PRIVACY INTERNATIONAL

Privacy International's Contribution to the IGF Best Practice Forum on Cyber Security September 2017

Privacy International was founded in 1990 and is based in London, UK. It is a leading charity organisation promoting the right to privacy across the world.

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)?

It is important to outline what "good" cyber security looks like. Good cyber security policies, practices and legislation put people and their rights at the centre. The basis of any good strategy should simultaneously protect individuals and their data, protect devices, and protect networks, thus fostering trust, stability and confidence in the technological systems integral to our day to day lives. Access to innovative technology and infrastructure is included in almost all SDG targets. In addition, SDG 9, Industry, Innovation and Infrastructure, states that "*investment in infrastructure and innovation are crucial drivers of economic growth and development."* To achieve these goals and targets, the development and use of innovative technology and infrastructure must be secure and reliable.

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 cyber security, including situations where vulnerable or insecure systems result in hacks and data breaches, are catastrophic for privacy, and undermine trust in digital technologies as a driver for development as a whole. Unfortunately, the systems that play an essential role in our lives *are* fragile and vulnerable. And yet, rather than addressing the root problem of insecure systems, governments and companies pour resources into costly data intensive projects, build devices, networks and services that accumulate vast data stores without proper regard to risk, security, or data minimisation. In other words, instead or managing and reducing risk, these actors are creating new ones, that ultimately makes people less secure.

Many countries have insufficient or no legislation to protect personal data against unauthorised access, leaving many people vulnerable to excessive data being collected on them. Because of this lack of adequate legal framework (and the effective enforcement mechanisms) data is often poorly secured, and ultimately stolen without the means to bring any accountability nor transparency about such events. Data breaches have a knock-on effect for a country's cyber security as they cause people to lose trust in systems, cost the economy greatly and direct resources towards retrospectively securing systems that should have been built securely from the outset.

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? *[Many of these challenges are connected, so we have grouped them together where applicable]*

The lack of Secure Development Processes combined with an immense growth in the technologies being created and used on a daily basis/Unauthorised access to devices that take an increasing role in people's daily lives/Denial of Service attacks and other cybersecurity issues that impact the reliability and access to Internet services:

Devices: While it is cheap to connect devices to the internet, it is generally agreed among security experts that the security of devices such as routers, webcams and other household objects connected to the internet known as the "Internet of Things" is very poor. Many of these devices have serious security flaws such as no or default passwords, and are difficult or even impossible for everyday users to change. Therefore, many of these internet-connected devices are vulnerable, and the proliferation of insecure connected devices in turn are a potential threat to personal and network security. Securing devices should be a key cyber security objective, both for the risk they pose in relation to the personal data they generate, collect, store and transmit and for the security risks they pose as integrated in or as part of a network, where they can even become attack vectors.

Policy-makers and regulators need to address how they will encourage manufacturers of connected devices to make devices more secure, particularly when there is currently no economic incentives to do so.

Networks: Every conceivable thing is being connected to the internet because it is cheap to do so without regard to security, creating many vulnerabilities and a large attack surface. This makes network security all the more important. How to secure networks is an integral yet often neglected part of cyber security policy discussions. Good network security means reducing the attack surface and then allowing the right people through the right devices to access the right services on a network, and keeping everyone and everything else out.

Protecting and defending a network can mean protecting a home Wi-Fi connection, a company's intranet, a telecommunications network accessed by the public, a bank's network, an industrial control system (ICS) in a factory, or a nation's critical infrastructure such as a power grid. The failure to adequately protect networks was famously demonstrated in October 2016 when malware, known as Mirai, powered a huge denial of service (DDoS) attack, enabled by a botnet of hundreds of thousands of infected internet connected devices.

