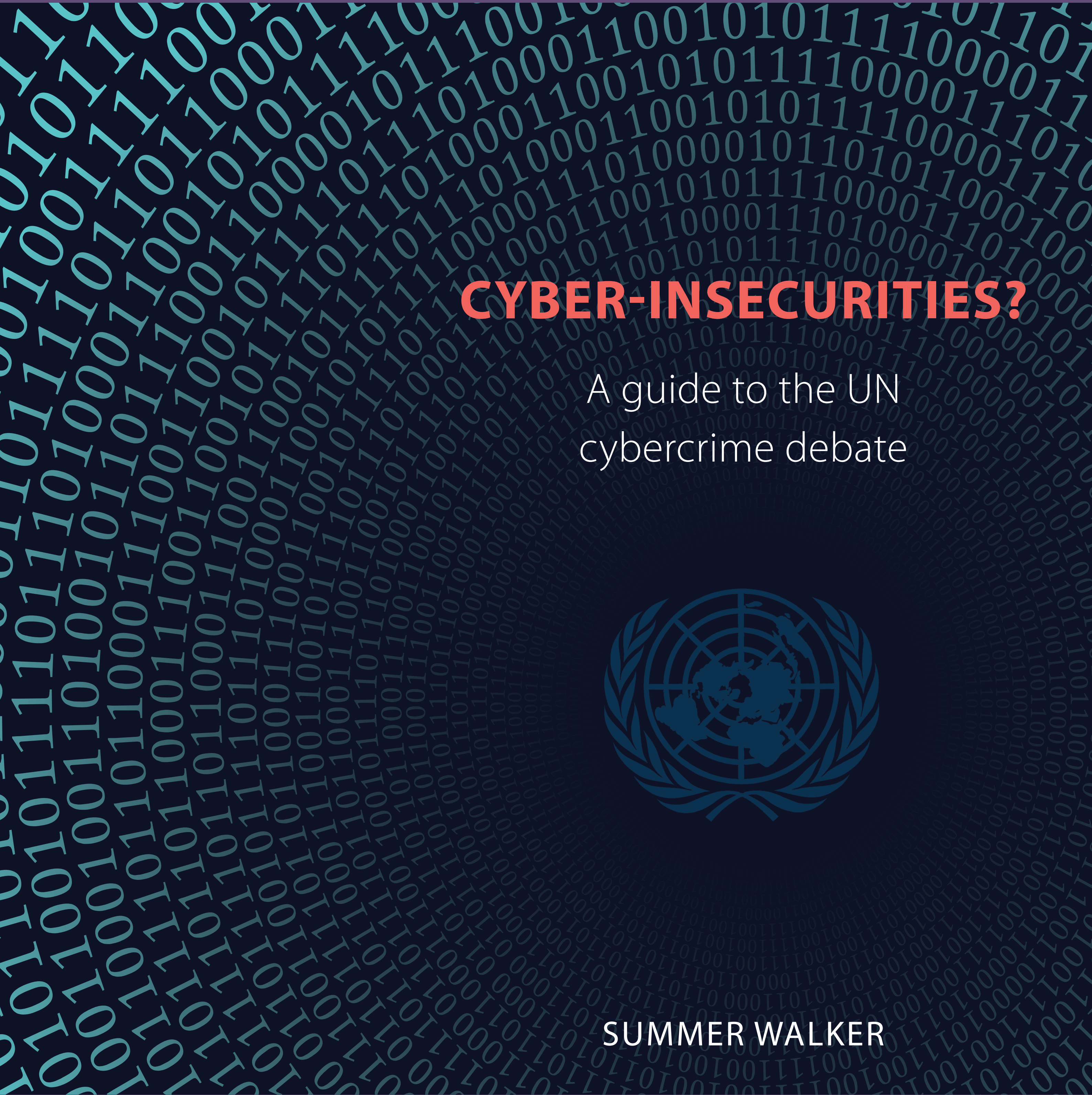
THE GLOBAL INITIATIVE
AGAINST TRANSNATIONAL
ORGANIZED CRIME

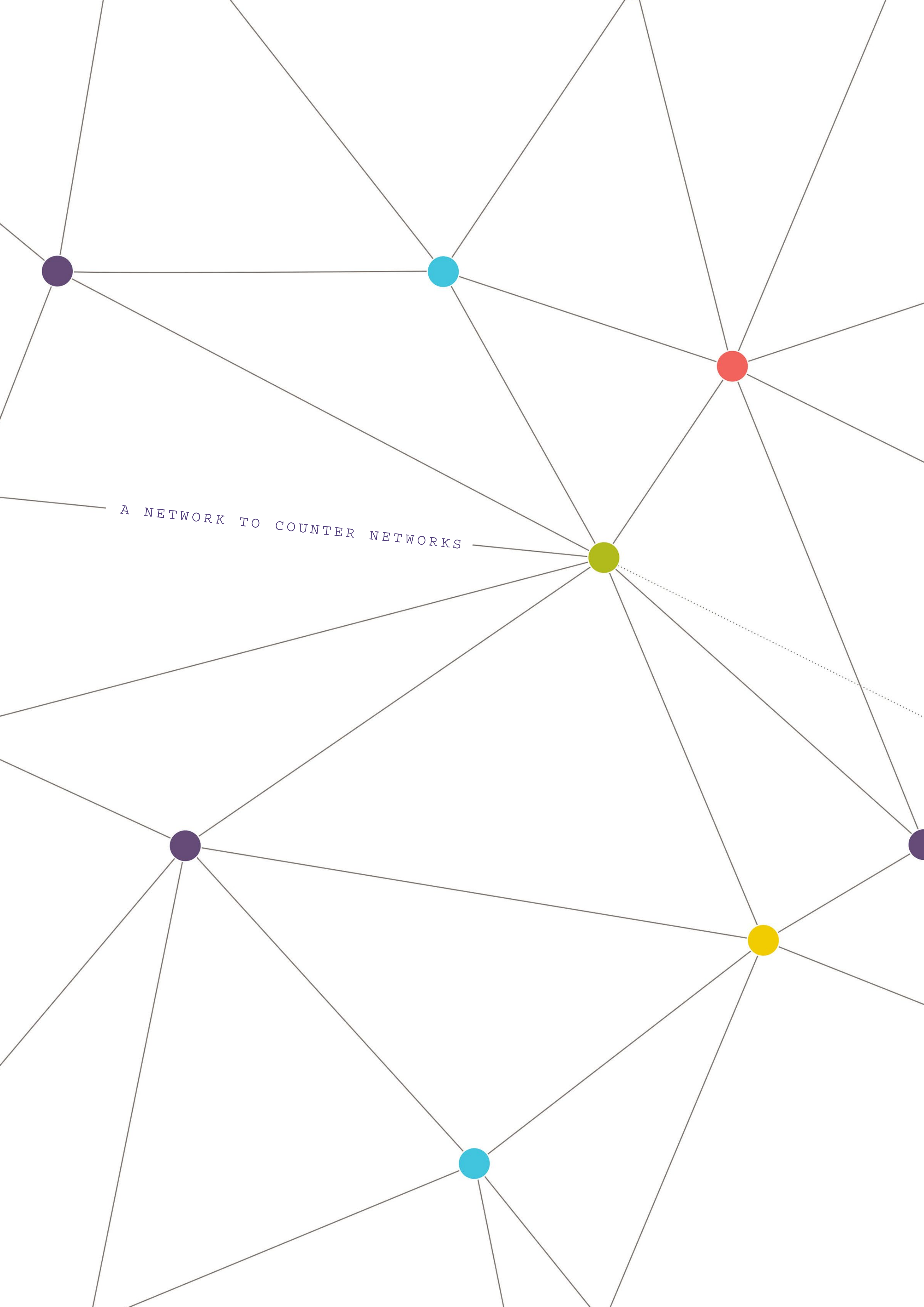


CYBER-INSECURITIES?

