UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

Enhancing Cooperation to Address Criminal and Terrorist Use of ICTs

Operationalizing Norms of Responsible State Behaviour in Cyberspace

SAMUELE DOMINIONI

ACKNOWLEDGEMENTS

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. This study was produced by UNIDIR's Security and Technology Programme, which is funded by the Governments of Germany, the Netherlands, Norway and Switzerland and by Microsoft. The author wishes to thank the following individuals for their invaluable advice and assistance on this report: Giacomo Persi Paoli (UNIDIR), Andraz Kastelic (UNIDIR), Molihei Makumane (UNIDIR), Kerstin Vignard (UNIDIR), Wenting He (UNIDIR), Marie Humeau and Jacco-Pepijn Baljet (the Netherlands), Carmen Valeria Solis Rivera (Mexico), Neil Walsh (UNODC), Shane Cross (Interpol), Sergey Golovanov and Anastasiya Kazakova (Kaspersky), Erika Kawahara (UNODA); and the participants of the UNIDIR multi-stakeholder dialogue "Enhancing International Cooperation Mechanisms For Cybercrime And Cyberterrorism Investigations" held on 30 September 2021.

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.

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.

ABOUT THE AUTHOR

Samuele Dominioni is a researcher in the Security and Technology Programme at UNIDIR. Before joining UNIDIR, he held research positions in both academic and think tank settings. He holds a PhD in international relations and political history from Sciences Po, France, and IMT School for Advanced Studies, Italy.

Table of contents

Executive summary

Information and communications technologies (ICTs) are increasingly used for malicious ends, including criminal and terrorist purposes, which also entail recruitment, financing and propaganda. Because of the growing digitization of our societies and rapid technological development, the magnitude and nature of criminal and terrorist use of ICTs could be seen as a threat to international security. Because of the transnational dimension of these threats, effective cooperation among members states is vital. In 2015 the United Nations General Assembly approved without a vote resolution 70/237, which welcomed the 2015 report of the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. The report includes a specific norm — known as norm D – on international cooperation to address criminal and terrorist use of ICTs. Based on norm D and the further details outlined in the 2021 GGE report, this report explores current problems for effective cooperation, in particular with respect to information exchange and the handling of electronic evidence.

The report identifies challenges at three distinct levels of international cooperation: legal, operational and human.

At the **legal level**, there are three main clusters of problems, which are detrimental for effective cooperation:

- Lack of domestic legislative maturity necessary to tackle malicious use of ICTs or to engage in international assistance requests in a timely manner.
- Lack of similar conceptualization or harmonization on what concerns offences, which can hinder the exchange of information or electronic evidence. Disagreement on technical terms or definitions can hamper cooperation. Moreover, the conceptualization of what the terrorist use of ICTs entails is particularly contested.
- The speed of technological developments outpacing (domestic) legislative processes. The delay between identifying new malicious uses of ICTs and the time to update the legislation can be critical to effective international cooperation.

At the **operational level**, there are three other main clusters of challenge for effective international cooperation:

- Problems related to the mechanisms of cooperation, which include lack of clarity around the responsible points of contact (24/7 networks), and the bureaucratic process of mutual legal assistance (MLA) requests
- Challenges relating to the handling of electronic evidence, which include ensuring electronic authenticity when transferring the evidence
- Lack of resources to engage in international requests on investigations concerning criminal and terrorist use of ICTS, which may lead States to, for example, prioritize requests connected to domestic investigations

Finally, at the **human level**, there are two main types of challenge:

- Lack of knowledge regarding tools and processes of cooperation, including which protocols are in place for transferring digital evidence abroad
- Lack of experience and skills, in particular in writing mutual legal assistance requests

Considering these challenges, this report identifies actionable options that States can adopt to enhance their capacity to address and engage in international cooperation on investigations regarding criminal and terrorist use of ICTs.

At the **legal level**, possible solutions include:

- Developing national and international cybercrime strategies, which would help to develop or consolidate inter-agency collaboration, especially regarding information exchange among different domestic authorities (avoid working in silos), and to expand channels for cooperation in cyberspace in relevant field (from Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) to the diplomatic, including the signature of new mutual legal assistance treaties)
- Adopting a technology-neutral approach when drafting new bills or legal amendments to keep up with the speed of technological developments
- Keeping a flexible approach when responding to a request for assistance from another State (e.g. in the case of dual criminality, focusing on substance over definitions)

At the **operational level**, this report proposes three different sets of options:

- Finding alternative solutions to mutual legal assistance requests, which could include long-arm research warrants and direct requests as per the Second Additional Protocol to the Budapest Convention
- Setting up sufficiently secure and clear policies for dealing with electronic evidence, such as those that promote the adoption of a non-disclosure agreement that defines the confidentiality around procedures and information to be exchanged (such as Traffic Light Protocols), or use of verified open-source digital forensic tools to prove the authenticity and integrity of digital evidence
- Developing efficient governance structures and policies to avoid confusion and reduce costs, which can include defining a central authority that oversees legal assistance requests and designating a single point of contact (24/7) as the first respondent

Finally, concerning the **human level**, the report identifies two possible options for addressing the challenges identified:

- Reinforcing skills for acquisition and sharing of information and knowledge in cyber investigation – Interpol provides law and enforcement personnel trainings to develop cyber skills and technical capabilities (such as digital forensics, malware analysis) to conduct cyber investigation
- Leveraging networks and creating synergies within regional or international dedicated expert forums or workshops, such as the CSIRT–Law Enforcement Cooperation Workshops organized by the European Union Agency for Cybersecurity (ENISA) and Europol, to increase effective collaboration among practitioners
- Improving mutual legal assistance request-writing skills, such as through the use of the United Nations Office on Drugs and Crime's mutual legal assistance writing tool or through legal advisors deployed to embassies and consulates worldwide.

Abbreviations

AU	African Union
CERT	Computer Emergency Response Team
CIS	Commonwealth of Independent States
CSIRT	Computer Security Incident Response Team
EIO	European Investigative Order
EU	European Union
ICT	Information and communications technology
GGE	Group of Governmental Experts
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
OEWG	Open-Ended Working Group
UNCTAD	United Nations Conference on Trade and Development
UNODC	United Nations Office on Drugs and Crime


to the Dungeon
1986 Brain'
mjads (pvt) Ltd VIRUS_SHOE '
RECORD v9.0 Dedicated to th'
'e dynamic memories of millions o'
f virus who are no longer with u'
's today - Thanks GOODNESS!! '
' BEWARE OF THE er..VIRUS : \th'
'is program is catching prog'
'ram follows after these messeges'
$'
'.....'
'#@%$'
'@!!'
; ds = 0
; set stack
; virus
ax,cs
ds,ax
offset firsthead]
curhead],al
offset firstsector]
cursector],cx
; read

1. Introduction

Rapid developments in information and communications technologies (ICTs) are swiftly transforming the world's societies and economies. Along with new opportunities and positive effects brought by this digital revolution, States are confronting new threats and new challenges to their polities. Indeed, as ICTs are becoming a fundamental aspect of societies and economies, their security is becoming more relevant to national security.[1] Unfortunately, ICTs are increasingly used for malicious ends, including for criminal and terrorist purposes,[2] which also entail recruitment, financing and propaganda. These malicious activities are increasingly worrisome phenomena not only at the domestic level, but also at the regional and international levels. Cybercrime is one of the most disruptive and economically damaging criminal activities.[3] According to one estimate, $945 billion is lost to cybercrime each year.[4] Terrorist use of ICTs is a constant threat, which could be characterized by multiple facets. Although there has not yet been a violent terrorist attack through cyberspace, it is considered to be "one of the most catastrophic known of the unknowns".[5] It has long been recognized that there is a transnational dimension to most events and incidents relating to the criminal and terrorist use of ICTs. Indeed, given the borderless and anonymous nature of cyberspace interactions, criminals and terrorists can leverage the ubiquity that ICTs allow to successfully bypass and elude States' sovereignty.

