ICC Business Roundtable on Cybercrime

SUMMARY REPORT

Meeting on 10 January 2022, 15:00-16:00 CET (UTC+1)

The Roundtable was convened by the ICC Global Digital Economy Commission Working Group on Cybersecurity and featured four invited speakers and over 70 participants from more than 30 countries.

Invited speakers:

- **Rene Summer**, Lead, ICC Digital Economy Commission Working Group on Cybersecurity and Director, Government & Industry Relations, Ericsson
- **Dominique Lazanski**, Director, Last Press Label and Visiting Fellow, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)
- **Kaja Ciglic**, Senior Director, Digital Diplomacy, Microsoft
- **Nick Ashton-Hart**, Special Adviser, International Internet Policy, ICC United Kingdom

Setting the scene

To set the scene for the discussion, speakers reflected on legal, regulatory and policy instruments and frameworks of note, designed to help prevent and prosecute cybercrime. Speakers also briefed participants on the current United Nations General Assembly (UNGA) initiative to develop a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

Key cybercrime trends and considerations

The cost of cybercrime was estimated at €5.5 trillion in 2020 - an amount that doubled since 2015 and that is expected to double once more by 2030 if nothing is done to slow down cybercrime. Over the past years the targets of cybercriminals got broader: in addition to classic crimes (data theft and alteration, phishing and ransomware), innovations that power the 4th Industrial Revolution and critical infrastructures are targeted. More than diversification, the complexity, scale and frequency of cyberattacks continued to rise.

The private sector invests heavily in developing and deploying secure technologies. Current trends related to the spending on cybersecurity are estimated at $150 billion in 2021. In addition, businesses spend significant time supporting and collaborating on initiatives to promote norms for responsible uses of technology and information. Examples of launched initiatives include the Global Forum on Cyber Expertise, the Cybersecurity Tech Accord, the Paris Call for Trust and Security in Cyberspace.

However, despite these considerable efforts, the business community and governments alike continue to be exposed to unacceptable and growing criminal and state sponsored malicious cyber activities. Bold and decisive action to curtail these activities is no longer an option, it is a necessity.

Fighting cybercrime – where are we at?

The most comprehensive multilateral cybercrime treaty to date is the **Council of Europe Convention on Cybercrime**, commonly referred to as the Budapest Convention. The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with

infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. It is signed by 68 countries to date (ratified by 66), both members and non-members of the Council of Europe (CoE). The Russian Federation remains the only CoE member not to have signed on to the Convention.

In January 2022 a two-year process to develop a new global convention on cybercrime gets underway under the 3rd Committee of the United Nations General Assembly, in the **Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes** (AHC). Originally proposed by the Russian Federation, the AHC is seen by many states as a vehicle to create a competitor agreement to the Budapest Convention. The main argument for a new treaty is that there is no expressly global treaty on cybercrime and that the Budapest Convention is only a European instrument - even though it is open to any member-state that wants to join and many non-European states already have. The timing of this initiative is not accidental; the parties to Budapest have finalised a new protocol to Budapest which industry has participated in drafting and which considerably modernises and updates Budapest's provisions.

The AHC will have six meetings, three each in New York and Vienna and at the end requires only 60% of participating governments to support for it to be submitted to the UN General Assembly in 2023 for adoption.

Towards an international convention on cybercrime – the business perspective

Against this backdrop, speakers and participants discussed the prospects for a new international convention on cybercrime, as well as potential impacts on business.

Considerations on the process:

- The objective is an outcome that doesn't exist at the global level but there is a real risk that the substance would duplicate or contradict existing agreements;
- Since the expertise on cybercrime in the UN system is focused in Vienna at the UN Office on Drugs and Crime having this process overseen by the UN in New York carries the risk that conversations would concentrate on political interests over substance;
- Given that the process requires the support of only 60% of participating governments to reach an agreement on the outcome, there is a considerable risk of controversial or potentially harmful positions to be included - a consensus-based process does not carry that same risk;
- Ultimate adoption is by the UN General Assembly (which seeks to adopt outcomes by consensus but might vote on contentious issues), which magnifies the opportunity for political considerations and deal-making;
- States have shared their input and ideas for the convention's scope and substance and the Russian Federation has already tabled a draft treaty for consideration at the first meeting of the AHC. However, all other states that submitted positions, would prefer to start with a general conversation on scope and objectives, rather than start with text negotiation right away – a position also supported by business.

Business perspectives on a new convention

- Business is in favour of international efforts to reduce cybercrime's impact and increase the consequences for those who engage in it as the private sector is a primary victim of such crimes. The private sector must be integrally involved throughout the process of developing a new convention, as it is on the front lines of combatting cybercrime daily. Businesses know first-hand which legal and policy measures are effective - and which are less so - in transboundary online crime prevention and prosecution efforts and why.
- Any treaty outcome on cybercrime must draw upon existing treaties and agreements and not duplicate or create unintended negative consequences through conflicting or ambiguous provisions;
- The scope of an international convention on cybercrime should focus on widely-understood criminal acts which have common, or compatible, definitions in many different legal jurisdictions. States must not include any crime that has a cyber component but criminalize offences that are cyber dependant. Agreement on definitions is key. These must be precise enough to not allow for misinterpretation or serving national interest, therefore vague concepts (such as threat against the country) should be avoided.
- A new convention should encourage effective international cooperation between national law enforcement and prosecutorial agencies in investigating and prosecuting cybercrime.
- There must be a balance of sanctions with related safeguards including independent judicial review, sanctions imposed by processes independent of investigatory processes, and reflective of the international acquis of international human rights law and norms. This balance also helps reduce the potential for unintended negative consequences when measures in treaty form are transposed into international law.
- Negotiators must seek to ensure that human rights protections are clearly factored in at every step of the negotiations, and that rights to free expression, access to information and privacy are preserved in line with certain minimum standards of proportionality and necessity.
- One participant also noted that a new convention provides an opportunity for greater collaboration between governments and the private sector in matters related to lawful data access. This is especially the case for cloud service providers. States should use this opportunity to recognize the need to resolve any existing conflicts of laws, jurisdictional and sovereignty issues in this space. Moreover, any lawful data access framework needs to include the requirement that access to digital information is only allowed pursuant to lawful process and create an opportunity for technology providers to challenge such process on behalf of their customers to ensure that governments are acting within the law and are respecting the rights of their users. Moreover, except in limited cases, individuals and organizations have a right to know when governments access their digital information. Secrecy should be the exception not the rule.
- The convention should include options for refusal on the grounds of dual criminality, refusal in respect of political offences, and refusal of a request made for the purpose of punishing or persecuting the individual on grounds of their race, religion, gender, or other protected characteristics.
- Participants stressed that the need for cooperation across all regions and stakeholders and regions. Clear and continuous communication is necessary to develop a common understanding of issues and challenges, as well as to share experiences, best practices and build capacity.

Next steps

This report will be used to inform the work of the ICC Digital Economy Commission Working Group on Cybersecurity as well as ICC's positions and input to the Ad Hoc Committee.

ICC will be closely monitoring the process to develop an international convention on cybercrime and will continue to organize roundtables with the business community to discuss and contribute to this process.

To further contribute to this report, please email timea.suto@iccwbo.org.