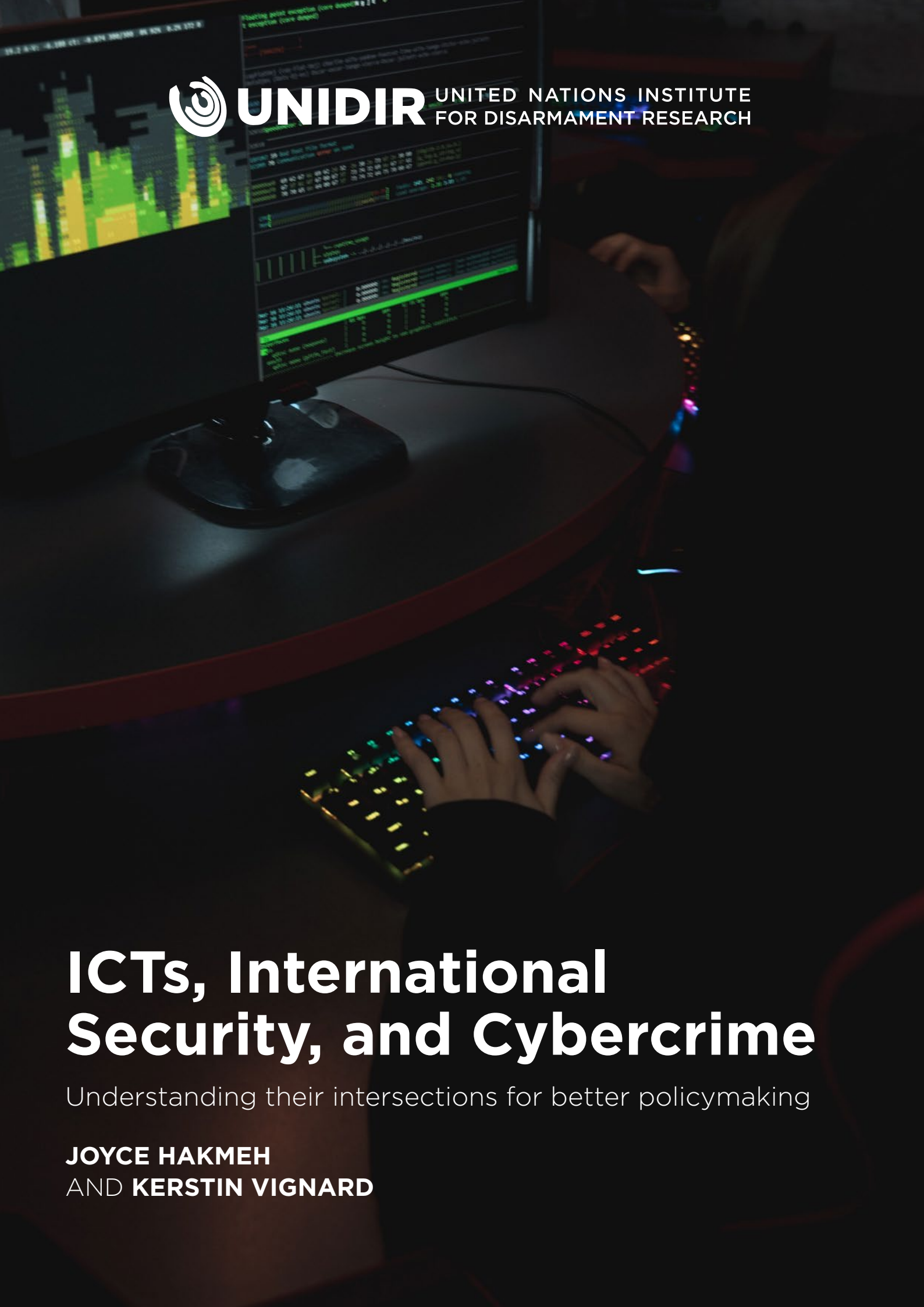


UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

ICTs, International Security, and Cybercrime

Understanding their intersections for better policymaking

JOYCE HAKMEH
AND **KERSTIN VIGNARD**

ACKNOWLEDGEMENTS

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This project is part of the Cyber Workstream of the Security and Technology Programme, which is supported by the Governments of France, Germany, the Netherlands, Norway, and Switzerland and by Microsoft.

In addition, the authors are grateful for the thoughtful comments and suggestions received from Moliehi Makumane, Sir David Omand, Allison Peters, Juliet Singsley, Neil Walsh and others at various stages of this work.

ABOUT UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

CITATION

J. Hakmeh, K. Vignard. 2021. ICTs, *International Security, and Cybercrime: Understanding their Intersections for Better Policymaking*, Geneva, Switzerland: UNIDIR, 2021.

NOTE

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members, or sponsors.

CONTENTS

ABOUT THE AUTHORS

Joyce HAKMEH is a senior research fellow with the International Security programme at Chatham House and co-editor of the *Journal of Cyber Policy*. She specializes in cyber policy, including cybersecurity, cybercrime and cybergovernance, and provides regular analysis on issues that sit at the nexus of technology and geopolitics. In addition, Hakmeh serves as the Chair of the Global Forum on Cyber Expertise (GFCE) working group on cybercrime.

KERSTIN VIGNARD is an international security policy professional with over 25 years' experience at the United Nations. She has a particular interest in the nexus of international security policy and technology and led UNIDIR's team supporting the Chairs of five United Nations Groups of Governmental Experts (GGEs) on cybersecurity and the 2019–2021 Open-Ended Working Group. From 2012 to 2019, Vignard was Chief of Operations and Deputy to the Director at UNIDIR, where she is currently a non-resident Senior Fellow.

ABBREVIATIONS

AI	Artificial Intelligence
APT	Advanced Persistent Threat
CBM	Confidence-Building Measure
CCPCJ	Commission on Crime Prevention and Criminal Justice
CD	Conference on Disarmament
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DPPA	Department of Political and Peacebuilding Affairs
ECOSOC	Economic and Social Council
G7	Group of Seven
GGE	Group of Governmental Experts
ICJ	International Court of Justice
ICTS	Information and Communications Technologies
IEG	Open-ended Intergovernmental Expert Group
ILC	International Law Commission
IT	Information Technology
OCHA	Office for the Coordination of Humanitarian Affairs
OEWG	Open-ended Working Group
UNDC	United Nations Disarmament Commission
UNIDIR	United Nations Institute for Disarmament Research
UNODA	United Nations Office for Disarmament Affairs
UNODC	United Nations Office on Drugs and Crime


BEHAVTORAL MUSHMELON RECREATTON
DEFAMATORY BLUEBONNET REPLICATTON
SYSTEM MEMLETON

EXECUTIVE SUMMARY

- Information and Communication Technologies (ICTs) can be exploited for criminal purposes (through cybercrime) or used to undermine international security (through so-called cyber-attacks or cyber operations). However, the international security and crime dimensions of ICTs are distinct issues, with different processes, tools, and frameworks designed to address them, albeit they increasingly overlap in some ways.
- As cyberthreats continue to grow in complexity and scale, it is becoming increasingly difficult to differentiate the perpetrators of cyberattacks as they operate in the same space and sometimes their interests converge.
- This complex landscape often means that it is difficult to identify with confidence the perpetrators behind a certain attack or their motivation in the early stages of the incident. This makes close coordination between the "first responders" (e.g. a Computer Security Incident Response Team (CSIRT)) and law enforcement crucial.
- States need to be aware of this complex reality and of the intersections between cybercrime and incidents impacting international security and be able to reflect this awareness in their policies and practices whether nationally or internationally. A failure to do so risks developing incoherent national policy responses that could be ineffective in addressing the broad range of cyberthreats to which States are exposed.
- There is a need for greater understanding of how international frameworks and policy discussions on combatting cybercrime and promoting responsible State behaviour in the use of ICTs may be better leveraged for coherent responses.
- The international community is launching new negotiation processes in 2021 on both cybercrime and on ICTs and international security. Greater awareness is thus needed of how the two topics intersect, of existing commitments, and of gaps where new tools, mechanisms, or greater collaboration may help to address criminal use of ICTs that may threaten international peace and security.
- In 2015 all United Nations Member States agreed to a set of 11 voluntary norms of responsible State behaviour in their use of ICTs; this commitment was reaffirmed in 2021. Several of these existing commitments – in particular, norms 13(c), (d) and (h) – help to address specific areas where additional efforts are needed when international security and cybercrime intersect. These agreed commitments should be built upon in the negotiation of a new cybercrime convention.
- National and international siloes (including conceptual, bureaucratic and procedural ones) remain a key challenge to better policies and responses to cyberthreats. Nationally, structured cooperation and coordination between the law enforcement and criminal justice sectors on the one hand and the first responders on the other is often missing. Internationally, there is a lack of structured, formal exchanges between the First and Third Committees of the United Nations General Assembly and a lack of awareness on how the processes in the two forums overlap and link to each other – including how recommendations of previous Groups of Governmental Experts (GGEs) on ICTs and international security apply to cybercrime-related issues.

- Many delegations lack experts with the substantive expertise necessary to actively engage in the United Nations processes related to ICTs. This and the limited capacity within many delegations more generally remain key impediments for participation.
- While the new Open-ended Working Group (OEWG) will meet in New York, the location of the cybercrime negotiations will alternate between New York and Vienna. This may help to foster synergies between the two negotiation processes but may also place additional financial and coordination challenges, in particular on smaller delegations.
- The lack of a common narrative and rhetoric around ICT threats has often led to the substantive discussion on ICTs in the context of international security being framed in terms of "cyberwarfare". However, most destabilizing and hostile activities witnessed to date occur outside situations of armed conflict, yet they pose significant and growing threats to international security and stability.
- As the international community takes forward its discussions on ICTs, cybercrime and international security, action in the following areas may help to operationalize and strengthen international cooperation at the intersection of these issues:
  - ✓ Prioritizing building relevant national capacities that benefit both combatting cybercrime and maintaining international peace and security;
  - ✓ Further strengthening international cooperation to address the intersections of cybercrime and international security;
  - ✓ Promoting greater exchanges between the two United Nations processes;
  - ✓ Further research on topics at the intersection of cybercrime and international security.

I. INTRODUCTION

In our digitally interdependent world, daily headlines bear witness to how information and communications technologies (ICTs) can be exploited for criminal purposes (through cybercrime) or used to undermine international security (through so-called cyberattacks or cyber operations). However, although both use digital technologies, the international security and crime dimensions of ICTs are distinct issues, with different processes, tools, and frameworks designed to address them at the national and international levels.

Cybercrime encompasses a vast category of activities, ranging from online child exploitation to identify theft and financial scams targeting individuals, to illegal access of information technology (IT) systems, to ransomware attacks that shut down whole corporations or institutions.[1] In the context of international peace and security, a cyberattack or cyber operation is generally politically motivated, whether conducted by a State or non-State actor such as a terrorist organization, and may be offensive or defensive in nature. Cybercrime is often presumed to be perpetrated by non-State actors, of which only a small subset of these crimes have an impact on international peace and security. However, this is increasingly shifting as cybercrime grows in frequency, magnitude, sophistication, and scope, targeting a variety of critical infrastructures and presenting risks for misperception, escalation, and the erosion of trust between States.

There are some instances where there may be an overlap or blurring of cybercrime and international security concerns—depending, for example, on the incident type, its target, the severity of its impact, and the motivation of the perpetrator or any other actor behind the malicious cyber activity, as well as the wider context. Identifying the actors behind malicious cyber activity presents particularly difficult technical and political challenges. An action that may appear to have been perpetrated by non-State criminal actors may actually have a connection to sa State and so can threaten international peace and security. A United Nations Group of Governmental Experts (GGE) recently underscored that malicious non-State actors are of sparticular concern to international stability: "the diversity of malicious non-State actors, including criminal groups and terrorists, their differing motives, the speed at which malicious ICT actions can occur and the difficulty of attributing the source of an ICT incident all increase risk".[2]

The precise moment when the transnational threat posed by some types of cybercrime may have an impact on international peace and security can be challenging to identify. In the early stages of detecting, investigating, and mitigating the impact of an incident, it may be difficult or impossible to identify the actor behind it or their motivation. It may be a financially motivated criminal act, a State-supported act, or a politically motivated act undertaken by a State. The international security dimension may be initially obscured as the majority of malicious ICT acts occur in "peacetime", not during an armed conflict. Thus, initially it can be difficult to know whether a specific cybercrime incident ultimately may have implications for international security or stability.

---

1 A common approach to defining cybercrime is to differentiate the offences based on whether they are **cyber-dependent** crimes that can only be committed using computers, computer networks or other forms of ICT or whether they are **cyber-enabled** crimes, which are traditional crimes facilitated by ICTs.

2 United Nations Group of Governmental Experts (2021, para. 14).

Throughout the lifecycle of a cyberincident with significant impact, different actors at the domestic, regional, and international levels may have distinct roles in developing a response. The "first responders" to an incident may be from a technical organization, such as an incident response team (e.g. a Computer Emergency Response Team (CERT) or a Computer Security Incident Response Team (CSIRT)), or from an IT department within a public or private sector entity. Investigations may initially involve law enforcement entities before national security concerns are raised—and even then, law enforcement will continue to have an important role to play in investigating and responding to the incident. Over the lifecycle of an incident investigation, it may become clearer that there is an international security dimension that was not initially evident, which might necessitate enlarging the circle of responders to include members of the policy, diplomatic, justice, and defence communities.