A guide to the UN cybercrime debate

SUMMER WALKER

March 2019



A NETWORK TO COUNTER NETWORKS

CYBER-INSECURITIES?

A guide to the UN cybercrime debate

SUMMER WALKER

March 2019

The Global Initiative Against Transnational Organized Crime
WMO Building, 2nd Floor
7bis, Avenue de la Paix
CH-1211 Geneva 1
Switzerland

www.GlobalInitiative.net

Contents

Introduction

This brief focuses on cybercrime in an international context, exploring in particular why the United Nations is still trying to find its footing as an agenda-setting institution on countering cybercrime.

There is no internationally accepted definition of cybercrime. For the purposes of this brief, however, it is understood as a crime in which a computer is either the object of the crime – for example, through hacking, phishing or spamming – or in which a computer is used as a tool to commit an offence, such as child pornography or hate crimes.[1]

Three types of crimes are often used to explain cybercrime: cyber-dependent offences, cyber-enabled offences and a specific crime type, such as online child sexual exploitation. Cyber-dependent crimes threaten the 'confidentiality, integrity and availability of computer data and systems'; cyber-enabled crime refers to offences that also occur offline, but in which criminals may deploy technology to achieve their ends.[2]

> *'At the UN, states have struggled to address cybercrime in a coherent manner.'*

Because internet services are available globally, they provide a platform that can be taken advantage of. As information communication technology (ICT) rapidly develops, people are often unaware of the risks associated with such technology, including cybercrime. In the past, cybercrime was committed mainly by individuals or small groups but, in recent years, complex cybercriminal networks have brought together individuals from across the globe in real time to commit cybercrimes.[3]

One study in 2018 on crimes related specifically to illicit access to networks or computers found that cybercrime costs roughly US$600 billion globally; it affects nearly two-thirds of people who use online services; and it is rapidly increasing owing to new technologies and cybercrime service centres.[4] Globally, cybercrime was the second most reported crime in 2016.[5] A study found that 'hackers are attacking computers and networks at a near-constant rate, with an average of one attack every 39 seconds'.[6] Cybercriminals now focus on using ransomware to extort money from businesses and individuals.[7]

As social services and businesses move their processes online, they become vulnerable to a range of cyber risks. The WannaCry ransomware attack, for example, where hackers threatened to disable systems or delete files to extract a payment, hit an estimated 230 000 computers around the world. The attack disrupted the activities of numerous major organizations, including the UK's National Health Service and Russian government ministries.[8] In the case of healthcare, cyber-attacks can harm critical infrastructure needed to care for patients or may expose personal medical records. Hence, these kinds of crimes have multi-layered impacts on individuals, institutions and society as a whole.

The annual global cost of cybercrime:

US$600 BILLION

These heightened risks do not mean, however, that there is a slowdown in the development of new technologies or new uses for existing technologies as companies forge ahead with technological applications, such as the Internet of Things and artificial intelligence.

The cross-jurisdictional nature of internet activity makes responding to this kind of criminal activity difficult at a national level. In response to cybercrime attacks, some countries have passed national laws that govern digital crime; they are also obligated to respect certain regional frameworks that have been adopted. Some of these laws include the Arab League Model Cyber Law, the Commonwealth Model Law on Computer and Computer-related Crime, the Directive on Fighting Cybercrime within ECOWAS (the Economic Community of West African States) and the Convention on Cybercrime of the Council of Europe, known as the Budapest Convention.[9]

At the same time, at the UN, states have struggled to address cybercrime in a coherent manner. The increased use of cyber-tools and -platforms for political and military objectives by states has generated a lack of trust among governments over cyber-related issues. While states are aware that cybercrime is a common international concern, they do not share a common understanding of how cooperation should work to address the challenge. This lack of congruity in the international response is connected to a growing breakdown in trust among governments, private companies and citizens regarding how cyberspace could, or should, be regulated – even at national and regional levels. Among states, and between stakeholders, this want of a shared vision hinders the ability to address cybercrime at the UN.

Cybercrime: The role of the UN

The UN is the key forum for regulating multi-jurisdictional issues. Several proposals on cybercrime and cybersecurity were considered during the 73rd UN General Assembly (GA) in September 2018. While it was believed that Russia would submit a draft cybercrime treaty to the UN secretary general and request a discussion within the Third Committee of the GA, in the end, a brief resolution was submitted and approved, which requests the secretary general to seek states' views on the challenges of countering the use of ICT for criminal purposes and present a report at the 74th session.[10] This resolution establishes a new reporting process on cybercrime, alongside existing mechanisms, such as the open-ended Intergovernmental Expert Group Meeting on Cybercrime (henceforth EGM).

This mirrors the cybersecurity debates held in the First Committee on Disarmament and International Security during the 73rd GA, which resulted in two separate processes on cybersecurity in the context of international security. The first, sponsored by Russia, creates an open-ended working group of the GA to develop rules, norms and principles of responsible behaviour regarding a specific set of previously agreed-upon norms from earlier UN processes.[11] The second, sponsored by the United States, establishes a group of governmental experts under the secretary general who will study cooperative measures to address existing and potential threats in the sphere of information security, as well as how international law applies to the use of ICT by states.[12]

Within the cybercrime debates, three broad issues, all interlinked, hamper progress on cooperation:

- Who should regulate cyberspace?
- Who should have access to data?
- Who should regulate online content?[13]

Who should regulate cyberspace?

There is disagreement about the need for a UN agreement on regulating cybercrime. The existing convention from the Council of Europe (CoE) is viewed by some as a sufficiently robust starting point for global cooperation, whereas others believe a new instrument with global inputs is needed.

Who should have access to data?

Transborder access to data is viewed by some states as an infringement of their national sovereignty, while others want to ensure that safeguards exist to protect privacy and freedom of expression online (transborder issues are discussed in more detail later).

Who should regulate online content?

The rapidly evolving nature of cybercrime, and technology in general, combined with vastly different domestic agendas for cybercrime, have made it difficult for countries to agree on the boundaries for cybercrime cooperation – which will leave some states wary of potential overreach in the realm of human rights.

