Internet Policy Observatory Pakistan Contribution to the IGF Best Practice Forum on Cyber Security
September 2017

About The Observatory

Internet Policy Observatory Pakistan is nonprofit organization that conducts public interest research on ICT policy and regulation in Pakistan. It provides researchers, governments, regulators, operators, multilateral institutions, development agencies and community organizations with the information and analysis required to develop innovative and appropriate policies for modern age digital technologies. iPOP contributes to the gathering of up to date ICT data and establish repository of information for furthering research and policy formulation on Internet Regulation, Surveillance, Privacy, Net-Neutrality, Media Regulation and Freedom of Expression. The Observatory also aims to promote interaction between researchers, activists, academics and institutions for conducting public interest ICT policy research and advocacy campaigns.

1) **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 is one of the corner stones of modern information communication technologies and their ability to contribute economic and social development is unmatched. A culture of good cybersecurity helps to build trust in the digital environment, enabling economic growth, social inclusion, and innovation. As ICTs and internet technologies increasingly become essential to everyday life in developing countries, its security is becoming more of an international development issue. Effective use of technology is critical to realization of many of the Sustainable Development Goals. Recent research at the observatory has shown that lack of trust in internet technologies has resulted in reduction of adoption of ICTs. Following are some examples where good cybersecurity can help building trust and further SDGs.

- ***Develop industry, innovation, and infrastructure (SDG 9):*** Good cybersecurity can increase the availability and management of internet infrastructure, leading to the increase in agricultural and business productivity, innovation and development.

- ***Achieve gender equality and empower all women and girls (SDG 5):*** Cybersecurity capacity building on staying safe online for women and girls can boost technology adoption and empower women to achieve SDGs.

2) **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)?**

The role of Information and Communication Technologies as a key driver of sustainable development is evident from the fact that 95 per cent of the global population is now covered by a mobile cellular signal. However, poor cybersecurity and vulnerability of infrastructure can thwart the growth and trust in ICTs and internet technologies for Sustainable Development. The recent breaches and hacks at global level has again highlighted the critical importance of the issue and the role global community needs to play in ensuring that trust is reinforced in this wonderful technology by adopting mutual frameworks and agreements that can curb poor cybersecurity. Cyber hacks and breaches break the trust of businesses online which has a direct impact on productivity and economic growth in developing countries where more and more enterprises are adopting this technology for delivery of goods and services.

3) **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 multistakeholder environment, the following cybersecurity challenges:**

- ***Denial of Service attacks and other cybersecurity issues that impact the reliability and access to Internet services***

  The coming of new age IOT devices with internet access, massive adoption of pirated/cracked software's and underestimation of the importance of anti-malware protections are contributing to the spread of bots and increasing the risks of DDoS attacks. The cyber gangs involved in developing DDoS botnets are increasingly investing heavily in creating botnets of network devices such as routers and dsl modems in developing countries. These impact the reliability and access to internet services in developing communities which directly impact on achieving Sustainable Development Goals. Developing countries need to play their role and ensure that networks are monitored for such attacks on critical national infrastructure and setup a global rapid response team to mitigate such attacks.

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

  Mobile device have seen an explosive proliferation in the last decade and are always connected even when roaming in our pockets making them susceptible to the growing security problems. Mobile devices are a high value target because they are always online, store massive amounts of some personal data, and equipped with small cameras, microphones, and positioning devices. Mobile devices security model is very simple and making it more vulnerable to security threats unless the weakness in the models are removed using a multistakeholder strategy that involves all stakeholders.

- ***Potential abuse by authorities, including surveillance of Internet usage, or the use of user-provided data for different purposes than intended***
  The main challenge for developing countries is the transition of all human rights to the digital sphere. Many governments have upgraded their capacity to use more advanced digital tools for censorship and surveillance. Highly intrusive biometric identity systems supported by international development organizations like the World Bank and United Nations for achieving Sustainable Development Goals (SGDs) have sprung up for profiling every citizen in the country with the potential to interferes with the individual's right to privacy. Surveillance on the internet is on the rise at an alarming rate many countries are looking up to the efforts of CIA and other counterparts in west on surveillance on the internet. Unless the globalized world is able to address the issue of mass surveillance of five eyes countries and openly debate about cyber weapons surveillance and abuse on the internet will remain part of the cyber strategy being adopted by most countries.

