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

Cybercrime:
Working Together to Mitigate Peace and Security Threats

In January 2022, United Nations (UN) member states will begin discussing a global treaty against cybercrime. Greater international cooperation on this topic is urgently needed, as criminal cyberattacks, for example against hospitals and power grids, risk leading to panic or even loss of life. Purely national countermeasures are not enough as perpetrators are often located abroad. A new global regulatory framework should therefore:

- reaffirm proven standards, in particular those of the Council of Europe's Budapest Convention on Cybercrime,
- respond to escalation risks and protection gaps with appropriate policy instruments, and
- prevent human rights violations committed under the pretext of fighting crime.

07|21

MISCHA HANSEL AND JANTJE SILOMON | 2021

Cybercrime is becoming a growing threat to international peace and security. Attacks against critical infrastructures such as hospitals and energy suppliers endanger basic public services. In some cases, states cover for cybercriminals or even use their activities for political purposes. This topic is therefore highly volatile internationally, and escalating interstate tensions in the wake of cyberattacks is a real threat. In view of the upcoming UN negotiations on a "Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes,"[1] three points are essential. First, existing best practices of cross-border cooperation should be strengthened. Second, new instruments that can help to curb escalation and close protection gaps need to be developed. Finally, repressive regimes must be prevented from committing human rights violations under the pretext of fighting crime.

CRIMINAL CYBERATTACKS TAKE ON A NEW QUALITY

The spring and summer of 2021 saw several major ransomware attacks on targets in the United States. In some cases, Russian-speaking cybercriminals attempted to extort ransom by encrypting critical data. One such attack on the billing system of a major pipeline operator had particularly serious consequences: halted operations led to the near collapse of fuel supplies in several US states. In response, US President Biden hinted at retaliating by carrying out cyberattacks against critical infrastructures in Russia should further attacks occur. A few weeks later, he also invoked a "real shooting war" scenario that might materialise because of future escalations in cyberspace.[2]

> „INTERNATIONAL COOPERATION IS LAGGING WHEN IT COMES TO PROSECUTING CYBERCRIME."

Criminal cyber operations not only cause considerable damage, but threaten peace at the global level, for example when ransomware attacks are carried out by non-state actors as seen in the example above.

BLURRING THE LINES BETWEEN CRIME AND POLITICS

Several factors increase the risk of escalation associated with this form of cybercrime. First, cybercrime is characterised by a growing division of labour and competition. Some providers make specialised servers available, others trade in security vulnerabilities, while yet others rent or sell ready-to-use malware. Competition for "customers" adds further complexity to the issue: when in doubt, cybercriminals may be willing to cater to more risk-tolerant customers, including those who accept or even seek to cause the most damage. Second, it is not always possible to distinguish between criminal ransomware attacks and politically motivated sabotage. In both cases, the target's critical data is encrypted, thus blocking access to it. Finally, state actors sometimes engage in strategic cooperation with criminal groups, disguising politically motivated cyberattacks. This undermines international norms and rules by providing a basis for credible deniability on behalf of the state actor.

Overall, international cooperation is lagging when it comes to prosecuting cybercrime. As a result, companies that have been attacked are starting to take defence into their own hands, in some cases even hiring private security firms to offensively act against criminal infrastructures. Such "hack-backs" pose dangers of their own, however, including inadvertent harm to innocent third parties.

„GAPS IN INTERNATIONAL COOPERATION MUST BE CLOSED WITHOUT OPENING THE DOOR TO MISUSE."

ONWARD TO A NEW SET OF RULES?

More effective international measures would therefore be an important contribution to international peace, particularly because the norms of responsible state behaviour agreed within the UN context have thus far only dealt with cybercrime indirectly. The UN Ad Hoc Committee convened on Russia's initiative to discuss an international treaty against cybercrime at the beginning of next year is to be welcomed – at least in principle.

The Russian draft treaty is nonetheless problematic in several respects.[3] First, criminal offences in cyberspace are only very vaguely defined, allowing for political misuse under the guise of combating crime. Moreover, its lack of reference to human rights standards suggests that it may primarily be aimed at legitimising internet censorship and surveillance. Thus, the Russian initiative could – in and of itself – become a risk to (societal) peace. Second, the draft precludes direct cross-border access to the data held by internet providers – unlike the Budapest Convention of the Council of Europe, for example, which more than 20 non-European states have also ratified. In this regard, the Russian draft would be a step backwards, particularly in the age of cloud services, where evidential traces are widely dispersed and fleeting and where traditional mutual legal assistance requests therefore have little chance of success.

With that said, there is no question that current deficiencies must be remedied, such as the global trade of surveillance and hacking tools. Thus far, very few states have addressed this topic sufficiently, despite the fact that crimes using such tools are being committed abroad. Another obstacle to effective cross-border cooperation is a lack of resources, which has limited states' ability to access and utilise the relevant data, particularly in countries in the Global South. This is in the interest of all states, however, as it can help to prevent the emergence of new "safe havens" for cybercriminals.

A QUESTION OF BALANCE

Negotiators will need to strike a delicate balance: gaps in international cooperation must be closed without opening the door to misuse. To ensure this, civil society should be actively involved in negotiations and in monitoring implementation. In addition to a clear commitment to human rights, a new treaty should remain "backwards compatible" by interlinking with existing cooperation obligations. Otherwise, the progress made in the fight against cybercrime could be jeopardised. Furthermore, any agreements related to cybercrime should complement and support – and in no way weaken – the UN norms of responsible state behaviour.

Agreement on a universal definition of private hack-backs and on sanctioning these activities under criminal law, for example, could clarify an important aspect of the duties of due diligence incumbent on states, currently outlined only in abstract terms as part of the UN norms. Finally, countries in the Global South must be provided with greater support to facilitate their participation in transnational investigations. A global agreement that contributes effectively to peace can only emerge if the advantages are shared by states across all regions.

ENDNOTES

[1] United Nations General Assembly 2021. Resolution 75/282 – Countering the Use of Information and Communications Technologies for Criminal Purposes, https://undocs.org/en/A/RES/75/282

[2] The White House 2021. Remarks by President Biden, 27.07.2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/27/remarks-by-president-biden-at-the-office-of-the-director-of-national-intelligence

[3] Kommersant 2021. Draft United Nations Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes, unofficial translation, https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_E.pdf

ABOUT THE AUTHORS

Dr Mischa Hansel is the head of the research focus “International Cybersecurity” at the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH). **Dr Jantje Silomon** is a researcher at the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH).

ABOUT THE PROJECT

This Policy Brief was written by IFSH’s “International Cybersecurity” team, funded by the German Foreign Office.

ABOUT THE INSTITUTE

The Institute for Peace Research and Security Policy (IFSH) researches the conditions for peace and security in Germany, Europe and beyond. The IFSH conducts its research independently. It is funded by the Free and Hanseatic City of Hamburg.

Funded by:

Hamburg | Ministry of Science, Research, Equalities and Districts

DOI: https://doi.org/10.25592/ifsh-policy-brief-0721E

Copyright Cover Photo: Picture Alliance / REUTERS | Kacper Pempel

IFSH – **Institute for Peace Research and Security Policy** at the University of Hamburg
Beim Schlump 83 20144 Hamburg Germany Phone +49 40 866077-0 ifsh@ifsh.de www.ifsh.de