The UN norms of responsible state behaviour in cyberspace

Guidance on implementation for Member States of ASEAN

March 2022

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

In partnership with

UK Government
Australian Government
CYBER & CRITICAL TECH COOPERATION PROGRAM

Author
Bart Hogeveen - Head of Cyber Capacity Building

Acknowledgements
The author would like to acknowledge contributions by officials and participants working with the governments of Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, the Philippines, Singapore, Thailand and Vietnam.

Our particular appreciation goes to:

- the Department of Foreign Affairs, Department of ICT, Office of the President and the National Security Council, the Philippines
- the Ministry of Foreign Affairs and Badan Siber dan Sandi Negara, Indonesia
- the Ministry of Information and Communications, Ministry of Foreign Affairs, and the Diplomatic Academy Vietnam, Vietnam
- the National Cybersecurity Agency, Ministry of Foreign Affairs, and CyberSecurity Malaysia, Malaysia

In addition, the author is indebted to contributions from Dr Fitriani, Ms Farlina Said, Dr Moonyati Yetid, Mr Eugene Tan, Mr Ben Ang and the Global Forum on Cyber Expertise and support from the UK Foreign, Commonwealth and Development Office and the Australian Department of Foreign Affairs and Trade and their embassies and high commissions in Southeast Asia.

This publication is the output of a project funded by the UK Government and the Australian Government (Cyber and Critical Technology Cooperation Program). More information can be found at https://www.aspi.org.au/cybernorms. The views expressed in this work are not necessarily those of the UK or Australian governments or of the participating governments. The author is responsible for its content, any views expressed or mistakes.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI International Cyber Policy Centre

ASPI's International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber, emerging and critical technologies and issues related to information and foreign interference and focuses on the impacts those issues have on broader strategic policy. The centre has a growing mixture of expertise and skills and teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building, satellite analysis, surveillance and China-related issues. The ICPC informs public debate in the Indo-Pacific region and supports public policy development by producing original, empirical, data-driven research. The ICPC enriches regional debates by collaborating with research institutes from around the world and by bringing leading global experts to Australia, including through fellowships. To develop capability in Australia and across the Indo-Pacific region, the ICPC has a capacity-building team that conducts workshops, training programs and large-scale exercises for the public and private sectors.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional.

ASPI

Tel +61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC

First published March 2022.
ISSN 2209-9689 (online).
ISSN 2209-9670 (print).

Funding support for this publication was provided by the UK and Australian governments.

Report design and layout by Pixelwise Creative Media

Foreword

Global digital growth is continuing to fundamentally transform the lives of people, businesses and institutions, bringing people out of poverty, increasing wider prosperity, welfare and enabling new ways for governments and citizens to engage with each other. It is also creating a more connected world and supporting globalisation with greater access to free markets, democratic systems, prosperity and innovation.

But as we become more reliant on cyberspace, malicious cyber activity has grown in intensity, complexity and severity over recent years, with rising incidents of cybercrime and hostile states targeting critical national infrastructure, democratic institutions, business and media. There is too much at risk to allow cyberspace to become a lawless world and we need to continue to work together to identify the rules of the road in how international law applies to state behaviour in cyberspace just as it does to activities in other domains.

The 11 norms, as part of the UN framework of responsible state behaviour in cyberspace, is a way to help develop those rules of the road and the UK, as part of our outreach, is committed to supporting partners across all continents be better able to both implement the norms but also be better empowered to join in the international debate in the UN.

This ASPI programme has provided an insight into meaningful measures being put in place across ASEAN to deliver the norms, showcasing the region as trailblazing good practice and policies. Sharing and communicating these is in itself a confidence building measure and the examples shared in this report will have an impact across the global debate.

The UK, as a responsible democratic cyber power is proud to have supported this report and we look forward to future activity in the ASEAN region and globally to help shape the future frontiers of an open and stable international order in cyberspace.

- Will Middleton, Foreign, Commonwealth and Development Office, UK

Advances in cyber and critical technology underpin our future prosperity but they also have the potential to harm national and economic security interests and undermine democratic values and principles. The countries that can harness the current wave of innovation while mitigating its risks will gain significant economic, political and security advantages and will be at the forefront of 21st century leadership.

As states increasingly exert power and influence in cyberspace, it is important that there are clear rules in place. In other words, cyberspace is not the Wild West, all countries have agreed that existing international law applies in cyberspace and all countries have endorsed UN norms of responsible state behaviour.

The Plan of Action to Implement the ASEAN Australia Strategic Partnership 2020–2024 details our joint commitment to an open, secure, stable, accessible and peaceful ICT environment. Australia will continue to work closely with our ASEAN partners to deepen understanding and implementation of longstanding agreements of international law and norms in cyberspace.

This report, produced by APSI in partnership with Australia's Cyber and Critical Technology Cooperation Program and the UK Foreign, Commonwealth and Development Office, is the result of a multi-year cyber-capacity building program focused on supporting the effective implementation of UN norms throughout ASEAN.

These 11 norms lay the groundwork for collective expectations for state behaviour in cyberspace. They are the bedrock on which regional and bilateral agreements around state behaviour in cyberspace are built and create a mutually reinforcing set of agreements and expectations.

Australia is grateful for ASPI's tireless work on this important cyber-capacity building project helping to kickstart the process of understand and actioning the norms and behaviours which are central to an open, free, safe and secure cyberspace.

- Dr Tobias Feakin, Ambassador for Cyber Affairs and Critical Technology, Australia

Contents

Introduction

This document is the result of a multi-year cyber capacity-building program by ASPI in partnership with the UK Foreign, Commonwealth and Development Office and the Australian Department of Foreign Affairs and Trade (Cyber and Critical Technology Cooperation Program). Through the project, the partners sought to support member states of the Association of Southeast Asian Nations (ASEAN) with the implementation of the United Nations (UN) norms of responsible state behaviour in cyberspace. The content of this publication is primarily based on experiences, inputs and outputs from activities run under this program.

What are norms?

Norms in international affairs are generally defined as 'a collective expectation for the proper behaviour of actors with a given identity'.

Norms are norms for the following reasons:

- They are widely shared and agreed among a large group of states; norms exist only because we all believe they exist and apply.
- They exert a moral attractiveness for states to conform to norms; states prefer to be seen to endorse, follow and promote norms, and to be responsible members of the international community.
- They assign specific duties and obligations, albeit non-legal, for specific actors; most norms in cyberspace are regulative in character at the national level, as they recommend that states prescribe, prohibit or permit certain activities.
- They are dynamic; they develop as expectations and opinions in society about what's responsible and acceptable change over time.
- People, organisations and states will—from time to time—contest or violate norms; this doesn't mean that a norm does not exist as long as the norm remains accepted by a large and influential enough community, and the violator is held to account.

Source: Based on Martha Finnemore, Cybersecurity and the concept of norms, Carnegie Endowment for International Peace, 30 November 2017, pp. 1–2.

The UN norms were first agreed by a UN group of governmental experts in 2015. The group's report was subsequently endorsed by consensus at the UN General Assembly in 2015 through resolution 70/237. It called on all member states 'to be guided in their use of ICTs' by the 2015 report. The focus on the operationalisation and implementation of the UN norms was also front and centre in the 2019–2021 round of UN First Committee negotiations. The report of the OEWG recommended that states 'further support the implementation and development of norms'. The 2021 UNGGE report offers an additional layer of understanding to help governments with their implementation.

In 2018, the ASEAN leaders expressed a commitment to operationalise the UN norms as a core element in ASEAN's approach to promoting regional stability in cyberspace. That same year, the ASEAN ministers responsible for cybersecurity subscribed in principle to the norms. At the 2019 ASEAN Ministerial Conference on Cybersecurity, they agreed to establish a working committee to develop a framework for implementation.

> Participants reaffirmed the importance of a rules-based cyberspace as an enabler of economic progress and betterment of living standards,and agreed in-principle that international law, voluntary and non-binding norms of State behaviour, and practical confidence building measures are essential for stability and predictability in cyberspace.
>
> - Chairman's statement of the third ASEAN Ministerial Conference on Cybersecurity, 2018.