- ***Confidentiality and availability of sensitive information, in particular in medical and health services***
  Most of the modern health systems are using digital technology for saving very private and sensitive information. These systems are further connected to the internet which makes them very susceptible to cyber threats and sophisticated cyber weapons. The international community need to work on a legal binding framework that provides amnesty to such systems from cyber threats to ensure its data remains confidential and available. Furthermore, developing countries should be supported on designing and implementing cyber security frameworks and standards by development organizations that are pushing the rollout of these systems.

- ***Online abuse and gender-based violence***
  Women and children are most affected by online abuse in the developing countries. Government's needs to take the lead to tackle the issue and join hands with all stakeholders to mitigate and educate about online abuse and gender based violence if it seriously want to address the issue. Further, international rapid response units need to be setup to provide immediate support and relief to the victims of such abuse at a global level.

- ***Security risks of shared critical services that support Internet access, such as the Domain Name System (DNS), and Internet Exchange Point (IXP) communities***
  Internet is a shared resource that has become an engine of economic growth for all countries. Any security threat or risk to services that support internet access can directly

impact all fabric of modern society. As more and more countries connect to the internet business, industries, government with critical infrastructures protecting the shared resources has become of vital importance. Also, multistakeholder approach needs to be adopted in managing these resources with equal representation of all stakeholders. This will ensure that critical resources are protected for a global interest.

- ***Vulnerabilities in the technologies supporting industrial control systems***
  Industrial control systems (ICS) are used across a wide range of critical infrastructure sectors, including energy, manufacturing, transport, water, waste and healthcare. Traditionally these systems were isolated and operated independent from the internet. However, due to the revolution in the industrial sector many of these systems have converged making them vulnerable to cyber threats. The state of cyber security of such systems in developing countries is extremely poor making them more vulnerable in case of a cyber-attack. It is recommended to enable a common security language across all industry sectors and support industry associations to implement sound security practices in current standards.

- ***The lack of Secure Development Processes combined with an immense growth in the technologies being created and used on a daily basis***
  Secure development processes needs to be embedded in the development platforms and all stakeholders including governments, academia, civil society and most importantly key industry players need to raise awareness on best secure coding practices and available frameworks for security. Industry giants along with governments can sponsor national initiatives that can create national standards for secure development processes embedded in the digitalization process.

- ***Unauthorized access to devices that take an increasing role in people's daily lives***
  Most countries have drafted laws and implemented legislations to criminalize "unauthorized access". Access to unauthorized devices can result in disclosure of confidential, sensitive or embarrassing information that can result in loss of credibility, reputation, market share, and competitive edge impacting Sustainable Development Goals 8 (decent work and economic growth) Goal 1 (no poverty) and Goal 5 (Gender equality).

4) **Many Internet developments do not happen in a highly coordinated way - a technology may be developed in the technical community or private sector, and used by other communities and interact in unexpected ways. Stakeholders are managing complexity. This both shows the strength and opportunities of ICTs and Internet Technologies, but also the potential risks. New technologies may be insufficiently secure, resulting in harms when they are deployed: conversely we may adopt security requirements or measures that prevent the development,**

deployment, or widespread use of technologies that would generate unforeseen benefits. Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?

The strength and weakness of internet technology is that it's autonomous and highly uncoordinated with the interplay between benefits and risks of newly deployed technologies unseen. This makes the responsibility of each stakeholder in the community critical for the continuous growth and development of this powerful technological revolution. Governments and international development organizations have a very influential role to play in the progress and growth of this technology ensuring that shared resources are secured, criminal states are sanctioned and cyber criminals living in safe heavens persecuted and brought to justice. Civil society, industry and academia need to play a greater role in increasing awareness about cybersecurity. Global civil society organization involved in protecting digital rights and freedom on the internet need to provide assistance and mentor local civil society organizations/advocacy groups to ensure that balance between privacy and security is achieved.

5) **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?**

The future of cyber security is looking more complex and challenging as organizations develop and adopt technologies such as big data, cognitive computing and AI supported analytical/automated systems. Failure of AI system has the potential to damage human society on a global scale as already some of the world's greatest minds including Stephen Hawking, Bill Gates, and Musk, have expressed concerns about the potential for super automated AI systems can evolve to a point where humans could no longer keep control of them.

United Nations as a globally accepted forum needs to provide leadership and define framework for behaviors and norms acceptable in the virtually connected world especially when countries having greater cyber capabilities can use them to damage critical infrastructures of least-friendly nations.

Arzak Khan
Founder & Director
Internet Policy Observatory Pakistan
director@ipop.org.pk
www.ipop.org.pk