Even though most cybercrime incidents do not have direct implications for international security, some could have an impact on it. Indeed, "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".[6] In this regard, the ability for a public authority to address a cyber incident rapidly and with the proper tools is key to assessing as soon as possible the nature and the perpetrators of the malicious event and putting in place adequate countermeasures to mitigate and respond to it. The State's capacity to investigate the nature of the incident is a vital component of avoiding misperceptions and misunderstandings that could trigger escalatory responses, which could endanger international peace and stability.

Given the transnational dimensions of these phenomena, and the chance that they could turn into threats to international security, the United Nations General Assembly approved without vote resolution 70/237, which welcomed the 2015 report of the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. The report includes a specific norm – norm D – on international cooperation to address criminal and terrorist use of ICTs. Namely, norm D affirms that:

1 For example, in April 2021, the United States Department of Homeland Security declared that ransomware is a threat to National Security. Williams (2021). See also Mueller (2017); New Zealand (2020).
2 WEF (n.d.); UNGA (2021b); International Institute for Counter-Terrorism (2021); ICT4Peace & UNCTED (2016).
3 WEF (n.d.).
4 Smith et al. (2020).
5 Broeders et al. (2021).
6 Hakmeh & Vignard (2021, 3).

> 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.[7]

This topic has been further addressed by the General Assembly through two different processes. Alongside the GGE, the General Assembly convened, through resolution 73/27, an Open-Ended Working Group (OEWG) to further develop the rules, norms and principles of responsible behaviour of States. The reports of the last session of the GGE (2019–2021) and of the first OEWG both reaffirmed the achievements of resolution 70/237. In particular, the GGE report reaffirmed norm D and expanded on possible further actions:

> 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.[8]

The OEWG report recognized that, "[t]he 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."[9]

Despite the international community being aware of the risks of criminal and terrorist use of ICTs, there are still some problems in the operationalization of norm D. This report identifies challenges and proposes actionable options to United Nations Member States to enhance international cooperation to address criminal and terrorist use of ICTs.

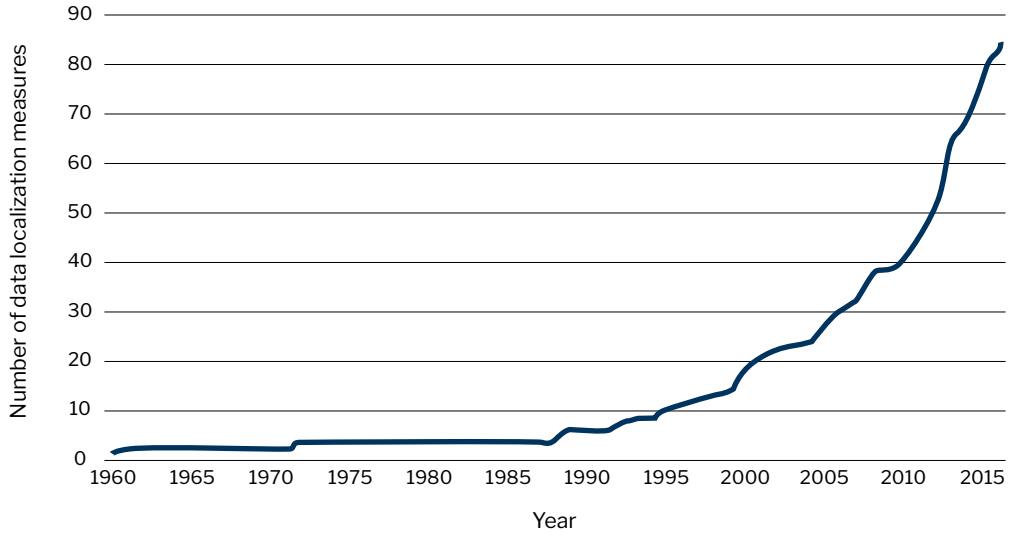
1.1 Framing the problems and methodological aspects

At the global level, there are multiple sources of concern regarding international cooperation on criminal and terrorist use of ICTs. The unresolved challenges, including the lack of a harmonized international legal framework, may have detrimental consequences for effective cooperation, and, in turn, for international peace and stability.[10] For example, the lack of coordinated and global approaches to tackle malicious use of ICTs may trigger incoherent national policy responses that could prove to be ineffective in curbing the magnitude of the threat.[11] A State that encounters problems getting access to data in other jurisdictions may adopt laws that require service providers that have a presence in the State to hold data on servers within its sovereign territory.[12] This form of unilateral policy may further fragment cyberspace, causing additional erosion of trust in the international system. In recent decades, States have increasingly adopted policies on data localization (see Figure 1). The outcomes of this approach are contrary to the spirit stressed in the 2010 GGE report:

7 UNGA (2015, para. 13(d)).
8 UNGA (2021a, para. 33).
9 UNGA (2021b, para. 16).
10 Hakmeh & Vignard (2021); Tropina (2020, 148–160).
11 Hakmeh & Vignard (2021).
12 Wu (2021).

> 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.[13]

Figure 1. Increase in data-localization measures globally, 1960–2015
Source: Wu (2021).



Notwithstanding the great division on how best to address criminal and terrorist use of ICTs, there is a new global initiative that aims to counter these threats. In December 2019, the United Nations General Assembly passed resolution 74/247, in which it decided:

> to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime.[14]

The committee of experts will have its first substantial session in January 2022 and aims to reach a consensus on a convention that would open a new phase for the harmonization of national and regional legislation and legal frameworks. Nevertheless, the process leading to a possible final convention could be long, and its success should not be taken for granted due to diverging views on many aspects of the topic among the Member States.[15] At the same time, the new OEWG (2021–2025) will also keep on addressing the

13 UNGA (2010, para. 12).
14 UNGA (2019, para. 2).
15 Walker (2021). The preliminary agenda foresees the consideration and adoption of the convention by the General Assembly at its Seventy-Ninth Session, in 2024. See UNGA (2020).

interplay between international security and cybercrime, with a view to promoting common understandings on "existing and potential threats in the sphere of information security, inter alia, data security, and possible cooperative measures to prevent and counter such threats".[16] Meanwhile, as pointed out in norm D, States shall strengthen and further develop mechanisms that can facilitate rapid exchanges of information and assistance.

The operationalization of norm D could include a vast variety of tools and mechanisms. Therefore, based on scoping interviews carried out during the preliminary research phase, this report focuses on information exchange and the handling of electronic evidence, which are two critical aspects of effective cooperation between States in cases of investigation and prosecution.[17] It does not offer a comprehensive overview of all the possible challenges and solutions in operationalizing norm D.

This report looks at current problems involving information exchange and handling electronic evidence at three distinct levels implicit in international cooperation: legal, operational and human. The legal level concerns the frameworks and mechanisms that permit collaborative initiatives among different States, including the legislative maturity to address certain criminal and terrorist offences. The operational level refers to the investigative and prosecutorial activities carried out by law and enforcement agencies and justice authorities. The human level looks at the knowledge and skills of officers and practitioners working in the field of international cooperation. The report proposes options for operationalizing information exchange and transferring electronic evidence that public authorities may implement to enhance effective cooperation in investigations regarding criminal or terrorist use of ICTs.

This report first looks at the challenges and difficulties that States are experiencing when engaging in these requests for assistance (section 2). Subsequently, it proposes operationalizable options that States may adopt to facilitate rapid information exchange and transfer of electronic evidence (section 3).

From a methodological standpoint, the research relied on three main methods:

1. Review of existing literature, instruments and legal frameworks on cooperative instruments for investigations of criminal or terrorist use of ICT
2. Targeted semi-structured interviews with cybercrime and cyberterrorist experts
3. A multi-stakeholder dialogue, which convened representatives of United Nations Member States, officers of intergovernmental organizations, legal and law enforcement personnel, and private sector representatives to discuss the challenges and opportunities of international cooperation in the investigation and prosecution of criminal and terrorist use of ICTs.