In compiling this document, ASPI intends to contribute to the ongoing UN and ASEAN working groups, and offer participants region-specific perspectives based on real and observed examples of good practice. The information was gathered through various regional workshops and training activities that took place between 2019 and 2021, and supplemented with open-source research.

This document consists of two main parts:

a. An explanation of the norms implementation process.

b. Practical guidance on implementation with examples from the ASEAN region.

Each government is responsible for its own pathway to implementation and for informing other states of its efforts. Expectations of national and regional implementation will alter as states start to focus on local implementation and as understanding of the norms' meaning grows.

This document should help kickstart that process of understanding and actioning. It should be considered a living document that supports a gradually maturing regional approach.

This document will help policymakers and state officials answer questions such as:

- What examples can governments consider to demonstrate their efforts in implementing the UN norms?
- How can a state demonstrate that it is implementing and following the UN norms of responsible state behaviour in cyberspace?
- Where can a state find advice, assistance and support to advance further implementation efforts?

PART A

THE IMPLEMENTATION PROCESS EXPLAINED

Part A: the implementation process explained

In this first part of the document, the process for implementation of the UN cyber norms is explained. It starts with a clarification of the concept of international norms, how the cyber norms work and what practical steps make up an implementation effort. Examples of mechanisms and tools to demonstrate implementation efforts are also provided. At the end, we elaborate on the reasons why states would want to make an effort to implement the UN norms of responsible state behaviour in cyberspace.

United Nations

General Assembly

Full text of the UN cyber norms

a. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

b. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

c. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

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

e. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

f. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

g. States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

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

i. States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

j. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

k. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

What are the UN norms of responsible state behaviour in cyberspace?

The UN norms of responsible state behaviour in cyberspace (Figure 1) are 11 voluntary and non-binding rules that describe what states should and should not be doing in cyberspace.

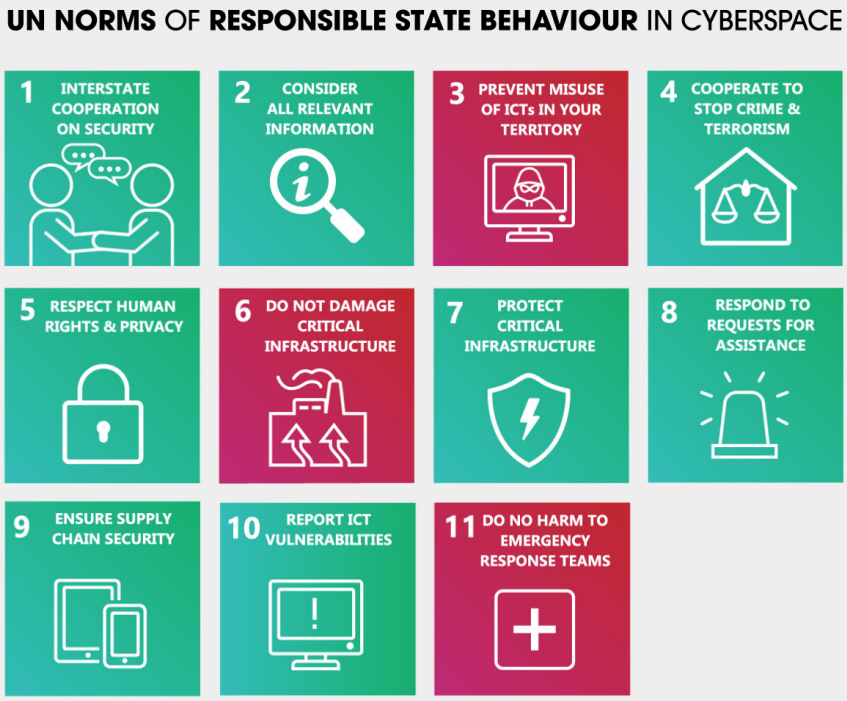


Figure 1: The UN norms of responsible state behaviour in cyberspace

The content of the 11 norms reflects the expectations that the broader international community has of each state and regional organisation.[1] They express a common opinion of what is considered to be responsible behaviour by states. Naturally, this collective opinion of what is responsible and what is irresponsible behaviour develops over time as understanding of cybersecurity deepens, incidents occur, and more governments contribute to the process.

The purposes of the norms as reflected in UNGA Resolution 70/237 are *to reduce risks to international peace and security, and to contribute to conflict prevention*.[2] They have been crafted to deal with state-to-state actions that could potentially carry the highest risks to international peace and security and the welfare of citizens.

Norms in *international affairs* are political agreements. They do not infringe on a state's sovereignty or impose legal obligations on states.[3] In fact, the norms provide a common basis for a state to design strategic direction, develop capabilities and execute actions in a responsible manner.

The UN norms process

International efforts to establish norms of responsible state behaviour in cyberspace concentrate around the work of two groups: the UNGGE and the OEWG.

The first UN group of governmental experts convened between 2004 and 2005, and a sixth round of negotiations concluded in 2021. Four rounds concluded with consensus reports, in 2010, 2013, 2015 and 2021. The OEWG was first established in 2019, and a second round has commenced in 2021 for a period of five years.

The UNGGE and OEWG are predominantly intergovernmental negotiation processes with—at times—opportunities for consultations with non-government organisations and civil society. Those consultations have, however, a non-official character.

The UN cyber groups

UN Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security

2004-05 2009-10 2012-2013 2014-2015 2016-17

UN Group of Governmental Experts (UNGGE) on Advancing responsible state behaviour in cyberspace in the context of international security

2019-21

UN Open-ended working group (UN OEWG) on developments in the field of information and telecommunications in the context of international security

2019-21 2021-25

Member states of ASEAN have been participating in all the meetings of the UNGGE and the OEWG that have convened since 2004. Figure 5 shows ASEAN member states' participation in the UNGGE and OEWG since 2004. Stars indicate a country's membership of the UNGGE, and its active participation in the OEWG as determined by written submissions or oral statements.

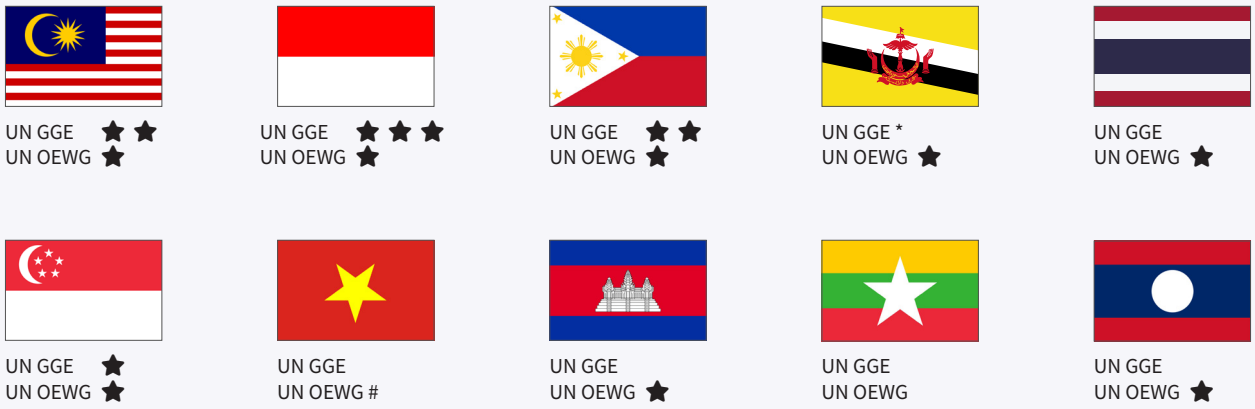


Figure 5: ASEAN member states' participation in UN norms processes 2004-2021.
Notes: * Although Brunei has not participated in the UNGGE or the OEWG, it did offer a national views document in 2017; it was the first ASEAN member state to do so. # Although Vietnam did not offer written submissions or made any statements, representatives formally attended OEWG meetings in New York.