These issues are specific to cybercrime deliberations but, at the same time, they are also tied more generally to fundamental debates about cyberspace at the UN. These debates within the area of cybercrime, and related to cyberspace at large, often divide key UN member states – and therefore stymie cooperation. Divergent perspectives on the role of cyberspace in society lie at the heart of many of the disagreements over cooperation. This brief examines these overarching debates, explores how they manifest in cybercrime deliberations and takes stock of the current UN agenda on cybercrime.

'Debates within the area of cybercrime, and related to cyberspace at large, often divide key UN member states.'

Differing perspectives on cyberspace hamper consensus

Diverging approaches about who should regulate cyberspace, have access to data and regulate online content are interrelated and connected to basic principles of the UN System. These include national sovereignty and human rights, in particular the right to privacy and freedom of expression.[14]

Two broadly differing approaches to internet governance are envisioned by different groups of states. At one end of the spectrum, Russia, China, the Shanghai Cooperation Organization (SCO) member states and a number of developing countries favour a state-led governance approach based on territorial integrity and sovereignty. This position is partially a response to early US technological superiority, such as US control over the global website naming system Domain Name Service, which triggered fears of US exploitation of an open internet for political purposes.[15] China and Russia in particular have championed 'digital sovereignty' – in other words, exercising jurisdiction over ICT infrastructure and digital activity in a state's territory.[16]

Western states, on the other hand, including the US and EU member states, support a multi-stakeholder model, which includes private-sector actors, such as technology companies. This can be seen in the Organization for Economic Cooperation and Development (OECD)'s principles for internet policymaking, which reiterate support for a multi-stakeholder approach.[17]

Content regulation and access to data are two key elements that play out in the cybercrime discussions.[18] Some note that a tripolar order in regulation has arisen, with China representing the state-led approach, the EU following a citizen-first approach and the US letting the private sector take the lead, with the government responding after negative events occur.[19] China's state-led model includes the 'great firewall',[20] crackdowns on privacy tools, such as virtual private networks, and regulations requiring data from its citizens to be stored in China. To cite one example, Apple must store iCloud content for Chinese users, including encryption codes, within China with a Chinese-owned telecommunications company.[21] And it is largely understood that all data on WeChat, China's most popular messaging application,[22] is accessible to the Chinese government.

In the US, data regulation has been driven by private companies, with service providers largely determining data privacy and access rights. And while it may seem as though the US private sector is driving policy, the exposed National Security Agency's surveillance programme revealed that the government is willing to allow its intelligence agencies to monitor citizens' data outside democratic norms.[23] At the other end of the spectrum, the EU's General Data Protection Regulation (GDPR) is now the strongest statute affording citizens' their right to digital privacy.[24]

These different approaches reflect the divergent stances taken by governments on control of cyberspace and data ownership. They are differences that play out in a number of UN agendas, including counterterrorism, human rights, and international peace and security, and they have hampered the ability of states to set a universal mandate for cybercrime. As cybercrime discussions among UN member states remain in exploratory stages, the central debates track closely the different prevailing viewpoints held by states on government versus citizens' rights in cyberspace.

Cybercrime and the UN System: Platforms for discussion

The Commission on Crime Prevention and Criminal Justice (CCPCJ) has served as the primary UN outlet for cybercrime debates. In 2010, Russia proposed a cybercrime treaty at the Twelfth UN Crime Congress, but negotiations failed over issues of national sovereignty, on one side, and protection of online rights on the other.[25] Consequently, the CCPCJ established the EGM, as well as the Global Programme on Cybercrime within the UN Office on Drugs and Crime (UNODC), funded by Australia, Canada, Japan, Norway, the UK and the US.[26] The EGM was formed to conduct a study of cybercrime and responses by states, the international community and the private sector. This resulted in the Comprehensive Study on Cybercrime, which has been used as a reference document by member states.[27]

The EGM, working under the auspices of the CCPCJ since 2011, continues to be the main mechanism for ongoing cybercrime discussions at the UN.[28] Some have called the expert group 'the only platform within the United Nations' to exchange information and examine options for responses to cybercrime.[29] A decision was taken for the group to continue operating as a mechanism to discuss national legislation, best practices, technical assistance, international cooperation, and new national and international approaches to cybercrime. In 2017, the CCPCJ consolidated the group's role by asking it to function as 'the platform for further discussion on substantive issues concerning cybercrime'.[30]

'There is no agreement that a UN treaty or protocol on cybercrime is necessary.'

Frequency of cybercrime attacks:

1 EVERY 39 SECONDS

The CCPCJ and cybercrime

The thematic focus of the CCPCJ's 2018 27th session was cybercrime, which was requested by the UN's Economic and Social Council. States held a thematic session on the topic and a workshop on criminal-justice responses to prevent and counter cybercrime. Some of the key challenges discussed were the evolving nature of cybercrime, fears of a digital underground economy that trades in data and facilitates other forms of crime or terrorism, and difficulties in legal proceedings related to cloud computing and data access.[31] In responding to cybercrime, states highlighted the need to update procedural law, facilitate access to electronic evidence, establish public–private partnerships, build capacity and exchange best practices.[32]

Within this framework, states continue to lay the groundwork for international cooperation on the issue. In 2018, the EGM approved a four-year work plan to collect and consolidate member-state recommendations and conclusions on strengthening practical responses to cybercrime.[33] For this, the EGM will hold annual meetings leading up to a stocktaking meeting in 2021. Each meeting will have a specific thematic focus: legislation, frameworks and criminalization in 2018; law enforcement and investigations, including electronic evidence and criminal justice in 2019; and international cooperation and prevention in 2020.[34] The results of the stocktaking will be submitted to the CCPCJ for consideration in 2021. Although it is unclear what the potential outcome of the initiative will be, the major obstacles in cybercrime discussions are already evident in the EGM's 2018 deliberations, and these reflect the broader debates around national sovereignty, privacy, data and governance.

One overarching obstacle, however, facing the EGM and its stakeholders, and a relatively serious one, is that there is no agreement that a UN treaty or protocol on cybercrime is necessary.

Should there be a UN agreement on cybercrime?

From the above discussions, it is clear that individual states and regions have taken steps towards establishing their own legislative frameworks to govern cybercrime. However, a gap continues to exist at the international level, where there is no legally binding instrument that all countries can refer to.

The EGM remains the forum for multilateral engagement on cybercrime largely because states have not settled on a more formal mechanism. The EGM's 2018 report made two recommendations, which track with the two dominant positions: either member states should develop a new international legal instrument on cybercrime within the framework of the UN that takes into account the concerns and interests of all member states, or they should use and/or join existing multilateral legal instruments on cybercrime, such as the Budapest Convention, as these are considered by many states to be best-practice models guiding appropriate domestic and international responses to cybercrime.[35]

'The Budapest Convention has the furthest global reach and is viewed as the counterpoint to a UN agreement.'