The majority of cybercrime incidents do not have implications for international security. However, some may, and it is critical that there is a greater understanding of how international frameworks and policy discussions on combatting cybercrime and promoting responsible State behaviour in the use of ICTs may be better leveraged for coherent responses. There have been international discussions on both issues at the United Nations for a number of years; however, they have matured largely in silos, and there is a general lack of awareness among the different stakeholders – including policymakers, practitioners, institutions, and organizations – about how each topic is being addressed through different tools and frameworks. Some governments lack understanding of how previously agreed norms to guide the responsible behaviour of States in their use of ICTs may strengthen international cooperation in cases of criminal use of ICTs and how such cooperation may help to facilitate the implementation and enforcement of these norms.

The international community is launching new negotiation processes in 2021 on both cybercrime and ICTs and international security.[3] This provides an opportunity to clarify how the two topics intersect, to further socialize existing commitments, and to identify gaps where new tools and mechanisms or greater collaboration may help to address criminal use of ICTs that may threaten international peace and security. The objective of this report is to serve as an initial, non-exhaustive exploration of some of these intersections. This will help focus ongoing discussions in the First and Third Committees of the United Nations General Assembly on practical areas for future collaboration, while recognizing the separate and distinct nature of these negotiations. For example, as the First Committee (which focuses on international security issues) reached consensus agreement in 2015 on promoting international cooperation in cases of criminal use of ICTs, the Third Committee (which addresses cybercrime issues among others) may be able to better leverage these commitments, just as widely accepted international norms and commitments related to addressing cybercrime may be better leveraged in international security discussions. Identifying opportunities for international cooperation in such cases is critical to implementing and enforcing those norms. As noted by the most recent GGE report, cooperation through, for example, responding to requests for assistance to halt malicious activity emanating from a State's territory "may help minimize damage, avoid misperceptions, reduce the risk of escalation and help restore trust".[4]

3 UNGA (2020a); UNGA (2021a).
4 United Nations Group of Governmental Experts (2021, para. 55).

Section II offers an overview of some of the intersections between cybercrime and cyberattacks that have an impact on national and international security and briefly illustrates these intersections through the example of ransomware, a form of cybercrime. The case of ransomware helps to highlight the need for a coherent approach to cyber policymaking nationally and globally that captures these intersections. Section III examines States' existing international commitments to responsible State behaviour in cyberspace and how these may apply to combatting cybercrime. Lastly, section IV identifies challenges and offers recommendations as to how the two international discussions may benefit from greater exchange and what mechanisms and tools may need to be created, adapted, or strengthened to do so. An overview of United Nations system actors, processes and activities on international security and cybercrime appears in annex 1 and relevant outcomes of First Committee-based processes in annex 2.

II. UNDERSTANDING THE INTERSECTIONS

A complex landscape

Today, cyberthreats, whether cybercrime or cyberattacks, are considered a global risk that affect economies, societies, and livelihoods and even international peace and security. Governments, the private sector, and non-governmental organizations – and the global community as a whole – have a role to play in confronting, combatting, reducing, and mitigating their potential harms.

The perpetrators of these threats are many. One way to differentiate them is to identify whether they are State actors or non-State actors and, within this broad categorization, to understand their skill levels and whether they are criminally or politically motivated. But a perpetrator may belong to both groups or, in some instances, a criminal group or individual criminal might be deployed by a State to assist with a cyberattack, acting as an intermediary or proxy for the State in the conduct of malicious ICT actions. In other instances, a State might pretend to be an organized criminal group to mask its actions and escape repercussions. As cyberthreats continue to grow in complexity and scale, it is becoming increasingly difficult to delineate between the two categories of actor – State and non-State – as they operate in the same space where sometimes their interests converge.

In broad terms, perpetrators who have high criminal intent range from being highly skilled with the capacity to develop and deploy their own cyber tools (e.g. organized criminal groups), to having low skills but high criminal intent and still being able to inflict harm through tapping into tools developed by others in what is known as crime-as-a-service (e.g. ransomware as a service – see the text box on page 8). The prevalent low cyber hygiene and good cyber-security measures within many private and public sector organizations around the world combined with an increasing number of these attacks is increasing the impact of these attacks and raising concerns among many States.

State actors could also be categorized based on their capabilities: some States have high cyber capabilities that could be deployed for defensive or offensive cyber activities; other States have low capabilities but are able to use cyber tools that are often developed by private companies for purposes such as counterterrorism and fighting crime but also for offensive hacking and surveillance purposes. As enhanced cyber capabilities proliferate, with relatively easy access to a wide range of actors, and as there are ways for States to leverage their cyber capabilities in compliance with international law as well as in violation of it, the cyberthreat landscape is becoming increasingly complex.

To better understand the existing cyberthreat landscape, table 1 shows one way to look at the range of perpetrators and their motivations based on the victims of the attacks. However, and as noted above, these categories are not rigid nor is this classification static.

Table 1. Aggressors and victims of cyberthreats[5]

		VICTIMS		
		Governments	**Companies**	**Citizens**
FOREIGN AGRESSORS[6]	**Governments and Advanced Persistent Threat (APT) groups[7]**	Espionage Sabotage	Intellectual property theft	Information operations and propaganda
	Companies	Infiltrating corrupted ICT products	Commercial espionage	Monetizing personal data
	Criminals for gain	Large-scale fraud (against tax or welfare systems)	Ransomware and fraud	Extortion and small-scale fraud
	Hacktivists	Disrupt over grievances	Deface websites and cut off customers with denial of service	Revenge attacks and doxing over issues

As mentioned above, there are incidents where cybercrime and international security concerns may overlap or blur together depending on the incident itself and the motivation and identity of the perpetrators or the actors behind them. State-sponsored incidents can aggravate inter-State tensions and can trigger a collective response from a number of States even when the incident may have targeted only one State. A criminal incident may escalate to a national security issue that might not have an international security implication. However, as described below, there are growing expectations on the part of States of the need to exercise due diligence in not knowingly allowing their territories to be used for malicious activities using ICTs by criminals, to assist in bringing those criminals to justice, and to prevent them from operating with impunity. The lack of cooperation from States, in particular around incidents that have severe consequences, might also lead to tensions being aggravated.

5 This table was developed by David Omand, former head of the United Kingdom's Government Communications Headquarters (GCHQ, an intelligence and security organization) as part of his teaching material in his current role as visiting professor in the Department of War Studies at King's College London.

6 While this table elaborates on the types of foreign aggressor and their motivation in the context of an international security landscape, it is important to note that perpetrators can also be of domestic origin, targeting victims and organizations within their own country.

7 "APT refers to knowledgeable human attackers that are organized, highly sophisticated and motivated to achieve their objectives against a targeted organization(s) over a prolonged period" (Ahmad et al, 2019).

Cybercrime and cybersecurity responses

Given the complexity of the landscape, identifying with confidence the perpetrators behind a certain attack or their motivation in the early stages of the incident is difficult. It necessitates a close coordination between the first responders and law enforcement since, at any stage of the incident response lifecycle, the division of roles and responsibilities between the different actors may change depending on the incident type, its target, the severity of impact, and the motivation of the perpetrators. This reflects the reality of cyberattacks, where lines are often blurred making it difficult to establish whether an attack was financially motivated, State-sponsored, or a combination of the two.[8] Hence, when developing measures to mitigate cyberthreats, whether nationally or internationally, States need to be aware of this reality and the intersections and to be able to reflect them in their policies and practices. Failing to do that risks developing incoherent national policy responses, which can be ineffective in addressing the broad range of cyberthreats to which States are exposed.

In terms of national measures, a State's approach to defining cybersecurity and cybercrime can be subject to a variety of interpretations. For instance, as there is no universally agreed definition of what cybercrime means, a common approach has been to describe it in terms of a set of conducts or a collection of acts, making it an umbrella term rather than assigning a single definition. On the one hand, this captures the reality of cybercrime. On the other, it can present challenges to successfully fighting cybercrime, in particular with regards to international cooperation and the cross-jurisdictional complexity that might emerge from adopting different approaches.[9] Internationally, it is important to understand these different national approaches in the context of global policymaking to create a common understanding and agreements that can be operationalized in a national context. Table 2 illustrates an approach to delineating between cybersecurity and cybercrime based on common definitions, the distinct regulatory focus as well as the application of these regulations in relation to the occurrence of the incident.

8 There has been considerable work examining State responsibility, looking at it, for instance, as a spectrum ranging from "State prohibited" to "State integrated" to help understand national responsibility for attacks in cyberspace. See the spectrum of State responsibility in Healey (2012).

9 This also leads to human rights concerns being raised, in particular by adopting cybercrime laws that widen the definition of cybercrime to a broad array of acts using vaguely defined terms that restrict rights and can be used to control online speech.

Table 2. Defining cybersecurity and cybercrime

CYBERSECURITY	CYBERCRIME
Definition	
Cybersecurity is typically defined as the protection of confidentiality, integrity and availability of computer data and systems in order to enhance security, resilience, reliability and trust in ICT. The concept usually covers political (national interests and security), technical and administrative dimensions.	Cybercrime is defined as offences committed against computer data, computer data storage media, computer systems, and service providers. The concept usually covers categories of offences such as illegal access, interfering with data and computer systems, fraud and forgery, illegal interception of data, illegal devices, child exploitation and intellectual property infringements.
Regulatory focus	
Cybersecurity regulation focuses on protecting national infrastructure as well as the public and private sector against cyberattacks. A strong cybersecurity stance protects computer systems from unauthorized access or being otherwise damaged or made inaccessible. It aims to reduce the risk of cyberattacks and protects against the unauthorized exploitation of systems, networks and technologies through the use of technologies, processes and controls on technical, procedural and institutional levels. Cybersecurity focuses on the policy and procedure for securing and protecting systems and assets.	Cybercrime regulation focuses on outlining what the country considers cyber-dependent crimes and cyber-enabled crimes, providing the country with instruments to criminalize the offences and authorising investigation and prosecution of cybercrime offences. Cybercrime regulations provide focus on substantive law such as misuse of devices, procedural law such as preservation of data, and other provisions such as mutual legal assistance treaties and evidence collection. These are put in place in order to protect citizens by identifying those responsible for committing crimes, dismantling their operations, and bringing them as individuals/organized criminal groups to justice.
Incident chronology	
Cybersecurity regulations typically work to prevent attacks before they occur. Security is a continuous cycle including incident response and revision of processes which happen after the detection of a breach.	Cybercrime regulations generally define and detect criminal activities in cyberspace after they occur, and provide powers to law enforcement to investigate the activities after they have occurred, to bring the offenders to justice.

Source: Interpol (2021).

As mentioned on the previous page, cybersecurity measures and cybercrime measures are interrelated and complementary, but they are not identical. Generally speaking, the former aims at making States more secure and resilient against cyberthreats and at protecting national security, critical national infrastructure, and economic well-being.[10] The latter is geared towards providing a criminal justice response to these threats. However, combined they aim to address the full range of cyberthreats. Figure 1 illustrates the difference in scope as well as the intersections with regards to the strategies that are meant to define the scope of these measures, highlighting the important role that intentionality plays in that regard.

Figure 1. Cybersecurity and cybercrime strategies

<table>
<tr><td colspan="2">National interests and security, trust, resilience, reliability of ICT</td><td colspan="2">Rule of law, human rights, and crime prevention and criminal justice</td></tr>
<tr><td colspan="2">Cybersecurity strategies</td><td colspan="2">Cybercrime strategies</td></tr>
<tr><td>Non-intentional ICT security incidents</td><td>Intentional attacks against the confidentiality, integrity, and availability of computer systems and data</td><td>Computer-related and content-related offences</td><td>Any offence involving electronic evidence</td></tr>
</table>

Source: UNODC (2013, 228), based on Seger (2012, 20).

The key role of the impact and severity of an attack in defining the response

Given the difficulty in determining whether an attack is a cybercrime or State-sponsored, and the increasing in cyberthreats to critical national infrastructure from States and non-State actors, some States have taken the incident type, the target, and the severity of impact as key metrics with which they categorize the incidents and define the responsible agency and its role and responsibilities in responding to the attack from its early stages.[11] This categorization would be revised based on how the incident develops and what the investigations reveal.

10 The United Nations General Assembly's Second Committee, which focuses on Economic and Financial Matters, adopted a series of consensus resolutions in 2002, 2003 and 2009 on "Creation of a global culture of cybersecurity". These called for priority attention be given to cybersecurity planning and management, highlighted the importance of international information sharing and collaboration to confront transnational threats, and noting the importance of protecting critical Infrastructure. See United Nations General Assembly resolutions 57/239 (UNGA, 2003), 58/199 (UNGA, 2004) and 64/211 (UNGA, 2010a). Resolution 64/211 contains in an annex a voluntary self-assessment tool for national efforts to protect critical information infrastructures.

11 See for example the United Kingdom's cyber incident prioritization framework (UK National Cyber Security Centre, 2018).

This approach necessitates having national infrastructure in place with clear lines of responsibility as well as a close coordination and alignment between law enforcement and national cybersecurity agencies to allow them to work collaboratively in defending against the growing cyberthreats. A vast amount of practical collaboration "on the ground" already exists between the two sectors at the national, regional, and international levels. While this collaboration has achieved positive results in disrupting criminal activity, it is largely limited to the States with existing capabilities. The need for further capacity-building and international cooperation on fighting cybercrime to be able to confront the growing threats and risks is a frequent priority highlighted in a variety of forums.

