Statements Delivered by Signatories of the Cybersecurity Tech Accord during the Second Intersessional Consultation of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC)

Vienna, 13-14 June

Statement Delivered by Szilard Pfeiffer, Security Engineer & Evangelist at Balasys on behalf of the Cybersecurity Tech Accord

The importance of technical assistance has been highlighted multiple times and it is not possible to overestimate its importance. Organisations handling incidents, irrespectively of the sector they belong to, must have required knowledge and expertise to perform the task correctly and efficiently. However, the current discussion is not mentioning the role of the private sector explicitly which then leaves things open to interpretations and assumptions. It is quite easy to assume that only public and/or state entities are the ones who can provide and receive technical assistance. The same holds for capacity building, by not being explicit, it can be assumed that only public sector is the intended audience.

This omission must be addressed, and the Convention must be explicit in its intentions, because the situation in the private sector is far from uniform. Some organisations from private sectors have capabilities and expertise that only a few states can match and even fewer surpass. This is offset by a vast number of organisations which have only rudimentary expertise in handling incidents. And many others do not have any capabilities or expertise at all. This is very dangerous situation as the majority of victims of cyber crime are from non-public sector. If the non-public sector cannot identify an incident, let alone do something about it, it would not be possible to reduce the level of crime.

As said, some private organizations posses expertise to handle incidents and most multinational organisations fall into this category. By their nature multinationals are handling trans-border incidents. Not only incidents affecting the organisation itself but also incidents involving multiple organisations. In essence, we are coordinating (in a loose sense of the word) incident handling between multiple organisations when needed. This is done seamlessly and we are doing this for decades.

This state of affairs, and the role private sector is playing in combating incidents, is cursory acknowledged in various forums and documents but never really moved forward. In practice public and/or state entities do not acknowledge, let alone utilise these capabilities. Private sector is mostly held at arm's length and, with a very few exceptions, is expected only to provide information to, and follow advices from, state entities.

The Convention should call on its signatories to explore how public and private sectors can deepen their cooperation. This cooperation should, where possible and appropriate, treat private organisations as peers or an extended arms of state institutions. It is possible to envisage a scenario where private organisation would undergo some kind of vetting and certification process which would then enable them to act as associated part of a public institution.

In conclusion, the Convention should be explicit of the role of private sector in technical assistance and capacity building. The Convention must state that private sector is also entitled for technical assistance and that it is also encouraged to develop its capabilities. Additionally, signatories of the Convention should be strongly encouraged to explore new and novel ways how private sector can work together with, and be considered a peer of, the public sector.

Statement Delivered by Gaus Rajnovic, Cyber Security Manager at Panasonic on behalf of the Cybersecurity Tech Accord

The first international milestone in the fight against cybercrime was the Council of Europe's Budapest Convention. The Budapest Convention not only defined the concepts of cybercrime, but also contained procedural rules. To this day, the convention remains one of the starting points for international regulation of cybercrime. It may also serve as a good guideline for the regulation to be developed by the United Nations.

However, all regulations can contain points of debate. In the case of the Budapest Convention, the issue of privacy is one such point. It has been the subject of criticism over the last two-decade history of the convention. The convention sets out obligations for collecting, recording, and intercepting content data in real-time, transmitted by computer systems. It is important to highlight that the vast majority of the content data that is transmitted through the internet is encrypted. This means that data can only be collected and recorded in encrypted form. To break the encryption, law enforcement agencies need a backdoor in the system or a deliberate weakening of the encryption. These are theoretically and technologically feasible, but they raise practical feasibility concerns, doubts concerning proportionality and security risks.

Before continuing, I would like to emphasize that I do not intend to question the importance of fighting against cybercrime, but merely to find a way to minimize both security risks and privacy concerns.

In order to deliberately weaken any encryption algorithms, the active involvement of all the major players in the technology sector is essential, as they should implement these weakened encryption algorithms in their commercial products. At the same time, we should not forget the free software movement alongside the big tech giants. In this community, efforts to weaken encryption may be resisted because of their strong commitment to both trusted technologies and privacy. It is important to emphasize that the encryption software products we currently use in most web, cloud, and mobile technologies on our smartphones and laptops have been developed by technology companies and members of the free software movement communities.

Even if methods to weaken encryption can be successfully enforced, the question is what the drawbacks are alongside the benefits they bring. For law-abiding citizens, surveillance is likely to be 100% successful, but for criminals, this rate might not be significantly higher than it is now.

For instance, free software is never backed by a single organization, company, or state, but by decentralized communities that no one directly governs. The essence of free software is the right that users are free to modify the functionalities according to their needs. This means that cybercriminals can also evade the surveillance and weakened encryption that law enforcement agencies are able to break. In other words, our tools against the most dangerous cybercriminals and terrorists will be no more effective than they are today.

Whatever solution we choose, let us not forget that backdoors in our security systems can be exploited not only by us, but also by our enemies – against us. Cybercriminals today are still working hard to find specific software flaws that can be used to break into computer systems to acquire or corrupt as much data as possible. These criminals, knowing that there is a backdoor in every encrypted communication on the internet, would probably devote all their resources to finding and exploiting it. If even one of these criminal groups succeeds, the impact is currently unimaginable.]