In parallel to the UN-facilitated intergovernmental negotiation processes, various multistakeholder and other government-led initiatives have formed too. Examples include:

- Cyber Tech Accord: a commitment of 150+ companies to work together and follow a set of principles that seeks to protect and empower users and customers
- Paris Call for Trust and Security in Cyberspace: a multistakeholder commitment to work together to reduce risks to the stability of cyberspace and to build up confidence, capacity and trust
- Agreement on Cooperation in the Field of ICTs: a proposal by the Shanghai Cooperation Organisation's six member countries for an international code of conduct
- World Wide Web Foundation Contract for the Web: an internet community-led initiative to advance principles of accessibility, affordability, availability and rights-based principles of respect for human rights and privacy for all in the operations of the internet.

What do norms do?

Norms typically codify existing state practice. The UN norms, as introduced in UNGA Resolution 70/237, set the standards of what the international community considers responsible on the basis of observed behaviour by state actors in the past and currently. With these agreed norms, activities and intentions of states can be subjected to assessments. States can be complimented on their response to an incident, or national practices can be heralded as global good practice. Also, states can be reprimanded if they haven't done enough to prevent an incident, or if they have used cyber capabilities in an irresponsible manner.

In practice, governments will use international norms, such the UN norms of responsible state behaviour in cyberspace, in three ways:

1. To serve as a point of reference to reassure other states of their good intentions and to demonstrate that they are constructive members of the international community.
2. To serve as a point of reference to guide national cybersecurity policy and national cybersecurity investments.
3. To serve as a point of reference to hold other actors responsible for behaviour that is not in line with the UN norms for responsible state behaviour.

> ***'States should avoid and refrain from the use of ICTs not in line with the norms'***
>
> — Report of the OEWG, paragraph 24

Governments that embrace the UN norms and can report on their efforts contribute to predictability, trust and confidence in cyberspace.

How do norms work?

The implementation of internationally agreed political agreements is always challenging. As they have been crafted through an intergovernmental negotiation process, their language and terminology can be ambiguous. For that reason and in the absence of an overall blueprint, it is important that states find their own way and form their own view and approach to embracing the UN's normative framework.

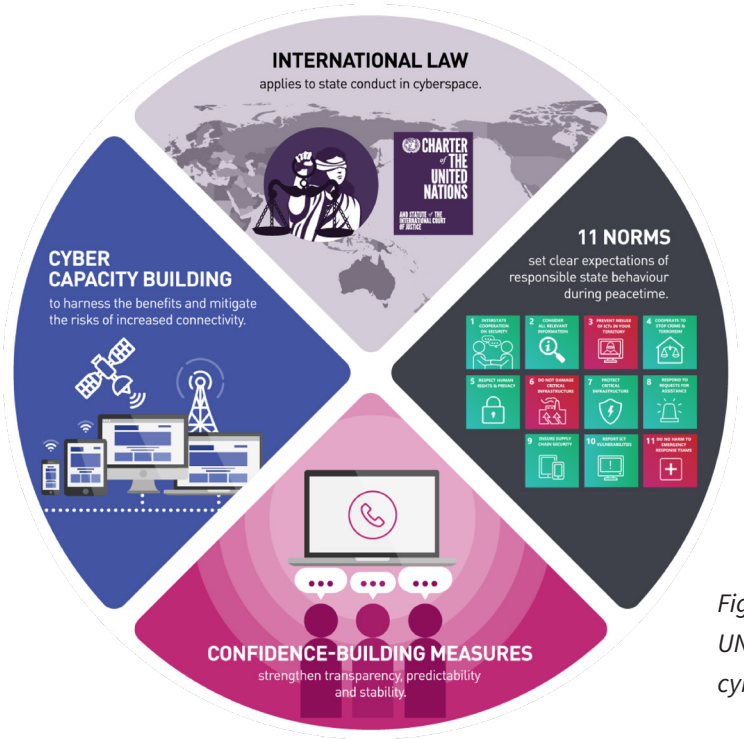


Figure 2: The four components that make up the UN framework of responsible state behaviour in cyberspace.

The 11 norms should be seen in their entirety and not as a 'pick-and-choose' menu. It is important that governments review their efforts in a comprehensive manner covering aspects that touch on issues of national (cyber)security, security of ICTs as well as on constructive inter-state relations.

Furthermore, governments need to keep in mind that the 11 norms are part of a broader framework that also includes the recognition that international law applies to state conduct in cyberspace, a set of confidence-building measures and a commitment to coordinated capacity building.[4] Together, those four components make up the UN framework of responsible state behaviour in cyberspace (Figure 2).

In general, the more states show commitment to the norms and actively engage in their implementation, the more robust the norms become and the more compelling the call for compliance becomes.

What does the implementation of international norms involve?

States can demonstrate their implementation of international norms of behaviour in various ways (see figure 3). Typically, implementation occurs at three different levels: at the level of political endorsement, national laws and policies, and actions on the ground (Figure 3).

1. First, political endorsement can be demonstrated, for example, through voting in favour of relevant resolutions at the UN General Assembly, by subscribing to ASEAN leaders' statements and by (prime) ministerial statements.
2. Second, states can integrate or internalise norms (explicitly or implicitly) in national legal frameworks, strategies and national policies.
3. Third, a state can demonstrate implementation by referring to its government practices in the form of its institutional capabilities, doctrine and procedures, and actions. Those practices can offer de facto evidence of a state's effort to follow norms of responsible behaviour, as they demonstrate an ability and willingness to act.

Implementation of international norms of responsible state behaviour

Endorsement		
Voting in UN forums, such as General Assembly	ASEAN statements	Ministerial statements
↓		↑
Integration and internalisation		
Legal framework	Strategy documents	National policies
↓		↑
Practice		
Capabilities	Doctrine and procedures	Actions

Figure 3: A framework for the implementation of norms.
Source: The author.

Responsibility for the implementation of the UN norms rests with governments. In practice, however, meaningful implementation will rely on individual governments' ability and willingness to consult and collaborate with industry, civil society organisations, the internet technical community and academia, and on governments' ability to ensure a whole-of-government approach.

> Meaningful implementation requires the involvement of multiple stakeholders and a whole-of-government approach.

For the purpose of including views, expertise and capabilities of non-government stakeholders, mechanisms such as a national action plan or a national road map are proven methods that help build a national or whole-of-economy approach to cybersecurity.

> A National Action Plan is an effective method to form an integrated approach to implementation.

What's a trajectory for the implementation of norms?

Building a national approach to cybersecurity let alone the implementation of the UN norms is neither straightforward nor instant. Typically, stakeholders go through a step-by-step process of gradually increasing their understanding, maturity and comfort with the topic (see figure 4).

1. A first step is to build awareness across the government of its international responsibilities. This could be achieved through a dedicated training program or awareness campaign on the UN norms.
2. This should lay the foundation for a cross-governmental recognition that the government is committed to the UN's normative approach and is willing to be guided by it in its national and international cybersecurity activities.
3. What follows could be an assessment of where the country stands in its implementation efforts. Such a baseline assessment could be done by a third party or through a whole-of-government mapping process.

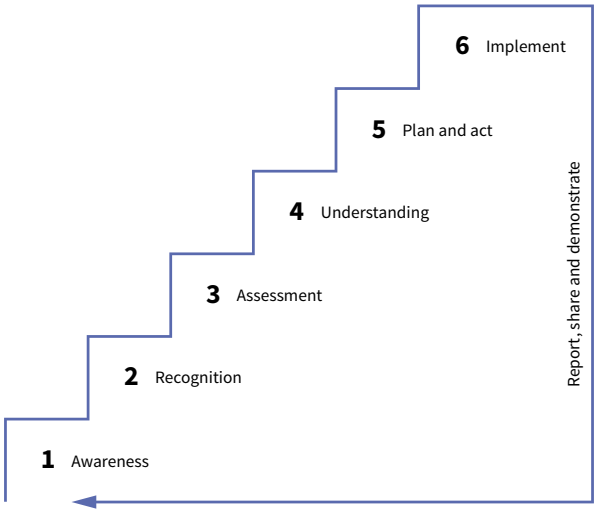


Figure 4: A step-by-step process towards implementation.