RANSOMWARE AS A CASE STUDY

Recent ransomware attacks against critical national infrastructure sectors, such as healthcare systems and oil pipelines, have raised alarms about the growing threat that ransomware poses to national security. The increasing availability of "ransomware as a service" – whereby a wide range of actors, whether States, criminals, or terrorist organizations – are able to deploy ransomware tools to inflict harm on citizens, societies, and economies without themselves having the necessary skills or resources to develop those tools is exacerbating the problem. This accessibility combined with the willingness of some victims to pay the ransom is increasing the incentives to conduct these attacks. In addition, the criminal use of cryptocurrencies, which allows for a masking of the identity of the ransom recipients, is further enabling these crimes.

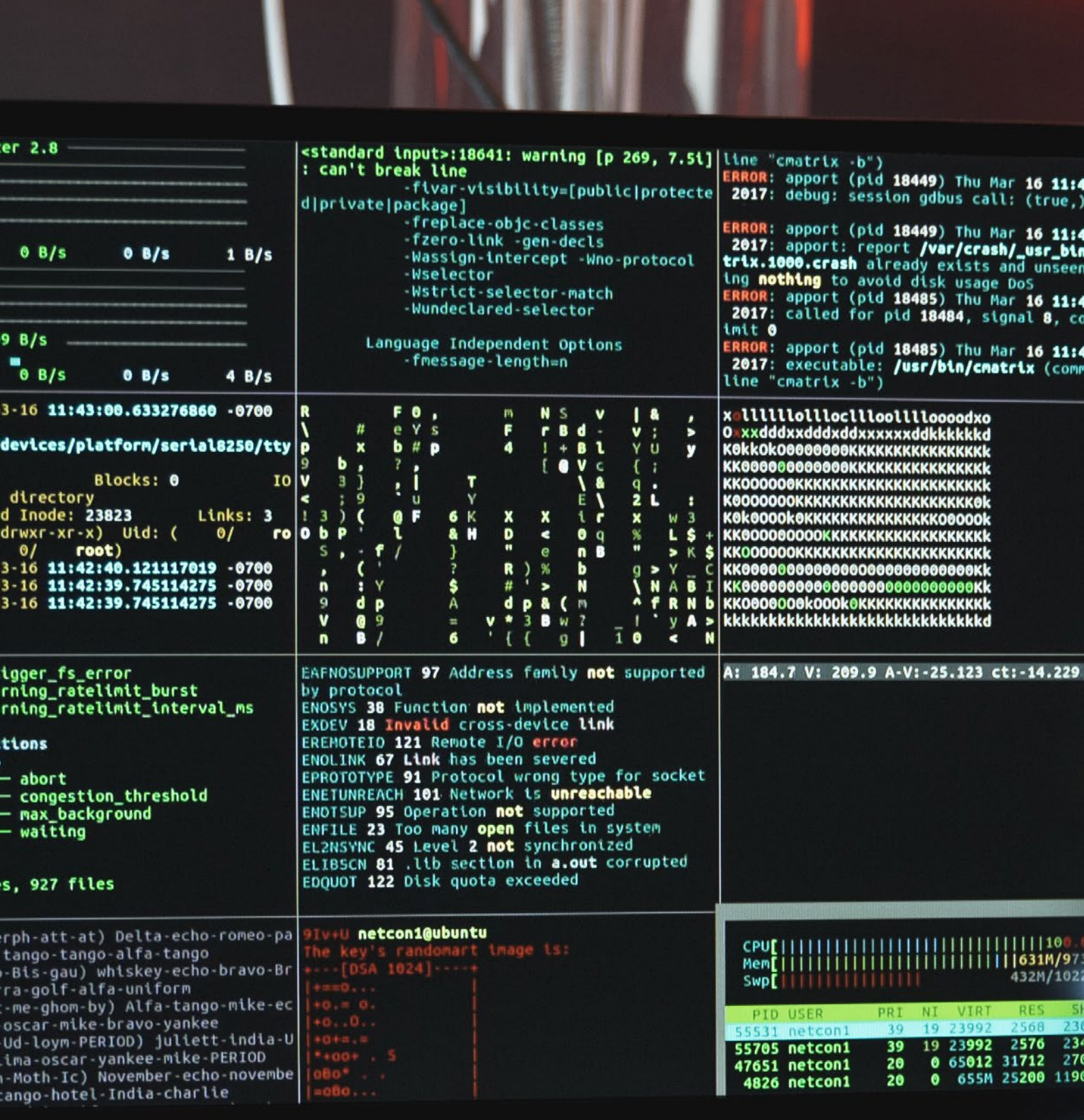
The attention that this cybercrime issue has recently received from a number of world leaders is arguably unprecedented, reinforcing the fact that threats to national security can also arise from criminal activities. While responses to cybercrime have always had international cooperation at their heart, the growing national security risks of ransomware has pushed a number of States to call for a globally coordinated approach against it that goes beyond law enforcement cooperation to also include diplomatic action at the most senior levels. It has also led to the establishment of taskforces and joint working groups such as that agreed on between the United States of America and the European Union which aims to address the rise of ransomware attacks in the United States and Europe. The need for this joined-up effort, which should complement national efforts, is hailed as the obvious approach to prevent ransomware attacks from continuing to grow in severity and size. The 2021 Carbis Bay communiqué of the Group of Seven (G7) spells this out clearly, where it commits the G7 leaders to work together to disrupt criminal ransomware networks.[12] This aligns with a recommendation issued in 2015 by the GGE and endorsed by the General Assembly that highlights the need for States to cooperate in prosecuting the terrorist and criminal use of ICTs.[13]

12 G7 (2021).
13 UNGA (2015a, para. 13(d)); UNGA (2015b, para. 2).

In addition, there is a growing expectation on States to step up their efforts to prevent their jurisdictions from being used as safe havens where cybercriminals can operate freely with impunity. The G7 communiqué calls on States to hold those criminals to account. This is also in line with the 2015 United Nations recommendations, which calls on States not to knowingly provide safe havens on their territory for either State or non-State actors to use ICTs to commit internationally wrongful acts.[14]

The conversation on the shared responsibility that States have towards each other to protect against cyberthreats, including criminal activities, is not a new one precipitated by recent events. Indeed, States have been discussing this since 1998 and they have agreed on a set of expectations or norms of responsible State behaviour, which they are expected to observe (described in section III). The global attention that ransomware has received has raised the awareness that cybercrime, like State-sponsored attacks, can aggravate inter-State tensions, even when the perpetrators are not acting on behalf of States. The measures that States have taken in response can be seen as concrete steps contributing to operationalizing an existing agreement, which was originally developed in the context of an international security negotiation but is now being applied to a cyber-crime issue. This is a positive trend that might encourage other States to think about ways in which they too can reflect these agreements within their regional and national contexts. This momentum could also be used by the international community, and specifically the related United Nations negotiations on ICTs, to highlight the importance of the intersections between cybercrime and international security and how they complement each other. It can also be used to seek ways to deepen States' understanding of how measures and agreements from the two international discussions can reinforce each other.

14 UNGA (2015a, para. 13(c)); UNGA (2015b, para. 2).


er 2.8
0 B/s 0 B/s 1 B/s
9 B/s
0 B/s 0 B/s 4 B/s
<standard input>:18641: warning [p 269, 7.5i]
: can't break line
-fivar-visibility=[public|protecte
d|private|package]
-freplace-objc-classes
-fzero-link -gen-decls
-Wassign-intercept -Wno-protocol
-Wselector
-Wstrict-selector-match
-Wundeclared-selector
Language Independent Options
-fmessage-length=n
line "cmatrix -b")
ERROR: apport (pid 18449) Thu Mar 16 11:4
2017: debug: session gdbus call: (true,)
ERROR: apport (pid 18449) Thu Mar 16 11:4
2017: apport: report /var/crash/_usr_bin
trix.1000.crash already exists and unseen
ing nothing to avoid disk usage DoS
ERROR: apport (pid 18485) Thu Mar 16 11:4
2017: called for pid 18484, signal 8, co
limit 0
ERROR: apport (pid 18485) Thu Mar 16 11:4
2017: executable: /usr/bin/cmatrix (comm
line "cmatrix -b")
3-16 11:43:00.633276860 -0700
devices/platform/serial8250/tty
Blocks: 0 IO
directory
d Inode: 23823 Links: 3
drwxr-xr-x) Uid: (0/ ro
0/ root)
3-16 11:42:40.121117019 -0700
3-16 11:42:39.745114275 -0700
3-16 11:42:39.745114275 -0700
igger_fs_error
rning_ratelimit_burst
rning_ratelimit_interval_ms
tions
- abort
- congestion_threshold
- max_background
- waiting
s, 927 files
EAFNOSUPPORT 97 Address family not supported
by protocol
ENOSYS 38 Function not implemented
EXDEV 18 Invalid cross-device link
EREMOTEIO 121 Remote I/O error
ENOLINK 67 Link has been severed
EPROTOTYPE 91 Protocol wrong type for socket
ENETUNREACH 101 Network is unreachable
ENOTSUP 95 Operation not supported
ENFILE 23 Too many open files in system
EL2NSYNC 45 Level 2 not synchronized
ELIBSCN 81 .lib section in a.out corrupted
EDQUOT 122 Disk quota exceeded
A: 184.7 V: 209.9 A-V:-25.123 ct:-14.229
erph-att-at) Delta-echo-romeo-pa
tango-tango-alfa-tango
-Bis-gau) whiskey-echo-bravo-Br
ra-golf-alfa-uniform
-me-ghom-by) Alfa-tango-mike-ec
oscar-mike-bravo-yankee
Ud-loym-PERIOD) juliett-india-U
lima-oscar-yankee-mike-PERIOD
-Moth-Ic) November-echo-novembe
cango-hotel-India-charlie
9Iv+U netcon1@ubuntu
The key's randomart image is:
+---[DSA 1024]----+
CPU[
Mem[
Swp[
432M/102
PID USER PRI NI VIRT RES
55531 netcon1 39 19 23992 2568
55705 netcon1 39 19 23992 2576
47651 netcon1 20 0 65012 31712
4826 netcon1 20 0 655M 25200

III. STATES' COMMITMENTS TO RESPONSIBLE BEHAVIOUR IN CYBERSPACE AND THEIR RELEVANCE TO ADDRESSING CYBERCRIME

ICTs and international security at the United Nations

In 1998, a Russian-sponsored resolution placed the issue of ICTs and international security on the agenda of the General Assembly's First Committee.[15] From this first resolution, the digital environment, international security, and the spectre of transnational threats such as crime and terrorism have been linked. The preamble of the resolution notes that "the dissemination and use of information technologies and means affect the interests of the entire international community" and calls attention to the necessity of preventing the misuse or exploitation of information resources or technologies for criminal purposes. It then, among other things, invited Member States to inform the Secretary-General of their views and assessments on the "Advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality".[16]

Since 2004, the General Assembly has established a series of six GGEs composed of national experts from a limited number of Member States, and an OEWG open to the whole United Nations membership.[17] These have studied the evolving threat landscape, the application of international law, the developing normative framework for responsible State behaviour, and measures for international cooperation. The assessments and recommendations of these groups have been transmitted to the General Assembly for its consideration.

Over this same period, discussions on criminal use of ICTs have developed in the General Assembly's Third Committee, within support from specialized agencies such as the United Nations Office on Drugs and Crime (UNODC), and through regional instruments such as the Council of Europe's 2001 Convention on Cybercrime (also known as the Budapest Convention).[18]

The United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ) has played a role in advancing discussions on responses to cybercrime. In 2011 the General Assembly requested the CCPCJ to establish an Open-ended Intergovernmental Expert Group (IEG), to "conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime".[19]

---

15 General Assembly resolution 53/70 (UNGA, 1999a) was based on a report of the First Committee (UNGA, 1998).

16 An annual resolution has kept this issue on the First Committee's agenda, with regular invitations to States to submit their views. Few had chosen to do so, with a peak of 24 in 2017. Early resolutions included 53/70 of 4 December 1998 (UNGA, 1999a), 54/49 of 1 December 1999 (UNGA, 1999b), 55/28 of 20 November 2000 (UNGA, 2000), 56/19 of 29 November 2001 (UNGA, 2002a) and 57/53 of 22 November 2002 (UNGA, 2002b).

17 Since 2004 there have been six GGEs on ICTs and international security, with four (2010, 2013, 2015, 2021) delivering consensus reports. UNGA (2010b); UNGA (2013); UNGA (2015a); UNGA (2021d) The OEWG was established by resolution 73/27 (UNGA, 2018) and its final report is contained in UNGA (2021b).

18 While an analysis of regional instruments is beyond the scope of this report, other regional instruments include the African Union (Malabo) Convention, the Arab Convention on Combatting Information Technology Offences; the Agreement on Cooperation among the State Members of the Commonwealth of Independent States in Combatting Offences relating to Computer Information, and the Shanghai Cooperation Organization Agreement. For an overview on existing international and regional instruments on cybercrime, see UNODC (n.d.).