Some states caution that fundamental disagreements over 'scope, national sovereignty and jurisdiction' could hinder negotiations for a UN agreement.[36] While the UNODC's 2013 Comprehensive Study on Cybercrime warns against compartmentalized cooperation on cybercrime,[37] the most observable progress that has been made is at the regional level, where there has been cooperation on cybercrime legislation within the Commonwealth of Independent States, the Organization of American States, the African Union and the SCO, among others.[38] The Budapest Convention has the furthest global reach and is viewed as the counterpoint to a UN agreement.

Number of devices affected by WannaCry attack:

230 000

Table 1: Summary of current and proposed mechanisms established to respond to cybercrime

Current mechanisms
Budapest Convention
The Shanghai Cooperation Organization
Commonwealth Model Law on Computer and Computer-related Crime
Organization of American States – Inter-American Cooperation Portal on Cyber-Crime and a Working Group[39]
African Union Convention on Cyber Security and Personal Data Protection[40]
Directive on Fighting Cybercrime within ECOWAS[41]
Arab League Model Cyber Law
Suggested/proposed mechanisms
To use the Budapest Convention as basis for law-enforcement cooperation
To use the UN Convention against Transnational Organized Crime (UNTOC) to complement regional and bilateral engagement
To negotiate a new global instrument/universal treaty on cybercrime

Arguments for a global universal treaty

A group of states, including China, Russia and a number of developing countries, would like to see a global instrument on cybercrime, claiming that a newly negotiated legal document with global inputs is necessary. This argument is based on the fact that these states were not involved in the drafting process of the Budapest Convention (which, it has been suggested, should provide the basis for an international treaty). Many claim the convention does not reflect their concerns, in particular national sovereignty concerns over transborder access to information and electronic evidence, even if many of those issues are now being attended to.[42] This major contention relates to one article – Article 32(b), which allows states to obtain information in another country if the lawful owner of the data consents, without the need for government approval.[43]

In 2017, BRICS members reiterated a desire for a 'universal regulatory binding instrument on combatting the criminal use of ICTs under the UN auspices'.[44] This debate also played out during the Conference of Parties to UNTOC in October 2016, with some states calling for a new legal instrument on cybercrime, claiming the Budapest Convention does not provide enough scope for cooperation on the issue. Others said strengthening existing instruments, including UNTOC and the Budapest Convention, was the right direction.[45]

Russia (a CoE member that has not signed the Budapest Convention) has led the push at the UN for a multilateral agreement on cybercrime. In October 2017, Russia submitted a new draft UN Convention on Cooperation in Combating Cybercrime to the secretary general[46] and, as mentioned, was expected to propose it as a discussion item at the GA in 2018[47] but instead secured a resolution tasking the secretary general to produce a report on the challenges of countering the use of ICT for criminal purposes.[48]

Arguments against a universal treaty

The Budapest Convention already provides a basis for a universal treaty

In terms of the arguments against the need to start a new treaty process, most EU and OECD member states favour the Budapest Convention, and consider it as a strong basis for a global instrument, arguing that it fosters multilateral cooperation on cybercrime and includes many signatories from other global regions.

The Budapest Convention is a binding instrument addressing cross-border cybercrime cooperation and encouraging harmonization of laws. Having entered into force in 2004, the convention has 56 states parties, including a number of countries outside the CoE, such as the US, Japan, Canada, Senegal, Sri Lanka, the Philippines, Turkey, Morocco and the Dominican Republic, and is open to ratification by other states. Observer countries include South Africa, Ghana, Colombia and Mexico.[49] Many Western countries believe the convention has established best practices for cooperation and provides adequate safeguards for digital rights. They highlight the cross-regional membership as a sign that it can be used as an international framework.

Additionally, some note that existing UN instruments, such as UNTOC, also provide a basis for cooperation on cyber-related criminal activity and that these can complement regional and bilateral engagement.[50] However, others have actively criticized UNTOC for falling critically short in this regard.

Transborder access to data and electronic evidence

The issues surrounding transborder access to data and electronic evidence are critical for cooperation in cybercrime investigations and simultaneously causes of contention. In this area, recommendations from the 2018 EGM report urge member states to

> respect the sovereign rights of other States in formulating policies and legislation that meet their national conditions and needs in addressing cybercrime. … The volatile nature of electronic data transmission and storage, such as in so-called clouds, may require engaging in multilateral discussions on innovative and expanded mutual assistance between States to ensure timely access to electronic data and evidence.[51]

Transborder access to data, including electronic evidence collection, hinges on jurisdictional authority, national sovereignty and government reach. Any data, including content held in the cloud, or web searches or text messages, is personal information stored, transferred or published by (mostly) private companies within one or several countries. Private data may often not be the sole possession of the private individual, but of the company hosting the data. As discussed earlier, some states are trying to bring their citizens' data into their territory to ensure their legal frameworks apply. But the reality remains that data is transmitted across jurisdictions: cloud computing means that data may be stored in one country and accessed in another, and cybercrimes are launched across borders where the victims may be broadly dispersed. Service providers, data and involved parties often sit in different jurisdictions, and within different jurisdictions privacy protection and what constitutes warranted access to data differ. From another perspective, states view accessing their citizens' data without governmental consent as a breach of national sovereignty.

However, accessing data across borders is crucial to enable cybercrime investigations and prosecutions. Most requests for transborder data go through the Mutual Legal Assistance (MLA) process, entailing bilateral or multilateral agreements that often include due process safeguards set by the country that houses the data.[52] Many states complain about the slow speed of MLA requests, which can take up to 10 months.[53] Cloud computing works in such a way that the location of the data may not be known, and responses to requests for data can take longer than the data-retention period, resulting in electronic evidence being destroyed in some instances.[54] Many governments share frustrations over inability to access evidence from the dark web or through companies that provide encryption or other privacy services.

States interpret transborder access to data as an infringement of national sovereignty in a number of ways. MLA requests may go to the country where the service provider is located, rather than the data leaving the country that holds it. Investigators can access extraterritorial data from an active device without consent from the country where the information is situated. There may also be voluntary assistance from service providers outside of legal channels.[55] Cross-border hacking has also been used in investigations, which raises red flags around transparency and cooperation.[56]

'Accessing data across borders is crucial to enable cybercrime investigations and prosecutions.'

In addition to MLA requests, there are regional agreements that also facilitate cooperation. And states can submit direct requests to service providers for information. States also use formal and informal methods to request assistance and avoid duplication, such as through INTERPOL channels.[57]

A Second Additional Protocol to the Budapest Convention is currently being discussed on the issue of transborder access to data, with a draft expected in 2019.[58] This protocol seeks to improve on the following areas: MLA; draft provisions on direct cooperation with providers in other jurisdictions with regard to requests for subscriber information; preservation requests; and emergency requests.[59] It also seeks to create a stronger framework and better safeguards for existing practices, including requirements surrounding data protection.[60] At the same time, states are continuing to move unilaterally on the issue. In March 2018, for example, the US passed legislation that will compel service providers to hand over data outside the MLA process, depending on certain circumstances.[61] Efforts to widen the scope and methods for obtaining stored content outside of state–state cooperation are unlikely to encourage cooperation from states that see this as an infringement of their national sovereignty.