4. The outcome of the baseline assessment will inform the government of its strengths and areas for improvement.
5. This could then lead to domestic investments in particular areas of cybersecurity, to requesting assistance from the global cyber capacity-building community, or to offers of expertise to others.
6. At the end of these steps, one can presume a state to be implementing the UN norms commensurate with its own means and capabilities.

The implementation of norms is a dynamic process that evolves as a country's maturity in cybersecurity grows over time. At the same time, it's unlikely that any state will ever reach a state of 'full implementation', just as no state will ever be 100% cybersecure.

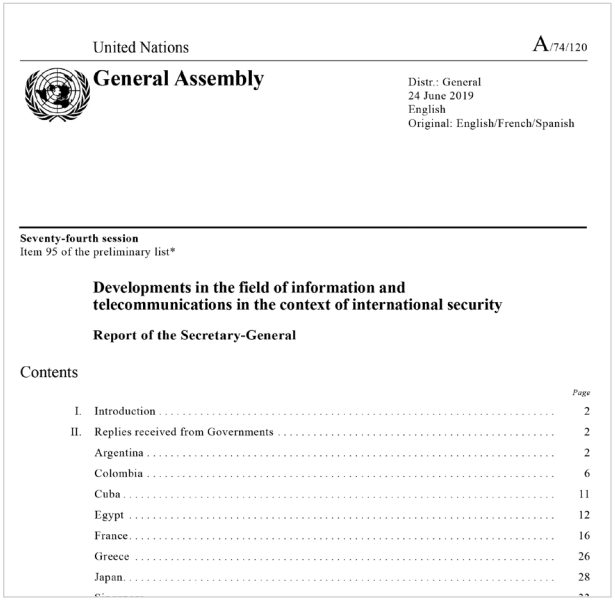
How can governments demonstrate implementation?

For the purpose of the UN norms (to reduce risks to international peace and security, and to contribute to conflict prevention), it is critical that states demonstrate what they're doing and what they intend to do. Therefore, documenting and reporting are critical in implementation.

There are several ways for states to make their views, achievements and known capacity shortfalls known.

❶ Reporting through the UN Secretary-General

On regular occasions, the UN Secretary-General invites member states to share their views and assessments (see figure 6). Governments can share their 'general appreciation of the issues of information security; efforts taken at the national level to strengthen information security and promote international cooperation in this field; the content of concepts such as the application of international law; and possible measures that could be taken by the international community to strengthen information security at the global level'.



United Nations A/74/120

General Assembly

Distr.: General
24 June 2019
English
Original: English/French/Spanish

Seventy-fourth session
Item 95 of the preliminary list*

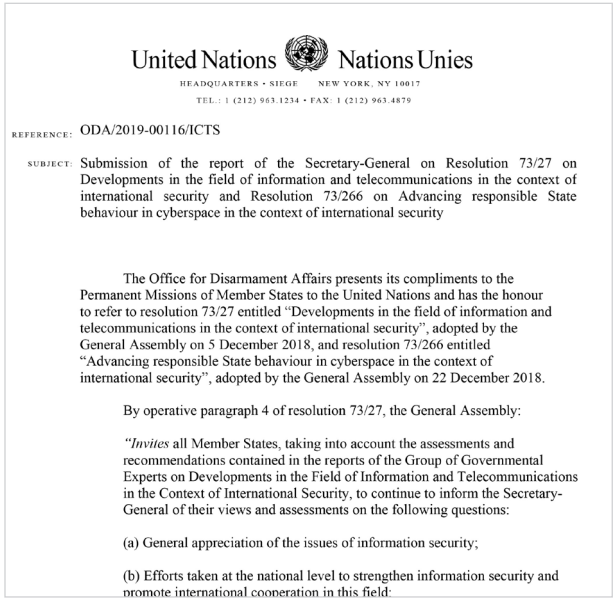
Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General

Contents

		Page
I.	Introduction	2
II.	Replies received from Governments	2
	Argentina	2
	Colombia	6
	Cuba	11
	Egypt	12
	France	16
	Greece	26
	Japan	28

National views submitted in 2019



United Nations Nations Unies

HEADQUARTERS • SIEGE NEW YORK, NY 10017
TEL.: 1 (212) 963.1234 • FAX: 1 (212) 963.4879

REFERENCE: ODA/2019-00116/ICTS

SUBJECT: Submission of the report of the Secretary-General on Resolution 73/27 on Developments in the field of information and telecommunications in the context of international security and Resolution 73/266 on Advancing responsible State behaviour in cyberspace in the context of international security

The Office for Disarmament Affairs presents its compliments to the Permanent Missions of Member States to the United Nations and has the honour to refer to resolution 73/27 entitled "Developments in the field of information and telecommunications in the context of international security", adopted by the General Assembly on 5 December 2018, and resolution 73/266 entitled "Advancing responsible State behaviour in cyberspace in the context of international security", adopted by the General Assembly on 22 December 2018.

By operative paragraph 4 of resolution 73/27, the General Assembly:

"*Invites* all Member States, taking into account the assessments and recommendations contained in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) General appreciation of the issues of information security;

(b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

Invitation by the UN Secretary-General to states to share national views

Figure 6: UN member states' views and assessments

❷ Submissions through UN working groups

As part of the ongoing OEWG process, member states are encouraged to provide written submissions or statements to the working group. The statements are shared by the UN Secretariat to other member states, the chair(s) and non-government stakeholders. States are also encouraged to participate in a UN-facilitated survey of their national efforts and experiences.

❸ ASEAN Regional Forum

The ARF's semi-annual Inter-Sessional Meeting on ICT Security offers participants an opportunity to exchange their views on the regional and global ICT landscape and their efforts and initiatives. For the ARF's annual security outlook, member countries are asked to submit a contribution that includes a section for 'cyber/ICT security'.

❹ Recognition by third party/ies

A state can engage third-party organisations to perform an external assessment and prepare a report. This could be done through a capacity-building relationship, such as ASPI's national norms implementation reports (see figure 7). ASEAN member states can also make use of their academic and think-tank organisations such as those represented in ASEAN–ISIS and the Council for Security Cooperation in the Asia Pacific (CSCAP).

Figure 7: ASPI national norms implementation reports

Why would states make an effort to implement the UN cyber norms?

There are a few reasons why states would make the effort to implement international norms, such as the UN norms of responsible state behaviour in cyberspace.

1. **Cyber resilience**. By following the recommendations from the norms and through acts of implementation, States are effectively strengthening their national cybersecurity maturity. Therefore, implementation of the norms is directly contributing to a nation's ability to protect against malicious cyber activity, reduce exposure to risks and vulnerabilities in ICTs, and respond to malicious ICT activity.
2. **International credibility**. Most states want to be, and be seen as, responsible members of the international community. Showing demonstrable support for norms of responsible behaviour adds to a country's international and regional credibility. Domestically, the implementation of international norms helps governments provide direction to their national cybersecurity policy and developments.
3. **Contribute to norm-setting**. The effective demonstration of implementation allows states to shape the common opinion of what is and what is not considered responsible behaviour of states and ensure that international expectations align with the local and regional context.
4. **Reassurance, accountability and transparency**. In a situation in which a large enough group of states can show demonstrable implementation of the UN norms, each within its own means and capabilities and within its national and regional context, a global environment is created in which states can be reassured of each other's willingness and ability to prevent unnecessary tensions and unintended conflict. Altogether, this adds to the accountability and transparency of state activities in cyberspace.

PART B

PRACTICAL GUIDANCE ON IMPLEMENTATION, WITH EXAMPLES FROM THE ASEAN REGION

In this second part of the document, each of 11 UN norms is presented, clarified, and accompanied with instructions and examples.

For each of the 11 norms, the full and agreed text is presented. However, parts of the text are marked **bold** or underlined. These are the phrases and concepts from the original text that were further explored in the 2021 UNGGE report and are presented under 'additional guidance'. Text is taken in its entirety from the 2021 UNGGE report, but edited for readability.

As a next step, a set of 'questions to help your thinking' is presented. The questions should help policymakers and analysts form a view on what their government is already doing in terms of implementing the UN norms, and what types of examples they could include in their analysis or reporting.