19 UNGA (2011, para. 9).

Based on an agreed methodology and a collection of topics, a draft study was presented at the second meeting of the IEG in 2013.[20] This study was the topic of deliberation of the following meeting. At its fourth meeting, the IEG adopted a workplan for the period 2018–2021, with the aim of discussing in a structured manner the key issues dealt with in the study. These issues included legislation and frameworks, criminalization, law enforcement, investigations, electronic evidence and criminal justice, international cooperation, and prevention.[21] In April 2021, a stocktaking meeting took place aimed at discussing the preliminary conclusions and recommendations resulting from the work done by the IEG between 2018 and 2020 and to decide on its future work. A report including a consolidated list of 63 conclusions and recommendations was adopted by the IEG in April 2021.[22]

In addition, a new ad hoc intergovernmental committee was established by the General Assembly in December 2019.[23] It was mandated to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes. The process began with a three-day organizational session held in a hybrid format in New York between 10 and 12 May 2021 in order to agree on the modalities of the process. On 26 May 2021, the General Assembly adopted resolution 75/282, entitled "Countering the use of information and communications technologies for criminal purposes", which defines the modalities of the new negotiation process scheduled to commence in January 2022.[24]

In October 2020, First Committee adopted by a vote the resolution "Developments in the field of information and telecommunications in the context of international security", which establishes a new five-year OEWG to meet from 2021 to 2025.[25] Deeper consideration of the interplay between international security and cybercrime could be considered to be within the new OEWG's mandate "to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security, inter alia, data security, and possible cooperative measures to prevent and counter such threats", particularly as the resolution establishing that group specifically notes the necessity to prevent the use of information resources or technologies for criminal purposes.

As the First Committee continues its discussions about ICTs and international security, via the new OEWG for 2021–2025 and possibly other formats, and as the Third Committee embarks on negotiation of a United Nations convention on countering the use of ICTs for criminal purposes, it is timely to consider how existing agreements might be better leveraged by States in these new processes.[26]

20 UNODC (2013).
21 UNODC (2018).
22 UNODC (2021a).
23 UNGA (2020a).
24 UNGA (2020d).
25 UNGA (2021a).
26 The General Assembly's Second Committee consensus resolutions on "Creation of a global culture of cybersecurity" are also valuable documents which underscore the importance of national responsibility for cybersecurity, the necessity of capacity building, and the need for international information sharing and collaboration to confront transnational threats. See UNGA (2003); UNGA (2004); UNGA (2010a).

Existing commitments from GGE and OEWG reports

The threat assessments of the consensus reports of the 2010, 2013, 2015, and 2021 GGEs as well as the 2019–2021 OEWG have all noted that the malicious use of ICTs by criminals may be a threat to international peace and security.[27] Various reports have highlighted that malicious actors, including criminal groups, may have differing motivations, including financial gain. The threat assessments of these groups over the past decade have highlighted that criminal organizations may offer their services as proxies to State and non-State actors. These reports have noted that criminals are the source of many malicious tools and methodologies and the growing sophistication and scale of criminal activity in this environment. The 2019–2021 OEWG report observed that some non-State actors have demonstrated capabilities previously available only to States.

These bodies established by the First Committee have recognized that criminal actors, whether serving as proxies or on their own, may engage in malicious and harmful activities in the ICT environment of such consequence that they may threaten international security or stability, or create risks of escalation or misattribution. At the same time, recognizing that the majority of cybercrime does not have an impact on international security, the groups have been cautious to respect the mandates of the forums and processes dedicated to combatting cybercrime. Thus, the GGEs and the OEWG have limited their assessments and recommendations to promoting international cooperation to address criminal misuse of ICTs that may have an impact on international security.

The recognition that transnational threats to international security require cooperative measures to address them was present in the first consensus GGE report of 2010: "The risks associated with globally interconnected networks require concerted responses. Member States over the past decade have repeatedly affirmed the need for international cooperation against threats in the sphere of ICT security in order to combat the criminal misuse of information technology, to create a global culture of cybersecurity and to promote other essential measures that can reduce risk."[28] The synergistic relationship between international security and combatting criminal malicious use of ICTs was underscored in the report of the 2021 GGE, which noted that responding to threats involving criminal groups can contribute to international peace and security.[29] Cooperative measures may help to build capacity, reinforce the established framework for responsible State behaviour, and contribute to building trust between States.

As the GGEs' assessments have focused on the subset of criminal activity that may have implications for international security, they have avoided general recommendations on how to strengthen international responses to cybercrime and have rather focused on specific areas where additional efforts are needed when international security and cybercrime intersect.

27 UNGA (2010b, paras 5, 8); UNGA (2013, para. 6); UNGA (2015a, paras 7, 28(e)); UNGA (2021b, para. 16); United Nations Group of Governmental Experts (2021, para. 14).
28 UNGA (2010b, para. 12).
29 United Nations Group of Governmental Experts (2021, para. 31).

The GGEs have recommended that States intensify cooperation against criminal use of ICTs[30] and have suggested a variety of measures for doing so. Importantly, this includes recognition that cooperation with requests from other States to assist with investigating ICT-related crime or to mitigate malicious ICT activity emanating from their territory should be undertaken in a manner consistent with national and international law. The 2021 GGE emphasized the importance of providing assistance to investigations in a timely manner.[31]

The 2015 GGE recommended 11 norms of responsible State behaviour, which all Member States agreed to be guided by via consensus resolution 70/237. Among these, three are of particular relevance.

First, norm 13(d) addresses international cooperation specifically to address criminal use of ICTs:

> States should consider how best to **cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats**. States may need to consider whether new measures need to be developed in this respect.[32]

First Committee processes have recommended specific measures to strengthen international cooperation, coordination and effective responses to criminal use of ICTs which may have an impact on international peace and security. These measures include:

- Strengthening and further developing mechanisms to facilitate **exchanges of information** and **assistance** between national, regional and international organizations and agencies to raise ICT security awareness and reduce the operating space for online criminal activities;[33]
- Building the **capacity of relevant regional organizations** and agencies;[34]
- **Harmonizing legal approaches** as appropriate.[35]

The First Committee processes have underscored that further work on international dialogue and exchange should not duplicate ongoing work by other international organizations and forums that address the criminal use of ICTs.[36] In recognition of the importance of this work and the magnitude of the threat, the 2021 GGE recommended that efforts at the United Nations and regional levels to address criminal use of ICTs should be strengthened.[37] This includes the importance of **using existing processes, initiatives and legal instruments**, while considering additional procedures or communication channels to facilitate information exchange and assistance as needed.[38] In particular, **enhancing mechanisms for law enforcement cooperation**

30 UNGA (2013, para. 22)
31 UNGA (2021d, para. 33).
32 UNGA (2015a, para. 13(d)).
33 United Nations Group of Governmental Experts (2021, para. 33).
34 United Nations Group of Governmental Experts (2021, para. 33).
35 UNGA (2013, para. 22).
36 UNGA (2015a, para. 33).
37 United Nations Group of Governmental Experts (2021, para. 35).
38 United Nations Group of Governmental Experts (2021, para. 35).

to reduce incidents which could be misinterpreted as hostile State actions was highlighted.[39] Lastly, the 2021 GGE has encouraged States to develop cooperative **partnerships with industry, academia, and civil society** to respond to criminal use of the Internet and ICTs.[40]

However, the GGEs and OEWG have recognized that considerable prerequisites at the national level are required in order for international cooperation to be effective to combat criminal use of ICTs that may have an impact on international security, and that these prerequisites are further removed from the spheres of influence of foreign ministries. The 2021 GGE noted that national policies, legislation, structures, and mechanisms are prerequisites in order to facilitate cooperation on technical, law enforcement, legal, and diplomatic matters.[41] In this regard, specific actions at the national level recommended to support international cooperation to combat criminal use of ICTs which may threaten international peace and security include:

- **Establishing structures and mechanisms to formulate and respond to requests for assistance** to address internationally wrongful acts using ICTs;
- **Strengthening cooperative mechanisms between relevant agencies** internally to address serious ICT incidents, including the consideration of **exchanges of personnel** in areas such as incident response and law enforcement;[42]
- Developing appropriate **protocols and procedures for collecting, handling and storing online evidence**;[43]
- Strengthening **practical collaboration between law enforcement and prosecutorial agencies**,[44] as well as promoting coordination between national technical and policy capacities;[45]
- Supporting **capacity-building** to combat the use of ICTs for criminal and terrorist purposes, including by **strengthening legal frameworks, law enforcement capabilities, and strategies**;[46] specific emphasis has been put on capacity-building in the area of **digital forensics**,[47] including **sharing of good practices**;
- **Strengthening efforts at the United Nations and regional levels** to respond to criminal use of the Internet and ICTs;[48]
- **Developing partnerships with** relevant international **organizations, industry, academia, and civil society**.[49]

39 UNGA (2013, para. 26(f)).
40 United Nations Group of Governmental Experts (2021, para. 35).
41 United Nations Group of Governmental Experts (2021, para. 32).
42 UNGA (2015a, para. 17(a)).
43 United Nations Group of Governmental Experts (2021, para. 33).
44 UNGA (2013, para. 22).
45 UNGA (2021b, para. 59).
46 UNGA (2013, para. 32(a)).
47 UNGA (2015a, para. 21(h)); UNGA (2021b, annex para. 29).
48 United Nations Group of Governmental Experts (2021, para. 35).
49 United Nations Group of Governmental Experts (2021, para. 35).

Second, norm 13(c) creates a voluntary obligation for a State not to knowingly provide safe havens on its territory for State or non-State actors to use ICTs to commit internationally wrongful acts:[50]

> States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.[51]

The 2021 GGE provided specific guidance concerning this norm, including that:[52]

- States will **take reasonable steps** within their capacity to end ongoing activity through means that are proportionate, appropriate and effective, and in a manner consistent with international and domestic law;
- In the event that a State lacks the capacity to address such an act, it may **consider seeking assistance** from other States or the private sector;
- An **affected State should notify** the State from which the activity is emanating, and the **notified State should acknowledge** receipt of the notification; however, acknowledgement of receipt does not indicate concurrence with assessments contained therein and notification does not in itself imply that the notified State is responsible for the act;
- The GGE underscored that this norm **does not create an expectation that States monitor all ICT activities** within their territory.

Finally, norm 13(h) addresses responding to requests for assistance, and is particularly important when dealing with those acts that have the potential to threaten international peace and security:[53]

> States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.[54]

The 2021 GGE provided specific guidance concerning this norm, including that:[55]

- **National structures and mecshanisms** in place **to detect and mitigate ICT incidents** with the potential to threaten international peace and security contribute to the effectiveness of this norm;
- States should **offer any assistance** they have the capacity and resources to provide, and that is reasonably available and practicable in the circumstances;
- **Common templates**, developed at the bilateral, multilateral or regional level, for requesting assistance and responding to such requests can facilitate cooperation and the timeliness of response;
- Engaging in **cooperative mechanisms** that **define the means and mode of crisis communications** and of **incident management and resolution** can strengthen observance of this norm.

50 United Nations Group of Governmental Experts (2021, para. 29).
51 UNGA (2015a, para. 13(c)).
52 United Nations Group of Governmental Experts (2021, para. 30).
53 United Nations Group of Governmental Experts (2021, para. 29).
54 UNGA (2015a, para. 13(h)).
55 United Nations Group of Governmental Experts (2021, paras 52–55).

IV. EXISTING CHALLENGES AND WAYS FORWARD

Existing challenges

National coordination and capacity

As noted in section II, when a significant ICT incident occurs, many technically focused actors are engaged in mitigation and response (the so-called first responders, whether a CERT or CSIRT, an IT security unit in a public or private organization, or law enforcement agencies). However, depending on the incident, it may be elevated to the policy level for a response. Yet, there are often silos within national governments between those in law enforcement and criminal justice and those who may respond to incidents that threaten international peace and security. Many governments have yet to name or establish a leading entity inside the government to clarify the different roles and responsibilities and ensure effective coordination between these different stakeholders.

Siloed international processes

As noted in section III, the General Assembly discusses the international security dimension of ICTs in the First Committee and cybercrime in the Third Committee. The specialist nature of committee work, their mandates and the profiles of those who participate from delegations means that, in many cases, there is limited consideration of cross-cutting elements and the deeper connections between these issues has not been actively explored. To date, there has been no structured, formal exchange between the First and Third Committees on these topics, nor is there much awareness among many delegations of the state of discussions in the other forum.[56] The report of the fourth IEG meeting took note of these silos:

> The Expert Group also discussed how cybersecurity and cybercrime were related and what were the differences between them. Several speakers indicated that the two were different concepts within the very broad range of challenges that the use of modern information and communications technology presented and that they should therefore be discussed in different and more appropriate forums within the United Nations, such as the International Telecommunication Union or the Group of Governmental Experts on Information Security. Several speakers noted nonetheless that the topics were interlinked as, in practice, issues related to cybersecurity needed to be addressed to effectively counter cybercrime.[57]

The new five-year OEWG has a slightly different name than previous groups: the Open-ended Working Group on *security of and in the use of* information and communications technologies. The mandate of the new OEWG expands on that of the first OEWG, with additional emphasis on States' initiatives and State participation, and mentions, for the first time, the concept of "data security". The preamble of the resolution establishing the OEWG states that "it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes".[58]

---

56 At the request of the Chair of the OEWG, in September 2019 UNIDIR produced a paper which mapped the actors, processes and activities that directly address ICTs and international security and international law, as well as those addressing topics outside the purview of First Committee, such as cybercrime, cyberterrorism, human rights, Internet governance, and sustainable development. Feedback received from OEWG delegations and other stakeholders following the process emphasized that they were unaware of the number of United Nations processes and entities addressing criminal use of ICTs. See An Initial Overview of UN System Actors (2020).