16 UNGA (2021c, 1). See also Hakmeh & Vignard (2021).

17 Electronic evidence can be non-volatile or volatile. Non-volatile evidence is stored on hardware (from a smartphone to a server). Volatile evidence is temporary stored on hardware but is then deleted once the power source is removed. Therefore, it must be acquired while it exists and then stored on hardware to be used for investigative or prosecuting purposes. This report adopts the Council of Europe definition of electronic evidence, which is "any evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network". See Council of Europe (2019).

1.2 Multilateral tracks to investigate and prosecute

States and the international community at large have been working on tackling cyber threats for at least three decades. Due to the borderless nature of most of the malicious uses of ICTs, States have been engaged in developing instruments that could support investigations and prosecutions beyond their polity. However, due to a lack of global consensus on a universal harmonized legal framework for addressing criminal and terrorist use of ICTs, there are multiple regional, bilateral and sometimes unilateral solutions to address these threats.[18] This fragmented international landscape hinders rapid and effective investigation and prosecution of criminal and terrorist use of ICTs.

Box 1. Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime, also known as the Budapest Convention, was adopted in November 2001 and entered into force in July 2004. Despite being developed by the Council of Europe, the Convention is open to all States in the world, and it is currently the most comprehensive and widely signed legally binding international treaty on this topic: 66 States have ratified the Convention, and a further 11 have signed it or been invited to accede.

As the sole legally binding international instrument on cybercrime, the principal objectives of the Budapest Convention are threefold:

1) harmonizing national legal frameworks
2) supporting cybercrime investigation
3) enhancing international cooperation to combat cybercrime

In addition, the Convention provides guidance for countries to develop comprehensive national legislation against cybercrime and serves as an international cooperation framework between the States parties. However, given the fact that there are some States that consider the Convention as a product of certain States, its international impact remains limited to a selection of countries.

Initiatives concerning criminal use of ICTs include the 2001 Council of Europe Convention on Cybercrime (Budapest Convention, see Box 1), the 2013 European Union (EU) Directive on Attacks against Information Systems, the League of Arab States Model Law and the 2010 Arab Convention on Combating Information Technology Offences (see Box 2), the 2014 African Union (AU) Convention on Cybersecurity and Data Protection, the 1992 Organization of American States (OAS) Inter-American Convention on Mutual Legal Assistance in Criminal Matters, the 2002 Commonwealth Model Law on Computer and Computer Related Crime, and the 2001 Commonwealth of Independent States (CIS) Agreement on Cooperation in Combating Offences related to Computer Information (see Box 3).

18 Tropina (2020, 148–160).

Box 2. Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information

In 2001, the Commonwealth of Independent States (CIS) adopted the Agreement on Cooperation in Combating Offences related to Computer Information, which aims to establish a legal framework for cooperation among States parties in combating offences related to computer information. The Agreement was signed by most of the CIS member States and entered into force on 14 March 2002.

The Agreement calls on its States parties to adopt necessary organizational and legal measures to implement the Agreement's provisions as well as to harmonize national cybercrime legislation. Within the framework of the Agreement, cooperation is to be carried out directly between the competent authorities of States parties and on the basis of requests for assistance made by these authorities. The cooperation between States parties includes information exchange on the prevention, detection, suppression, uncovering and investigation of offences relating to computer information (Article 5a). An offence related to computer information is defined by the Agreement as a criminal act of which the target is computer information.

All these instruments have taken stock of the Budapest Convention and further developed regional approaches to the malicious use of ICTs. Nevertheless, only the Budapest Convention, the Arab Convention and the CIS Agreement have established mechanisms for cooperation on what concerns electronic evidence.[19]

Box 3. Arab Convention on Combating Information Technology Offences

The objective of the Arab Convention on Combating Information Technology Offences is to enhance cooperation between Arab States in combatting information technology offences with a common criminal approach. The Convention was opened for signature in 2010 by member States of the League of Arab States. It has been signed by all 22 member States and 11 of them have ratified it.[20] It entered into force on 7 February 2014.

The text of the Convention lays out different categories of information technology offence to which it applies, procedural provisions, as well as legal and judicial cooperation mechanisms between States parties. With regards to cooperation on digital evidence, the Convention calls on the parties to provide assistance to each other to the fullest extent for the purpose of gathering electronic evidence of offences (Article 32); outlines procedures for mutual assistance requests (Article 34); and guarantees the presence of a specialized body in each State party to collect evidence in electronic form (Article 43). Within the cooperation framework, one party may request another to investigate, access, seize, secure or disclose the stored information technology information located within the territory of the party from which assistance is requested (Article 39).

19 Tropina (2020, 148–160).
20 The Arab states that have ratified the Convention include Algeria, Bahrain, Egypt, Iraq, Jordan, Kuwait, Oman, Palestine, Qatar, Sudan, and the United Arab Emirates, as of 27 October 2021.

On the global multilateral level, in 2010 the United Nations initiated a Comprehensive Study on Cybercrime, which was eventually published in 2013 and served as the basis for developing a global harmonization of existing legal frameworks. As mentioned above, in 2019, building on the Comprehensive Study, the General Assembly decided to establish an open-ended ad hoc intergovernmental committee of experts to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes (Cybercrime Ad Hoc Committee). However, it remains to be seen if this committee will agree upon new tools and mechanisms for expedited assistance and cooperation in investigations of criminal or terrorist use of ICTs.

Regarding the terrorist use of ICTs, norm D specifies that it includes "recruitment, financing, training and incitement purposes, planning and coordinating attacks and promoting their ideas and actions, and other such purposes".[21] Relevant international instruments already criminalize certain practices. Among them at the United Nations level are the 1999 International Convention for the Suppression of the Financing of Terrorism and the 2000 Convention against Transnational Organized Crime. Other international instruments include the 2005 Council of Europe Convention on the Prevention of Terrorism, the 2017 EU Directive on Combating Terrorism, the 2016 EU Network and Information System (NIS) Security Directive, the 1999 AU Convention on the Prevention and Combating of Terrorism, the 2002 Inter-American Convention against Terrorism, and the 2007 Association of Southeast Asian Nations (ASEAN) Convention on Counter Terrorism. However, there is not – for the time being – an international treaty or convention that globally addresses harmonization and international cooperation in countering terrorist use of ICTs.

Yet, legal frameworks developed in the field of criminal use of ICTs can also be used to address certain kinds of terrorist offence. In fact, public authorities can rely on the combination of incriminated terrorist activities and specific provisions against cybercrime to tackle terrorist use of ICTs.[22] Therefore, for these cases, States can rely on cooperation mechanisms developed in the context of bilateral or multilateral agreements that address cybercrime. For example, cooperation and assistance among States regarding certain cyber aspects of terrorism are covered in the Budapest Convention. The provisions listed in this Convention can be applied regardless of how the act of terrorism is committed.[23]

21 UNGA (2021a, para. 31).
22 Couzigou (2019); Bodin et al. (2015).
23 Sieber (2006, 395–449).

2. Existing challenges to international cooperation

For all types of malicious use of ICTs that States address, there are some concrete problems and challenges that hamper rapid and effective international cooperation. This report focuses, in particular, on those challenges regarding information exchange and the transferring of electronic evidence on three distinct levels:

1. Legal
2. Operational
3. Human

The following three subsections illustrate each of these different clusters of challenges in turn.