Looking at the issue from another angle, technology companies and some governments can be hesitant about cooperating owing to the lack of safeguards for online rights and privacy. Although a number of recommendations in the EGM report, and elsewhere, call for improved partnerships with the private sector, some states have developed contentious relationships that hinder cooperation. As mentioned, private companies are often the technical holders of private data, and can exist in different legal regimes from a government agency making a request for cooperation. And even within the same legal jurisdiction, technology companies have taken stances on providing data, such as Google's refusal in 2018 to cooperate with the authorities and provide location data in a robbery investigation in the US.[62] At the same time, many of the same companies do cooperate with national security agencies[63] or trade in personal data with little transparency. The GDPR is a regional attempt to harmonize privacy laws and set regulations for how organizations manage data. Nevertheless, the lack of a shared understanding across regions on what constitutes privacy and adequate safeguards will continue to inhibit the ability to cooperate on cybercrime investigations between governments, and between government agencies and the private sector, and will make it difficult to reach consensus on a global instrument to govern cybercrime.

The proportion of online users affected by cybercrime:

TWO-THIRDS

The disconnect on this issue leads to the larger unanswered question of what are the boundaries of cybercrime and cybercrime cooperation.

What are the boundaries of cybercrime?

To varying degrees, over the last 20 years, people have moved their communications, social relationships, financial transactions, political interactions, and cultural and entertainment activities into the digital space. Even individuals' geo-locations can be detected thanks to hand-held devices. This way, domestic frameworks for cybercrime and cybersecurity have the ability to reach deeply into the private lives of citizens.

In addition, cybercrime is rapidly evolving. While cyber-dependent crimes are already illegal in many countries, the rapidly evolving nature of cybercrime means the list of possible offences continues to grow. This can be seen in the suggested offences listed in the EGM report, ranging from copyright infringement to the incitement of minors to commit suicide.[64] While states grapple with defining the limits and scope of what cybercrime actually entails, they continue to see emerging forms of digital crimes, for instance those related to cryptocurrencies, the Internet of Things and the dark net. This has led some experts to suggest that legislation should be technologically neutral.[65]

'The test for effective cybercrime cooperation will be ensuring that ongoing efforts do not allow for precedents that encourage government control and overreach.'

For cyber-enabled crimes, many of the underlying crimes are already on the UN agenda. For instance, two CCPCJ resolutions in 2018 address the use of ICT in human trafficking. The first calls on states to respond to new uses of technology for trafficking-related activity, including working with law enforcement, service providers, businesses and research communities to understand and address the issues.[66] The second calls on the need to protect children from trafficking risks facilitated by ICT.[67] It may also mean that the cyber dimension of key UN themes, such as gender equality, are addressed in forums outside of the CCPCJ. For instance, the UN Human Rights Council (UNHRC) recently published a report on online violence against women and girls by the Special Rapporteur on Violence against Women.[68] As cybercrime develops on the UN agenda, recognizing overlaps and productively addressing shared agendas will be important.

States' use of criminal proxies to carry out cyber-attacks blurs the line between cybercrime and cybersecurity, as it relates to international security. Some state-led cyber-attacks have been known to deploy hackers and criminal groups, so that the authorities shield themselves from accountability. For instance, in 2016 a Chinese national was sentenced in the US on charges related to gaining unauthorized access to US military computers and stealing information. Although Beijing was implicated, it was never held accountable.[69] When states employ hackers, they may also give these actors a free pass to carry out other criminal activity.[70] Additionally, states may themselves carry out an attack and falsely attribute it to a hacker, which could be considered a false-flag attack.[71]

Within this widening net of online or ICT-related offences, states have adopted different approaches in setting the scope for domestic legal regimes governing cybercrime. One report found that, in Gulf countries and neighbouring states, 'the general trend for prosecution was that digital rights and freedoms were penalized and ruled as "cybercrime" cases delegated to general courts'.[72] China has passed laws requiring people in online forums to register using their real names and holding chat-group administrators responsible for chat content.[73] Typically, Western countries are seen as showing more latitude when it comes to permitting online freedoms, but even that has grey areas, as can be seen in the failed prosecution of a US activist based on Facebook comments.[74]

The UNHRC has voiced its support for online rights. Its July 2018 resolution on human rights and the internet urges states to adopt laws that protect privacy and guard against 'arbitrary and unlawful' collection and use of personal data.[75] It notes that technology such as encryption is important for confidentiality, calls on businesses to continue to create technologies that protect communications and asks states not to interfere with the use of these technologies.[76] This follows upon earlier resolutions, such as the 2016 resolution promoting freedom of expression online and condemning internet shutdowns.[77] The steps taken by the UNHRC illustrate how cybercrime cooperation is situated within a much larger conversation about government control over cyber elements, and could have an impact on a wide range of human rights, including the rights to privacy and dignity, which are guaranteed in universal treaties that most countries have signed and which are therefore binding.

In this way, setting a scope for cybercrime cooperation has been difficult, both in terms of differing government perspectives and the rapidly evolving nature of cybercriminal activities. The test for effective cybercrime cooperation will be ensuring that ongoing efforts within the framework of the EGM, and now the 2019 secretary general's reporting process, do not allow for precedents that encourage government control and overreach.

Relationship between cybercrime and cybersecurity

The boundaries of cybercrime also relate to the connections and overlaps between cybersecurity and cybercrime. Cybersecurity, in terms of its risk to international security, is addressed by the GA's First Committee on Disarmament and International Security. A number of incidents over the past years have raised concerns over governments' growing use of criminal proxies. For instance, in September 2018, the US government lodged a criminal complaint against an individual from North Korea in the global ransomware attack WannaCry, which demanded US$300 in Bitcoins to fix disabled computers. (The hacker is thought to have been working on behalf of the North Korean government and is suspected of also being involved in the 2014 hack of the Sony Corporation, as well as the US$81 million theft from the Bank of Bangladesh in 2016.[78]) This is just one example among many that suggests that cooperation on cybercrime may be hindered by acknowledged or covert state interests.

In addition to its primary focus on states, the UN Governmental Group of Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) has also discussed the potential risks posed by the malicious activities of non-state actors, including criminal proxies. Its 2015 report addresses the potential overlap between state and criminal activity, warning states against using proxies or allowing non-state actors to use territory to commit 'wrongful acts using ICTs'. Yet it also cautions against attributing cybercrimes to a state whose territory and ICT infrastructure was used for an attack without substantiating evidence. It also notes the potential speed of attacks and the difficulty in attributing cybercrimes as a risk to international security. In general, the GGE encourages cooperation in prosecution and investigation.[79] Similarly, the cybercrime EGM discussed the relationship between state and criminal activity, noting that each should be addressed in different forums, while the links between the two are recognized.[80]

The UN Security Council has held informal meetings in recent years about the use of cyber-tools by states for military or political purposes.[81] A November 2016 open Arria-Formula meeting on cybersecurity chaired by Spain and Senegal addressed the potential uses of ICT by states that threaten international security, including the need to protect infrastructure.[82] In April 2017, Ukraine organized an Arria-Formula meeting on 'hybrid wars as a threat to international peace and security' focused on the changing character of warfare connected to new technologies and strategies.[83]

However, the Security Council's primary focus related to cybercrime is the use of ICT in relation to terrorism.

