Mythbusting: cybercrime versus cybersecurity

***December 15, 2022**,*

by Mallory Knodel, Sheetal Kumar, Maarten van Horenbeeck, Wim Degezelle (IGF Best Practice Forum on Cybersecurity).

2022 has been an eventful year for people solving problems in cyberspace. Cyberattacks are a hallmark of the Russo-Ukrainian War, which escalated this year. The UN First Committee continued their two parallel cybersecurity treaty processes. A UN General Assembly ad hoc committee on a cybercrime treaty began in earnest. These high level events indicate the need for multistakeholder policy attention towards cyberspace now more than ever.

The goal of this 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. In general the suggested strategy is to remove the policy decision making out of the criminal frameworks so as to balance the implications on human rights, while promoting cybersecurity as an incentivized, normative framework that depends on cross sector collaboration, and can be compatible with human rights.

We have chosen the “myth busting” approach because policy advocates are likely already familiar with the concepts separately, or in context, but would benefit from a nuanced description of the tensions between them as a way to depart from the way they are usually described.

Introduction

The Internet Governance Forum (IGF), convened by the United Nations Secretary-General, is the global multistakeholder platform facilitating the discussions of public policy issues pertaining to the internet. As part of its mandate (2015), IGF facilitates the exchange of information and identifies best practice identified by experts and academics working on area issues. Since 2014, IGF Best Practice Forums have focused on cybersecurity related topics as a multistakeholder group. From 2018 onwards, the BPF on Cybersecurity started investigating the concept of cultures of cybersecurity, identifying the norms and values in development of these practices. As a global initiative, the IGF BPF on Cybersecurity leverages an international and cross-stakeholder approach in their operationalization of cybernorms. The BPF recognizes the significance of powerful norm promoters and of ensuring incentives as critical in global governance. Its 2020 output states “norm development, even without results, creates socialization, which can be critical for further success” (IGF, 2020).

While the BPF framework is based on United Nations Group of Governmental Experts norms, recognizing the unique position of the UN in promoting international peace and security, the BPF adopted a political science definition of norms as a “collective expectation for the proper behavior of actors with a given identity” (Katzenstein, 1996). There are eleven items in the 2020 analysis of international norms agreements, from which two norms come out as the most commonly referred ones: calls for cooperation to promote stability and security in cyberspace, and recognition of human rights or privacy rights online (IGF, 2020).

As identified by the Best Practice Forum, our analysis also leverages a human rights focus in global internet governance, with a key focus on a “global” perspective as both cybersecurity and cybercrime are themselves nuanced concepts that to some extent depend on geopolitical context. The following myth busting, moreover, will disambiguate the key policy differences between cybersecurity and cybercrime so that their advocacy strategies could align. Our emphasis here will be on removing the policy decision making out of the criminal frameworks so as to balance the implications on human rights. Rather, we promote cybersecurity as an incentivized, normative framework that depends on cross sector collaboration, and, as seen in the IGF Best Practice Forum, can be compatible with human rights.

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

Cybersecurity is a cooperative approach which partly handles criminal law - including that which is more narrowly handled under cybercrime.

While both cybersecurity and cybercrime make references to securitization of computational systems, their approaches are not as compatible as they were made out to be. Cybersecurity defines a technical approach to securing computational systems from attacks or errors; and cybercrime is about punishing unauthorised interference with computational systems with criminal intent. Sometimes cybercrime is controversially defined to include crimes committed with digital technologies. The only commonality they have is that they are about security of computer systems, but they are not antagonistic as this myth makes them out to be. Rather, cybersecurity recognises the vulnerabilities in digital systems, whereas cybercrime aims to prevent damage to these systems through punitive means (Privacy International, 2018).

In line with our reference, we can identify good practices in both these areas. Cybersecurity strategies should be based firstly on protecting individuals, devices, and networks: centre policies and practices on people and their rights. Secondly, these cybersecurity policies should aim to establish a framework rather than an isolated law, as these should encompass complementary initiatives and approaches. Specifically, these policies should identify and prioritise critical infrastructure, establish response teams for security incidents, and maintain a proper threat assessment to help in decision-making and prioritisation of a country. The last aspect of best practice in this area would be about implementing comprehensive data protection laws, to safeguard against exploitation of personal data.