2.1 Legal

Given the borderless nature of the malicious activities under consideration, one of the most relevant aspects for international cooperation is the legal framework that permits collaborative initiatives among different States. The possibility to investigate and prosecute, which includes the exchange of information and electronic evidence, is strictly dependent on the jurisdiction; criminal or terrorist use of ICTs may involve more than one.[24]

There are three main sources of legal challenge relating to international cooperation in investigating criminal and terrorist use of ICTs:

1. Various levels of legislative maturity
2. Different understandings of the offences
3. Legislative inertia

2.1.1. Legislative maturity

According to the United Nations Conference on Trade and Development (UNCTAD), 154 States (79 per cent of Member States) have enacted cybercrime legislation. However, adoption patterns vary by region; Europe has the highest adoption rate (93 per cent) and Asia and the Pacific the lowest (55 per cent).[25] These trends cause significant challenges to extending requests for assistance in investigating and prosecuting crime within and outside a region. As pointed out by the Comprehensive Study on Cybercrime:

> Fragmentation at the international level, and diversity of national cybercrime laws, may correlate with the existence of multiple instruments with different thematic and geographic scopes. While instruments legitimately reflect socio-cultural and regional differences, divergences in the extent of procedural powers and international cooperation provisions may lead to the emergence of country cooperation "clusters" that are not always well suited to the global nature of cybercrime.[26]

More recent academic research has claimed that, "the regional solutions, including the Council of Europe Convention and other instruments have not yet solved the problem of harmonization of procedural instruments and international cooperation in criminal investigations to a degree that would allow a fast transborder data exchange".[27] Transferring electronic evidence and information is mainly done through pre-existing bilateral or multilateral treaties, agreements or memoranda of understanding among States. The most common form of these legal bases is

24 Brenner (2006, 189–206).
25 UNCTAD (n.d.).
26 UNODC (2013, xi).
27 Tropina (2020, 155).

the so-called Mutual Legal Assistance Treaty (MLAT), which establishes "treaty based reciprocal obligations to provide legal assistance, developed as evidence gathering tools in regard to specific transnational crime" (see box 4).[28] Therefore, a State's capacity to cooperate in investigating and prosecuting criminal or terrorist use of ICTs depends also on the number and nature of its MLATs.[29] The lack of a proper domestic legislative maturity to tackle malicious use of ICTs and to engage in international assistance requests is thus detrimental for effective cooperation.

Box 4. Mutual legal assistance

Mutual legal assistance (MLA) in criminal matters is a process through which States seek and provide assistance to other States in servicing judicial documents and gathering evidence for use in criminal cases. It is generally governed by a mutual legal assistance treaty or authorized by domestic legislation.

MLA is particularly essential in the fight against cross-border crimes such as cyber-related crimes, by facilitating transborder access to electronic evidence. The Budapest Convention is the only international instrument including MLA provisions in cybercrime cases. For instance, the Convention invites its States parties to provide mutual assistance to the widest extent possible in the investigation or prosecution of cyber-related criminal offences (Article 25), in addition to outlining procedures for mutual assistance requests in the absence of applicable international agreements (Articles 27 and 28).

2.1.2 Different understandings of the offences

Having legislative measures as well as assistance agreements or treaties may not be sufficient for effective international cooperation on these matters. Lack of compatible conceptualization and harmonization concerning offences can be a potential hindering factor for the exchange of information or electronic evidence. In this case, the two types of malicious use of ICTs mentioned in norm D, criminal and terrorist, hold different connotations. For criminal use of ICTs, there are more chances to overcome a lack of a full harmonization of offences: as affirmed in the Comprehensive Study on Cybercrime, "a key factor in establishing dual criminality is the substantive underlying conduct, and not the technical terms or definitions of the crime in national laws".[30]

The case of terrorist use of ICTs is different. This concept poses conceptualization conundrums that can have far-reaching consequences for cooperation. Depending on the scope of the understanding of what "terrorist" refers to, for example – if it includes preliminary activities or only the execution of the attack (with digital or physical effects?) – different legal frameworks may not meet the principle of dual criminality. Thus, the concept of terrorism, characterized by political differences and multiple facets, remains a challenging topic for cooperation.[31]

28 Boister (2018, 313).
29 For example, as of October 2021, the United States had 70 MLATs with other countries and regional organizations. See US Department of States (2021).
30 UNODC (2013, 202).
31 Broeders et al. (2021); Couzigou (2019).

2.1.3 Legislative inertia

The slow pace of legislative processes in developing, updating and harmonizing the domestic legal framework to address the criminal and terrorist use of ICTs adequately is the third legal problem with a direct impact on international cooperation. Given the speed of developments in ICTs, in order to have effective assistance among States, the legal framework of each country must be frequently (re)evaluated and updated to tackle new challenges and threats. In fact, the delay between identifying a new malicious use of ICTs and amending or designing legislation is critical. The process can be long, and it is usually composed of three steps: recognition of a new malicious use of ICTs; identification of gaps in the penal code; and drafting new legislation.[32] For example, it is said that most States do not yet have effective legislative solutions to address the growing worrisome phenomenon of deepfakes, which is considered to have implications for the security and stability of the international system.[33]

2.2. Operational

This subsection analyses the main challenges regarding the operational aspects of the mechanisms of cooperation among States concerning information exchange and the transfer of electronic evidence. In particular, it focuses on problems related to:

1. Mechanisms of cooperation
2. Handling of electronic evidence
3. Resources

2.2.1. Mechanisms of cooperation

States can share information or request data from other States through different channels. Among the most common are points of contact, such as 24/7 networks, for direct law enforcement cooperation (for information exchange), and requests for mutual legal assistance (MLA, for requesting electronic evidence). There critical challenges related each.

i. Concerning points of contact, the existence of multiple networks can generate confusion regarding which network or contact points to reach out to in case of an incident.[34] Globally, there are multiple 24/7 networks with overlapping outreach (G7 24/7 Cybercrime Network; 24/7 Network of Contact Points at Europol; Interpol National Central Bureau NCB for I-24/7; Budapest Convention 24/7 Points of Contact). In some cases, a State has different contact points in various agencies or institutions.[35]
ii. MLAs are the most common tools for requesting access to electronic evidence located abroad.[36] Nevertheless, there is a general understanding that the MLA process is outdated, bureaucratic and often inefficient.[37] The most common problems encountered by State authorities when they write or process an MLA are the following:

    a. The formalism and length of the process: the MLA must follow formal protocols.[38] On average an MLA request takes around 150 days (about 5 months) to be processed by the receiving State.[39]

32 ITU (2012).
33 UNIDIR (2021a).
34 UNIDIR (2021b); Author's interview with an anonymous cybersecurity expert, 1 September 2021.
35 UNODC (2013).
36 James & Gladyshev (2016, 18).
37 UNIDIR (2021b); Boister (2018); Osula (2015, 1–4).
38 UNODC (n.d.a).
39 UNODC (2013).

b. In certain cases, the MLA request must be written in a language that is acceptable to the receiving State.[40]
c. The data requested is not in the territorial jurisdiction of the receiving State, but it is in a third country.[41]
d. The receiving State does not respond or does not provide all the information or data requested. [42]
e. Not all countries provide clear guidelines on how to write an MLA request.[43]

2.2.2 Handling of electronic evidence

Ensuring data authenticity and integrity is key for investigative and prosecutorial purposes. If the data is altered, tampered with, modified or even deleted, then the investigation or prosecution can be compromised. During the investigative and prosecutorial phases, public authorities need to collect evidence from other countries. The requesting State must rely on the requested actor (either another public authority or a service provider) to collect or handle and then transfer the digital data. Challenges in this phase can relate to data-retention policies; to the existence of a non-disclosure clause to customers or clients;[44] and to the methods to ensure digital evidence authenticity.[45] The subsequent phase concerns transferring the data from the requested to the requesting State. This phase is less critical than the first, as it is a customary practice to transmit digital evidence through secured and encrypted channels (e.g. agency emails, trusted or on-premise file-hosting services)[46] or stored on physical media and handed over to the requesting State.[47] Supporting documentation with the chain of custody is generally provided.[48]

2.2.3 Resources

International cooperation for investigations concerning criminal and terrorist use of ICTs requires resources allocated to this specific task. However, not all States have the human capacity, a sufficient budget or a dedicated institutional structure to deal with cybercrime.[49] The lack of resources may lead States to prioritize specific investigations over others, with negative consequences for international cooperation in the field of criminal and terrorist use of ICTs. For example, an MLA request that contains no connection with any domestic investigation in the requested State may not be considered a priority.[50]

2.3 Human

Finally, this subsection identifies challenges concerning the human element, particularly the level of knowledge and skills of practitioners who must deal with international requests for accessing information or electronic evidence. At this level, there are two main clusters of problem:

1. Lack of knowledge regarding tools and processes
2. Lack of skills concerning specific tasks

40 Boister (2018).
41 UNIDIR (2021b).
42 James & Gladyshev (2016).
43 UNODC (n.d.a).
44 Rodriguez & Molina Granja (2017).
45 Cryptographic algorithms (such as MD5 or SHA256) are commonly used to prove digital evidence authenticity and integrity. However, there are cases of disagreement among public authorities from different countries on what digital forensic tools to use for the investigation. Author's interview with Sergey Golovanov and Anastasiya Kazakova, 8 October 2021.
46 Author's interview with Sergey Golovanov and Anastasiya Kazakova, 8 October 2021.
47 UNIDIR (2021b).
48 Author's interview with an anonymous cybersecurity expert, 2 September 2021.
49 UNODC (n.d.a); Interpol (2021).
50 UNIDIR (2021b).