Next is a table of examples of observed good practice from the ASEAN region. The examples serve as evidence of ASEAN states putting in place relevant laws, policies and institutional capabilities and performing relevant actions. Also, suggestions for further reading are presented.

Finally, the implementation of the particular norm is illustrated with a case study, diagram, explainer note or reference to existing ASEAN agreements.

United Nations

General Assembly

GUIDANCE FROM THE UN MEMBER STATES

Agreed text

Consistent with (1) **the purposes of the United Nations**, including to maintain international peace and security, States should cooperate in (2) **developing and applying measures to increase stability and security** in the use of ICTs and (3) **to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security**

Additional guidance

(1) The maintenance of international peace and security and international cooperation are among the founding purposes of the United Nations. It is the common aspiration and in the interest of all States to cooperate and work together to promote the use of ICTs for peaceful purposes and prevent conflict arising from their misuse.

(2) States are recommended to put in place or strengthen existing mechanisms, structures and procedures at the national level, such as:

- relevant policy, legislation and corresponding review processes
- mechanisms for crisis and incident management
- whole-of-government cooperative and partnership arrangements
- cooperative and dialogue arrangements with the private sector, academia, civil society and the technical community.

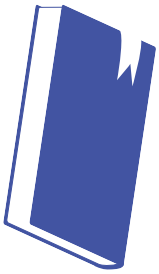
States are also encouraged to compile and streamline the information they present on the implementation of the norms, including by voluntarily surveying their national efforts and sharing their experiences.

(3) States are encouraged to refrain from using ICTs and ICT networks to carry out activities that can threaten the maintenance of international peace and security.

Questions to help your thinking

When you are considering implementation efforts to give effect to this norm, answers to the following questions can guide you:

- Is my country represented in relevant multilateral, multistakeholder, technical and regional forums that address cybersecurity and regional peace and security? If so, where and how?
- Does my government have the means and capabilities to engage in the international forums and bodies it considers important? If so, what are they?
- Has my government developed strategic direction in terms of principles and objectives for its international cybersecurity engagement? Does the government have a vision for the future of cyberspace? If so, what are those?



Further reading

- UN Office for Disarmament Affairs, **Cyberdiplomacy**, e-learning course, online.
- Joseph S Nye Jr, **The regime complex for managing global cyber activities**, Global Commission on Internet Governance, paper series no. 1, 2014, online.
- Department of Foreign Affairs and Trade, **International Cyber and Critical Technology International Engagement Strategy**, Australian Government, 2021, online.

Observed examples of regional good practice

This page lists examples of good practice that have been observed in the ASEAN region.
This list gives an idea of what concrete measures of implementation are and what states can demonstrate as their practices of implementation.

Actions

- Participate in cybersecurity forums as part of existing bilateral, multilateral or multistakeholder frameworks. Examples include:
  - political forums such as ASEAN, the ASEAN Regional Forum and the East Asia Summit
  - law enforcement forums such as Interpol and the UN Office on Drugs and Crime (UNODC)
  - technical standards forums such as Internet Engineering Taskforce (IETF), International Organisation for Standardisation (ISO), International Telecommunication Union (ITU) and incident response communities such as the Forum of Incident Response Security Teams (FIRST), Asia-Pacific CERT (APCERT) and Organisation of Islamic Cooperation (OIC) CERT.
- Participate in the OEWG and UNGGE and/or their informal and intersessional meetings.
- Conduct bilateral, trilateral, or multilateral cyber policy dialogues, such as the Australia–Indonesia dialogue or the Japan–ASEAN dialogue.
- Organise workshops, working groups and/or meetings aimed at training, awareness-raising or advancing a cyber policy issue.

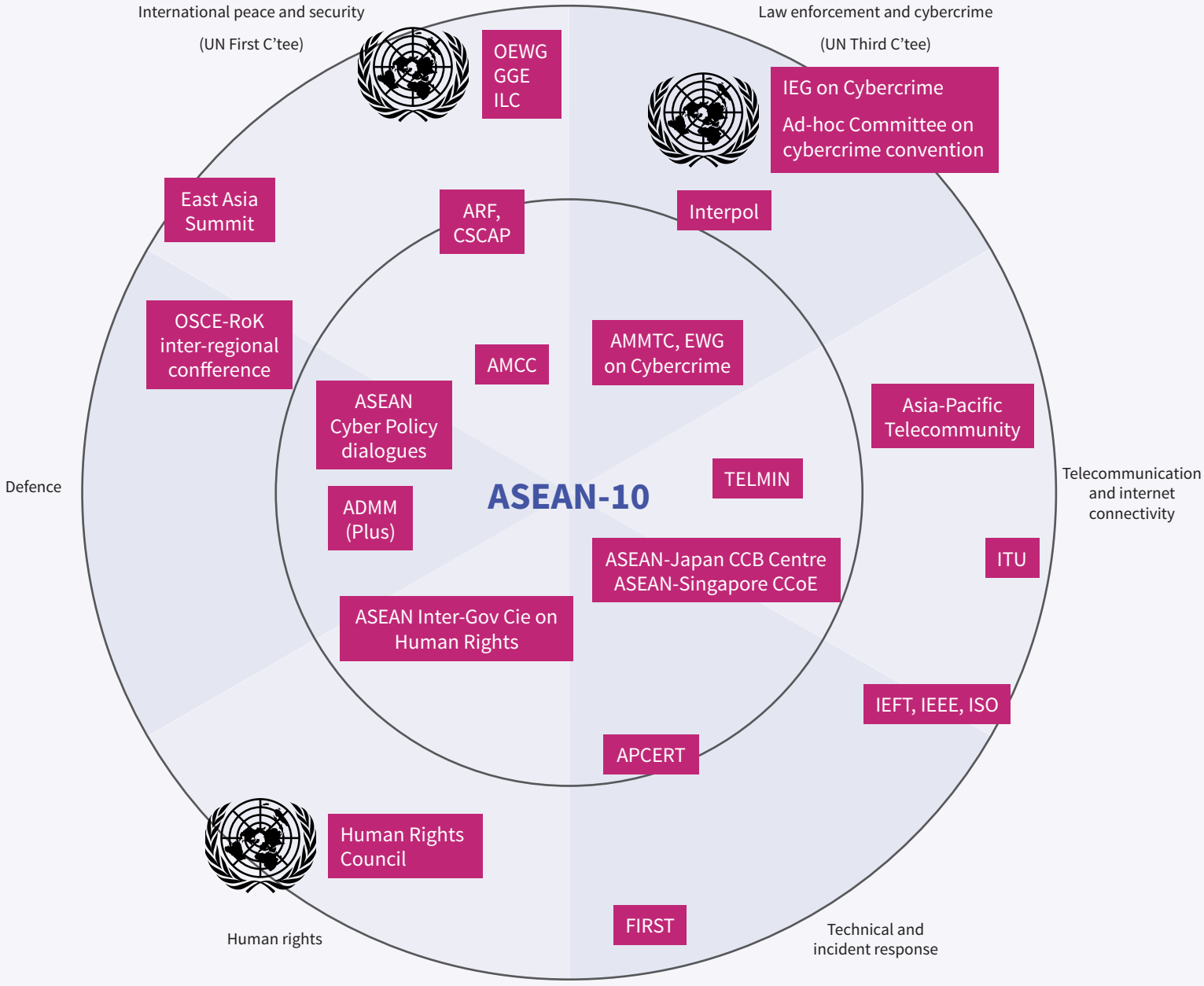
Institutional capabilities

- Operational staff such as individual experts or teams/units established within the Ministry of Foreign Affairs, at HQ or at diplomatic missions abroad, who can engage in international cooperation and be part of international dialogues.
- Operational staff such as individual experts or teams established within the national cybersecurity agency, the police, armed forces or authorised CERT who can engage in international cooperation and be part of international dialogues.
- Active participation of national technical experts in developing and setting international technical standards for ICT security and other technologies.
- Membership and participation in capacity-building initiatives such as opportunities provided through the ASEAN–Japan Cyber Capacity Building Centre, the ASEAN–Singapore Cybersecurity Centre of Excellence, the Cybersecurity Alliance for Mutual Progress and the Global Forum on Cyber Expertise (GFCE).

