11 // 2024

spotlight

BETWEEN A ROCK AND A HARD PLACE

The UN Cybercrime Convention

In December 2024, UN members will vote on a worldwide Cybercrime Convention negotiated since 2019. While the convention is problematic, this Spotlight shows why a conditional acceptance nonetheless seems the best way forward. For this purpose, we first present the different meanings of cybercrime and outline the existing regulatory framework. We then examine the UN negotiations and the possible human rights implications of the convention, showing that it reflects the contestation of human rights norms and a growing division in the UN, yet supporting the convention at this point also enables long-term influence on its implementation.

Adopting a global treaty on cybercrime is a rare opportunity to demonstrate that multilateralism in the UN can bridge divisions among states. Photo: © Lena Herbst.

BY ANJA P. JAKOBI AND LENA HERBST

The fact that cybercrime is not strictly defined makes it an inherently political term, used differently depending on what is being criminalized in which context. In its most basic understanding, cybercrime is a 'cyber-enabled crime' and thus refers to well-known crimes facilitated by the internet and digital technology: from fraud via email to digital harassment and illegal marketplaces. In addition, 'cyber-dependent crimes' can only be committed through this technology. Computer systems are thus necessary instruments for cybercrimes but also targets of cybercrime, such as when criminals compromise software, hardware, and networks. This also implies that there is no definite list of cybercrimes, nor do cybercrimes have much in common beyond the name, and various activities can be labeled 'cybercrime' depending on a given national context. For instance, the United States has a different understanding of free speech than many European states, and censorship in Russia or China defines crimes that are unknown in other countries. All this is reflected in the content users can post legally. At the same time, a large part of the digital infrastructure is in private hands, and regulatory efforts on the national level typically involve the storage of communication data and transmission to authorities on request. Any increased monitoring and surveillance of cyberspace shrinks possibilities of anonymity – this can be beneficial for countering crime yet can also endanger civil liberties and political opposition in non-democratic regimes.

EXISTENT INTERNATIONAL EFFORTS AGAINST CYBERCRIME

As a global treaty among states worldwide, the UN Convention would change existing international norms against cybercrime. Such global norms not only define crimes but also support the processes linked to global cybercrime governance, for instance, international law enforcement cooperation, joint operations across borders, or countering crime in cooperation with private companies that provide cyberspace infrastructure. International norms on cybercrime have emerged in different regions, such as regulations by the AU, ASEAN, or EU. Among these regional organizations, the Council of Europe

In December 2024 the United Nations General Assembly votes on the Cybercrime Convention, which was drafted by a committe since 2019. Photo: © Lena Herbst.

(CoE) adopted the first-ever convention against cybercrime in 2001 (in force since 2004). Despite its regional origin, the 'Budapest Convention' has been adopted by many states outside the CoE member base, most notably the US, which was also involved in negotiating it.

As an international convention, the Budapest Convention defines a range of crimes that states are expected to criminalize in national laws (Art. 2-11). Most of these criminalization requirements also found their way into the UN Convention, sometimes in more detail and with an updated presentation of current technology. They encompass different kinds of interference with computer systems, unauthorized data access, but also crimes like child pornography. It also contains many procedural aspects of accessing and monitoring communication data and data storage. At the same time, safeguard clauses exist (Art. 15) that explicitly refer to UN and CoE treaties on human rights. The Convention was supplemented by a protocol on hate speech in 2004, a topic not included due to differences among European countries and the US. The Budapest Convention represents an important international norm against cybercrime, being closely connected to the human rights framework of the CoE and other human rights norms. Yet, its universal status has always been contested. In an early competition for different rules, Russia, then a member of the CoE, began initiating debates on regulating cybercrime in the UN in 1999, ultimately leading to the nearly concluded negotiations.

HUMAN RIGHTS AND THE UN CYBERCRIME NEGOTIATIONS

The current draft convention is contested among states, and even initiating the process that led to it was not consensual but decided by a majority vote in 2019. Almost twenty years after Russia's initial attempt to establish such a UN treaty process, geopolitical changes and shifting majorities in favor of Russia's proposal led the UN General Assembly (GA) to establish the 'Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes' (AHC). The committee was tasked to "elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes," and it soon became an intense negotiation process open to all UN member states.

Accompanied by a selected multistakeholder community, the AHC drafted a comprehensive convention. After outlining the objective and some general provisions, the text defines the scope of applicable measures and criminal offenses. It further includes regulations on international cooperation, preventive measures, technical assistance and information exchange, and the convention's implementation. Ultimately, the convention's adoption requires consensus on all aspects. Yet, from the first substantive session in March 2022 onward, the negotiations were torn between a state-focused approach led by Russia, China, and allied developing countries and a multi-stakeholder, human rights-based approach supported by the US and Western countries. The AHC debated different approaches to *what*, *why*, *how*, and *by whom* cybercrime needs to be prevented and combated. Diverging perspectives showed in the negotiations on the convention's objective, the scope of criminalization, and the protection of human rights safeguards, revealing broader geopolitical fissures between states pushing for authoritarian multilateralism and supporters of multistakeholder, democratic governance.