2.3.1 Lack of knowledge

To effectively deal with outgoing or incoming requests for international assistance regarding criminal and terrorist use of ICTs, legal and law enforcement staff must be aware of the different options and investigative tools available. In fact, education, training and capacity building are primary challenges for many investigation units today.[51] In this regard, it is essential that "law enforcement officers and agencies have received training in investigating and managing cybercrime cases, and cases involving electronic evidence".[52]

There are multiple risks associated with inadequate knowledge of the tools and processes, which include not being able to quickly address – or not address at all – the requests for assistance. Research has shown that domestic agencies often work in silos with "little awareness and poor coordination of information, initiatives, investigations and capabilities between them".[53] The lack of knowledge was clearly depicted in a survey conducted in 2016 among the personnel of public authorities in charge of dealing with MLA requests of 23 countries around the world. The survey showed that 26 per cent of respondents did not know if their government had information-exchange protocols to transfer digital evidence abroad.[54]

2.3.2. Lack of skills

The lack of skills for investigations of criminal or terrorist use of ICTs refers to the capacity of the personnel of public authorities to perform tasks related to international cooperation. Research conducted for this report shows that one of the most critical aspects of practical international cooperation is the lack of skills for dealing with MLA requests.[55] Additional evidence is found in the above-mentioned survey:

> When asked about the major challenges to writing MLA requests for electronic evidence, 57% ... of respondents identified that the acquisition of appropriate documents from the requested country was a challenge. 51% ... identified "appropriately describing the required scope of digital evidence" as a challenge. Both protocols for digital evidence, and the exchange protocols for digital evidence was identified by 46% ... of respondents.[56]

51 James and Jang (2014, 1–8).
52 Global Cyber Security Capacity Centre (2021).
54 Interpol (2021, 31).
54 James & Gladyshev (2016).
55 UNIDIR (2021b).
56 James & Gladyshev (2016, 28).

3. Filling the gaps: solutions-oriented options

Over the last two decades, relevant developments in tackling criminal and terrorist use of ICTs have included improvements in international cooperation and assistance for investigation and prosecution. For example, in 2014, the Cybercrime Convention Committee of the Budapest Convention assessed the functioning of the mutual legal assistance provisions of the Budapest Convention and adopted a set of recommendations. In 2017, the Committee then "reviewed the follow up given by Parties to these recommendations and documented good practices".[57] In another regional setting, the Inter-American Development Bank 2020 Cybersecurity Report underlines that "[t]hroughout Latin America and the Caribbean, visible progress has been made across all aspects covered by the [Cybersecurity Capacity Maturity Model for Nations] from 2016 to 2020".[58] Nevertheless, as shown in section 2, several challenges remain. In this section, operationalizable options are proposed for each challenge identified to fill the gaps in current international cooperation.

3.1 Legal

The 2021 GGE report underlines that "[o]bservance 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."[59] However, one of the most significant challenges at this level is the lack of global harmonization of legal frameworks. Despite the growing consensus among the international community that "harmonizing global legal responses to cybercrime is critically important",[60] there is still a disagreement on how to achieve it.[61] This topic goes beyond the scope of this report; it will probably be addressed by the work for the proposed new United Nations convention on cybercrime. For the time being, there are two solutions-oriented options concerning the legal challenges identified:

1. Develop national and international cybercrime strategies
2. Adopt a neutral and flexible approach

3.1.1 Cybercrime strategies

A solid domestic legislative framework is vital for engagement in international cooperation investigations and prosecutions regarding criminal and terrorist use of ICTs.[62] At the international level, there is a series of policy-oriented texts that guide and inform States on developing a comprehensive national cybercrime strategy.[63] These texts include recommendations on how to prepare the country to engage in international cooperation in cybercrime investigations. In this regard, States should:

i. Develop or consolidate inter-agency coordination (avoid working in silos)
ii. Make cybersecurity a priority of both national and foreign policy agendas (train diplomats in cyber-related issues)
iii. Engage in international discussion (there are multiple forums, including the OEWG)

57 Council of Europe (2020, 13).
58 Inter-American Development Bank and Organization of American States (2020, 22).
59 UNGA (2021a, para. 32).
60 Boister (2018, 189).
61 UNIDIR (2021b).
62 UNIDIR (2021b).
63 See, for example, ITU (2018); Interpol (2021).

iv. Open or expand channels of cooperation on cyberspace (at all levels, from Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) to the diplomatic, including the signature of new MLATs)
v. Harmonize their national legal framework and policies with their international commitments

Confronting and engaging at the international level with peers and organizations is vital to improving coordination and synergies among States and developing and enhancing trust. States may require technical assistance in drafting their legal frameworks and building their domestic cybercrime strategies. Multiple actors promote projects aimed at increasing cyber-capacities to tackle cybercrime in many countries around the world.[64] For example, the Cybersecurity Capacity Centre for Southern Africa (C3SA) is implementing the Cybersecurity Capacity Maturity Model for Nations for the members of the Southern African Development Community (SADC), while DiploFoundation is implementing the Cybersecurity Online Course worldwide.

3.1.2. Neutral and flexible approaches

Neutrality and flexibility are crucial components of successful engagement in cross-border cooperation. They can be adopted at two levels: in the development and in the operationalization of national legal frameworks.

Regarding development, the pace of technological development and innovation is rapid, whereas legislative processes are often long. Therefore, it is advisable to adopt a "technology-neutral" approach to formulating and drafting new rules or amending existing provisions. This leaves room for additional and future ICT developments. For example, States should avoid providing specific definitions of a technological device (e.g., a smartphone or a personal computer). Otherwise, the definition can become obsolete relatively quickly and the legislative framework may not remain suitable for investigations and prosecutions, both domestically and internationally.

Regarding operationalization, in the case of requests for international assistance, the requested State has more leverage, as cooperation is, in general, subject to its law.[65] The principle of dual criminality is one of the factors that can hinder the process of responding to a request. The requested State should take a flexible approach when receiving a request, focusing more on the substance than on the technical definition of the offence for which the request was sent. This approach has already been put in practice: "[i]ncreasingly suppression conventions make provision for watering double criminality down" as "it shall be deemed to exist if the offence is within the scope of the convention, and not by implication in the domestic law of the requested state (which may not have got around to enacting the offence)".[66] In sum, flexibility is a key requirement for speeder and more effective cooperation.