The internet and counterterrorism

The 2018 review of the Global Counter-Terrorism Strategy highlights the 'increasing use, in a globalized society, by terrorists and their supporters, of information and communications technologies, in particular the Internet and other media, and the use of such technologies to commit, incite, recruit for, fund or plan terrorist acts'.[84] It also notes risks connected to the use of cryptoassets, and encourages countering the terrorist narrative online.[85] The cybercrime EGM also suggests that states consider criminalizing 'the use of the Internet to commit acts related to terrorism'.[86] Many of the same issues that unfold in cybercrime debates are also present in those that address combating the use of ICT to commit terrorist acts, including electronic evidence, and balancing national security and human rights.

The review of the Global Counter-Terrorism Strategy includes a number of references calling for cooperation in combating the use of ICT for terrorism purposes, including in the area of social media. It also supports an open internet, and the right to privacy in online activity and in communication surveillance, interception and collection.[87] Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights are referenced multiple times to anchor the human-rights responsibilities when dealing with ICT-related activity.[88]

The Security Council's Counter-Terrorism Committee has briefed the council several times on potential uses of ICT for terrorist purposes, particularly in relation to recruitment and incitement.[89] Building on an earlier programme, the executive directorate of the Counter-Terrorism Committee (CTED) also launched a project, Tech Against Terrorism, in November 2017 to work with technology companies to share best practices while advocating for industry self-regulation.[90]

There are also collaborative efforts among agencies to address ICT-related issues that impact both terrorism and criminal investigations. Building on Security Council Resolution 2322, which emphasizes the need to evaluate methods and best practices related to investigative techniques and electronic evidence,[91] an initiative between the CTED, UNODC and the International Association of Prosecutors seeks to build cooperation among investigators, prosecutors and central authorities that receive MLA requests to improve the ability to collect electronic evidence.[92]

UN agency efforts

UN agencies raise awareness, build technical capacity and draft guidance for member states on the issue of cybercrime. The International Telecommunication Union (ITU), which helps govern global telecommunications networks – but not the internet, to date – offers several programmes to combat cybercrime. Within the ITU, the Cyber Threat Insight programme offers two tools to member states to combat cybercrime. HORNET provides technical assistance through a strategically deployed network of sensors, which captures data about malware and other attacks, to provide states with information on threats, so that they can better understand them and help mitigate them.[93]

The second tool, the Abuse Watch Alerting and Reporting Engine, increases the ability of the Computer Incident Response Teams to collect and analyze data for malicious activity.[94] More broadly, the ITU's Global Cybersecurity Index is a survey measuring states' commitments to cybersecurity, based on five pillars: legal, technical, organizational, capacity building and cooperation.[95]

The UN's Chief Executives Board, the highest-level coordination body for the UN System, established the UN Group on Cybercrime and Cyber Security, co-led by the ITU and the UNODC, to lead coordination within the UN on cybercrime and cybersecurity. It also tasked them with drafting a policy on how the UN System mainstreams cyber-issues into programming.[96] The UNODC's Global Programme on Cybercrime provides technical assistance to states in confronting cybercrime.[97] The programme hosts an online cybercrime repository, including a case-law database.[98] The UNODC and the ITU also authored the 2013 Comprehensive Study on Cybercrime, used by the EGM in its deliberations.[99]

Other efforts include a recent agreement between INTERPOL and EUROPOL to reduce the use of cryptocurrencies by criminals and those who finance terrorists to launder money and support criminal activities.[100] Meanwhile, the UN's Office of Information and Communications Technology is working with other UN bodies to strengthen cybersecurity efforts through its Digital Blue Helmets programme.[101]

Conclusion

Fundamentally different conceptions of the role of ICT and the internet in society limit states' ability to respond to cybercrime in a collective, aligned way. States will continue to debate their key differences when it comes to their citizens' right to privacy and to national sovereignty.

Steps taken by some of the UN committees and UN initiatives seek to find areas where countries may eventually become more aligned in their response to this complex and divisive area of crime. In the EGM, states are working to develop norms around cybercrime and set parameters for cooperation. The EGM stocktaking reveals that states are still determining these parameters, while the frontiers and scope of cybercrime keep expanding. At the same time, there is no clear solution yet in sight to shrink the distance between different countries on critical digital issues: the current climate of geopolitical mistrust is hampering the UN's ability to address cybercrime.

Ultimately, states themselves will decide whether there is a need for a multilateral agreement to counter cybercrime. Whatever that outcome may be, the encroaching and changing nature of cybercrime indicates that the UN will need an approach that is flexible and able to adapt to new risks, and identify appropriate cooperative measures among states that adopt markedly different approaches to cyberspace and its challenges.

Acknowledgements

The author would like to thank the Government of Norway for funding this report and Camino Kavanagh for reviewing it.

Notes

1 Techopedia, Cybercrime definition, https://www.techopedia.com/definition/2387/cybercrime.

2 UNODC, Global Programme on Cybercrime, http://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

3 INTERPOL, Cybercrime, https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

4 McAfee, Executive summary, The economic impact of cybercrime – no slowing down, February 2018, https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf.

5 100+ Terrifying cybercrime and cybersecurity statistics and trends, 2018 edition, https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/.

6 Ibid.

7 Ibid.

8 Danny Palmer, WannaCry ransomware crisis one year on: Are we ready for the next global cyber attack? ZDNet, 11 May 2018, https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/.

9 UNODC, An international treaty on cyber crime, current status? September 2011, https://www.unodc.org/documents/southeastasiaandpacific/2011/09/cybercrime-workshop/ppt/Cybercrime_Asia_Sept_2011.pdf.

10 The resolution is titled 'Countering the use of information and communication technologies for criminal purposes', see https://www.un.org/press/en/2018/ga12107.doc.htm.

11 UN Doc. A/Res/73/27, 11 December 2018.

12 UN Doc. A/Res/73/266, 2 January 2019.

13 There are a number of issues in the cybersecurity debates that are outside the scope of this paper. For more on this background, see Camino Kavanagh, The United Nations, cyberspace and international peace and security: Responding to complexity in the 21st century, UNIDIR, 2017.

14 Privacy is reflected in Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR); freedom of expression is reflected in Article 19 of the UDHR and Article 19 of the ICCPR.

