: Global Governance Spotlight
5 | 2021

sef:

A UN Cybercrime Convention – Putting human rights and development front and centre

Mischa Hansel

In January 2022, the United Nations (UN) member states will commence negotiations on a global treaty to counter cybercrime. More international cooperation in this field is urgently required, for cybercrime attacks on IT systems can put lives at risk, as the ransomware incidents against hospitals in numerous countries show. Cybercrime has been a global threat for some time, regularly also affecting countries in the Global South, where IT security often fails to keep pace with rapid digitalisation. It particularly impacts future-focused sectors such as e-commerce and mobile financial services, which are crucial for economic development. Making matters worse, many countries are poorly integrated into international cooperation between law enforcement agencies.

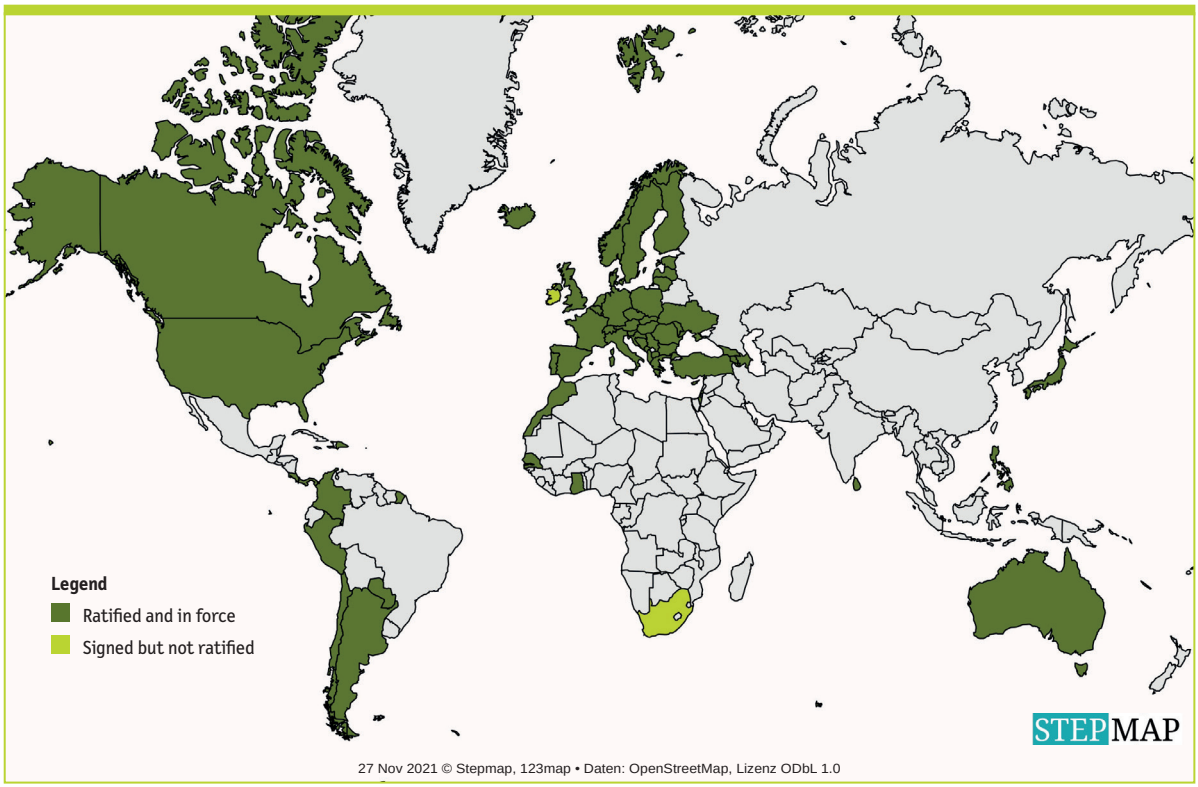
In light of the above, now is the time for a comprehensive global treaty against cybercrime. But there are risks as well. Vague commitments – on the monitoring of Internet traffic, for example – could be used by authoritarian regimes as a pretext to clamp down on activists and opposition forces, ostensibly in order to combat crime. To prevent this, human rights must be strengthened as a frame of reference and civil society actors must be able to contribute substantively to the negotiations. There is also a need for broader-scale capacity-building in countries of the Global South. And finally, a key task is to close existing loopholes, while not ignoring the social factors behind the drift into cybercrime. A global coalition for a human rights-compliant and development-centred regime would then be possible.

Towards a global treaty?

The dramatic increase in ransomware attacks on hospitals, the energy supply and public authorities reveals the full destructive potential of cybercrime operations. These attacks cause the encryption of critical data, with decryption software provided only after a ransom has been paid. Due to the transnational nature of most of these operations, international cooperation across police services and law enforcement agencies is essential in order to shut down the criminal infrastructures or extradite offenders. However, this is rarely successful, due to the lack of harmonised legislation, inadequate political support and ineffective procedures.