64 See Cybil Cyber Capacity Knowledge Portal (n.d.).
65 Boister (2018).
66 Boister (2018, 347–48).

3.2 Operational

As affirmed in the GGE 2021 report, "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."[67] Therefore, from an operational standpoint, considering the challenges identified, there are three solution-oriented options:

1. Alternative tools to MLAs
2 Handling of electronic evidence
3. Governance

3.2.1 Alternative tools to MLAs

Given the challenges of MLA requests and, in particular, their bureaucratic nature, it could be useful to look at alternatives to the MLA that can be used for obtaining information or evidence from another State. Among these tools, there are:

i. Long-arm search warrant: This is a domestic court order that directly addresses the private sector companies of another State to provide some information (usually non-content) about specific individuals.[68]
ii. European Investigative Order (EIO): This is a "judicial decision issued in or validated by the judicial authority in one EU country to have investigative measures to gather or use evidence in criminal matters carried out in another EU country".[69] Different from the MLA, EIOs provide practitioners with a single standard form for obtaining evidence. It outlines strict deadlines and establishes limited possibilities for refusal by the executing State.[70] The existing MLAT system could be reformed by drawing on useful elements of the EIO.[71]
iii. Direct request under the Second Additional Protocol to the Budapest Convention: In November 2021, the Committee of Minister of the Council of Europe adopted a Second Additional Protocol to the Budapest Convention that addresses enhanced cooperation and disclosure of electronic evidence. The draft document published provides for:

    a. Direct cooperation with service providers (Article 6) and entities providing domain name registration services (Article 7) in other States parties for the disclosure of information to identify suspects
    b. Expedited forms of cooperation between parties for the disclosure of subscriber information and traffic data (Article 8)[72]

The Second Additional Protocol is expected to be open for signatures starting from March 2022.

3.2.2. Handling of electronic evidence

In order to effectively handle evidence, States can rely on a set of policies that would help authorities to deal with electronic evidence.

67 UNGA (2021a, para. 33)
68 This practice has been particularly used to request non-content information from United States companies. Because the Stored Communications Act (SCA) did not exclude the possibility for foreign governments, it was left to each company to decide whether or not to voluntarily disclose non-content data to foreign governments (Westmoreland and Kent, 2015). With the introduction in 2018 of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), in order to request access both to content and non-content data from US companies, foreign governments must sign a CLOUD Agreement with the United States. See US Department of Justice (2019)
69 Eurojust (n.d.)
70 Eurojust (n.d.).
71 Author's interview with an anonymous cybercrime expert, 2 September 2021.
72 Council of Europe (2021).

Operationalizable options include:

i. Developing a data-retention policy for both the public and private sectors that clearly specifies who has the authority to dispose of data and for how long data has to be kept
ii. Adopting a non-disclosure agreement that defines the confidentiality around procedures and information to be exchanged (Traffic Light Protocols can be helpful)[73]
iii. Facilitating the creation of Information Sharing and Analysis Centres (ISACs), which support information-sharing in the public and private sectors[74]
iv. Accepting verified open-source digital forensic tools to prove the authenticity and integrity of digital evidence
v. Training the personnel of legal and law enforcement agencies on proper handling techniques (Interpol has just released an in-depth online course accessible to all law enforcement agencies); and training judiciary on how digital evidence is handled and can be admitted as evidence

3.2.3 Governance

As outlined in the OEWG report, "[t]he 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".[75] Therefore, a State's governance system for managing incoming or outgoing requests for assistance in international investigations is a key aspect of cooperation. Unfortunately, in many countries, "knowledge, intelligence and resources are often spread out over several agencies with little awareness or poor coordination of information, initiatives, investigations and capabilities between them".[76] A good governance system can have positive impacts on both institutional responsiveness and resource scarcity. Two solutions for States can be proposed:

i. Defining a central or responsible authority or a procedure that oversees legal assistance requests (e.g., for electronic evidence), both outgoing and incoming. In certain countries, inter-institutional cooperation is challenging because of a lack of information or the existence of contrasts or competition among them.[77] Therefore, the authority or procedure should act as a "central body that deconflicts the work of the various national stakeholders engaged in the investigation and prosecution of cybercrime incidents".[78]
ii. Designating a single point of contact (24/7) as the first respondent for urgent cases and for providing technical assistance and information, and for preserving data.[79] This single point of contact and the above central authority can be the same agency or institution.

3.3. Human

As observed in section 2.3, there are two main hindering factors that have a negative impact on international cooperation: lack of knowledge regarding tools and procedures

73 Under a Traffic Light Protocol, three are four different colours must be applied to documents when sharing information with recipients. The colours define the level of confidence that recipients must adopt. For more information, see https://www.first.org/tlp.
74 The EU Agency for Cybersecurity (ENISA) demonstrated the benefits to both the private and public sectors, including, for the private sector, raising "the level of cybersecurity in the organization which is a member of an ISAC and prevent/ respond to the incidents which occur"; and, for the public sector, accessing "knowledge about the cybersecurity level in critical sectors. It also provides information about threats and incidents. This is helpful as it enables them to better fulfil their legal tasks." See ENISA (2018, 15).
75 UNGA (2021b, para. 54).
76 Interpol (2021, 31).
77 Author's interview with an anonymous cybersecurity expert, 3 September 2020.
78 Interpol (2021, 32).
79 Kastelic (2021).

and lack of skills in writing requests for assistance and cooperation. As outlined in the 2021 GGE report, "States are encouraged to strengthen and further develop mechanisms that can facilitate exchanges of information and assistance between relevant national, regional and international organizations."[80] The following option could address these challenges:

1. Reinforcing acquisition and sharing of information and knowledge
2. Improving MLA management skills

3.3.1 Fostering acquisition and sharing of information and knowledge at the domestic, regional and international levels

To reinforce acquisition and sharing of information and knowledge, training for practitioners could be organized that is oriented to enhance their KSA (knowledge, skills and abilities) on cyber investigations.[81] For example, Interpol provides legal and law enforcement personnel with training to develop cyber skills and technical capabilities (such as digital forensics, malware analysis) to conduct cyber investigations.

In order to increase effective collaboration among practitioners, networks can be leveraged and synergies created within regional or international dedicated expert forums or workshops. These include the CSIRT–Law Enforcement Cooperation Workshops organized by the EU Agency for Cybersecurity (ENISA) and Europol. Informal networks among practitioners are a vital resource of information and knowledge sharing.[82]

3.3.2 Improve MLA management skills

To write MLA requests, practitioners can rely on the Legal Assistance Request Writer Tool of the United Nations Office on Drugs and Crime (UNODC). This web-based tool "provides guidance to practitioners through each step of the drafting process and further helps them draft MLA requests by filling in all appropriate and relevant information".[83]

To properly assist the requesting country in preparing and sending an MLA, States can send legal advisors or legal and law enforcement representatives to their embassies worldwide to train and advise local practitioners. For example, the United States has a global programme, the Transnational and High-Tech Crime Global Law Enforcement Network (GLEN). This brings together International Computer Hacking and Intellectual Property (ICHIP) prosecutors, computer forensic analysts, and national law enforcement agents focused on delivering training and technical assistance to foreign counterparts to combat intellectual property and cybercrime activity. It also assists in the collection and use of electronic evidence to combat all types of crime, including transnational organized crime.[84]

80 UNGA (2021a, para. 33).
81 UNODC (n.d.a).
82 Author's interviews with two anonymous cybersecurity experts, 29 and 30 August 2021.
83 UNODC (n.d.b).
84 US Department of Justice (2021).

4. Conclusion

Criminal and terrorist use of ICTs is a growing and worrisome phenomenon that could endanger the stability and peace of the international system. The increasing capacity of criminal and terrorist actors to cause harm is making it more difficult for States to differentiate the perpetrators behind cyberattacks.[85] Given that criminal and terrorist actors operate in the same domain as State actors, and sometimes with similar techniques and converging interests, their attacks can be misinterpreted.[86] If public authorities cannot quickly and effectively assess the nature and identify the perpetrators of an attack, then incoherent action could undermine concrete and effective responses to criminal or terrorist use of ICTs and erode trust among the international community.

States are aware of the risks associated with poor international coordination to address such threats. In the context of the First Committee of the United Nations General Assembly, both the GGE and the OEWG recognized the relevance of these threats for international stability. The 2015 and 2021 GGE reports also proposed ways forward to curb criminal and terrorist use of ICTs, including strengthening and further developing mechanisms for exchanging information and electronic evidence.