Laws and policy

- Endorsement of UN resolutions and ASEAN and ARF statements.
- Strategy documents that outline a state's interests and ambitions in international cooperation on ICT security, for instance by means of an international cybersecurity strategy or a national cybersecurity strategy with a designated chapter on international collaboration.
- Interventions in UN and ASEAN meetings, written submissions and statements by cabinet ministers about matters of international cybersecurity.
- Signing of memorandums of understanding with third countries or global industry partners.

EXPLAINED: ASEAN's cyberdiplomacy landscape



This diagram lists the various ASEAN platforms where states, executive agencies and technical bodies convene and discuss, action and evaluate norms of responsible behaviour in cyberspace. In the outer ring, corresponding UN / global platforms and forums are presented.

For the purpose of implementing norm #1 and to review their current cyberdiplomacy engagement, states could check which forums they're participating in, who their representatives are and what agenda they're pursuing.

United Nations

General Assembly

GUIDANCE FROM THE UN MEMBER STATES

Agreed text

In case of ICT incidents, States should (1) **consider all relevant information**, including the larger context of the event, (2) **the challenges of attribution** in the ICT environment and the nature and extent of the consequences.

Additional guidance

(1) A State that is victim of a malicious ICT incident should consider all aspects in its assessment of the incident. Such aspects, supported by substantiated facts, can include:

- the incident's technical attributes
- its scope, scale and impact
- the wider context, including the incident's bearing on international peace and security
- the results of consultations between the States concerned.

(2) Attribution is a complex undertaking, and a broad range of factors should be considered before establishing **the source of an ICT incident**.

States should **exert caution**. Accusations of organising and implementing wrongful acts brought against States should be substantiated. Invoking the responsibility of another State for an internationally wrongful act **involves complex technical, legal and political considerations.**

States that are subject to malicious ICT activity, and States from whose territory such malicious ICT activity is suspected to have originated, **are encouraged to consult** among relevant competent authorities.
In their response, States could avail of the full range of diplomatic, legal and other consultative options available to them, as well as voluntary and political commitments that allow for the settlement of disagreements and disputes through consultation and other peaceful means.

Observance of this norm implies that States establish or strengthen:

- relevant national structures
- ICT-related policies, processes and legislative frameworks
- coordination mechanisms, as well as partnerships and other forms of engagement with relevant stakeholders to assess the severity and replicability of an ICT incident.

Cooperation at the regional and international levels, including between national computer emergency response teams (CERTs) / computer security incident response teams (CSIRTs), the ICT authorities of States and the diplomatic community, can strengthen the ability of States to detect and investigate malicious ICT incidents and to substantiate their concerns and findings before reaching a conclusion on an incident.

Questions to help your thinking

When you are considering implementation efforts to give effect to this norm, answers to the following questions can guide you:

- Does the government have processes or frameworks in place that combine technical forensic data with policy assessments and broader political–economic considerations?
- Does the government possess skills, techniques and expertise, or access thereto, to form a whole-of-government opinion on the sources of a major ICT incident?
- Which government agencies are involved in an assessment and decision-making process following an ICT incident? Do they represent all relevant portfolios, such as defence, foreign affairs/diplomacy, law enforcement and economic/industry?
- Does the government have the means and capabilities to respond to a major ICT incident originating from abroad?
- Does the government have a stated approach to attributions, such as a policy on whether it would attribute ICT incidents to another state, and, if so, which options for such attribution would it consider?
- Is the national CERT well connected to other CERTs and can it leverage international partnerships for threat information exchange?

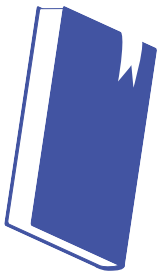
Attribution is the act of assigning responsibility for an act to someone. In this case, it's the process of reaching a political decision to hold another state or non-state actor publicly or privately responsible for a cyber incident.

Why these questions?

The essence of this norm is a call for states to exercise restraint when considering assigning responsibility for a cyber incident to another state. States should not jump to conclusions and before drawing policy conclusions should make a careful assessment of the situation.

This raises the capacity question of whether a victim country has the ability to make assessments of cyber incidents that are comprehensive, conclusive and beyond reasonable doubt.

Given the caution that tends to be exercised by attributing authorities, those addressed as well as other stakeholders in the international community should take attributions—public or private—very seriously.



Further reading

- Florian J Egloff, Max Smeets, '**Publicly attributing cyber attacks: a framework**', Journal of Strategic Studies, 2021, online.
- Cybersecurity and Infrastructure Security Agency, **National Cyber Incident Scoring System**, US Government, online.
- Ministry of Communications and Information, **Public report of the committee of inquiry into the cyber attack on Singapore Health Services**, Singapore Government, 2019, online.

Observed examples of regional good practice

This page lists examples of good practice that have been observed in the ASEAN region.
This list gives an idea of what concrete measures of implementation are and what states can demonstrate as their practices of implementation.

Actions

- The publication of regular national cyber threat reports, such as Singapore's Cyber Landscape and Indonesia's HoneyNet project.
- Singapore's establishment of a temporary commission of inquiry following the SingHealth data breach.
- Policy statements on the practice of doing—or not doing—public attributions.

Institutional capabilities

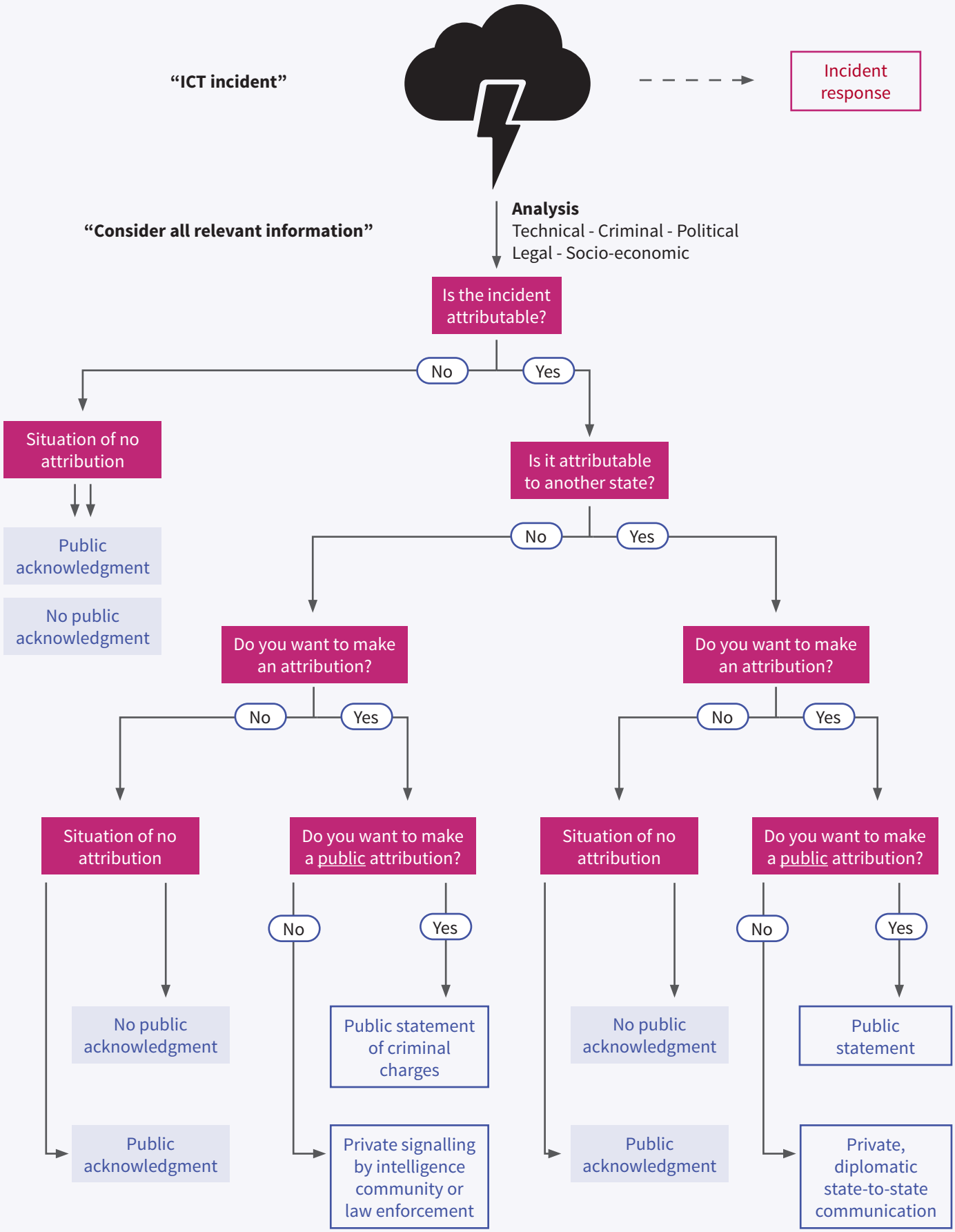
- An ability to coordinate a whole-of-government approach in reaching an informed position on an ICT incident. This means that the government has a process in place that links technical forensics with broader policy considerations, and that the government has identified which agencies need to be involved.
- An ability to mobilise and deploy a variety of sources of national power across the spectrum of crisis response (prevention, diplomacy, incident management, and recovery). Examples from the region include Malaysia's National Cyber Coordination and Command Centre or the Philippines' National Cybersecurity Inter-Agency Committee.
- An ability to engage in inter-CERT cooperation and initiate, facilitate or contribute to adequate information sharing.

