ICC Cybersecurity Issue Brief #2

Implementing norms and rules for responsible state behaviour in cyberspace and enhancing cooperation to counter cybercrime

Executive summary

Cyberspace is now an intrinsic part of the development of every country, creating enormous opportunities and enabling everything from distance learning to innovation and economic efficiencies. This paper offers concrete recommendations on two fronts to encourage the international community to take action to ensure this space is safe and secure for all.

To guarantee the timely and global implementation of existing norms and rules for responsible state behaviour in cyberspace, governments should:[1]

1. Develop a common implementation framework for the widely agreed norms and international law—the Cyber Development Goals (CDGs)—and build capacity for implementation.

   Setting CDGs would not only help set common objectives, but would also help track progress on implementation and inspire international and multistakeholder collaboration;
2. Establish common workable cyber attribution standards;
3. Establish deterrence doctrines and make them publicly available;
4. Call out violations of the widely agreed international cybersecurity framework;
5. Create a standing forum for action.

To ensure the development of effective international provisions to help curb cybercrime and encourage international cooperation, governments should, amongst other principles:[2]

1. Ensure compatibility with existing international obligations and instruments to avoid unintended negative consequences from overlapping or conflicting provisions;
2. Focus on widely-understood criminal acts which have common, clear and compatible definitions in many different legal jurisdictions;
3. Focus on crimes dependent on digital technologies, to avoid treating traditional crimes enabled by such technologies as cybercrime;
4. Balance sanctions with related safeguards;
5. Make available the capacity building and technical assistance necessary to ensure all countries are able to implement the provisions.

1 Further recommendations may be found in Part 1 of this Issue Brief
2 Further recommendations may be found in Part 2 of this Issue Brief

Introduction

Given the destructive consequences of cyberattacks on a global scale, policy agendas are dominated by conversations around safety and security in cyberspace, whether considering the development of new, and the implementation of existing cyber norms and rules, or establishing effective solutions to curb cybercrime. Such dialogues encourage a cohesive global approach to curbing cyberthreats and enhancing global security and stability.

Business considers it imperative for the international community to come together to ensure such conversations inspire concrete action to halt the growing trend of cyberthreats on businesses, communities and governments worldwide.

In December 2021, ICC released its first Cybersecurity Issue Brief[3], outlining the costs and risks associated with cyberthreats, drawing attention to the fact that international norms, rules, and agreements exist to help mitigate these risks and curb the growing trend of cyberthreats.

The time has come to move forward with the implementation of many years of diplomatic discussions and negotiations in international and regional fora. ICC, as the world business organisation with a network of more than 45 million companies in over 100 countries, calls on governments to make implementation a priority and take action to control and help reverse the tide of deteriorating cybersecurity and cyber safety conditions.

This Issue Brief offers concrete recommendations on how to do so, in two major areas:

i. fostering urgent, large-scale and effective implementation of the widely agreed existing norms and rules for state behaviour in cyberspace, by setting shared Cyber Development Goals; and

ii. reaching common understanding on international rules on cybercrime and facilitating cooperation.

3 ICC Cybersecurity Issue Brief #1: Call for Government Action on Cybersecurity

Part 1
Implementation of the existing international cybersecurity framework

Cybersecurity discussions in international fora have focused on norms, rules, and principles of behaviour, and accompanying confidence-building measures, to guide responsible state behaviour in cyberspace. The agreement on 11 norms for responsible state behaviour in cyberspace, reached through the UN Group of Governmental Experts on information security (GGE) in 2015 was the first step towards a common framework. Since then, the norms were reinforced in several workstreams at the United Nations. The work of the first UN Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) culminated in a 2021 report (the OEWG Report) that reaffirmed member states' commitment to the applicability of international law in cyberspace and the 11 GGE norms for state behaviour.[4] The 2021 GGE report also further reiterated this commitment.[5]

The OEWG Report further confirms the view that norms reduce cybersecurity risk and prevent conflict, but also that there is a continuous need for their development. In addition, the OEWG Report has recommended that, on a voluntary basis, states survey their current national efforts to implement such norms and share identified good practices to inform the further development of cyber norms.

Call for agreement on the applicability of international law in cyberspace

While (with few exceptions such as the Budapest Convention on Cybercrime) international law today does not have specific rules for regulating cyberspace, most states and international organisations (for example the G20[1], the European Union[2], ASEAN[3], and the OAS[4]) have affirmed that existing international law, and especially the UN Charter in its entirety, applies to the use ICTs by states.