This report, building on these considerations, identifies a set of challenges at three distinct levels – legal, operational and human. It proposes solutions-oriented options in the framework of the existing international treaties and conventions concerning the criminal and terrorist use of ICTs. These are summarized in annex 1. Each of the solutions offered in the three levels considered refers to the indications provided in the GGE 2021 report. The report's focus is on information exchange and handling electronic evidence, which are two critical aspects of effective cooperation between States in investigation and prosecution. Improving States' capacities and trust to rapidly deal with requests for information and electronic evidence is a key factor that increases investigative capabilities and reduces the chances of resorting to incoherent policy responses, which, in turn, could have detrimental effects on trust among States and on international peace and stability.

85 Hakmeh & Vignard (2021).
86 Hakmeh & Vignard (2021).

Annex 1: Challenges and solutions to enhance international cooperation to address criminal and terrorist use of ICTs

	Legal			Operational			Human	
Challenges	Different levels of legislative maturity	Different concep-tualization of offences	Legis-lative inertia	Bureaucratic MLA procedures	Improper handling of electronic evidence	Lack of resources	Lack of knowledge	Lack of skills
Solutions	Develop interna-tionally consistent cybercrime strategies Engage in inter-national forums on cyber-related issues (e.g. OEWG)	Adopt flexible approach to rule operation-alization Focus on the substance not on the definition of the offence	Adopt tech neutral approach to rule develop-ment	Find alterna-tive tools: • Long-arm search warrant • European Investi-gative Order • Second Additional Protocol to the Budapest Convention Avoid working in inter-institutional or agency silos	Designate: • Central authority with coordinative powers • One single point of contact (including for 24/7 networks) Accept open-source digital forensic tools	Designate: • Central authority with coordinative powers • One single point of contact (including for 24/7 networks) Accept open-source digital forensic tools	Reinforce or develop KSA (Knowledge, Skills and Abilities) Leverage expert forums, workshops and conferences for practi-tioners	Use the UNODC Legal Assistance Request Writer Tool Rely on legal advisors of embassies and consulates


R
T
Y
F
G
H
J
K
V
B
N
M

Bibliography

Bodin, Silvia, Marc Echilley & Odile Quinard-Thibault. 2015. 'International Cooperation in the Face of Cyber-terrorism: Current Responses and Future Issues.' Themis competition. As of 18 October 2021: http://www.ejtn.eu/Documents/THEMIS 2015/Written_Paper_France_1.pdf

Boister, Neil. 2018. *An Introduction to Transnational Criminal Law*. Oxford: Oxford University Press.

Broeders, Dennis, Fabio Cristiano & Daan Weggemans. 2021. 'Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International.' Studies in Conflict & Terrorism Ahead-of-Print: 1-28. As of 18 October 2021: https://doi.org/10.1080/1057610X.2021.1928887

Brenner, Susan W. 2006. 'Cybercrime Jurisdiction.' *Crime, Law and Social Change*, 46:189–206. As of 18 October 2021: https://doi.org/10.1007/s10611-007-9063-7

Council of Europe. 2019. 'Electronic Evidence in Civil and Administrative Proceedings'. Strasbourg: Council of Europe. As of 18 October 2021: https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

— 2020. 'Cybercrime Convention Committee (T-CY) The Budapest Convention on Cybercrime: Benefits and Impact in Practice.' Strasbourg: Council of Europe. As of 18 October 2021: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac

— 2021. 'Towards a Protocol to the Budapest Convention.' 14 April 2021. As of 18 October 2021: https://rm.coe.int/towards-2nd-additional-protocol/1680a22487

Couzigou, Irene. 2019. 'The Criminalization of Online Terrorism: Preparatory Acts Under International Law.' *Studies in Conflict & Terrorism*. Pages 1–20. https://doi.org/10.1080/1057610X.2019.1678882

Cybil Cyber Capacity Knowledge Portal. n.d. As of 18 October 2021: https://cybilportal.org

Eurojust (European Union Agency for Criminal Justice Cooperation). n.d. 'European Investigation Order'. Eurojust. As of 18 October 2021: https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/european-investigation-order-eio

ENISA (European Union Agency for Cybersecurity). 2018. Information Sharing and Analysis Centres (ISACs): Cooperative Models. 14 February 2018. As of 18 October 2021: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

Global Cyber Security Capacity Centre. 2021. *Cybersecurity Capacity Maturity Model for Nations (CMM)*. 2021 Edition. Oxford: University of Oxford. https://gcscc.ox.ac.uk/dimension-4-legal-and-regulatory-frameworks#collapse3008461

Hakmeh, Joyce & Kerstin Vignard. 2021. 'ICTs, International Security and Cybercrime: Understanding the Intersections for Better Policymaking.' Geneva: UNIDIR. As of 18 October 2021: https://unidir.org/publication/icts-international-security-and-cybercrime

ICT4Peace Foundation & UNCTED (United Nations Counter-Terrorism Committee Executive Directorate). 2016. *Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes*. As of 18 October 2021: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/ICT4Peace-Private-Sector-Engagement-in-Responding-to-the-Use-of-the-Internet-and-ICT-for-Terrorist-Purposes-2.pdf

Inter-American Development Bank and Organization of American States. 2020. 'Cybersecurity Risks, Progress, and the Way Forward in Latin American and the Caribbean.' Inter-American Development Bank. As of 18 October 2021: https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

International Institute for Counter-Terrorism. 2021. 'Cyber Report January–March 2021'. August 2021. As of 18 October 2021: http://www.ict.org.il/Article/2708/CyberReportJanuary-March2021#gsc.tab=0

Interpol. 2021. 'National Cybercrime Strategy Guidebook.' April 2021. Interpol. As of 18 October 2021: https://www.interpol.int/content/download/16455/file/National Cybercrime Strategy Guidebook.pdf

ITU (International Telecommunications Union). 2012. *Understanding Cybercrime: Phenomena, Challenges and Legal Responses*. Geneva: ITU.

— 2018. *Guide to Developing a National Cybersecurity Strategy*. Geneva: ITU.

James, Joshua I. & Pavel Gladyshev. 2016. 'A Survey of Mutual Legal Assistance Involving Digital Evidence.' Digital Investigation: *The International Journal of Digital Forensic & Incident Response* 18(C): 23–32. https://doi.org/10.1016/j.diin.2016.06.004

James, Jousha I. and Jake Jang. 2014. 'An Assessment Model for Cybercrime Investigation Capacity.' *Lecture Notes in Electrical Engineering*, 276: 1–8. https://doi.org/10.1007/978-3-642-40861-8_51

Kastelic, Andraz. 2021. 'International Cooperation to Mitigate Cyber Operations against Critical Infrastructure'. Geneva: UNIDR. As of 18 October 2021: https://unidir.org/criticalinfrastructure

Mueller, Milton. 2017. *Will the Internet Fragment?* Cambridge: Polity Press.

New Zealand. 2020. 'Position Paper on New Zealand's Participation in the February 2020 Session of the 2019–2020 Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.'

Osula, Anna-Maria. 2015. "Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorial Located Data." *Masaryk University Journal of Law and Technology*, 9:1. As of 18 October 2021: https://doi.org/10.5817/MUJLT2015-1-4

Rodriguez Rafael, Glen D. & Fernando Molina Granja. 2017. 'The Preservation of Digital Evidence and its Admissibility in the Court.' International Journal of Electronic Security and Digital Forensics, 9(1): 1–18. https://doi.org/10.1504/IJESDF.2017.081749

Sieber, Ulrich. 2006. 'International Cooperation Against Terrorist Use of the Internet.' *Érès «Revue internationale de droit penal»*, 77:395–449.

