uh.

- Unclear sentence, i recommend reformulate for clarity:
  Where human rights advocates push back in cybersecurity policy making against the geopoliticised use of vulnerabilities and other “cyber capabilities” as strategic tools that manoeuvre power in cyberspace, those tactics are part and parcel of sovereign states’ fights against cybercrime

Myth 3: The security of information is a consideration for both cybercrime and cybersecurity. (It’s controversial!)

Feedback

- They would instead put the information and data security in the first place from the enterprise agreements. Because of the demand for compliance, they also care about business secrets. Human Rights may not be the first place they think about. But at the national or international level, human rights could be the first place for governments and international cooperation. But there will be more conflicts between national security and human rights. As I know the case of Edward Snowden and the PRISM project. He is a whistleblower to protect human rights, but his behavior harmed the benefit of the U.S. and probably created a danger to diplomacy.

- On the phenomenal aspects such as the Intellectual Property, it has been recognised as a basic right in the Charter of Nations. Certainly, the litigation and prosecution of many behaviours linked to the potential infringement of property rights should be scaled down. This can be strengthened by the proper use of an administration of Justice in the Civil field, not the Criminal field. Nevertheless, except if we take a colonialist outdated view, a violation of infringement of intellectual property, is one of the rights of the people, Intellectual property (that applies to individuals,) is not the same as a trade patent (that applies to bussiness companies or large corporations, subject to compliance not enforcement of laws.).

- Needs expansion. More elaboration of definition. Of security information

- First paragraph unclear. Bring concrete examples.

Myth 4: Countering cybercrime improves cybersecurity.

Feedback

- Of course. When law enforcement involves too much or mandates the cybersecurity policy, it will limit the technical innovation, e.g., if the government regulates the business merge and acquisition of their up or downstream suppliers or distributors, probably also eliminate the innovation from the business and make higher cost and less benefit to consumers. That is why we persuade the multistakeholder model in the policy-making process.

- Agreed on "When cybercrime laws are being developed, they should thoughtfully consider the impact on defenders, who often rely on the same techniques to validate and protect systems, but have no criminal or malicious intent."

- I think I might have phrased Myth 4 a bit differently. I think framing this as a myth is counterproductive, as the two disciplines should work together to achieve related goals.

The starting section: "One would think that in most cases, work to counter cybercrime improves cybersecurity. However, mature cybercrime laws, such as outlawing security research or development of exploit code,can actually negatively impact the ability of defenders to improve cybersecurity overall." I would not consider the laws that outlaw security research or the development of exploit code "mature." In fact, I would consider them a relic of an earlier time when there was no distinction between white and black hat hackers. Mature countries on cybersecurity have already resolved these statutes to allow for white hat hacking and pen testing. But I think that could all be a product of the space you had to condense these super complex subjects!

Myth 5: Cybercrime and Cybersecurity both improve with enforcement.

Feedback

- I don't think I have any words for this paragraph.

- Agreed on we can’t and SHOULD not prescribe to everyone how to act online.I do not agree with the gender distinction proposed in the draft. A correct measure or parameter would be to distinguish by age, regardless of the gender of the consumer. Discrimination by gender, even though it is widespread and must be estimated, is much less than the discrimination by age or behaviour that the entire population exercises at different times in their lives. If cyber-security dbenfit is - in a certain aspect to prevent behaviours as cyber-bullying, behaviouts which in some phases of a human life comes even from the most intimate circles, this -not gender - is the narrower approach to implement. Gender has the sense of self. Age brings the sense of community.

Comments on the overall draft paper

- Good: helped me develop my own thinking.

- There's one typo in the Conclusions, where the last bullet refers to "these four myths" when there are actually five!

- This is a great paper - thank you for the efforts of all who contributed. I think the paper would benefit from some additional discussion of tools/approaches to operationalizing the development and implementation of the specific "policies" at issue and how the balance of sectoral needs/desires can be best addressed. Can you identify a process for engaging stakeholder interests that may be a challenged by cultural dynamics, for example?

- Great paper. Thank you for discussing the intersection of cyber and human rights.

- The draft paper intends more with human rights and technical side. In the conclusion paragraph, the government stakeholder could do nothing to help the cybersecurity policy framework. If you are a citizen without any cybersecurity awareness, the only stakeholder to you is government or law enforcement. As discussed in the last virtual meeting, there is a cyber (or digital) security divide at a different level. We need to consider it. A recommendation about the structure of the conclusion paragraph. Please combine advice to the government stakeholder in one point. If we want to use the multistakeholder model to give advice, one list with different stakeholders at one point will be better.

- appropriate cybersecurity programs and policies to avoid some of the outcomes that may require law enforcement to react should be put in practice not only by corporations - whose purpose and existence is to obtain economic profit or benefit, - but on the part of civil society and the State.

- Abstract in beginning, instead of conclusion. More details in paragraphs

- I love the framing of the paper because I agree with you that using myth busting is a great technique to crystalize some key concepts that may be misunderstood. I appreciate that you try to address both cybercrime & cybersecurity in a compare and contrast format - very useful. I think an underlying goal of this paper is to focus more on the human rights of both cybersecurity and cybercrime and I think you could actually stand to tease that out a bit more possibly in a subsequent paper?

Contributors

We would like to thank the following contributors for their feedback (listed in alphabetically, the order does not correspond to the order of the comments cited above):

- Andrew Cormack, Jisc
- Delfi Ramirez ISOC UK - Segonquart Studio
- Jackie Singh, Director at Surveillance Technology Oversight Project,
- Paul Mitchell - MAG chair
- Tatyana Bolton, Google
- YingChu Chen, Assistant Research Fellow, Taiwan Institute of Economic Research
- "YouthIGF" (Student, political science)