The question today remains not *if* international law applies in cyberspace, but *how*.

The private sector relies on a secure, stable and trustworthy policy and regulatory environment to foster opportunity, spur innovation, and create value for communities. A common interpretation of existing international law is necessary to ensure legal certainty and the predictability of state behaviour, that informs investment decisions by the private sector.

Therefore, we encourage all states to (continue to) provide their national views on international law and share information on their national practices.

1 See the G20 Leaders' Communiqué, Antalya Summit, 15-16 November 2015
2 See the statement delivered by the EU to the United Nations 1st Committee Thematic Discussion on Other Disarmament Measures and International Security, 2018
3 See the ASEAN-United States Leaders' Statement on Cybersecurity Cooperation, 2018
4 See the OAS report on International Law and State Cyber Operations

Despite this reinforced agreement of the 11 norms by consensus of all UN member-states more than six years ago, implementation of the norms has been very uneven, and with little disclosure by states of what they have implemented and how they observe them.

4 Available at: https://undocs.org/en/A/75/816.
5 Available at: https://www.un.org/disarmament/group-of-governmental-experts/

The accelerated implementation of agreed norms by all states is urgently needed, to effectively prevent bad actors—whether states, their proxies, or third parties—from continuing to operate from states where they retain the freedom to do so without negative consequences.

The most striking obstacles to a more rapid and effective implementation of norms are:

1. **a lack of capacity** in several dimensions, including legislative and financial, to implement norms as well as accountability measures associated with them, and
2. the lack of **political will** to prioritise addressing global cybersecurity threats through collective action leveraging the norms and their implementation. This could be further addressed through the:
    - **a.** development of a common implementation framework for the agreed norms and international law—such as the CDGs;
    - **b.** establishment of common workable cyber attribution standards;
    - **c.** establishment and publication of deterrence doctrines;
    - **d.** calling out violations of the international cybersecurity framework; and
    - **e.** creation of a standing forum for action.

At the end of 2021, a new OEWG with a five-year mandate has begun elaborating on these topics, building on the previous agreements reached.[6] While early in the process, we hope that states will strengthen existing agreements, support each other through capacity building, and elaborate new rules that would plug the existing gaps in the global cybersecurity framework. To address the above-mentioned obstacles, ICC recommends that the OEWG supports a multi-step process.

1. Firstly, the OEWG must prioritise conversation on a recognised minimum technical, legal and policy framework at the national level necessary to support the implementation of cyber norms globally.
2. After such a framework is agreed, more resource and support will be needed to assist states in reaching this minimum level. This implementation process should be supported by increased transparency by governmentsin their implementation progress, and meaningful consultations with non-governmental stakeholders on cyber norms and policy by the OWEG and any other multi-national initiatives. A mapping of existing initiatives and organisations that help build state capacity (at local, regional and global scale) would be a helpful tool to lend support, inspire action and help avoid duplication.
3. Following implementation of such norms, an accountability regime sould be devised.

Implementation: an urgent need and a major challenge

At the present time there is no agreement on what technical, legal and policy frameworks each country should have as prerequisites to be able to implement the norms agreed at the regional or international level. For example, recent data suggests that only 118 of 192 UN member-states have a Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT).[7] These are key organisations, at the front line of seeing and responding to threats in real-time and bringing together public and private sector stakeholders to cooperate to detect and respond to cybersecurity incidents and identify the perpetrators so they can be addressed through judicial cooperation frameworks. CERTs/CSIRTs are also the drivers of international cooperation and trust building on cybersecurity matters, routinely working with their counterparts in other countries and regions to find the source of an incident and address it effectively.

Given the OEWG's mandate to facilitate the implementation of the existing cybersecurity framework, it is the primary forum for the development of **a common implementation framework for the agreed norms and**

6 https://meetings.unoda.org/meeting/oewg-ict-2021/

7 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

international law. On the model of the Sustainable Development Goals, these could be thought of as the "Cyber Development Goals" (CDGs) that would define the necessary technical, legal and policy framework and capacities needed for implementation and inspire collective action. Framing this implementation framework as the CDGs would help rally the international community behind shared objectives, set measurable indicators to track progress and inspire multistakeholder collaboration from the grassroots to the international level. International cooperation, enabled by such a minimum framework, would also considerably enhance online trust, including the trust of individuals, businesses and governments.