Laws and policy

- Declared policies and positions on attribution, such as whether the state is prepared to do attributions and whether it will apply international law.
- Policies and procedures that describe how the state would respond to a cyber incident originating from the territory of another state.
- The state's view on the subject of how international law applies to the use of ICTs by states, including on the adoption of the responsibility of states for internationally wrongful acts. For instance:
    - Singapore submitted a national contribution as part of the 2021 UNGGE
    - Malaysia, in its 2020 national cybersecurity strategy, announced that it would formulate an opinion on the application of international law.

This flowchart describes generic steps in an attribution process. Answers (yes/no) to each of the steps involve the consideration of a complex array of issues. For the purpose of implementing norm #2, states could check whether they have processes, capabilities and skills in place to inform answers to these questions. States should also consider their generic policy for public and political attribution. Do they have an active political attribution policy? A restrained attribution policy? Or a policy of not doing public political attributions?

EXPLAINED: A step-by-step process for attribution



United Nations

General Assembly

GUIDANCE FROM THE UN MEMBER STATES

Agreed text

States should not (1) **knowingly** allow (2) **their territory to be used** for internationally wrongful acts using ICTs.

Additional guidance

(1) if a State is aware of or is **notified in good faith** that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory, **it will take all appropriate and reasonably available and feasible steps** to detect, investigate and address the situation.

(2) A State should not permit another State or non-State actor to use ICTs within its territory to commit internationally wrongful acts.

Observance of this norm implies the following:

(a) A State will take **reasonable steps within its capacity to end** the ongoing activity in its territory through means that are proportionate, appropriate and effective and in a manner consistent with international and domestic law.

(b) States are **not expected to monitor all ICT activities** within their territory.

(c) A State that is aware of but lacks the capacity to address internationally wrongful acts conducted using ICTs in its territory may **consider seeking assistance from other States or the private sector** in a manner consistent with international and domestic law.

(d) States could consider establishing **structures and mechanisms to formulate and respond to requests for assistance**.

(e) **An affected State notifies** the State from which the activity is emanating. The notified State should **acknowledge receipt of the notification** to facilitate cooperation and clarification and make every reasonable effort to assist in establishing whether an internationally wrongful act has been committed.

What is an internationally wrongful act?

An 'internationally wrongful act' is an act that constitutes a breach of a state's international obligation and is attributable to a particular state or states under international law.[5]

According to the letter of the International Law Commission's articles, internationally wrongful acts do not vary with the gravity of the breach. However, in practice, internationally wrongful acts will concern 'breaches' and typically 'serious breaches' of international obligations that inflict harm on other states and/or jeopardise regional or international peace and security.[6]

State responsibility for internationally wrongful acts applies equally during situations of peacetime (non-armed conflict) and armed conflict.

What can a state do to reassure other states that it is able and willing to prevent its territory from being used for internationally wrongful acts?

The implementation of this norm presumes that a state possesses adequate investigative and prosecutorial law enforcement capabilities, has an effective criminal code and can provide verifiable data of cybercrime prosecutions or other anti-crime measures. In practice, a state will be able to convincingly demonstrate a capacity to prevent the misuse of its territory for internationally wrongful acts (such as cyber incidents that affect another state gravely) only if it is able and willing to effectively combat domestic cybercrime and cybercrime at the lower end of sophistication.

What is cybercrime?

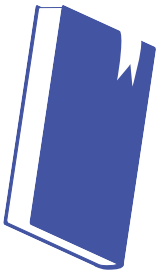
Cybercrime as such is not a defined legal term. Typically, a distinction is made between:

- a criminal act committed through the use of ICTs or the internet, in which the computer or network is the target of the offence (for example, deploying malicious software such as a virus)
- cyber-enabled crime, which is any criminal act that could be committed without technology or the internet, but is assisted, facilitated or escalated in scale by the use of technology (this includes a range of serious and organised crimes, such as cyber-enabled fraud or the distribution of child exploitation material, and terrorism).

Questions to help your thinking

When you are considering implementation efforts to give effect to this norm, answers to the following questions can guide you:

- Does the government have in place legislation that criminalises the misuse of ICTs?
- Does the government have the ability to take down criminal websites, servers and other infrastructure used for criminal purposes?
- Does the government have the ability to identify and assess potential wrongdoing in the national ICT domain?
- Does the government have policies that outline how it is governing the internet and domestic IT infrastructure?
- Do government agencies act against cybercrime, and does law enforcement prosecute the misuse of ICT in accordance with national legislation?



Further reading

- Interpol, **National Cybercrime Strategy Guidebook**, April 2021, online.
- Threat assessment reports, such as:
  - Interpol, **ASEAN cyberthreat assessment 2021**, online
  - BSSN and HoneyNet Indonesia, **Annual report 2020**, online.
- UN Office on Drugs and Crime, **Comprehensive study on cybercrime**, 2013, online.

Observed examples of regional good practice

This page lists examples of good practice that have been observed in the ASEAN region.

This list gives an idea of what concrete measures of implementation are and what states can demonstrate as their practices of implementation.

Actions

- Law enforcement actions in combating common forms of cybercrime, such as phishing, spoofing, DDoS attacks, and taking down botnets.
- Other examples include practices of rules-based filtering of the Domain Name System (for instance through arrangements with internet service providers) and clear licensing rules for network operations and domain registrars.
- Seeking community reports on cybercrime, such as Indonesia's patrolisiber.id.
- Effective cybercrime operations such as Interpol ASEAN desk's operations with various ASEAN member state police forces.

Institutional capabilities

- Operational and professional cyber units within police, law enforcement, judicial and counterintelligence services and in cybersecurity that can detect, investigate and prosecute.
- An ability to detect malicious ICT incidents in the state's territory, or access to an authorised third party that offers a detection capability.
- An ability to call in third-party assistance, for instance through reserve forces or pre-formed public–private partnerships with IT security companies.
- A point of contact to send and receive notifications in relation to serious cybercrime incidents.

Laws and policy

- Recognition of cybercrime as a national priority and subsequent action plans or road maps for countering serious cybercrime.
- A national cybercrime action plan or national cybersecurity strategy.
- Criminalisation of wrongful acts, including computer misuse, through specific cybercrime legislation, updated criminal codes, jurisprudence or police operational policies.
- Ratification of the Convention of Cybercrime (Council of Europe, 2004) or other international legal agreements that address cyber and ICT-related crimes.