Security of mobile devices, which are the vehicle of Internet growth in many countries, and fulfill critical goals such as payments:

A recent study found that on average 87.7% of Android devices are exposed to at least one of 11 known critical vulnerabilities. Failure to address a known vulnerability disproportionately impacts people in global south countries who are more likely to be using Android operating systems and/or using older devices which are no longer being provided with security updates, or the user is unable to pay to receive additional security support. A lack of security information from the private sector has created a very unequal playing field, or as the study puts it, "*there is information asymmetry between the manufacturer, who knows whether the device is currently secure and will receive updates, and the consumer, who does not. Consequently there is little incentive for manufacturers to provide updates*." This imbalance of security information and awareness needs addressing to improve security of mobile devices, particularly in the global south.

Potential abuse by authorities, including surveillance of Internet usage, or the use of user-provided data for different purposes than intended:

Security is often articulated across the world through an increase of surveillance regimes under the guise of cyber security. Prioritising surveillance is likely to weaken rather than strengthen security. Putting it succinctly, it is an epic folly of ethics to imagine you can protect your citizens from having others read their email, by reading their emails. To quote the European Court of Human Rights, this is undermining democracy under the cloak of defending it. Additionally, there is a good chance that essential measures to strengthen cyber security will be under-resourced or ignored, such as identifying vulnerabilities, supporting security research, preparing educational initiatives or doing public information campaigns.

Confidentiality and availability of sensitive information, in particular in medical and health services

Privacy International and partners have observed that governments are keen to develop data-intensive projects, but lack consideration for securing the personal data those projects generate. For example, some countries without data protection laws are developing projects including smart cities (e.g. India and Indonesia) or biometric voter registration systems (e.g. Kenya).

Data breaches continue globally, and the numbers involved are staggering. Continued scrutiny of the Aadhaar project in India has revealed serious flaws in security, where Aadhaar numbers were published alongside personally identifiable information on several government websites. The personal information of over 93 million voters in Mexico, including home addresses, were openly published on the internet after being taken from a poorly secured government database. This can be highly sensitive information; in Mexico for instance up to 100,000 people are reportedly kidnapped each year. Similarly, the personal information of over 55 million Filipino voters were made publicly available, the biggest data breach in the Philippines' history. A database containing the records of 650,000 patients in Sao Paolo, Brazil was made public, putting people at a variety of risks, from becoming victims of identity theft to persecution e.g. when the identities of women undergoing abortions were exposed**.**

Countries should implement legal frameworks that address data security concerns, imposing security obligations for government and companies, along with reporting requirements for information security incidents, that allow subjects to take actions to protect themselves from the consequences, and governments to be aware of the cybersecurity risks and threats in their countries.

Use of information collected for a particular purpose, being repurposed for other, inappropriate purposes. For instance, theft of information from smart meters, smart grids and Internet of Things devices for competitive reasons, or the de-anonymization of improperly anonymized citizen data.

These are increasingly important and pressing issues that Privacy International frames as "data exploitation" (see this short video explainer). Our devices and infrastructure are often designed for data exploitation. This must change. The individual must have control over his or her data, how it is generated, collected and used. The fundamental architecture of modern technology, its functions and operations, and deployment must be structured to prevent data exploitation. We would like to refer the BPF to resources from Privacy International's Data Exploitation program, which address the identified issues above and more.

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

Cyber security should be considered a public good, in the same way, for example, as public health, which promotes collective responsibility for the benefit of everyone. Therefore, cyber security discussions suit a multi-stakeholder environment as everyone has a stake and responsibility. Trust and confidence cannot be achieved by a single actor.

Privacy International has observed that many governments frame cyber security under vague national security definitions and place initiatives under the domain of intelligence agencies, which makes them harder to scrutinise and more likely to lead to unlawful surveillance. Secrecy does not equal security. Without strong safeguards, these initiatives are open to abuse. See Privacy International's investigation into Kenya's approach to cyber security here and here. More transparency is needed around cyber security initiatives if they are to keep individuals safe. Governments need to publicly provide reasons why certain cyber security initiatives are classified as national security and therefore should not be discussed and scrutinised publicly. We would welcome a discussion on the classification of cyber security as national security and the role of intelligence/security services in developing and implementing cybersecurity.

Lucy Purdon, Policy Officer
lucyp@privacyinternational.org
www.privacyinternational.org