Cybercrime policy, on the other hand, considers a nation’s constitution, and underpins the pertinent legislation, ideally with human rights protections and safeguards. Further, cybercrime should be narrowly interpreted, without losing its specificity to other ‘offline’ crimes that do not necessitate the use of a computer or other digital device. Lastly, considering the rapidly changing nature of technological interception, cybercrime policy should establish frameworks narrowed to “cyber-enabled major crimes” that complement and are consistent with existing criminal law instruments, including multilateral ones. This would refer to new ways of committing the same crime like fraud or distribution of child abuse images. If such comprehensivity is undertaken in a cybercrime framework, this would allow cross border cooperation in tackling these crimes, and prevent isolation of serious crimes under the banner of ‘cybercrime’.

This multitude that is contained in the frameworks of cybersecurity and cybercrime make it necessary for cyber policy to gather input from various stakeholders, and significantly, best practice should consider civil society to play an important role in this process.

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

The punitive, remedial, carceral and securitisation framing of cybercrime means that human rights must be balanced, e.g. individual privacy versus national security interests in investigating crimes. However, with cybersecurity, human rights can be more aligned with and compatible when people are placed at the centre of the security of cyberspace (FOC, 2016). In cybersecurity policy making, where human rights advocates push back against the geopoliticized use of vulnerabilities and other "cyber capabilities" as tools that manipulate power in cyberspace, that tactic and others are part and parcel of sovereign states' strategies to fight cybercrime.

In the activist toolkit "So is this Actually an Abolitionist Proposal or Strategy?" the following questions may help define a human rights approach through contrast. The approach taken by cybercrime versus cybersecurity might be considered as such, and explained below:

Question	Cybercrime	Cybersecurity
Do policy solutions expand the carceral system?	Yes	No
Do policy solutions benefit prisons and policing?	Yes	No
Will human rights advocates need to remain vigilant against the effects of the policy solution?	Yes	Yes
Does the solution reinforce existing State or economic power?	Yes	Yes
Are distinctions made between deserving and undeserving populations?	Maybe; Criminals may be denied access to online services.	No; Distinctions between employees, partners, customers are not inequitable.
Does the policy solution undermine popular resistance to its effects?	Maybe; Some forms of protest may be considered criminal.	No

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

It may be common for “information security” to be used by technical practitioners within the context of an organization as an engineering practice, but in some parts of the world it’s used as a term covering many other problems of the information space - for instance cultural and political stability. Directly speaking, in these contexts information security can sometimes mean that information itself is a security threat. From a human rights perspective, because of the needed balance with free expression, the term cybersecurity largely steers clear of addressing these often content driven issues.

In cybercrime this same issue is harder to avoid due to explicit issues such as those related to copyright law, however advocates should minimise or advocate to eliminate the presence of intellectual property in cybercrime legislation because it can easily introduce content considerations in cybercrime, which unchecked as a matter of State security is at greater risk of infringing on human rights of free expression than cybercrime.

Myth 4: Countering cybercrime improves cybersecurity.

One would think that in most cases, work to counter cybercrime improves cybersecurity. However, entrenched cybercrime laws, such as outlawing security research or development of exploit code, has been shown to negatively impact the ability of defenders to improve cybersecurity overall. 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.

Myth 5: Cybercrime and Cybersecurity both improve with enforcement.

In the cybercrime world, we often speak of enforcement of laws. Cybersecurity has its equivalent – compliance. However, that is only one part of building healthy cybersecurity.

A second portion is culture. Cybersecurity is so rapidly evolving that we can’t prescribe to everyone how to act online. There are some basic steps individuals and organizations can take to protect themselves, and where the goal of cybersecurity is to achieve maximum compliance. However, in the face of rapid change, cybersecurity also requires education, awareness and norms, which cannot be governed in such a way and need to be grown to create aware and knowledgeable citizens.

