Council of Europe – Cybercrime Division

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 measures facilitate the confidence and trust in ICTs and Internet Technologies, and thus, support sustainable human development and the protection of human rights, democracy and rule of law.

The prevention and control of cybercrime and measures to enhance cybersecurity are mutually reinforcing. Cybersecurity is about the protection of the confidentiality, integrity and availability of computer data and systems in order to enhance security, resilience, reliability and trust in ICT. This includes technical, procedural and institutional measures for the protection against, mitigation of and recovery from intentional attacks and non-intentional incidents affecting in particular critical information infrastructure. An effective criminal justice response to offences against ICT thus reinforces cybersecurity.[1]

Policies for the investigation, prosecution and sanctioning of cybercrime and international cooperation for cybercrime investigations, such as the adoption of the Budapest Convention on Cybercrime, enhance cybersecurity performance[2].

The Cybercrime Convention Committee[3] representing the Parties to the Budapest Convention in June 2017 launched the drafting of an additional Protocol[4]). This should further improve the capacity of States to protect their citizens against cybercrime and furthermore strengthen cybersecurity.

While the Committee is composed of representatives of Parties to the Budapest Convention, multiple stakeholders will be consulted.

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)?**

Given the role of ICT in all aspects of societies, most SDGs are related to ICT. Cybersecurity aimed at enhancing confidence, security and trust in ICT is thus directly or indirectly connected to SDGs.

Furthermore, measures on cybercrime and electronic evidence also have a direct impact on Goal 16 ("Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels")

Measures on cybercrime and e-evidence are strongly connected with the rule of law in cyberspace. Promoting the rule of law in cyberspace is a key objective of the Budapest Convention.

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 multi-stakeholder environment, the following cybersecurity challenges:**

[1] https://rm.coe.int/16802fa3e6 , page 7
[2] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Microsoft%20-%20Linking%20Cybersecurity%20Policy%20and%20Performance.pdf
[3] https://www.coe.int/en/web/cybercrime/tcy
[4] https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b

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

DOS and DDOS attacks impact the reliability and access to internet services. The Budapest Convention on Cybercrime provides the legal framework for the investigation, prosecution and sanctioning of these types of attacks. For the currently 55 Parties to the Budapest Convention and the many other countries that used the Convention as a guideline for domestic legislation it offers the means to criminalise and prosecute these types of crimes[5].

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

The notion of "computer system" as referred in the Budapest Convention includes mobile devices[6] and thus, the crimes committed against the confidentiality, integrity and availability of mobile devices represent crimes according to the legislation of countries implementing the Convention. This has a dissuasive effect and offers the framework for the sanctioning of such attacks.

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

Criminal law measures on cybercrime and electronic evidence should be subject to rule of law safeguards and conditions (see Article 15 Budapest Convention). However, the problem is less one of criminal law measure which covers specific criminal investigations and specified data needed as evidence. Such measures are normally strictly regulated and remedies are available. This is less the case with regard to measures carried out by national security services which may engage in mass surveillance and the bulk collection of data with limited safeguards. Stronger supervision and accountability of national security services would be needed.

- **Unauthorized access to devices that take an increasing role in people's daily lives**

Countries should take the necessary measures as to adopt legislation as to criminalize unauthorized access or illegal interception of data. Transposing the Budapest Convention on Cybercrime and enforcing legislation in line with its provisions, would offer States the legal framework for prosecuting unauthorized access to data (Articles 2 and 3 Budapest Convention) and have a dissuasive effect.

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**?

N/A

[5] https://rm.coe.int/16802e9c49
[6] https://rm.coe.int/16802e79e6

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

Cybersecurity can be assured only with a multi-stakeholder approach. This is why, when developing future policies on the strengthening of the rule of law in cyberspace, the Council of Europe encourages relevant stakeholders to contribute. In this way, future policies will represent commonly accepted solutions to make the cyberspace more secure.

6. **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?**

Criminal justice aspects – including the securing of electronic evidence - need a stronger reflection in cybersecurity policies. Prosecuting major cybercriminals will help have a direct impact on cybersecurity and enhance confidence and trust.