57 ECOSOC (2018, para. 20).

58 UNGA (2021a, preambular para. 12)

It remains to be seen whether the change in the title of the group may indicate interest by some in addressing a wider range of issues in the new OEWG than in previous cyber discussions initiated by the First Committee.

Limitations on delegations

Compounding the fact that First and Third Committee processes are siloed, with no structured exchanges on cyber-related matters, delegations may confront a range of challenges in understanding the linkages and differences between the two discussions.

Large delegations tend to have different people covering the different General Assembly committees. They may also distribute their substantive portfolios across United Nations offices such that, for example, international security and First Committee issues are covered by their Geneva-based delegation while criminal and Third Committee issues are covered by delegations in Vienna and New York. They may also be able to deploy experts from capital as members of delegations or to attend particular meetings. Smaller delegations, regardless of their duty station, may be limited to following only those issues deemed to be priorities for their government. They may therefore be unfamiliar with adjacent discussions.

The meetings of the 2021–2025 OEWG will be held in New York, while the meetings to negotiate a cybercrime convention will alternate between New York and Vienna. Many New York delegations were completely new to the international security and ICT discussion at the beginning of the 2019–2021 OEWG. This nascent capacity in the New York missions will be drawn upon heavily in coming years, with a five-year OEWG process and concurrent cybercrime negotiations. New York missions will probably need increased dedicated capacity to be able to actively engage in both processes.

Geographically dispersed discussions

The decision to alternate the cybercrime negotiations between Vienna and New York has benefits but may also create additional challenges. Vienna, home to UNODC and thus an international centre for cybercrime discussions, holds valuable institutional and expert resources. Having delegates from New York permanent missions following both the OEWG and the cybercrime negotiation may raise awareness of both processes and may create new opportunities for synergies between them. However, alternating the meetings between Vienna and New York may place additional financial burdens on small delegations if they decide to maintain consistency in their delegation regardless of meeting location. If they do not, it may raise the burden of coordination between their delegations in New York and Vienna to ensure a constant level of engagement and perhaps increase the challenge of adopting a holistic approach to First and Third Committee cyber processes. UNODC in Vienna and the United Nations Secretariat in New York will have an additional burden to coordinate their support with alternating locations for the meetings.

Lack of awareness of existing assessments, recommendations and voluntary agreements
Prior to the successful 2021 GGE and 2019–2021 OEWG, there was generally a poor awareness about the assessments and recommendations of past GGE reports—despite the fact that all Member States agreed via consensus resolution 70/237 to be guided in their use of ICTs by the 2015 GGE report.[59] It appears that the recommendations and assessments of past GGEs that focus on cybercrime-related issues, and specifically norm 13(d) of 2015, have not served to reinforce in any systematic way States' efforts in other forums such as the Third Committee. As the 2019–2021 OEWG report builds upon these assessments and recommendations and acknowledges the intersection of international security and cybercrime, States have a renewed opportunity to affirm a more holistic approach to the intersections of these topics.

Unpacking assumptions associated with particular terminology
Just as in any other policy discussion, rhetoric and narrative have an enormous influence in both determining States' attitudes and threat perceptions and in shaping their responses. With no internationally recognized definitions of cybersecurity or cybercrime, it is understandable that different actors hold different associations with these terms. For example, as noted in section II, the term cybersecurity is subject to a variety of interpretations, and for many it is first and foremost a technical issue. The First Committee processes have traditionally referred to "ICTs in the context of international security" rather than "cyber-security". In addition, much of the substantive discussion on ICTs in the context of international security is framed in terms of "cyberwarfare", such as how the existing legal framework applied during armed conflict applies in the digital domain. However, as recent cyberattacks on critical infrastructure in a number of countries demonstrate, the majority of destabilizing and hostile activities witnessed today occur outside situations of armed conflict. Yet interference in the internal affairs of States through digital means, for example through cyberattacks on electoral systems, are significant and growing threats to international security and stability.

Potential ways forward

The variety of actors that have a role to play in addressing the nexus between cybercrime and international security described in this report include the diplomatic, law enforcement, judiciary, and technical communities. As these actors have different roles and responsibilities and address challenges at different levels – and have different capacities to do so – there can be no single "one size fits all" set of recommendations. However, as the international community takes forward its discussions on ICTs, cybercrime and international security, further action in the following areas may help to operationalize and strengthen international cooperation at the intersections of cybercrime and international security.

59 UNGA (2015b, para. 2).

Prioritizing building relevant national capacities that benefit both combatting cybercrime as well as maintaining international peace and security

As noted by the OEWG, "The international community's ability to prevent or mitigate the impact of malicious ICT activity depends on the capacity of each State to prepare and respond. It is of particular relevance to developing States, in order to facilitate their genuine participation in discussions on ICTs in the context of international security and their ability to address vulnerabilities in their critical infrastructure."[60] The priority areas highlighted in GGE reports and the OEWG report to combat cybercrime and build capacity are of particular importance for addressing the international security dimension of criminal use of ICTs.

Strengthening national infrastructures, developing relevant national strategies, policies, and legislation, and building the necessary expertise in diplomatic, legal, policy, legislative, and regulatory areas have all been identified as essential steps.[61] Establishing a body at the national level that coordinates across the government may help to ensure clarity about roles and responsibilities of different actors, and that the substantive intersections are recognized and approached in a coherent manner. Investing in these areas at the national level is in many ways extremely cost-effective, as the benefits of doing so amplify the ability of a State to both combat cybercrime and address its international security implications.

Further strengthening international cooperation

Section III highlights several concrete actions that States have previously agreed that can strengthen international cooperation on cybercrime and cybersecurity. As the international community embarks on negotiating an international convention on countering the use of ICTs for criminal purposes in early 2022,[62] the relevant parts of the consensus agreements from the 2021 GGE and 2019–2021 OEWG should be included as already agreed assessments and recommendations. Rather than starting from scratch, agreed consensus recommendations from the 2015 GGE report and the 2019–2021 OEWG report could be further developed and strengthened. Failing that – at a minimum – the language that has already met international consensus in the General Assembly should be repeated or referenced. Delegations may wish to also refer to the guidance offered by the 2021 GGE, particularly in relation to norms 13(c) and (d).[63] Building on the existing agreement in the context of the United Nations cybercrime process will not only reinforce and renew States' commitments to these non-binding norms but will also make them enforceable in the context of the new treaty.

60 UNGA (2021b, para. 54).

61 See for example UNGA (2021b, para. 60): "In addition to technical skills, institution-building and cooperative mechanisms, States concluded that there is a pressing need for building expertise across a range of diplomatic, legal, policy, legislative and regulatory areas. In this context, the importance of developing diplomatic capacities to engage in international and intergovernmental processes was highlighted."

62 UNGA (2020c).

63 The report of the 2021 GGE will be presented to the Seventy-Sixth Session of the General Assembly. It remains to be seen whether the Assembly will simply note its transmission or whether it will go further, as it did in 2015, and agree by consensus that States should be guided in their behaviour by the assessments and recommendations of the GGE.

There are few non-governmental stakeholders that follow both the international security and cybercrime discussions. Actors from civil society, academia, and the private sector that actively follow one process may improve their understanding of the complex multilateral dynamics on ICT-related issues if they also raise their own awareness of the other process as well as deepen their understanding of the rules and working methods of United Nations bodies. In addition, non-governmental entities – including think tanks and civil society groups – may have more agility than States to convene discussions among relevant stakeholders and to generate ideas on areas at the intersections of the two processes.

Promoting greater exchanges between the two processes

While the First and Third Committees have their respective mandates and are dedicated forums for expert-level discussion on specific topics, opportunities for promoting more nuanced exchanges between the two processes should be pursued. This would raise awareness of the overlaps and synergies described in this report, and would develop further coherence in international responses. Such efforts could be both informal and formal in nature. A few possibilities include the following.

- The Chairs of the First and Third Committee processes may jointly issue a set of observations in their personal capacities about how delegations have described the intersections of cybercrime and international security. Such observations could help delegations in both processes harmonize their approaches on the areas of overlap as well as identify gaps that require priority attention separately in each forum.
- Similarly, an interested State or group of States could sponsor a resolution in both the First and the Third Committees calling for States to voluntarily submit their views on the intersections of cybercrime and international security. A relevant institution – such as the United Nations Institute for Disarmament Research – could be requested to analyse the inputs and report back to both Committees.
- Based on the above inputs, interested stakeholders, including States and non-governmental actors, could create an informal working group to deepen understanding of the intersections, share resources, and help to build awareness in both processes. Such an informal multi-stakeholder working group could also help to identify research and analysis gaps (see the following subsection).
- Based on national interventions in both the First and the Third Committees, it is evident that some States have made strides in developing and implementing a whole-of-government approach to cyber issues. Although these approaches are constantly revised and refined, the knowledge that States have gained could be useful for other States that are seeking to do the same. Such States could take on the role of "champions" for coherence and awareness between the two forums, using their interventions to remind delegations of the state of play, achievements, commitments, and recommendations of the other process. In the recently concluded GGE and OEWG, this "champion" function was successfully played by several experts from the GGE process who also served as head of their national OEWG delegation and were thus in a position to be bridges from the less transparent GGE process to the OEWG. These voices helped to reassure the wider United Nations membership that the two processes were not working at cross-purposes, that both processes would build on existing agreements, and that the outcomes would be complementary.

- Such champions, in partnership with other relevant stakeholders, could organize side events at crucial milestones of both the First and Third Committee processes. This would ensure continued awareness and the opportunity to revisit the intersections of the two processes and their approaches.
- States that chose to voluntarily use the "National Survey of Implementation of United Nations General Assembly Resolution 70/237", as recommended by the OEWG,[64] may wish to highlight in particular their cross-cutting efforts to implement norm 13(d). They may also wish to do so in their submissions informing the Secretary-General of their national views and assessments in this regard. The voluntary submissions of views by Member States on the challenges they face in countering the use of ICTs for criminal purposes, issued in 2019 as a report of the Secretary-General, could be useful reference material for preparation of survey responses.[65]
- Specialized international and regional agencies with expertise in law enforcement and cybercrime could be encouraged to participate as observers in both processes. For example, Interpol and Europol could bring valuable expertise to First Committee-based discussions of how to operationalize norm 13(d) and the recommendations concerning law enforcement, investigations, and handling of digital evidence and forensics.[66] They may also be useful partners to serve as a bridge for exchange on the areas of intersection between the two forums.
- Regional organizations are key stakeholders and crucial partners in awareness-raising, capacity-building, and coordination among their members. As regional bodies support operationalization of existing agreements within their member states, their active participation in both processes is essential. This participation could be enhanced by amplifying key messages around the synergies that exist between addressing cybercrime and international cybersecurity and around the need forf building relevant regional and national capacities. In addition to leading reflection on how cybercrime and security issues intersect in their specific regional context, they could lead regional efforts to gather lessons from their members on how these intersections are captured in national policies and practices. This would both establish a baseline of capacity and identify regional trends, gaps, or weaknesses that could receive priority for capacity-building and assistance efforts.

Filling the research gap

While many researchers and analysts focus on individual topics at the intersections of international security and cybercrime, few have situated this work within the context of the international policy processes established to address them. This report is an initial attempt to do so and will hopefully encourage much more analysis of this juncture.

64 UNGA (2021b, para. 65).
65 UNGA (2019b).
66 UNGA (2019c); UNGA (2020b); UNGA (2021c).

As the United Nations processes established under the auspices of the First and Third Committees develop, deeper analysis will be needed to unpack the substantive intersections highlighted in this report and how they may be addressed within the mandates of these two specialized forums. In addition, more research on national practices and the way in which existing practices in cybersecurity and cybercrime responses do or do not intersect may help the processes to develop more targeted recommendations. Such analysis could initially be based on the voluntary national submissions recommended above. Further work could identify common challenges and good practices. Case studies of particular forms of cybercrime and how they are addressed in the context of the maintenance of international peace and security could be particularly illustrative. The numerous existing indexes that examine national cyber development or maturity could be a useful starting point to explore possible linkages between national cyber development/maturity levels and enabling environments for serious cybercrime.

Were an informal multi-stakeholder working group to be established (as suggested above), there might be greater incentive for the research community to produce more policy-relevant analysis as there would be a place for its consideration and uptake.

Conclusion

Work in the First and Third Committees faces the challenge of developing policy recommendations and commitments in a domain where the technologies, actors, and risks are constantly evolving. The capacities of States to prevent, mitigate, and respond to these threats also vary considerably. Ultimately, the question is how to keep multilateral policy responses relevant, fit for purpose and in line with today's realities while preparing for tomorrow's developments and helping to raise the capacities of other States to do the same.

As briefly illustrated in this report, there is international agreement on many of the areas which require capacity development in order for States to combat cybercrime as well as the malicious use of ICTs in the context of international security. Giving priority attention to these areas could be a high reward investment in support of both domains.