Relatedly, one aspect of this elaboration on the norms in cybersecurity would be considering the linkages between cybersecurity frameworks and gender equality frameworks. Understanding how gender structurally operates within cybersecurity spaces is a crucial step in achieving a healthy system of cybersecurity. UNIDIR proposes a framework based on the design, defence, and response of cybersecurity activities so as to better identify how such gendered practices are part of the normative structure of this space, and to implement systems to mitigate gender inequality (Millar et al., 2021).

This reinforces the view that addressing cybersecurity and cybercrime from the points of view of communities most affected by power imbalance is critical for human rights as well as achieving success.

Conclusion

Prevention of cybercrime, and improving cybersecurity, are worthwhile efforts that are deserving of attention and development of expertise. However, in this document we hope we clarified the approaches to solving both will by definition be different, and an approach that is functional in one area, will not be functional in the other without serious adaptation and rethinking.

Today, cybersecurity and cybercrime policy practitioners are often asked to “stretch” between both domains. This poses risks in terms of approaches that may not cleanly translate from one to the other. Taking into account these five myths will help us understand where a solution may be the right fit for one, but not the other.

The authors of this paper recommend:

- **All stakeholders** put the principles of safety, human rights and frameworks front and centre when developing cybersecurity policy, and take a narrower lens when developing and advocating for cybercrime laws.
- **States** to avoid developing cybercrime laws that may negatively affect the work of cybersecurity defenders, by outlawing or criminalising their defensive activities, even though they may look like what a cybercrime law typically outlaws. They should do so by inviting other stakeholders to their conversations and enable an ongoing learning activity between these communities.
- **States** to develop proactive contributions to solving cybersecurity with other stakeholder groups and push accountable frameworks.
- **States** to actively narrow the range of issues covered in cybercrime to comprise “major crimes” and entirely exclude content-layer discussions.
- **States** to identify rights-respecting frameworks for accessing data by LEAs across borders given the necessary and proportionate principles.
- **Corporations** to invest in appropriate cybersecurity programs and policies to avoid some of the outcomes that may require law enforcement to react.
- **Civil society** to participate, and where possible, invite themselves to both cybercrime and cybersecurity discussions; and educate themselves on the different approaches each field requires. Start with these 5 myths and work your way into guidance as published by specialized organizations, as listed in the references.

Acknowledgements

This paper was developed throughout the 2022 intersessional work of the Internet Governance Forum. As a work in progress it was reviewed by a global multistakeholder community and we want to thank all interested parties who read the early drafts and who provided feedback on this paper. And to all who contribute to the Best Practice Forum on Cybersecurity, we thank them for sharing their expertise and experiences around approaches which have worked, and those which did not. We're a multi-stakeholder group of cybersecurity experts that are taking an outcome (incident)-focused approach to identifying appropriate cybersecurity efforts and anyone can join us.

References

Millar, Katharine; Shires, James; and Tropina, Tatiana. 2021. Gender Approaches to Cybersecurity: Design, Defence and Response. Geneva, Switzerland: United Nations Institute for Disarmament Research. https://doi.org/10.37559/GEN/21/01

United Nations Internet Governance Forum (IGF), About the Internet Governance Forum, 2015.

United Nations Internet Governance Forum (IGF), Cybersecurity Culture, Norms and Values, Best Practice Forum Cybersecurity, 2018.

United Nations Internet Governance Forum (IGF), Exploring Best Practices in Relation to International Cybersecurity Initiatives, Best Practice Forum Cybersecurity, 2020.

Peter J. Katzenstein, ed., The Culture of National Security: Norms and Identity in World Politics, New York: Columbia University Press, 1996, 5.

Privacy International, Understanding the Difference between Cyber Security and Cyber Crime, 2018.

Disclaimer:

The views and opinions expressed herein do not necessarily reflect those of the United Nations Secretariat. The designations and terminology employed may not conform to United Nations practice and do not imply the expression of any opinion whatsoever on the part of the Organization.