15 See Sarah McKune, An Analysis of the International Code of Conduct for Information Security, Citizen Lab, 28 September 2015, https://citizenlab.ca/2015/09/international-code-of-conduct/: 'The issue of participation in Internet governance is closely linked to that of "dominance" in the digital space, an SCO concept of Russian origin that is also highlighted in the Code. The Code flags inequalities and dominant-state advantages in the information space, including with respect to control of ICT supply chains, as serious threats to national security.'

16 Ibid.

17 OECD, OECD principles for internet policy making, 2014, https://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf, 8.

18 To view state approaches to internet controls, see Freedom House, Key internet control by country, https://freedomhouse.org/report/key-internet-controls-table-2017.

19 Urs Gasser, speaking at Governing Artificial Intelligence, IPI/UNU, Session I: Does the AI race threaten international peace and security?, 22 June 2018, https://www.ipinst.org/2018/06/governing-artificial-intelligence.

20 The Great Firewall of China, Bloomberg News, 30 November 2017, https://www.bloomberg.com/quicktake/great-firewall-of-china.

21 Matt Binder, Apple iCloud data in China now stored by state-owned company, Mashable, 18 July 2018, from https://mashable.com/2018/07/18/china-government-apple-icloud-data/.

22 Beyond a messaging app, WeChat can be used for payments, location sharing, personal identification, reading the news, among other uses. See Zheping Huang, All the things you can – and can't – do with your WeChat account in China, Quartz, 28 December 2017, https://qz.com/1167024/all-the-things-you-can-and-cant-do-with-your-wechat-account-in-china/.

23 See The NSA files, *The Guardian*, https://www.theguardian.com/us-news/the-nsa-files.

24 See https://www.eugdpr.org/key-changes.html.

25 UN rejects Russian cyber-crime treaty, https://www.itproportal.com/2010/04/21/un-rejects-russian-cyber-crime-treaty/.

26 Camino Kavanagh, The United Nations, cyberspace and international peace and security: Responding to complexity in the 21st century, UNIDIR, 2017, 44–45; UNODC, Global programme on cybercrime, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

27 Camino Kavanagh, The United Nations, cyberspace and international peace and security: Responding to complexity in the 21st century, UNIDIR, 2017, 45.

28 GA Resolution 65/230; see also UNODC, Comprehensive study on cybercrime, www.unodc.org/unodc/en/organized-crime/comprehensive-study-on-cybercrime.html. The EGM has held four sessions, in 2011, 2013, 2017 and 2018.

29 UN Doc. E/2018/30-E/CN.15/2018/15, May 2018, para 48, http://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_27/1803810E_18June2018_Advance_version.pdf.

30 CCPCJ Resolution 26/4, adopted in May 2017, referenced in UN Doc. E/2018/30-E/CN.15/2018/15, para 6.

31 UN Doc. E/2018/30 - E/CN.15/2018/15, paras 38–40.

32 Ibid., paras 43–45.

33 Un Doc. UNODC/CCPCJ/EG.4/2018/CRP.1, para 5.

34 UN Doc. UNODC/CCPCJ/EG.4/2018/CRP.1, https://www.unodc.org/documents/organized-crime/cybercrime/cybercrime-april-2018/V1800915.pdf.

35 UN Doc. E/CN.15/2018/12, paras 9s-t.

36 Ibid., para 15.

37 UNODC, Comprehensive Study on Cybercrime, United Nations, 2013.

38 UN Doc. E/CN.15/2018/12, para 21.

39 For further information, see https://www.oas.org/juridico/english/cyber.htm.

40 African Union Convention on Cyber Security and Personal Data Protection, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

41 Directive on Fighting Cybercrime within ECOWAS, http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED_Cybercrime_En.pdf.

42 Joyce Hakman, Building a stronger international legal framework on cybercrime, Chatham House, 6 June 2017, https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime.

43 See https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

44 Xinhua, Full text of BRICS leaders Xiamen Declaration, 5 September 2017, para 56, http://www.bricschn.org/English/2017-09/05/c_136583711_2.htm.

45 CoP UNTOC, Report of the Conference of the Parties to the United Nations Convention against Transnational Organized Crime on its eighth session, Vienna, 17 to 21 October 2016, UN Doc. CTOC/COP/2016/15, 7 November 2016, paras 76–80.

46 UN Doc. A/C.3/72/12, 16 October 2017.

[47] Russia to propose draft cybersecurity convention to UN General Assembly, TASS, 3 July 2018, http://tass.com/politics/1011749.

[48] UN Doc. A/RES/73/187, 17 December 2018.

[49] Council of Europe, Towards a protocol to the Budapest Convention, 19 March 2018, https://rm.coe.int/t-cy-pd-pubsummary-v6/1680795713; for a list of observers, see Parties/observers to the Budapest Convention and observer organisations to the T-CY, https://www.coe.int/en/web/cybercrime/parties-observers.

[50] UN Doc. E/CN.15/2018/12, para 15.

[51] Ibid., para 9(b).

[52] Katitza Rodriquez, The cybercrime convention's new protocol needs to uphold human rights, Electronic Frontier Foundation, 18 September 2017, https://www.eff.org/deeplinks/2017/09/cybercrime-conventions-new-protocol-needs-uphold-human-rights.

[53] Ibid.

[54] UN Doc. E/2018/30-E/CN.15/2018/15, para 40.

[55] UNODC, Comprehensive study on cybercrime, United Nations, 2013, 216.

[56] Katitza Rodriquez, The cybercrime convention's new protocol needs to uphold human rights, Electronic Frontier Foundation, 18 September 2017, https://www.eff.org/deeplinks/2017/09/cybercrime-conventions-new-protocol-needs-uphold-human-rights.

[57] UNODC, Comprehensive study on cybercrime, United Nations, 2013, 195, 208.

[58] Towards a protocol to the Budapest Convention, Council of Europe, 19 March 2018, https://rm.coe.int/t-cy-pd-pubsummary-v6/1680795713; Katitza Rodriquez, The cybercrime convention's new protocol needs to uphold human rights, Electronic Frontier Foundation, 18 September 2017, https://www.eff.org/deeplinks/2017/09/cybercrime-conventions-new-protocol-needs-uphold-human-rights.

[59] Council of Europe, Discussion guide for consultations with civil society, data protection authorities and industry, https://rm.coe.int/t-cy-2018-16-pdp-consultations-paper/16808add27.

[60] Ibid.

[61] Ron Cheng, Seizing data overseas from foreign internet companies under the CLOUD Act, *Forbes*, 29 May 2018, https://www.forbes.com/sites/roncheng/2018/05/29/seizing-data-overseas-from-foreign-internet-companies-under-the-cloud-act/#3779606716c0.

[62] Deana Paul, Google refused an order to release huge amounts of data. Will other companies bow under pressure? *The Washington Post*, 18 August 2018, https://www.washingtonpost.com/technology/2018/08/18/google-refused-an-order-release-huge-amounts-data-will-other-companies-bow-under-pressure/?utm_term=.e8e9ab80ac26.