Voluntary, non-binding norms of responsible behaviour of states aimed at promoting an open, secure, stable, accessible and peaceful ICT environment[1]

States should

- cooperate to increase stability and security in the use of ICTs and to prevent harmful practices;
- consider all relevant information in case of ICT incidents;
- exchange information to assist each other, and to prosecute terrorist and criminal use of ICTs;
- respect human rights on the internet and the right to privacy in the digital age;
- take appropriate measures to protect their critical infrastructure;
- respond to appropriate requests for assistance by other states whose critical infrastructure is subject to malicious ICT acts;
- ensure the integrity of the supply chain and prevent the proliferation of malicious ICT and the use of harmful hidden functions;
- encourage responsible reporting of ICT vulnerabilities and should share remedies to these.

States should not

- knowingly allow their territory to be used for internationally wrongful acts using ICTs;
- conduct or knowingly support ICT activity that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;
- conduct or knowingly support activity to harm the information systems of another state's emergency response teams (CERT/CSIRTS) and should not use their own teams for malicious international activity.

1 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015)

There is also a lack of clarity of the extent to which existing norms have been implemented. This is why ICC welcomed the efforts by Canada, Mexico, Australia and others to propose a national survey of implementation of United Nations General Assembly Resolution 70/237.[8] Systematic responses to such a survey would enable all stakeholders to have a clear view of what remains to be done to implement the norms in all states, which would in turn allow the development of targeted capacity building programs to address any challenges to implementation or gaps in capacity.

Furthermore, the survey could also serve as a vehicle to collect information on existing capacity building initiatives and organisations. We strongly encourage all states to support and make use of this proposed survey mechanism as part

8 https://www.internationalcybertech.gov.au/sites/default/files/2020-12/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf

of their response to the General Assembly's invitation to member states to continue to inform the UN Secretary-General of their national views and assessments on the implementation of norms and international law.

Finally, more resources are needed—and needed urgently—to address the deep shortages in capacity. We welcome the establishment of the Cybersecurity Multi-Donor Trust Fund at the World Bank, and we encourage states to pool resources in initiatives like the Global Forum for Cyber Expertise alongside industry.

Cyberspace is an intrinsic part of the development of every country, creating enormous opportunities and enabling everything from distance learning to innovation and economic efficiencies. Because it is genuinely globally interconnected, everyone is only as secure as the weakest link. It is in the interests of all states to increase the cybersecurity preparedness of all relevant stakeholders. When it comes to improving global cybersecurity, we are all in it together.

We need not just implementation, but adherence and accountability

Beyond the implementation of agreed cyber norms, in order for the international cybersecurity framework to be effective, there should also be accountability for actors that do not adhere to them. That is essential to deter bad actors of all kinds. To enable this, we urge states to:

- **Establish common workable cyber attribution standards**. There needs to be a common understanding of the technical and legal standards for attributing internationally wrongful cyber acts to states[9]. We encourage states to invest in capacity building in this space, to support multistakeholder collaboration for agreement in common definitions, and to publish what standards they use so all states can compare and contrast different approaches as they evolve their own. While we recognise all states may not accept one common definition, increased transparency on what each state's policies are will benefit all stakeholders and allow like-minded states to work together in greater numbers over time. This would also create greater legal certainty for states and the private sector alike, and would likely decrease the risk-reward trade-off, and allow for further, and broader ranging collaboration. Further work is needed to agree an attribution framework that is widely acceptable to both state and non-governmental stakeholders. ICC stands ready to be a part of such a multistakeholder initiative.
- **Establish—and make publicly available—deterrence doctrines.** Clear doctrines of measured consequences for cyberattacks in violation of international agreements will help deter further belligerence, as well as provide necessary clarity about what responses can be expected, which should decrease the likelihood of tensions escalating as a result.
- **Call out violations of the international cybersecurity framework**. The attribution of a cyberattack to a state that is in violation of international norms or law could include an explicit and direct articulation of which norm/law was transgressed and how. Where reasonable, greater transparency in the underlying information used to draw conclusions will lend greater credibility to any attribution and will further strengthen the recognition of norms while impact the reputation of states through an establishment of an impartial and fact-based country index published annually.

Furthermore, we encourage states to continue discussions and collaboration on possible future norms to address gaps as they emerge with the rapid development of the cybersecurity landscapes, for example to address the issue of cyber mercenaries, or supply chain attacks, among others.