Developing a better understanding of the intersections between cybercrime and international security, further strengthening the national, regional, and international mechanisms, tools and capacities to address these intersections, and encouraging greater structured exchange and appropriate collaboration between the expert forums dedicated to international policy and regulation in these fields will ultimately contribute to more cohesive and effective international responses in both domains.

REFERENCES

Ahmad, A., Webb, J., Desouza, K. C. & Boorman, J. (2019). *Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack*. Computers and Security, 86, pp.402-418. https://doi.org/10.1016/j.cose.2019.07.001.

An Initial Overview of UN System Actors, Processes and Activities on ICT-Related Issues of Interest to the OEWG, by Theme. 2020: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-existing-un-bodies-processes-related-to-mandate.pdf.

British National Cyber Security Centre. 2018. "New Cyber Attack categorisation system to improve UK response to incidents". National Cyber Security Centre. 11 April 2018: https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents.

Group of Seven. 2021. "Carbis Bay G7 Summit Communiqué: Our Shared Agenda for Global Action to Build Back Better", G7 Carbis Bay Summit. 11–13 June 2021, https://www.consilium.europa.eu/media/50361/carbis-bay-g7-summit-communique.pdf.

Healey, Jason. 2012. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks", Cyber Statecraft Initiative Issue Brief. Atlantic Council. January 2012: https://www.files.ethz.ch/isn/142271/022212_ACUS_NatlResponsibilityCyber.pdf.

Interpol. 2021. *National Cybercrime Strategy Guidebook*. April 2021: https://www.interpol.int/en/content/download/16455/file/National%20Cybercrime%20Strategy%20Guidebook.pdf.

Institute for Security and Technology. 2021. *Combating Ransomware. A Comprehensive Framework for Action: Key Recommendations from the Ransomware* Task Force. Ransomware Task Force: https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf.

Seger, Alexander. 2012. *Cybercrime Strategies*, Discussion Paper. Global Project on Cybercrime, Council of Europe. 30 March 2012: https://rm.coe.int/16802fa3e1.

United Nations General Assembly (UNGA). 1998. *Role of science and technology in the context of security, disarmament and other related fields, Report of the First Committee*, UN document A/53/576, 18 November 1998.

———. 1999a. *Developments in the field of information and telecommunications in the context of international security*, UN document A/RES/53/70, 4 January 1999.

———. 1999b. *Developments in the field of information and telecommunications in the context of international security*, UN document A/RES/54/49, 23 December 1999.

———. 2000. *Developments in the field of information and telecommunications in the context of international security*, UN document A/RES/55/28, 20 December 2000.

———. 2002a. *Developments in the field of information and telecommunications in the context of international security*, UN document A/RES/56/19, 7 January 2002.

———. 2002b. *Developments in the field of information and telecommunications in the context of international security*, UN document A/RES/57/53, 30 December 2002.

———. 2003. *Creation of a global culture of cybersecurity*, UN document A/RES/57/239, 31 January 2003.

———. 2004. *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*, UN document A/RES/58/199, 30 January 2004.

———. 2010a. *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*, UN document A/RES/64/211, 17 March 2010.

———. 2010b. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/65/201, 30 July 2010.

———. 2011. *Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, UN document A/RES/65/230, 1 April 2011.

———. 2013. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/68/98, 24 June 2013.

———. 2015a. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/70/174, 22 July 2015.

———. 2015b. *Developments in the field of information and telecommunications in the context of international security*, UN document A/RES/70/237, 30 December 2015.

———. 2018. *Developments in the field of information and telecommunications in the context of international security*, UN document A/RES/73/27, 11 December 2018.

———. 2019a. *Advancing responsible State behaviour in cyberspace in the context of international security*, UN document A/RES/73/266, 2 January 2019.

———. 2019b. *Countering the use of information and communications technologies for criminal purposes*, Report of the Secretary-General, UN document A/74/130, 30 July 2019.

———. 2019c. *Open-ended Working Group on developments in the field of information and telecommunications in the context of international security*, List of Participants, UN document A/AC.290/2019/INF/1, 17 September 2019.

———. 2020a. *Countering the use of information and communications technologies for criminal purposes*, UN document A/RES/74/247, 20 January 2020.

———. 2020b. *Opened-ended Working Group on developments in the field of information and telecommunications in the context of international security*, List of Participants, UN document A/AC.290/2020/INF/1, 19 February 2020.

———. 2020c. *Countering the use of information and communications technologies for criminal purposes, Equatorial Guinea and Russian Federation: revised draft resolution*, UN document A/75/L.87/Rev.1, 24 May 2021.

———. 2020d. *Countering the use of information and communications technologies for criminal purposes*, UN document A/RES/75/282, 26 May 2021.

———. 2021a. *Developments in the field of information and telecommunications in the context of international security*, UN document A/RES/75/240, 4 January 2021.

———. 2021b. R*eport of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/75/816, 18 March 2021.

———. 2021c. *Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, List of Participants*, UN document A/AC.290/2021/INF/1, 19 March 2021.

———. 2021d. *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN document A/76/135, 14 July 2021.

United Nations Economic and Social Council (ECOSOC). 2018. *Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 3 to 5 April 2018*, UN document E/CN.15/2018/12, 13 April 2018.

United Nations Office on Drugs and Crime (UNODC). 2013. *Comprehensive Study on Cybercrime (February 2013 Draft)*. New York: United Nations.

———. 2018. *Chair's proposal for the 2018–2021 work plan of the Open-ended intergovernmental expert group meeting on cybercrime, based on Commission on Crime Prevention and Criminal Justice resolution 26/4*, UN document UNODC/CCPCJ/EG.4/2018/CRP.1, 21 February 2018.

———. 2021a. *Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 6 to 8 April 2021*, UN document UNODC/CCPCJ/EG.4/2021/2, 19 April 2021.

———. n.d. *International and Regional Instruments, Cybercrime: Module 3: Legal Frameworks and Human Rights:* https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-and-regional-instruments.html.

ANNEXES

ANNEX 1:
Overview of actors, processes and activities in the United Nations system focused on international cybersecurity and cybercrime[67]

INTERNATIONAL SECURITY, INCLUDING INTERNATIONAL LAW

1. Principal organs, main bodies, and committees

1.1 General Assembly First Committee—Disarmament and International Security

The issue of developments in the field of ICTs in the context of international security was first introduced to the agenda of First Committee in 1998 via resolution 53/70, and presented annually thereafter. These First Committee resolutions established six Groups of Governmental Experts (GGEs, 2004–2005; 2009–2010; 2012–2013; 2014–2015; 2016–2017; 2019-2021), four of which produced consensus reports.

In 2018, Member States decided to establish a sixth GGE concurrently with an Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG), both of which commenced work in 2019 and concluded in 2021.[68] The mandates of these two processes both considered existing and potential threats; capacity-building; confidence-building measures; norms, rules, and principles for responsible State behaviour; and the application of international law to the use of ICTs. The mandate of the OEWG also included an additional element: to study the possibility of establishing regular institutional dialogue under the auspices of the United Nations.

The OEWG concluded its work in March 2021, adopting a substantive report containing consensus conclusions and recommendations, and a non-consensus Chair's summary reflecting the OEWG's discussions.[69] The sixth GGE concluded its work in May 2021 and will submit its report to the seventy-sixth session of the General Assembly.[70]

Prior to the conclusion of the 2019–2021 OEWG, which was tasked to study the establishment of regular institutional dialogue under the auspices of the United Nations, in October 2020 the First Committee adopted the resolution "Developments in the field of information and telecommunications in the context of international security" by a vote, establishing a new OEWG on security of and in the use of information and communications technologies 2021–2025.[71] At

67 The contents of this annex are updated and revised from a 2020 UNIDIR paper, *An Initial Overview of UN System Actors, Processes and Activities on ICT-Related Issues of Interest to the OEWG, by Theme (2020)*, which mapped the actors, processes and activities that directly address ICTs and international security and international law, as well as those addressing topics outside the purview of First Committee, such as cybercrime, cyberterrorism, human rights, Internet governance, and sustainable development. Feedback received from OEWG delegations and other stakeholders following the process emphasized that they were unaware of the number of United Nations processes and entities addressing criminal use of ICTs.
68 UNGA (2019a); UNGA (2018).
69 UNGA (2021b).
70 UNGA (2021d).
71 UNGA (2021a).

its organizational session in June 2021, Ambassador Burhanudeen Gafoor of Singapore was elected as Chair of the new OEWG. The first session of the OEWG will be held in late 2021 and the OEWG will submit a consensus report to the General Assembly at its eightieth session.

Traditionally, the annual resolution on ICTs and international security invites Member States to submit their national views on the subject, which are compiled and issued as reports by the Secretary-General. The most recent such report is A/75/123, as requested in resolution 74/28 entitled advancing responsible State behaviour in cyberspace in the context of international security.

Links and resources:

https://www.un.org/disarmament/ict-security/

OEWG: https://www.un.org/disarmament/open-ended-working-group/

GGE: https://www.un.org/disarmament/group-of-governmental-experts/

https://undocs.org/A/75/123

For a summary of recommendations of the consensus GGE reports of 2010, 2013, and 2015, on law and norms: https://unidir.org/sites/default/files/2019-10/GGE-Recommendations-International-Law.pdf

For a summary of recommendations of the consensus GGE reports of 2010, 2013, and 2015, on confidence-building measures (CBMs) and cooperative measures: https://unidir.org/sites/default/files/2019-10/GGE-Recommendations-Confidence-Building-and-Cooperative-Measures.pdf

1.2 General Assembly Sixth Committee—Legal

The Sixth Committee is the General Assembly's forum for consideration of legal questions by all Member States. The annual report of the International Law Commission (see below) is discussed in Sixth Committee. The Sixth Committee has yet to take up the topic of ICTs and international security.

Links and resources:

https://www.un.org/en/ga/sixth/

1.3 International Court of Justice

The International Court of Justice (ICJ) is one of the six principal organs of the United Nations. Its role is to settle legal disputes submitted by States and to give advisory opinions on legal questions referred to it by authorized United Nations organs and specialized agencies, such as the request by the General Assembly in resolution 49/75K on the legality of the threat or use of nuclear weapons. The topic of ICTs and international security has yet to be referred to the ICJ.

However in paragraph 86 of the advisory opinion on the legality of the threat or use of nuclear weapons, the ICJ recalled that the established principles and rules of humanitarian law applicable in armed conflict apply "to all forms of warfare and to all kinds of weapons", including "those of the present and those of the future".

Links and resources:

https://www.icj-cij.org/en

https://www.icj-cij.org/en/case/95

1.4 International Law Commission

The International Law Commission (ILC) is mandated by the General Assembly to encourage the progressive development and codification of international law. The 34 seats on the ILC are distributed by regional groups for five-year terms. The annual ILC report is discussed in the Sixth Committee. Although the ILC has yet to take up the topic of ICTs and international security directly, its long-term programme of work includes the topic "Protection of personal data in transborder flow of information". When considering adding new topics to its work programme, the ILC uses the following criteria:

> (i) the topic should reflect the needs of States in respect of the progressive development and codification of international law; (ii) the topic should be at a sufficiently advanced stage in terms of State practice to permit progressive development and codification; (iii) the topic should be concrete and feasible for progressive development and codification; and (iv) the Commission should not restrict itself to traditional topics, but should also consider those that reflect new developments in international law and pressing concerns of the international community as a whole.

Links and resources:

https://legal.un.org/ilc/

https://legal.un.org/ilc/programme.shtml#a53

1.5 Security Council

Under Chapter VII of the United Nations Charter (Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression), a Member State could bring a significant ICT incident to the attention of the Security Council, although this has yet to happen. Under Article 39, the Council "shall determine the existence of any threat to the peace, breach of the peace, or act of aggression" and determine measures "to maintain or restore international peace and security".

On 29 June 2021, during its presidency of the Council, Estonia organized the Council's first high-level debate on cyber security with the objective of contributing to a better understanding of the growing risks stemming from malicious activities in cyberspace and their impact on international peace and security as well as to addressing the global efforts to promote peace and stability in cyberspace. However, since 2016, the Council has been briefed on several occasions on the use of ICTs and international security through "Arria formula" meetings.[72] These meeting, which involve the participation of representatives from governments, regional organizations, the private sector, and civil society, have considered the potential of State use of ICTs in fuelling political or military tensions and the importance of critical infrastructure protection, hybrid wars as a threat to international peace and security, cyber stability, conflict prevention and capacity-building, and cyberattacks against critical infrastructure.

In 2017 the Security Council adopted resolution 2341 on the protection of critical infrastructure against terrorist attacks, which recognizes cybersecurity as an important element of protection.

Links and resources:

https://www.un.org/securitycouncil/

https://media.un.org/en/asset/k1e/k1egd92tkq

https://undocs.org/S/RES/2341(2017)

1.6 United Nations Disarmament Commission

The United Nations Disarmament Commission (UNDC) is a deliberative body that considers and makes recommendations on disarmament-related issues. Meeting for three weeks each year, the UNDC's agenda comprises two substantive items that are discussed for three consecutive years. Outputs of the UNDC have included consensus principles, guidelines and recommendations, which are then transmitted to the General Assembly. Topics are determined by Member States and agreed via a resolution in the First Committee. The UNDC has yet to take up the topic of ICTs and international security.

