Contribution to Cyber Security BPF

How does good cybersecurity contribute to the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?

Cybersecurity means different things to different stakeholders and these different understandings can overlap and even conflict with each other. Whether it is subjective (for example, involving a sense of safety) or objective (for example, dependent on concrete practices and resilient systems) – or even both, – the fact remains that there are many ways of conceptualizing and practicing cybersecurity and it is not always clear whether these different understandings, when in conflict with each other, are not also in the root of weak cybersecurity governance mechanisms. Because of that, a common understanding of what it means speaking and practicing cybersecurity is fundamental to conceive of coordinated action among different stakeholders.

In a world where almost everything is becoming connected, good cybersecurity practices matter not only to assure the continuing development of information technologies and the Internet, but are also fundamental in supporting Internet inclusion in developing countries, the exercise of different kinds of freedoms and rights and allowing for local populations to rely on alternative models of living. Safe and resilient systems are as important as user-friendly systems, particularly considering the growth in connectivity in these countries, which translate in increased use of the Internet for promoting local commerce and diffusing culture. “Literacy” in ICTs and on the risks involved in being connected may offer users a good account of what is at stake when their lives, as well as economic activities go online, particularly in terms of the safety of their activities as they are increasingly conducted through networked technologies.

How does poor cybersecurity hinder the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?

Poor cybersecurity has different impacts on different actors. For market actors, it results in significant costs and affect trust in their products and services. For governments, in may affect the provision of public services conducted *online* and threaten the integrity of citizen data collected and stored by governmental authorities for different legitimate purposes. The risks of poor cybersecurity to civil society are greater where the political opposition faced by activists threatens their own freedom and integrity. In many cases, information breaches may severely undermine the capacity of activists to actively engage in political contestation to governments and other actors and to produce independent assessment over sensitive political issues. And in a context where interconnection becomes increasingly diffused through mobile and smart devices, users become particularly threatened by unauthorized access to them, which may compromise personal data, as well as economic activities, banking information and others.

Assessment of the CENB Phase II policy recommendations identified a few clear threats. Do you see particular policy options to help address, with particular attention to the multi-stakeholder environment, the following cybersecurity challenges:

Cyberattacks (Denial of Service and others), the security of mobile devices, vulnerabilities in technologies of critical infrastructures (including those required to Internet access as well as industrial systems), as well as the confidentiality of sensitive/personal information are risks that must be addressed through policies developed by partnerships between public and private actors aiming at improving technical solutions as well as policy and legal frameworks. In this context, whereas private actors have been fundamental in developing security systems and solutions, it is important that public authorities also become aware of the cybersecurity risks to their activities. Such awareness could be raised by developing best practices and guidelines among different governmental entities. Awareness of information technologies and best practices of cyber security are also necessary on the individual and institutional levels in order for government authorities, companies, service providers and the community to better combat online abuse and gender-based violence.

On the technical level, it is particularly challenging not only to develop, but fundamentally to incorporate secure development processes in smart and mobile technologies.

As for surveillance, it undermines the privacy of users and may threaten freedom of expression and association. I believe that developing legal frameworks to protect users' data is an important step against different kinds of surveillance.

An issue that communicates with different threats identified in the aforementioned policy recommendations and that has not been listed is the importance of developing policies for informing people in developing countries about the risks of unauthorized access and to their data when they use the Internet. As policies of access allows for more people to benefit from ICTs, it is important to focus on how to provide the means for them to safely make use of information technologies.

Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?

The complexity of ICTs is precisely the reason why a multi-stakeholder approach to cybersecurity, in particular, and to Internet governance broadly, is fundamental. The private sector plays a core role in developing secure products and services, as well as in sharing knowledge and best practices with governments and non-governmental organizations. Governments play a fundamental role in developing policy and legal frameworks for a secure cyberspace, data protection, protecting critical information infrastructure and enforcing the law against cybercrime, online abuse and gender based violence. They are also important for regulating competition among market actors and, in

my view, have two negative obligations: not to fuel competition for creating insecurity (i.e., by acquiring vulnerabilities at the expense of companies affected, for example) and not undermining users' data protection. Non-governmental organizations activities are, thus, fundamental for pressing governments to abide to its obligations, such as respecting rights such as privacy and freedom of expression, increasing awareness over rights in the digital age, promoting responsible behavior and spreading best practices, as well as they have been important hubs for expanding access policies in developing countries, often being closer to the everyday reality and challenges faced by users than the other cited actors.

What is for you the most critical cybersecurity issue that needs solving and would benefit most from a multi-stakeholder approach within this BPF? Should any stakeholders be specifically invited in order for this issue to be addressed?

Cybercrime: cybercrime is an issue worldwide, and it is important to define clearly the activities that fall under this label. In this sense, multi-stakeholder coordination is important in that it allows identifying the most pressing issues.

State conflict: state conflict in Internet serious undermine the network's security, affecting companies (by weakening their products/services through systematic attempts to find vulnerabilities/develop exploits) and users/the civil society, particularly when it involves the spreading of misinformation and the theft of data.

Luísa Lobato

Researcher/PhD candidate (Pontifical Catholic University of Rio de Janeiro)