A standing forum for action is required

While progress has been made by states at the international level, it has to be acknowledged that cyberspace is growing increasingly insecure (for further information on this, please refer to the first ICC Cybersecurity Issue

9 See also topical analysis available here : https://digital-commons.usnwc.edu/ils/vol97/iss1/43/

Brief[10]). More needs to be done both on implementation and on accountability. To date, the response of the UN has been to convene working groups with a set mandate and a specific timeline to deliver work, with that work adopted by the General Assembly—but without a process for monitoring implementation.

Industry believes that the time has come to create a standing process that can deliver results in an ongoing basis, founded in a political commitment by states at a high level, with a programme of work that can evolve to address new issues as required and which can better monitor implementation of what has been agreed. The Cyber Programme of Action (PoA) proposed by more than 50 states in 2020[11] has real promise to deliver such a process. ICC stands ready to work with interested states to develop the concept and supports its establishment in the near future.

Ensuring all stakeholders can meaningfully participate in cyber policy development

ICC has previously recognised that, because the private sector has a significant role in the development and maintenance of technology, states have a responsibility and an obligation to ensure stakeholders are integrally part of all discussions of norms and their implementation, as states alone cannot effectively implement them without the rest of society. While making the ultimate decisions is the prerogative of member states, businesses and all other non-governmental stakeholders must be a meaningful part of formal and informal processes and negotiations at the OEWG and all other UN-convened processes on the topic.

Towards establishing Cyber Development Goals

To facilitate the implementation of the existing cybersecurity acquis (agreed norms and international law), a common implementation framework is needed. On the model of the Sustainable Development Goals, these could be thought of as the "Cyber Development Goals" (CDGs) that would define the necessary technical, legal and policy framework and capacities needed for implementation and inspire collective action. CDGs could include goals such as, but not limited to:

1. Develop and keep up to date national cyber security strategies[1]
2. Establish a Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT).[2] These would also facilitate cooperation mechanisms between public and private sector stakeholders to detect and respond to cybersecurity incidents, incident reporting and responsible and coordinated vulnerability management, as well as international cooperation and trust building on cybersecurity matters
3. Foster enabling environments to combat cybercrime and for cyber capacity building[3]
4. Put in place appropriate legal frameworks to support institutional capacities to combat cybercrime.
5. Raise awareness and build capacity of end-users[4]
6. Establish and publish cyber attribution standards
7. Develop—and make publicly available—cyber deterrence doctrines

CDGs would primarily be a common capacity building instrument at the nation state level and would depend on states' commitment to systematically track and report the implementation of United Nations General Assembly Resolution 70/237. This would bring clarity to what remains to be done to implement the norms in all states and allow the development of targeted capacity building programs to address any challenges to implementation or gaps in capacity.

1 See for example the ITU guide to develop national cyber security strategies
2 See for example the FIRST CSIRT Services Framework or the Carnegie Mellon University CERT Division
3 See for example the World Bank toolkit for Combatting Cybercrime and the Oxford Global Cyber Security Capacity Centre
4 See for example the US Cybersecurity and Infrastructure Security Agency's Cybersecurity Awareness Programme

10 ICC Cybersecurity Issue Brief #1: Call for Government Action on Cybersecurity
11 https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf

Part 2
Further development of cybercrime rules and increased international cooperation

Global business is, and has consistently been, a strong supporter of more effective measures to combat cybercrime. Given the rapidly increasing growth of transnational online crime, we welcome the increasing efforts of the international community to address this.

Currently, the two most significant instruments to facilitate collaboration on cybercrime and electronic evidence are mutual legal assistance treaties (MLATs) and the Council of Europe Convention on Cybercrime (Budapest Convention) and its additional protocols.

- MLATs[12] are an essential piece of national legal infrastructure, providing the legal basis that allows countries to cooperate on transboundary legal issues so that criminal acts can be stopped and those responsible brought to justice. However, far too few MLATs are up-to-date and as many are bilateral, there are many gaps in global coverage. Additionally, in order for MLATs to be effective, there must be harmonisation of the relevant criminal offenses in both jurisdictions to allow for any extradition provisions.
- The Budapest Convention, a criminal justice treaty developed by the Council of Europe and opened for signatures in 2001 is, to date, the most relevant international agreement on cybercrime and electronic evidence. It aims to provide states with (i) the criminalisation of a list of attacks against and by means of computers; (ii) procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards; and (iii) international police and judicial cooperation on cybercrime and e-evidence. It is complemented by two additional protocols, one concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems that entered into force in 2006 and one on enhanced co-operation and disclosure of electronic evidence, developed with the support of business and expected to be opened for signatures in May 2022.