Links and resources:

https://www.un.org/disarmament/institutions/disarmament-commission/

72 The 'Arria-formula meetings' are very informal, confidential gatherings which enable Security Council members to have a frank and private exchange of views, within a flexible procedural framework, with persons whom the inviting member or members of the Council (who also act as the facilitators or convenors) believe it would be beneficial to hear and/or to whom they may wish to convey a message." See https://www.un.org/securitycouncil/content/background-note.

2. Departments/offices and specialized entities

2.1 Department of Political and Peacebuilding Affairs

The Policy and Mediation Division of the Secretariat's Department of Political and Peacebuilding Affairs (DPPA) continues its work on digital technologies and conflict prevention, including through developing awareness and capacity of staff on the impact of digital technologies on DPPA's conflict-prevention mandate, including through the development of a cyberincident scenario exercise. The scenario is part of a broader capacity-building package aimed at identifying United Nations conflict-prevention tools and approaches that could be used in contexts where DPPA is already engaged in implementing a peace and security mandate and where a cybersecurity incident and the accompanying social media fallout risks escalating the wider conflict. In addition, building on its 2018 report and toolkit on Digital Technologies and Mediation in Armed Conflict, DPPA and swisspeace have produced "Social Media in Peace Mediation: A practical framework".

Links and resources:

https://dppa.un.org/en

https://dppa.medium.com/deep-fakes-dis-and-mis-information-and-hacking-preventing-conflict-in-the-cyber-age-ea3f0ba54af3

https://peacemaker.un.org/digitaltoolkit

https://www.swisspeace.ch/assets/publications/downloads/PeaceMediationSocialMedia_SwissPeace_UNO_Web_v1.pdf

2.2 Office for Disarmament Affairs

The mandate of the United Nations Office for Disarmament Affairs (UNODA) on ICT security is derived from the priorities established in relevant General Assembly First Committee resolutions. As such, it supports the chairs and the members of both the OEWG and the GGE. As part of the United Nations Secretariat, UNODA also supports the Secretary-General and his Executive Office on matters pertaining to international ICT security. In this capacity, it pursues the implementation of the relevant commitments included in the Secretary-General's Agenda for Disarmament. UNODA, in partnership with Member States, also contributes to awareness-raising and capacity-building, such as through the online training course on cyberdiplomacy and projects supporting States on norm implementation. UNODA's work on ICT security is closely coordinated with its work on other matters related to science and technology in the context of international security, as well as with broader work strands on emerging technologies within the Secretariat and the wider United Nations system.

Links and resources:

https://www.un.org/disarmament/ict-security/

https://www.disarmamenteducation.org/index.php?go=education&do=training-cyberdiplomacy

2.3 Office for the Coordination of Humanitarian Affairs

In 2014, the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) issued a policy paper entitled "Humanitarianism in the Age of Cyber-Warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies", which recommended advocating for a "humanitarian cyberspace". In 2021, OCHA released "From Digital Promise to Frontline Practice: New and Emerging Technologies in Humanitarian Action", which included a recommendation for States to adopt comprehensive cybersecurity strategies as well as develop the necessary domestic laws and regulations to protect the security of cyberspace and human rights in the digital environment. In addition, in 2017 OCHA established the Centre for Humanitarian Data, with the objective of helping to ensure that those in humanitarian situations have access to the data they need to make responsible and informed decisions, when they need it and in the right form. The Centre is focused on four areas: data services; data literacy; data responsibility; and predictive analytics.

Links and resources:

https://www.unocha.org/publication/policy-briefs-studies/humanitarianism-age-cyber-warfare

https://reliefweb.int/report/world/digital-promise-frontline-practice-new-and-emerging-technologies-humanitarian-action

https://centre.humdata.org/

2.4 United Nations Institute for Disarmament Research (UNIDIR)

The United Nations Institute for Disarmament Research (UNIDIR) conducts independent research and analysis, convenes multi-stakeholder expert workshops and conferences, and develops resources for policymakers on cybersecurity-related issues. Within the cyber workstream of its Security and Technology Programme, UNIDIR focuses on supporting the implementation of specific norms and recommendations previously agreed in multilateral processes and explores options to strengthen cyber stability and crisis-management mechanisms. UNIDIR holds an annual multi-stakeholder Cyber Stability Conference and maintains the Cyber Policy Portal, an online reference tool with cyber policy profiles of all 193 Member States. Through its role as consultant, UNIDIR also supports intergovernmental processes such as the United Nations GGEs and OEWG.

Links and resources:

www.unidir.org

CyberPolicyPortal.org

Summaries of consensus GGE recommendations 2010–2015 on international law and norms: https://unidir.org/sites/default/files/2019-10/GGE-Recommendations-International-Law.pdf; On CBMs and cooperative measures: https://unidir.org/sites/default/files/2019-10/GGE-Recommendations-Confidence-Building-and-Cooperative-Measures.pdf

3. Other

3.1 Conference on Disarmament

Since the First Special Session of the General Assembly on Disarmament in 1978, the 65 member Conference on Disarmament (CD) has been considered "the single multilateral disarmament negotiating forum of the international community". In recent years, some members of the CD have raised ICT-related issues under the thematic discussions on "New types of weapons of mass destruction and new systems of such weapons". In 2018, substantive discussions were held in CD Subsidiary Body 5 on the security dimensions of ICTs, artificial intelligence (AI), and machine learning. The CD has not agreed to re-establish subsidiary bodies in subsequent sessions.

Links and resources:

https://www.un.org/disarmament/conference-on-disarmament/

Report of Subsidiary Body 5, 2018: https://undocs.org/cd/2141

Summary of 2021 discussions: https://www.ungeneva.org/en/news-media/meeting-summary/2021/06/la-conference-du-desarmement-tient-un-debat-thematique-sur-les

3.2 Global Pulse

Global Pulse is an innovation initiative of the Secretary-General on big data and AI. Its mission is to accelerate discovery, development, and scaled adoption of big data innovation for sustainable development and humanitarian action. Some of its projects consider how to leverage data-driven innovations for peace and security. Examples include its study "Experimenting with Big Data and Artificial Intelligence to Support Peace and Security" and the work of its international Expert Group on Governance of Data and AI.

Links and resources:

https://www.slideshare.net/unglobalpulse/experimenting-with-big-data-and-ai-to-support-peace-and-security

https://www.unglobalpulse.org/policy/expert-group-on-governance-of-data-and-ai/

3.3 Secretary-General's Agenda for Disarmament

In 2018, with the objective of placing disarmament and non-proliferation at the centre of the work of the United Nations, the Secretary-General launched his Agenda for Disarmament, "Securing Our Common Future". In it, the Secretary-General commits to make available his good offices to contribute to the prevention and peaceful settlement of conflict stemming from malicious activity in cyberspace (Action 30) and to engage with Member States to help foster a culture of accountability and adherence to emerging norms, rules, and principles on

responsible behaviour in cyberspace (Action 31). Other action items in the Agenda include promoting multi-stakeholder dialogue and engagement on emerging technologies (Actions 27, 39, and 40), encouraging responsible innovation (Action 28), and keeping humans in control over the use of force (Action 29).

Links and resources:

https://www.un.org/disarmament/sg-agenda/en/

3.4 Office of the Secretary-General's Envoy on Technology

The Office of the Secretary-General's Envoy on Technology coordinates the implementation of the Secretary-General's Roadmap on Digital Cooperation, issued in June 2020. This Roadmap includes his vision of how the international community can leverage and expand the opportunities created by digital technologies while proactively addressing their risks and challenges. The Roadmap builds on recommendations made in the 2019 report of the High-level Panel on Digital Cooperation and on further input from Member States and other stakeholders. On the occasion of the 75th anniversary of the United Nations, the General Assembly issued a declaration containing a pledge to "improve digital cooperation".

Links and resources:

https://www.un.org/techenvoy/

https://undocs.org/en/A/74/821

https://www.un.org/techenvoy/content/roadmap-digital-cooperation

https://undocs.org/en/A/RES/75/1

https://www.un.org/en/digital-cooperation-panel/

CYBERCRIME

1. Principal organs, main bodies, and committees

1.1 General Assembly Third Committee—Social, Humanitarian, and Cultural Issues

Resolution 74/247 of 27 December 2019 established an open-ended Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Due to the COVID pandemic, the organizational session scheduled for 2020 was postponed until 10–12 May 2021.[73] On 26 May 2021, the General Assembly adopted resolution 75/282, entitled "**Countering the use of information and communications technologies for criminal purposes**", which welcomed the election of the officers of the Ad Hoc Committee, and decided that the six negotiating sessions will alternate between New York and Vienna, commencing in January 2022 and conclude in time to provide a draft convention to the General Assembly at its seventy-eighth session.

In an earlier resolution (73/187) the General Assembly requested the Secretary-General to seek the views of Member States on the challenges that they faced in countering the use of ICTs for criminal purposes and issue a report. The Report of the Secretary-General prepared pursuant to General Assembly resolution 73/187, entitled "**Countering the use of information and communications technologies for criminal purposes**" (A/74/130) reflects the responses of over 60 Member States.

Links and resources:

https://undocs.org/A/C.3/74/L.11/Rev.1

https://undocs.org/A/74/130

https://undocs.org/en/A/RES/75/282

On the basis of a recommendation by ECOSOC (see below), the General Assembly adopted resolution 74/173, "**Promoting technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime, including information-sharing**". This encourages States to implement measures to ensure that cybercrime can be investigated and prosecuted at the national level and facilitate effective international cooperation; urges training of relevant law enforcement and judiciary officials; and encourages appropriate technical assistance and capacity-building, as well as cooperation with the private sector and civil society.

Links and resources:

https://undocs.org/en/A/RES/74/173

73 For an explanation of the outcome of the Organizational session, see https://www.un.org/press/en/2021/ga12328.doc.htm

1.2 Economic and Social Council

The 54-member Economic and Social Council (ECOSOC) is another of the six principal organs of the United Nations. It coordinates the economic and social fields of the United Nations' work and serves as a forum for discussing and formulating policy recommendations for States and the United Nations system.

In July 2019, ECOSOC adopted the resolution "**Promoting technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime, including information-sharing**" (E/RES/2019/19), recognizing the important work of the Open-ended Intergovernmental Expert Group to Conduct a Comprehensive Study of Cybercrime (see below) as an "important platform for the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing responses and to propose new national and international legal or other responses for cybercrime". The resolution also encourages Member States to implement effective international cooperation on cybercrime investigation and prosecution; train officials to equip them to "effectively carry out their respective roles in investigating, prosecuting and adjudicating cybercrime offences"; and provide, upon request and based on needs, "appropriate technical assistance and sustainable capacity-building to strengthen the ability of national authorities to deal with cybercrime".

Links and resources:

https://www.un.org/ecosoc/en/

https://www.undocs.org/E/RES/2019/19

1.3 ECOSOC Functional Commission: Commission on Crime Prevention and Criminal Justice

The Commission on Crime Prevention and Criminal Justice (CCPCJ) is the United Nations' principal policymaking body in the field of crime prevention and criminal justice. The CCPCJ offers Member States a forum for exchanging expertise, experience and information in order to develop national and international strategies, and to identify priorities for combating crime. The CCPCJ is the governing body of the United Nations Office on Drugs and Crime (UNODC).

Thematic discussion at the 27th CCPCJ session (May 2018) focused on "Criminal justice responses to prevent and counter cybercrime in all its forms, including through the strengthening of cooperation at the national and international levels".

Links and resources:

http://www.unodc.org/unodc/commissions/CCPCJ/

https://www.unodc.org/unodc/en/commissions/CCPCJ/session/27_Session_2018/session-27-of-the-ccpcj.html

2. Specialized entities

2.1 United Nations Office on Drugs and Crime

The UNODC Global Programme on Cybercrime provides focused technical assistance for capacity-building, prevention and awareness-raising, international cooperation, and analysis, principally in developing countries.

Links and resources:

https://www.unodc.org/unodc/en/cybercrime/index.html

https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

2.2 Open-ended Intergovernmental Expert Group to Conduct a Comprehensive Study of Cybercrime

Via resolution 65/230, the CCPCJ established an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community, and the private sector, including the exchange of information on national legislation, best practices, technical assistance, and international cooperation, with a view to examining options to strengthen existing national and international legal or other responses to cybercrime and to propose new ones. At its seventh session, in April 2021, the expert group produced a procedural report with an annex containing conclusions and recommendations.

Links and resources:

https://www.unodc.org/unodc/en/cybercrime/egm-on-cybercrime.html

https://undocs.org/UNODC/CCPCJ/EG.4/2021/2

2.3 UNODC Cybercrime Repository

The cybercrime repository is a central data repository of cybercrime laws and lessons learned for the purposes of facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance. It includes databases on cybercrime case law, legislation, and lessons learned from national practices.

Links and resources:

https://sherloc.unodc.org/cld/v3/cybrepo/

2.4 United Nations Interregional Crime and Justice Research Institute

The United Nations Interregional Crime and Justice Research Institute (UNICRI) project "Security through Research, Technology and Innovation" (SIRIO) aims at analysing and promoting knowledge and technology solutions to address emerging security risks on issues such as supply chain security, critical infrastructures, cyberspace, AI, and big data analytics.

