Institute for Peace Research
and Security Policy
at the University of Hamburg

IFSH – INTERNATIONAL CYBERSECURITY

NEGOTIATING A GLOBAL CYBERCRIME CONVENTION: PROMISES AND PITFALLS

INTERDISCIPLINARY WORKSHOP

The harmful effects of cross-border criminal cyber-attacks were made abundantly clear as hospitals, energy providers, and other infrastructure services were indiscriminately hit or even targeted last year. There is a broad consensus on the need to strengthen cooperation between police and law enforcement agencies to combat these developments. What role could the scheduled UN negotiations on a convention against the criminal misuse of information and communication technology play? Are we on the way to an effective global legal framework, or is it more likely that yet further fragmentation will weaken existing cooperation mechanisms? André Dornbusch (German Federal Criminal Police Office), Louise Marie Hurel (Igarapé Institute), and Nnenna Ifeanyi-Ajufo (Swansea University) discussed these and related questions at the third interdisciplinary workshop organised by IFSH's "International Cybersecurity" team in cooperation with the German Federal Foreign Office. Mischa Hansel (IFSH) moderated the event attended by more than 100 academia, business, diplomacy, politics, civil society and media representatives.

Civil society, in particular, will suffer if the international community does not succeed in tackling cybercrime, as ransomware attack have shown. Further risks stem from unintended consequences, such as inadvertent interstate tensions or escalatory effects caused by private hack-backs. More cooperation at the international level should therefore be in everyone's interest but remains an uphill struggle. Some workshop participants were sceptical whether the Russian initiative, overshadowed by geopolitical tensions, could actually lead to a global agreement. While the Russian draft includes content-related offences such as aiding terrorism and separatism, the USA, the EU member states, and other partners want to limit an agreement to cybercrime in the narrower sense. This includes, for example, the sabotage of digital systems and data. Furthermore, there is a fundamental dispute about the extent to which non-state actors are allowed to participate in the negotiations.

This negotiation constellation is fragile and scattered with pitfalls. For example, criminal offences that are defined too narrowly could lead to a quickly outdated agreement overtaken by technical developments. It could also hinder practical cooperation between law enforcement agencies. At the same time, however, the provisions need to be as precise as possible in order to prevent misuse, as repressive regimes have used legal frameworks to silence critical voices. In other cases, state actors have resorted to disproportionate measures as they lack expertise and resources. A case in point is 2016 Brazilian local court ordering a nationwide shut down of WhatsApp, reportedly to enforce access to encrypted communication during a criminal investigation. To prevent reinforcing such tendencies, human rights standards and principles of the rule of law must be at the heart of any agreement. Civil

society actors should therefore actively participate in the preliminary negotiation process. Moreover, they should play a leading role in monitoring implementation.

Another challenge is not to undermine existing standards and commitments. Many examples in the discussion focussed on the practical benefits of having a uniform definition of criminal offences, such as in the Council of Europe's Budapest Convention. Rapid cross-border preservation of evidence and the possibility of requesting traffic data directly from foreign internet providers is equally important given widely dispersed and fleeting evidential traces. Again, the Budapest Convention is widely regarded as a model of such provisions. Signatory states could become subject to conflicting obligations if a new legally binding agreement with divergent terminology comes into force, limiting cross-border cooperation. Further risk arise from encroaching on the politically binding UN norms of responsible state behaviour, which could be undermined by divergent provisions in a future agreement.

At first glance, it might seem to be preferable to implement existing standards and make them universal instead of reinforcing legal and political fragmentation. Yet, the discussion showed that the situation is far more complex, referencing for example the various position of African states and the very small number that have ratified the Budapest Convention. Here and in other countries of the Global South, negotiating a new agreement would offer a real chance to shape the future of international cybercrime governance. International capacity-building could also be strengthened in this way, focussing on local problems and on ways to effectively address structural inequalities. The discussion also highlighted that at the practitioners' level, even seemingly small steps such as uniform definitions and time-saving procedures for mutual legal assistance make a big difference. The benefits of agreeing on some basic rules for policing operations, such as when dealing with botnets, were also debated. Overall, the participants were hopeful that a UN agreement based on practical experience could contribute to global cyber security. However, great care has to be taken not to create a treaty that from the onset is followed in letter but not spirit: implementation pitfalls have to be considered from the beginning and international capacity building efforts need to be realigned.