[63] For two examples of Google's proposed engagement with both the US Department of Defense and the Chinese government, see Sarah Sewall, Google was working on two ethically questionable projects. It quit the wrong one, *The Washington Post*, 7 October 2018, https://www.washingtonpost.com/opinions/google-was-working-on-two-ethically-questionable-projects-it-quit-the-wrong-one/2018/09/07/f95ee7b4-a639-11e8-97ce-cc9042272f07_story.html?utm_term=.ce9ca5925a21.

[64] UN Doc. E/CN.15/2018/12, para 10.f.i-xiv.

[65] Ibid., para 29.

[66] UN Doc. E/CN.15/2018/L.2/Rev.1, 16 May 2018, https://undocs.org/E/CN.15/2018/L.2/Rev.1.

[67] UN Doc. E/CN.15/2018/L.3/Rev.1, 17 May 2018, https://undocs.org/E/CN.15/2018/L.3/REV.1.

[68] UN Doc. A/HRC/38/47; see also Deborah Brown, Sidra Rizvi and Kyung Min Kim, Internet rights in focus: 38th session of the Human Rights Council, AccessNow, 19 June 2018, https://www.accessnow.org/internet-rights-in-focus-38th-session-of-the-united-nations-human-rights-council/.

[69] Jack Detsch, How Russia and others use cybercriminals as proxies, *The Christian Science Monitor*, 28 June 2018, https://www.csmonitor.com/USA/2017/0628/How-Russia-and-others-use-cybercriminals-as-proxies.

[70] Ibid.

[71] Tim Maurer, When states pretend to be terrorists or hacktivists in cyberspace, 18 April 2017, https://carnegieendowment.org/2017/04/18/when-states-pretend-to-be-terrorists-or-hacktivists-in-cyberspace-pub-68703.

[72] Mapping cybercrime laws and violations of digital rights in the Gulf and neighbouring countries, Gulf Centre for Human Rights, June 2018.

[73] Cheang Ming and Saheli Roy Choudhury, China has launched another crackdown on the internet – but it's different this time, CNBC, 26 October 2017, https://www.cnbc.com/2017/10/26/china-internet-censorship-new-crackdowns-and-rules-are-here-to-stay.html.

[74] The US FBI arrest and failed prosecution of Rakem Balogun in Texas used Facebook posts that criticized the police as justification for the arrest. See Sam Levin, Black activist jailed for his Facebook posts speaks out about secret FBI surveillance, *The Guardian*, 11 May 2018, https://www.theguardian.com/world/2018/may/11/rakem-balogun-interview-black-identity-extremists-fbi-surveillance.

[75] UN Doc. A/HRC/38/L.10/Rev.1, paras 8, 17.

[76] Ibid., para 9; https://documents-dds-ny.un.org/doc/UNDOC/LTD/G18/203/73/PDF/G1820373.pdf?OpenElement. The Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression called for states to repeal laws that restrict freedom of expression online, to restrict content only when an impartial judicial authority requests it, and to avoid disproportionate penalties on internet intermediaries. See Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/38/35, 6 April 2018, paras 65–66.

[77] James Vincent, UN condemns internet access disruption as a human rights violation, The Verge, 4 July 2016, https://www.theverge.com/2016/7/4/12092740/un-resolution-condemns-disrupting-internet-access.

[78] Mattha Busby, North Korean 'hacker' charged over cyber-attacks against NHS, *The Guardian*, 6 September 2018, https://www.theguardian.com/world/2018/sep/06/us-doj-north-korea-sony-hackers-chares.

[79] UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, 22 July 2015, paras 28e–f, 13c–d, 17e, 21h.

[80] UN Doc. E/CN.15/2018/12, para 20.

[81] Camino Kavanagh, The United Nations, cyberspace and international peace and security: Responding to complexity in the 21st century, UNIDIR, 2017; see also Arria-Formula meeting on hybrid wars, What's in Blue, 30 March 2017, http://www.whatsinblue.org/2017/03/arria-formula-meeting-on-hybrid-wars.php.

[82] Camino Kavanagh, The United Nations, cyberspace and international peace and security: Responding to complexity in the 21st century, UNIDIR, 2017, 25.

[83] Arria-Formula meeting on hybrid wars, What's in Blue, 30 March 2017, http://www.whatsinblue.org/2017/03/arria-formula-meeting-on-hybrid-wars.php.

[84] UN Doc. A/RES/72/284, Global counter-terrorism review 2018, para 35, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/72/284.

[85] Ibid., paras 22, 46.

[86] UN Doc. E/CN.15/2018/12, para 10(f)iii.

[87] UN Doc. A/RES/72/284, Global counter-terrorism review 2018, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/72/284, paras 19, 20.

[88] Ibid.

89 For instance, in December 2015 (Preventing terrorists from exploiting the internet and social media to recruit terrorists and incite terrorist acts, while respecting human rights and fundamental freedoms), and December 2016 (Preventing the exploitation of ICT for terrorist purposes, while respecting human rights and fundamental freedoms).

90 See Tech Against Terrorism, https://www.techagainstterrorism.org/about/; see also, UN Security Council Counter-Terrorism Committee, the Permanent Mission of the Republic of Korea, CTED and ICT4Peace launch next phase of Tech against Terrorism, https://www.un.org/sc/ctc/news/2017/11/30/permanent-republic-korea-cted-ict4peace-launch-next-phase-tech-terrorism/.

91 UN Doc. S/RES/2322 (2016), 3.

92 UN Security Council, Counter-Terrorism Committee, Information and communications technologies, https://www.un.org/sc/ctc/focus-areas/information-and-communication-technologies/; UNODC, Experts meet in Vienna, discuss lawful access to digital data across borders, 12 February 2018, https://www.unodc.org/unodc/en/frontpage/2018/February/experts-meet-in-vienna--discuss-lawful-access-to-digital-data-across-borders.html.

93 ITU, Cyberthreat Insight, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyberthreat_Insight.aspx.

94 ITU, AWARE, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/AWARE.aspx.

95 ITU, Global cybersecurity index, 3rd edition, https://www.itu.int/pub/D-STR-GCI.01-2017.

96 UN System, Chief Executives Board for Coordination, Action on cybercrime and cyber security, https://www.unsystem.org/content/action-cybercrime-and-cyber-security.

97 Funded by Australia, Canada, Japan, Norway, UK and the US, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

98 See UNODC, Repository, cybercrime, https://www.unodc.org/cld/v3/cybrepo/.

99 UNODC, Comprehensive study on cybercrime, February 2013, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

100 Crypto Economy, Europol and Interpol unite against the laundering of cryptocurrencies and financing of terrorism, 5 February 2018, https://www.crypto-economy.net/en/europol-and-interpol-unite-against-the-laundering-of-cryptocurrencies-and-financing-of-terrorism/.

101 UN Digital Blue Helmets, https://unite.un.org/digitalbluehelmets/resources.

THE GLOBAL INITIATIVE
AGAINST TRANSNATIONAL
ORGANIZED CRIME

www.globalinitiative.net

A NETWORK TO COUNTER NETWORKS