The United Nations could potentially start here by establishing a universally binding framework for cooperation against cybercrime. Thus far, cybercrime has been addressed as a sub-topic within the framework of the United Nations Convention against Transnational Organized Crime. In addition, the Commission on Crime Prevention and Criminal Justice (CCPCJ) set up by the UN's Economic and Social Council (ECOSOC) has convened expert groups on various occasions since 2011 in order to discuss ways of improving technical assistance and the exchange of information on legislation and best practices. As the latest move, Resolution 74/247, initiated by Russia and adopted by a majority in the UN General Assembly on 27 December 2019, provides for the establishment of an Ad Hoc Committee to elaborate, within

five years, a draft international convention which specifically counters the use of information and communications technologies (ICT) for criminal purposes. However, there are substantial differences of opinion on the scope and form of more intensive future cooperation. The relationship with existing regimes also remains unclear. This applies particularly to the 2001 Council of Europe (CoE) Convention on Cybercrime (Budapest Convention), which has been ratified by numerous non-CoE countries around the world and was comprehensively updated by an Additional Protocol in 2021.



Ratification status of the Council of Europe Convention on Cybercrime (30/11/2021)

Geopolitical conflicts

It is already becoming apparent that geopolitical issues and conflicts of interest will make the Ad Hoc Committee's work more difficult. Russia, for example, has already submitted a draft treaty which greatly expands the scope of criminalisation but gives a prominent role to national sovereignty, allowing international cooperation solely in relation to conventional requests for legal assistance. Under the Budapest Convention, by contrast, law enforcement agencies may submit data requests directly to commercial Internet service providers in another country without first obtaining the consent of its authorities. These opportunities have now been extended under the Second Additional Protocol, not least because the availability of cloud services means that cybercriminals are now able to cover their tracks very swiftly, with investigating authorities barely able to keep pace.

Other conflicts of interest relate to data protection issues and protection from the misuse of executive powers. For example, the Russian draft calls for the almost seamless collection and preservation of traffic data by the authorities or providers as part of crime prevention. What's more, crimes such as "political extremism" and "terrorism" are defined in extremely vague terms – in effect, giving carte blanche for the use of these provisions against any political opposition. The European Union member states' position, by contrast, is that a future treaty should cover a small number of precisely defined offences. Tendencies for camps to form are also becoming evident in relation to practical cooperation, e.g. against ransomware. As an example, China and Russia, which are accused of tacitly cooperating with cybercrime groups, were not invited to participate in the US-led International Counter-Ransomware Initiative.

Focusing solely on the world's top cyber powers – the US, China and Russia – is not enough, however. From a European perspective, the fact that the Russian resolutions on this topic have clearly resonated with democratic countries such as Nigeria, India and Brazil and that the Council of Europe's Cybercrime Convention has been ratified by very few countries on the African continent should give us pause for thought. It is essential, therefore, to recognise that cybercrime is a genuinely global

problem which does not only affect developed industrialised countries.

Cybercrime in the Global South

As one of the outcomes of the pandemic-induced economic crisis in countries of the Global South, criminal cartels have been able to recruit increasing numbers of skilled workers. These cartels seek their targets both within and outside their own regions. There is no sign of a global "Robin Hood effect" – the victims of cybercrime come from all over the world and from all social groups. And in the Global South in particular, cybercriminals pose a threat to sectors of key relevance to social development, such as digital financial services and e-commerce. Cybercriminals have it easy here, partly due to the widespread availability of illegal, poorly protected software in the Global South and the lack of technical, human and financial resources in many local law enforcement agencies.

However, not all the shortcomings in countering cybercrime, e.g. on the African continent, are homegrown. On the contrary, lack of access to data held by globally operating Internet companies is a further obstacle to successful investigations. On top of that, there is the lack of involvement in operational networks that support international cooperation among law enforcement agencies, notably in relation to offences which cannot be classed as cybercrime in a narrow sense but pose a particular threat to peace and development on the African continent.

They include the burgeoning trade in conflict goods (tropical timber, minerals, arms, drugs) on the dark web and Internet-based human trafficking. What's more, during phases of social instability, African countries are particularly vulnerable to incitement to violence or to disinformation on social media channels, which are often operated by service providers outside the African continent. These interests and priorities are reflected, not least, in the Malabo Convention, a regional agreement to promote cybersecurity and data protection, which includes content-related offences within the scope of cybercrime. This broad understanding of cybercrime clashes with the current negotiating position of the EU member states, which are lobbying for a lean convention, limited to a small number of cybercrimes, within the UN framework, in order to avoid duplication with other instruments and to limit the scope for abuse by authoritarian regimes.

In the Council of Europe's Convention on Cybercrime, which is regarded as a model by many European countries and the US, the criminalisation of content that is racist or glorifies violence is regulated on a purely optional basis through an Additional Protocol, but is not mandatory for all Parties. In view of the highly divergent understandings of the limits to freedom of speech, e.g. between the US and some European countries, anything else would be impossible to enforce.