Smith, Zhanna M., Eugenia Lostri & James A. Lewis. 2020. 'The Hidden Cost of Cybercrime'. *McAfee Report*. As of 18 October 2021: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

Tropina, Tatiana. 2020. 'Cybercrime: Setting international standards.' In *Routledge Handbook of International Cybersecurity* edited by Tikk, Anneken & Kerttuen Mika. Pages 148–160. London & New York: Routledge. https://doi.org/10.4324/9781351038904

United States Department of Justice. 2019. 'The Purpose and Impact of the CLOUD Act.' *White Paper*, April 2019, Washington: Department of Justice. As of 18 October 2021: https://www.justice.gov/opa/press-release/file/1153446/download

— 2021. '2020 ICHIP Activities.' 19 February 2021. As of 18 October 2021: https://www.justice.gov/criminal-opdat/2020-ichip-activities

United States Department of State. 2021. 'Criminal Matters, Requests from Foreign Tribunals, and Other Special Issues.' *Foreign Affairs Manual*. Washington: Department of State. As of 18 October 2021: https://fam.state.gov/searchapps/viewer?format=html&query=mlat&links=MLAT&url=/FAM/07FAM/07FAM0960.html#M962_1

UNCTAD (United Nations Conference on Trade and Development). n.d. 'Cybercrime Legislation Worldwide.' As of 18 October 2021: https://unctad.org/page/cybercrime-legislation-worldwide

UNGA (United Nations General Assembly). 2010. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. UN document A/65/201, 31 July 2010. https://undocs.org/A/65/201

— 2015. 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. https://undocs.org/A/70/174

— 2019. Countering the Use of Information and Communication Technologies for Criminal Purposes, UN document A/RES/74/247, 20 January 2020. https://undocs.org/A/RES/74/247

— 2020. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of information and Communication Technologies for Criminal Purposes. UN document A/AC.291/2, 15 June 2020. http://undocs.org/A/AC.291/2

— 2021a. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/76/135, 14 July 2021. https://undocs.org/A/76/135

— 2021b. Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. Final Substantive Report, UN document A/AC.290/2021/CRP.2. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

— 2021c. Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. Provisional agenda and annotations, UN Document A/AC.292/2021/1, 21 May 2021. https://undocs.org/A/AC.292/2021/1

UNIDIR (United Nations Institute for Disarmament Research). 2021a. 'The Innovations Dialogue'. 25 August 2021. As of 18 October 2021: https://unidir.org/events/2021-innovations-dialogue

— 2021b. 'Multistakeholder Dialogue on Enhancing Cybercrime and Cyberterrorism Investigations.' 30 September 2021.

UNODC (United Nations Office on Drugs and Crime). 2013. *Comprehensive Study on Cybercrime*. Vienna: UNODC. https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

— n.d.a. 'Module 7: International Cooperation Against Cybercrime'. As of 18 October 2021: https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html

— n.d.b. 'Mutual Legal Assistance Request Writer Tool.' As of 18 October 2021: https://www.unodc.org/mla

Walker, Summer. 2021. 'Contested Domain: UN Cybercrime Resolution Stumbles out of the Gate.' Global Initiative Against Organized Crime. 2 June 2021. As of 18 October 2021: https://globalinitiative.net/analysis/un-cybercrime-resolution

WEF (World Economic Forum). n.d. *Partnership Against Cybercrime*. Geneva: WEF. As of 18 October 2021: whttps://www.weforum.org/projects/partnership-against-cybercime

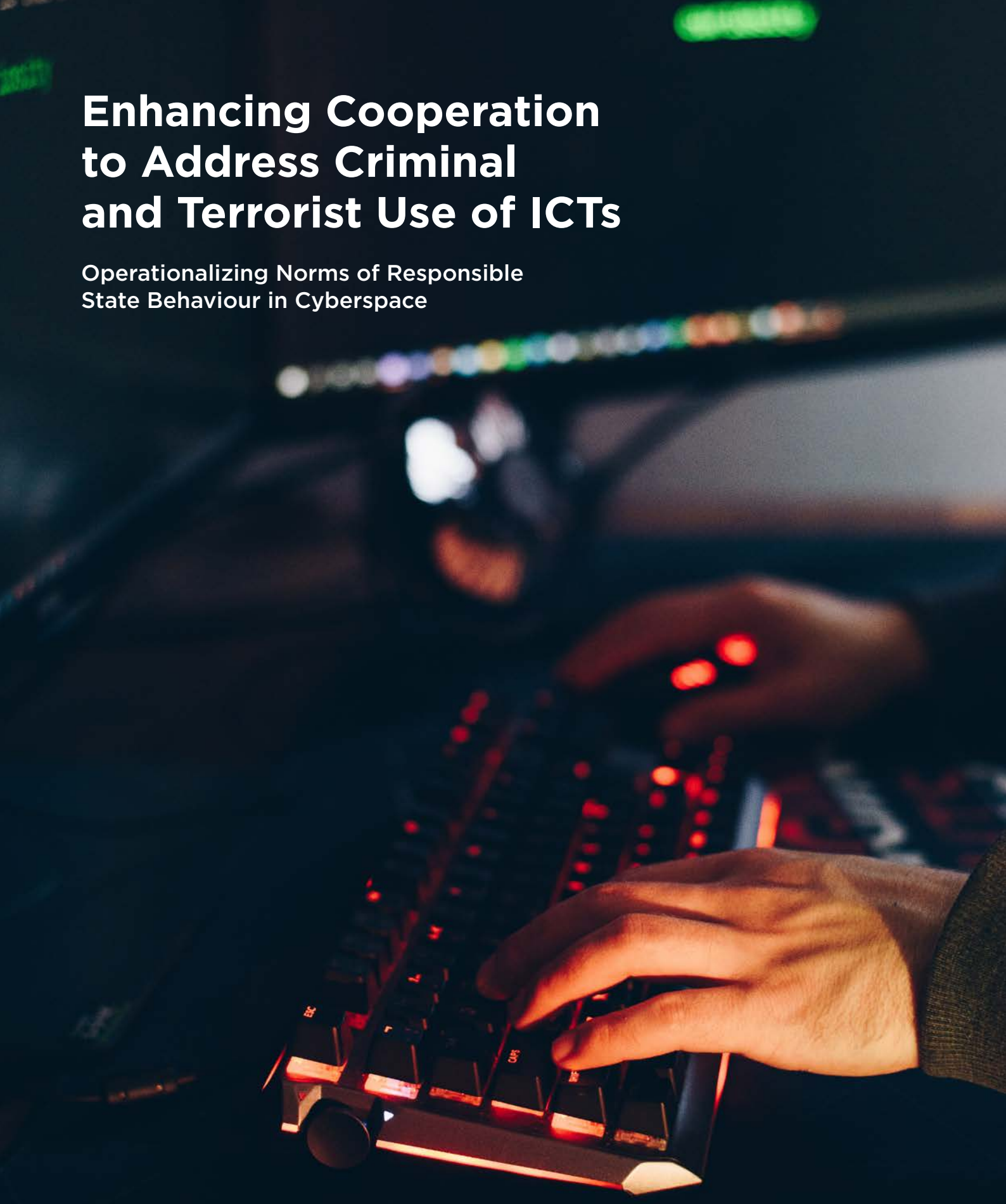
Westmoreland and Kent. 2015. 'International Law Enforcement Access to User Data: A Survival Guide and Call for Action.' *Canadian Journal of Law and Technology*, 13(2), 225–254.

Williams, Brad D. 2021 'DHS: Ransomware is National Security Threat.' Breaking Defense, 29 April 2021. As of 18 October 2021: https://breakingdefense.com/2021/04/ransomware-a-national-security-issue-new-report-argues-yes

Wu, Emily. 2021. 'Sovereignty and Data Localization.' *Paper – Cyber Project*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School. As of 18 October 2021: https://www.belfercenter.org/publication/sovereignty-and-data-localization

Enhancing Cooperation to Address Criminal and Terrorist Use of ICTs

Operationalizing Norms of Responsible State Behaviour in Cyberspace



UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

@unidirgeneva @UNIDIR un_disarmresearch