Against this backdrop, UN member states are preparing to negotiate a draft of a new international convention on cybercrime, based on UNGA Resolution 75/282 that established an Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC)[13], with the aim of presenting a draft convention to the UNGA at its 78th session, which will begin in September 2023.

Principles for international provisions on cybercrime

While it is very early in the process, we believe the following principles should underpin the work of the AHC to ensure the outcome has the most practical benefit:

1. The Budapest Convention, and its additional Protocols, should be the starting place for the negotiations to **ensure compatibility with existing international obligations and to avoid unintentional negative consequences from overlapping or conflicting provisions**. This would also allow negotiators to leverage the state of the art in international legal provisions, and the experience and expertise of the negotiators who concluded their work so recently.

12 The International Chamber of Commerce has highlighted the importance of MLATs for some time; our recommendations on the subject may be found in our Policy Statement, available here: https://cms.iccwbo.org/content/uploads/sites/3/2016/10/ICC-policy-statement-on-Using-Mutual-Legal-Assistance-Treaties-MLATs-To-Improve-Cross-Border-Lawful-Intercept-Procedures.pdf

13 Ad Hoc Committee - Home (unodc.org)

2. **The scope of the agreement's measures should focus on widely-understood criminal acts which have common, clear and compatible, definitions in many different legal jurisdictions**. This is fundamental as many elements of cross-border crime cooperation are greatly limited or rendered ineffective if the acts aren't similarly understood in all concerned jurisdictions. A convention on cybercrime should not include offences like terrorism, corruption, or trafficking simply because the incident leverages technology; these are dealt with by other international instruments.
3. Careful attention must be paid to the **definition of cybercrime.**

   A traditional crime should not be treated as cybercrime, merely owing to the fact that a computer or other digital tools were involved in its planning or execution. These types of crimes can generally be covered by other statutes and should only be included where the scale, scope, or speed of the offense is significantly increased by the use of the Internet, and where the definitions are commonly understood, for example as it relates to child sexual exploitation.

   The definition of cybercrime **should not include content-related crimes, especially where there is dispute around the protection of human rights and fundamental freedoms**. ICC urges that any new definition of cybercrime shall not allow for misinterpretation that might lead to content control or infringement upon fundamental rights such as freedom of speech.

   Novel cyber technologies and criminal activities, such as intentionally developing, spreading and using malicious codes as cyber offensive tools or weapons to attack government systems, critical infrastructures or ICT supply chains are important to consider. ICC encourages the AHC to investigate how to reduce the proliferation of offensive cyber capabilities and tools, like the evolving criminal Access-as-a-Service (AaaS) ecosystem, and the broader marketplace that provides various tools and methods to ultimately enable cyber-attacks for profit, without unintended negative consequences such as criminalising the activities of "white hats" who develop such tools in order to help others defend against attacks that use them.
4. **Sanctions must be accompanied with robust safeguards** including independent judicial review, sanctions imposed independently of investigatory processes, and fully supportive of the international acquis of human rights law and norms. This is essential to reduce the potential for unintended negative consequences when measures are transposed into national law.
5. **The negotiations should ensure that the capacity building and technical assistance necessary for all states to effectively implement the provisions will be available**. Many developing countries will require considerable assistance to implement the legal and practical frameworks integral to successful implementation of the agreement on cybercrime. The negotiations should ensure that this dimension is an integral part of the negotiations and the outcome.

Procedural considerations

As the AHC negotiates a new convention on cybercrime, we offer the following procedural recommendations for consideration:

1. **The process must integrate non-state actors throughout all aspects of the negotiations.** The very nature of the objective requires non-governmental voices at the table—from criminal law and human rights experts to civil society advocates to the private sector and academia. All aspects of the negotiations should facilitate their involvement from access to meetings to access to documents, both formal and informal. All relevant stakeholders should be empowered to provide written proposals to the consultation, in a systematic manner.
2. The AHC is working to a very ambitious timeline given the complexity of the issues it seeks to address. While the issues are urgent, we urge member-states **not to let an arbitrary timeline dictate a result that is less effective in practical implementation than it could be.**

3. While the process allows for voting, wherever possible **consensus should be the first choice for decision-making.** This will help ensure a result with the broadest potential buy-in and facilitate adoption.
4. **The instrument should have a high standard for ratifications** for the convention's entry into force. This will ensure that any new instrument does not unintentionally fragment the digital environment further.

About the International Chamber of Commerce

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 170 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

www.iccwbo.org Follow us on Twitter: @iccwbo