Russia, China, and allied states firmly pushed for criminalizing a broad range of cyber-dependent and cyber-enabled crimes based on sovereignty arguments. This would have implications for which and whose data can be accessed, collected, stored, and even transferred, making it likely to come at the expense of people's data and privacy and paving the way for mass surveillance and data misuse. The EU, US, and like-minded states, echoed by the multi-stakeholder community, have vehemently called for strong human rights safeguards and emphasized the criminalization of cyber-dependent crimes. Statements repeatedly warned against the potential harm of a bad treaty that allows for mass surveillance, restricts freedom of expression due to the criminalization of content, and provides insufficient protection for journalists and security researchers. The lack of enforcement regulations and interpretations left to domestic law could lead to severe consequences for human rights in cyberspace.

Despite inter-sessional consultations, informal discussions in working groups, proposed package deals, and compromises, an agreement between these fundamentally different perspectives became impossible. With voices getting louder that no treaty might be for the best, the planned concluding session was suspended and reconvened in August 2024. Member states again discussed an updated draft text of the Convention with a narrower scope but limiting any reference to human rights and articles 6 and 24. Despite Iranian attempts to delete the remaining human rights references, the final document found a consensus, with all articles being agreed *ad referendum* and proposed to the GA.

While many paragraphs of this draft UN Convention resemble those of the Budapest Convention, noticeable changes and gaps exist: The crimes covered include more recently emerging crimes, like the dissemination of intimate pictures, but exclude copyright infringements (Art. 10 in the Budapest Convention). The jurisdiction of the UN Convention is relatively broad and includes cybercrimes committed abroad but directed against a state party (Art. 22). Non-democratic states could use this to claim the application of this Convention against criticism abroad. Most severely, the Budapest Convention refers to human rights treaties (Art. 15), including those of the UN, but the UN Convention does not contain the same references. Additionally, paragraphs transferred from the Budapest Convention have been changed, such as Art. 29 of the UN Convention on real-time cooperation, which is based on the wording of Art. 20 of the Budapest Convention, but without its reference to the protection of human rights.

IMPLICATIONS: TO RATIFY OR NOT TO RATIFY

Important decisions on the treaty are due in December 2024. Despite its shortcomings, the draft convention was agreed upon in the AHC as a compromise and is scheduled for a vote at the ongoing GA. If adopted, the UN Cybercrime Convention would enter into force after 40 ratifications (Art. 65). On the one hand, the treaty's adoption is seen as a formality, because states have already agreed upon the draft resolution in the reconvened concluding session of the AHC. A treaty is also one of the few opportunities to demonstrate that multilateralism in the UN can bridge divisions among states. On the other hand, given the treaty's implications, its adoption might cause

Figure 1: International Norm Development on Cybercrime.

THE AUTHORS

Prof. Dr. Anja P. Jakobi is Visiting Professor at PRIF and Head of the Institute of International Relations (IIR) at the TU Braunschweig. Lena Herbst is a PhD student at the IIR, TU Braunschweig.

CONTACT
anja.jakobi@prif.org

PRIF, Baseler Str. 27–31, 60329 Frankfurt am Main
PVst, DPAG 43853, Entgelt bezahlt, ISSN-2512-627X

long-term problems, weighting UN member states' decisions on voting and proceeding. This sidelining of human rights implications has led to a broad coalition of civil society organizations and private sector entities urging states to vote against the resolution's adoption and to neither sign nor ratify the Convention, to avoid any harm resulting from the treaty. They warn against potential surveillance and data misuse due to lacking human rights safeguards and data protection. This lack of consideration for data protection concerning citizens' rights also causes states problems when considering existing domestic and supranational regulations. All in all, the existing draft Convention signifies a treaty in which the application of human rights has been more contested than in regional conventions. For these reasons, democratic states might be particularly tempted to reject the Convention and neither sign nor ratify it.

It is, however, unlikely that the draft Convention will fail to pass the GA. Therefore, it seems advisable to accept the treaty with reservations and become a state party to the Convention. Without internal critics, the 'Conference of Parties' (CoP), tasked with reviewing and implementing the convention, could develop additional measures and worsen a Convention that at least includes some human rights safeguards. In particular, due to Russia's and China's growing influence, rejecting the Convention could pave the way for 'digital authoritarianism' in a central UN norm on cyberspace. Still, accepting the Convention requires careful monitoring, not only of the CoP, but also of its results in practice. If reviews of the treaty show that its implementation means compromising human rights and data protection, states should continuously reevaluate whether to stay or leave the treaty, with the Budapest Convention as a remaining fallback option.

PRIF SPOTLIGHT: The Peace Research Institute Frankfurt (PRIF) is the largest institute for peace research in Germany. PRIF sets out to analyze the causes of violent international and internal conflicts, carrying out research into the conditions necessary for peace and working to spread the concept of peace.

V.i.S.d.P.: Henriette Franken, Press and Public Relations (PRIF), Baseler Straße 27–31, Frankfurt am Main, Phone (069) 959104-0, info@prif.org, www.prif.org. Design: Anja Feix · Layout: PRIF · Print: Druckerei Spiegler

References and further reading:
prif.org/spotlight1124-fn
DOI 10.48809/prifspot2411

Peace Research Institute Frankfurt
Leibniz-Institut für Friedens- und Konfliktforschung

Leibniz Association