Links and resources:

http://www.unicri.it/special_topics/SIRIO_Security_and_Innovation/

3. Instruments

3.1 United Nations Convention against Transnational Organized Crime [74]

The United Nations Convention against Transnational Organized Crime (UNTOC) was adopted by General Assembly resolution 55/25 and acts as the main international instrument in the fight against transnational organized crime. It entered into force in September 2003.

States parties to the Convention commit to a number of measures against transnational organized crime, including developing relevant legislation; creating frameworks for extradition, mutual legal assistance and law enforcement cooperation; and capacity-building. Given its broad remit of covering transnational organized crime, many States take the position that it provides a framework for effective international cooperation on cybercrime, whereas other States believe that it does not capture the existing and emerging challenges brought forward by cybercrime and therefore is not suitable and a new framework is needed.

Links and resources:

https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

74 The Convention is further supplemented by three Protocols, which target specific areas and manifestations of organized crime: the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children; the Protocol against the Smuggling of Migrants by Land, Sea and Air; and the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition.

ANNEX 2:
Relevant assessments and recommendations from First Committee-based processes since 2010

The following tables contain relevant assessments and recommendations from First-Committee-based processes since 2010. In the interest of clarity and accuracy, section and paragraph numbers are included.

2010 GGE report (A/65/201)

Section II. Threats, risks and vulnerabilities

5. Many malicious tools and methodologies originate in the efforts of criminals and hackers. The growing sophistication and scale of criminal activity increases the potential for harmful actions.

8. Of increasing concern are individuals, groups or organizations, including criminal organizations, that engage as proxies in disruptive online activities on behalf of others. Such proxies, whether motivated by financial gain or other reasons, can offer an array of malicious services to State and non-State actors.

Section III. Cooperative measures

12. The risks associated with globally interconnected networks require concerted responses. Member States over the past decade have repeatedly affirmed the need for international cooperation against threats in the sphere of ICT security in order to combat the criminal misuse of information technology, to create a global culture of cybersecurity and to promote other essential measures that can reduce risk.

2013 GGE report (A/68/98)*

Section I. Introduction: Threats, risks and vulnerabilities

6. Threats to individuals, businesses, national infrastructure and Governments have grown more acute and incidents more damaging. The sources of these threats comprise both State and non-State actors. In addition, **individuals, groups, or organizations, including criminal organizations, may act as proxies for States in the conduct of malicious ICT actions**. The potential for the development and the spread of sophisticated malicious tools and techniques, such as bot-nets, by States or non-State actors may further **increase the risk of mistaken attribution and unintended escalation**. The absence of common understandings on acceptable State behaviour with regard to the use of ICTs increases the risk to international peace and security.

Section III. Recommendations on norms, rules and principles of responsible behaviour by States

22. States should **intensify cooperation against criminal or terrorist use of ICTs**, harmonize legal approaches as appropriate and **strengthen practical collaboration between respective law enforcement and prosecutorial agencies**.

Section IV. Recommendations on confidence building measures and the exchange of information

26(f) **Enhanced mechanisms for law enforcement cooperation to reduce incidents that could otherwise be misinterpreted as hostile State actions would improve international security**.

Section V. Recommendations on capacity-building measures

32(a) Supporting bilateral, regional, multilateral and international capacity-building efforts to secure ICT use and ICT infrastructures; to **strengthen national legal frameworks, law enforcement capabilities and strategies; to combat the use of ICTs for criminal and terrorist purposes**; and to assist in the identification and dissemination of best practices;

2015 GGE report (A/70/174)

Section II. Existing and emerging threats

7. **The diversity of malicious non-State actors**, including criminal groups and terrorists, their differing motives, the speed at which malicious ICT actions can occur and the difficulty of attributing the source of an ICT incident all increase risk.

Section III. Norms, rules and principles for the responsible behaviour of States

13(c) States should **not knowingly allow their territory to be used** for internationally wrongful acts using ICTs;

13(d) States should consider how best to **cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats**. States may need to consider whether new measures need to be developed in this respect;

13(h) States should **respond to appropriate requests for assistance** by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

Section VI. How international law applies to the use of ICTs

28(e) States **must not use proxies** to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts;

Section IV. Confidence-building measures

17(a) Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents and develop additional technical, legal and diplomatic mechanisms to address ICT infrastructure-related requests, including the consideration of **exchanges of personnel in areas such as incident response and law enforcement**, as appropriate, and encouraging exchanges between research and academic institutions;

17(e) **Cooperate**, in a manner consistent with national and international law, with requests from other States in **investigating ICT-related crime** or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.

continues on the following page

Section V. International cooperation and assistance in ICT security and capacity-building

21(h) Encourage further work in **capacity-building, such as on forensics or on cooperative measures to address the criminal or terrorist use of ICTs**.

Section VII. Conclusions and recommendations for future work

33. The United Nations should play a leading role in promoting dialogue on the security of ICTs in their use by States and developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour. Further work could consider initiatives for international dialogue and exchange on ICT security issues. **These efforts should not duplicate ongoing work by other international organizations and forums addressing issues such as criminal and terrorist use of ICTs, human rights and Internet governance**.

2019–2021 OEWG final substantive report (A/75/816, Annex I)

B. Conclusions and recommendations

Section on Existing and Potential Threats

16. States recalled that a number of States are developing ICT capabilities for military purposes. They also recalled that the use of ICTs in future conflicts between States is becoming more likely. **The continuing increase in incidents involving the malicious use of ICTs by State and non-State actors, including terrorists and criminal groups, is a disturbing trend. Some non-State actors have demonstrated ICT capabilities previously only available to States**.

Section on Capacity-building

59. States concluded that **capacity-building can help to foster an understanding of and address the systemic and other risks arising from a lack of ICT security, insufficient coordination between technical and policy capacities at the national level**, and the related challenges of inequalities and digital divides.

Chair's summary (non-consensual) of the 2019-2021 OEWG (A/75/816, Annex II)

B. Overview of Discussions

Section on Confidence-building Measures

29. In their discussions at the OEWG, States noted the continuing relevance of the CBMs recommended in the consensus GGE reports. Several measures were highlighted as requiring priority attention, such as regular dialogue and voluntary information exchanges on existing and emerging threats, national policy, legislative frameworks or doctrine, national views on how international law applies to State use of ICTs, and national approaches to defining critical infrastructure and categorizing ICT-related incidents. **It was suggested that sharing of good practices in approaches to digital forensics and investigation of malicious cyber incidents could both increase cooperation and build capacity.** The value of developing shared understanding of concepts and terminology was also highlighted as a practical step for furthering international cooperation and building trust. Other such measures included developing guidance on the implementation of CBMs, training for diplomats, exchanging lessons on establishing and exercising secure crisis communication channels, personnel exchanges, scenario-based exercises at the policy level as well as operational exercises at the technical level between Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs). National transparency measures, such as voluntarily sharing responses to an implementation survey or issuing national declarations of adherence to the framework for responsible State behaviour, were suggested as other avenues to build trust and confidence regarding the intentions and commitments of States.

2021 GGE report (A/76/135)

Section II. Existing and emerging threats

14. The Group also reaffirms that the **diversity of malicious non-State actors, including criminal groups and terrorists, their differing motives, the speed at which malicious ICT actions can occur and the difficulty of attributing the source of an ICT incident all increase risk**.

Section III. Norms, Rules and Principles

Note: Guidance offered by the GGE in relation to Norm 13 (c): States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

continues on the following page

29. This norm reflects an expectation that if a State is aware of or is notified in good faith that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory it will take all appropriate and reasonably available and feasible steps to detect, investigate and address the situation. **It conveys an understanding that a State should not permit another State or non-State actor to use ICTs within its territory to commit internationally wrongful acts**.

30. When considering how to meet the objectives of this norm, States should bear in mind the following:

(a) The norm raises the expectation that a **State will take reasonable steps within its capacity to end the ongoing activity in its territory through means that are proportionate, appropriate and effective and in a manner consistent with international and domestic law**. Nonetheless, it is not expected that States could or should monitor all ICT activities within their territory.

(b) A State that is aware of but lacks the capacity to address internationally wrongful acts conducted using ICTs in its territory may consider seeking assistance from other States or the private sector in a manner consistent with international and domestic law. **The establishment of corresponding structures and mechanisms to formulate and respond to requests for assistance may support implementation of this norm**. States should act in good faith and in accordance with international law when providing assistance and not use the opportunity to conduct malicious activities against the State that is seeking the assistance or against a third State.

(c) An **affected State should notify the State from which the activity is emanating**. The **notified State should acknowledge receipt** of the notification to facilitate cooperation and clarification and make every reasonable effort to assist in establishing whether an internationally wrongful act has been committed. Acknowledging the receipt of this notice does not indicate concurrence with the information contained therein.

(d) An **ICT incident emanating from the territory or the infrastructure of a third State does not, of itself, imply responsibility of that State** for the incident. Additionally, notifying a State that its territory is being used for a wrongful act does not, of itself, imply that it is responsible for the act itself.

Guidance offered by the GGE in relation to Norm 13(d): States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect:

continues on the following page

31. This norm reminds States of the importance of international cooperation to addressing the cross-border threats posed by criminal and terrorist use of the Internet and ICTs, including for recruitment, financing, training and incitement purposes, planning and coordinating attacks and promoting their ideas and actions, and other such purposes highlighted in this report. **The norm recognizes that progress in responding to these and other such threats involving terrorist and criminal groups and individuals through existing and other measures can contribute to international peace and security**.

32. Observance of this norm implies the **existence of national policies, legislation, structures and mechanisms that facilitate cooperation** across borders on **technical, law enforcement, legal and diplomatic matters** relevant to addressing criminal and terrorist use of ICTs.

33. States are encouraged to **strengthen and further develop mechanisms that can facilitate exchanges of information and assistance** between relevant national, regional and international organizations in order **to raise ICT security awareness** among States **and reduce the operating space** for online terrorist and criminal activities. Such mechanisms can strengthen the capacity of relevant organizations and agencies, while building trust between States and reinforcing responsible State behaviour. States are also encouraged to **develop appropriate protocols and procedures for collecting, handling and storing online evidence** relevant to criminal and terrorist use of ICTs and provide assistance in investigations in a timely manner, ensuring that such actions are taken in accordance with a State's obligations under international law.

34. Within the United Nations, **a number of dedicated fora, processes and resolutions specifically address the threats posed by terrorist and criminal use of ICTs** and the cooperative approaches required to address such threats. Relevant General Assembly resolutions include resolution 65/230 on the Twelfth United Nations Congress on Crime Prevention and Criminal Justice establishing an open-ended intergovernmental expert group (IEG) to conduct a comprehensive study of the problem of cybercrime; resolution 74/173 on promoting technical assistance and capacity-building to strengthen national measures and international cooperation to counter the use of ICTs for criminal purposes, including information sharing; and resolution 74/247 on countering the use of ICTs for criminal purposes.

35. States can also **use existing processes, initiatives and legal instruments and consider additional procedures or communication channels to facilitate the exchange of information and assistance** for addressing criminal and terrorist use of ICTs. In this regard, **States are encouraged to continue strengthening efforts underway at the United Nations and at the regional level to respond to criminal and terrorist use of the Internet and ICTs**, and **develop cooperative partnerships with international organizations, industry actors, academia and civil society to this end**.

continues on the following page

Guidance offered by the GGE in relation to Norm 13(h): States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

51. This norm reminds States that **international cooperation, dialogue, and due regard for the sovereignty of all States are central to responding to requests for assistance** by another State whose critical infrastructure is subject to malicious ICT acts. The norm is particularly important when dealing with those acts that have the potential to threaten international peace and security.

52. Upon receiving a request for assistance, **States should offer any assistance they have the capacity and resources to provide, and that is reasonably available and practicable in the circumstances**. A State may choose to seek assistance bilaterally, or through regional or international arrangements. States may also seek the services of the private sector to assist in responding to requests for assistance.

53. **Having the necessary national structures and mechanisms in place to detect and mitigate ICT incidents with the potential to threaten international peace and security enables the effective implementation of this norm**. Such mechanisms complement existing mechanisms for day-to-day ICT incident management and resolution. For example, a State wishing to request assistance from another State would benefit from knowing who to contact and the appropriate communication channel to use. A State receiving a request for assistance needs to determine, in as transparent and timely a fashion as possible and respecting the urgency and sensitivity of the request, whether it has the capabilities, capacity and resources to provide the assistance requested. States from which the assistance is requested are not expected to ensure a particular result or outcome.

54. **Common and transparent processes and procedures for requesting assistance from another State and for responding to requests for assistance can facilitate the cooperation** described by this norm. In this regard, common templates for requesting assistance and responding to such requests can ensure that the State seeking assistance provides as complete and accurate information as possible to the State from which it seeks the assistance, thereby facilitating cooperation and timeliness of response. Such templates could be developed voluntarily at the bilateral, multilateral or regional level. A **common template for responding to assistance requests** could include elements that acknowledge receipt of the request and, if assistance is possible, an indication of the timeframe, nature, scope and terms of the assistance that could be provided.

55. Where the malicious activity is emanating from a particular State's territory, **its offer to provide the requested assistance and the undertaking of such assistance may help minimize damage, avoid misperceptions, reduce the risk of escalation and help restore trust**. Engaging in **cooperative mechanisms that define the means and mode of crisis communications** and of **incident management and resolution** can strengthen observance of this norm.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

@unidirgeneva @UNIDIR un_disarmresearch