Protecting human rights, enabling development

In order to forge as broad a coalition as possible for more intensive global cooperation against cybercrime despite these divergent standpoints and interests, the specific needs of the countries of the Global South should be considered, either in a future treaty or in other policy instruments.

As a core component, there should be a general commitment to more international capacity-building, preferably underpinned by the establishment of a multilateral fund. Given the severe budgetary constraints affecting many countries of the Global South, a lasting improvement in the resourcing of their law enforcement agencies cannot be expected any time soon. However, an agreement could also include guidelines on the prioritisation of legal assistance requests and transnational multilateral investigations. In the spirit of international solidarity, the decisive factor should be the actual or expected harm to society at large, regardless of where it occurs, not the local impacts.

As part of this capacity-building and practical cooperation, it is also important to curb the routine misuse of anti-cybercrime legislation that occurs in many countries. A global agreement should be aligned to rigorous rule-of-law standards, such as those established by the Council of Europe in its Convention on Data Protection. It should precisely define the offences and refrain from relativising fundamental human rights, such as the right to privacy. On the contrary, the requirement for human rights to be respected in all national and transnational investigations and law enforcement activities must be reaffirmed. In order to prevent abuse by the state, civil society actors should have the opportunity to be involved in negotiations and should also play a key role during the implementing and monitoring phase. And it goes without saying that efforts must be made to ensure that civil society actors from the Global South are not excluded from the process due to financial and logistical constraints; setting up regional liaison offices, for example, could help to address this issue.

Alongside negotiations on a binding international convention, more involvement of countries of the Global South in the institutional dialogue among law enforcement agencies would be welcome at

operational level. This can take place in a regional context, e.g. via the African Joint Operation against Cybercrime (AFJOC), initiated by INTERPOL. Beyond the regional level, however, forums for cooperation are also required, e.g. with European partner agencies. One example is the Joint Cybercrime Action Taskforce (J-CAT) set up by EUROPOL, in which Colombia, for example, is already involved as an institutional partner. Within networks such as these, countering Internet-based trade in conflict goods could be given particular priority.

A further point concerns the regulation of Internet platforms and software providers. The recent trade restrictions imposed by the US government on Israeli surveillance tech providers are merely the start of efforts to curb Western IT companies' support for oppression and torture. In addition to action against individual companies, more robust export controls and binding regulation of digital supply chains are required. This would pave the way for criminal prosecution of the persons responsible, as happened recently in France, where charges were brought against senior personnel at the French surveillance tech company Amesys. Regulations on disinformation and hate speech also do not go far enough if platform operators and service providers are merely required to comply with these provisions in their domestic markets. Instead, the overseas business operations of social media providers and digital platforms must be regulated on the basis of corporate due diligence.

And lastly, addressing the symptoms of cybercrime is not enough; in line with the UN's Sustainable Development Goals and an integrated approach, the social drivers must be considered as well. Unless economic prospects are created for millions of well-educated young people, e.g. on the African continent, efforts to clamp down on the cybercrime cartels' recruitment practices will be unsuccessful. This preventive approach is not without precedent. In the early 1990s, for example, US-Russian cooperation on the International Space Station provided employment opportunities in the civilian sector for Russian engineers, thus diverting them away from the lucrative but illegal proliferation of missile technology to Iran or North Korea. This farsightedness is necessary today, albeit on a much larger scale, in order to counter the pull factors of cybercrime in many countries of the Global South. While this cannot take place solely within the framework of the UN's Ad Hoc Committee, embedding this topic in the UN is a chance to address the prevention and countering of cybercrime in a wider context which includes human rights due diligence and development prospects.

Author

Dr Mischa Hansel | leads the research on International Cybersecurity (ICS) at the Institute for Peace Research and Security Policy, University of Hamburg (IFSH). @MischaHansel

References

Council of Europe 2001: Convention on Cybercrime, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000 1680081561.

Kommersant 2021: Draft United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Unofficial Translation, https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_E.pdf.

United Nations General Assembly 2020: Resolution 74/247: Countering the Use of Information and Communications Technologies for Criminal Purposes, https://undocs.org/A/Res/74/247.

Imprint

The Development and Peace Foundation (sef:) was founded in 1986 on the initiative of Willy Brandt. As a cross-party and non-profit-making organisation, the sef: provides an international high-level forum for shared thinking on urgent peace and development issues.

Global Governance Spotlight is a policy-oriented series whose purpose is to critique international negotiation processes from a global governance perspective.

Published by
Development and Peace Foundation (sef:)/
Stiftung Entwicklung und Frieden (sef:)
Dechenstr. 2 : 53115 Bonn : Germany
Phone +49 (0)228 959 25-0 : Fax -99
sef@sef-bonn.org : @sefbonn
www.sef-bonn.org

Editor
Dr Michèle Roth

Translation
Hillary Crowe

Design Basic Concept
Pitch Black Graphic Design
Berlin/Rotterdam

Layout
Gerhard Süß-Jung

Contents do not necessarily reflect the views of the publisher.

ISSN 2566-624X