CASE STUDY

HoneyNet—ASEAN

HoneyNet was established in 1999 as a volunteer initiative to fight malware and malicious hacking attacks. Its mission is 'to learn the tools, tactics and motives involved in computer and network attacks, and share the lessons learned'. HoneyNet is a US-based international non-profit research organisation with more than 30 local chapters across the world.

HoneyNet members and contributors run self-governed projects in the areas of conducting cybersecurity research, developing monitoring and prevention tools, and raising awareness. Products are made available as open source for the 'global community'.

HoneyNet activities are based on the deployment of 'honeypots' on a network, which serve as sensors for malware and malicious activities. They provide the rough data to conduct tactical and operational analyses and general cybersecurity threat intelligence.

HoneyNet chapters are examples of a global professional culture among cybersecurity researchers in which professionals are committed to extracurricular, open-source and volunteer work in addition to their academic, commercial or government day jobs.

Currently, in the ASEAN region, Indonesia, Malaysia and Singapore have active local chapters. Malaysia's and Indonesia's HoneyNet chapters have been embedded in their respective national CERT structures.

Highlights of Southeast Asian HoneyNet chapters include the following:

Dashboards. CyberSecurity Malaysia and Indonesia's National Cyber and Crypto Agency (BSSN) host live malware dashboards on their websites. The dashboards show malware types and their countries of origin. By collecting and sharing this data, these initiatives allow for further analysis and categorisation, thereby enabling the creation of a 'common operational picture', albeit at the technical level. Further sharing of threat information can be done through other community open-source platforms such as the Malware Information Sharing Platform (MISP).

Annual threat reports. As part of the HoneyNet initiative, BSSN has presented annual reports over 2018 and 2019. The reports contain information on activities carried out by BSSN and the Indonesia HoneyNet Project; summary reports on cyberattacks that occurred in Indonesia; results of traffic monitoring and the detection of cyberattacks and malware; analysis of the three most common types of malware that attack Indonesia; the introduction of HoneyNet portal public services; technological innovation; and an explanation of the research and development of the HoneyNet Project in Indonesia.

This case study describes a specific project and global community of practice that use open-source tools to help protect the internet from malicious software and hacking attacks. Communities are organised by national chapters.

For the purpose of implementing norm #3, states could check whether a local HoneyNet chapter exists in their jurisdiction and whether their national CERTs are connected. Alternatively, states could check whether they have people and tools in place that monitor malicious traffic on their country's networks.

United Nations

General Assembly

GUIDANCE FROM THE UN MEMBER STATES

Agreed text

States should consider how best (1) **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.

Additional guidance

This norm reminds States of the importance of international cooperation to addressing the cross-border threats posed by criminal and terrorist use of the Internet and ICTs, including for recruitment, financing, training and incitement purposes, planning and coordinating attacks and promoting their ideas and actions, and other such purposes highlighted in this report.

(1a) Within the United Nations, a number of dedicated fora, processes and resolutions specifically address the threats posed by terrorist and criminal use of ICTs and the cooperative approaches required to address such threats. These are:

- the open-ended intergovernmental expert group (IEG) to conduct a comprehensive study of the problem of cybercrime (UNGA 65/230)
- UNGA resolution 74/173 on promoting technical assistance and capacity building to strengthen national measures and international cooperation to counter the use of ICTs for criminal purposes, including information sharing
- UNGA resolution 74/247 on countering the use of ICTs for criminal purposes.

(1b) States can also use existing processes, initiatives and legal instruments to facilitate the exchange of information and assistance for addressing criminal and terrorist use of ICTs.

(1c) States are encouraged to develop cooperative partnerships with international organisations, industry actors, academia and civil society to this end.

Observance of this norm implies the existence of:

a. 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

b. mechanisms that can facilitate exchanges of information and assistance between relevant national, regional and international organisations in order to raise ICT security awareness among States and reduce the operating space for online terrorist and criminal activities.

c. appropriate protocols and procedures for collecting, handling and storing online evidence relevant to criminal and terrorist use of ICTs and providing assistance in investigations in a timely manner, ensuring that such actions are taken in accordance with a State's obligations under international law.

Questions to help your thinking

When you are considering implementation efforts to give effect to this norm, answers to the following questions can guide you:

- Is the government able to engage in international police cooperation?
- Does the government have sufficient means and capabilities to work with international partners in fighting cybercrime and countering terrorists' use of ICTs? If not, is the government seeking capacity-building assistance or third-party support?
- Does the government have policies, memorandums of understanding, mutual legal assistance treaties or other arrangements in place that guide international police and law enforcement cooperation? Do those arrangements cover cybercrime and terrorists' use of the internet?

Intergovernment and multistakeholder organisations and networks addressing cooperating in fighting cybercrime and terrorists' use of the internet

Counterterrorism

- Christchurch Call to Action
- Global Internet Forum to Counter Terrorism
- Jakarta Centre for Law Enforcement Cooperation (JCLEC)
- Tech against Terrorism
- Southeast Asia Regional Centre for Counter-Terrorism
- ASEAN Senior Officials Working Group on Counter Terrorism

Cybercrime

- Philippines Internet Crime Against Children Centre
- Interpol ASEAN Cyber Capacity Development Project
- Interpol ASEAN Cybercrime Operations Desk
- ASEAN Senior Officials Working Group on Cybercrime

ASEAN commitment to collaboratively prevent and combat cybercrime

1. ASEAN, Declaration on Transnational Crime (1997).
2. ASEAN Regional Forum, Statement on Cooperation in Fighting Cyberattack and Terrorist use of Cyber Space (2006).
3. ASEAN, Plan of Action to Combat Transnational Crime 2016–2025 (September 2017).

Further reading

- Council of Europe, **Convention on Cybercrime** (also known as the Budapest Convention), 2001, online.
- Ministry of Foreign Affairs and Trade, **Christchurch Call to Eliminate Terrorist and Violent Content Online**, New Zealand Government, 2019, online.
- UN Office on Drugs and Crime, **The use of the internet for terrorist purposes**, 2012, online.
- Global Initiative against Transnational Organized Crime, **Contested domain: UN cybercrime resolution stumbles out of the gate**, 2021, online.

Observed examples of regional good practice

This page lists examples of good practice that have been observed in the ASEAN region.

This list gives an idea of what concrete measures of implementation are and what states can demonstrate as their practices of implementation.

Actions

- Use existing law enforcement cooperation mechanisms, such as mutual legal assistance treaties, to enable (joint) operations against cybercrime and terrorist use of the internet.
- Participate in international training efforts to professionalise police and law enforcement conduct and operations in fighting cybercrime.
- Collaborate with Interpol, in particular through the ASEAN cyber capability desk and the ASEAN operational desk (see case study).

Institutional capabilities

- The establishment of dedicated cybercrime (police) units that can initiate and engage in transborder operations and information sharing.
- An ability to use Interpol's and Europol's 24/7 cybercrime operations centres to assist operations and secure digital evidence, and to connect with counterterrorism initiatives such as SEARCCT.
- An ability to access and apply assistance and advice offered through platforms such as the Global Internet Forum on Counterterrorism, JCLEC and the Philippines Internet Crime Against Children Centre.
- An ability to provide and/or accept capacity-building resources to enhance law enforcement in cybercrime and countering violent extremism online.

Laws and policy

- Endorsement of the ASEAN Declaration to Prevent and Combat Cybercrime (2017), which includes measures to strengthen cooperation and coordination among ASEAN members.
- Participation in the UN open-ended intergovernmental expert group on cybercrime, chaired by UNODC.
- Ratification of the Convention of Cybercrime (Council of Europe, 2004) or other international legal agreements that address cyber and ICT-related crimes.
- Subscription to the Christchurch Call to Action, expressing a commitment to address the issue of terrorist and violent extremist content online.

This case study describes Interpol-facilitated forms of regional police cooperation with member states of ASEAN in fighting cybercrime.

For the purpose of implementing norm #4, states could check their current relations with Interpol and police-to-police relations with other states. They could review Interpol resources, such as the threat assessment and cybercrime strategy guidebook, to inform national policymaking and develop operational doctrines.

CASE STUDY

Interpol–ASEAN cooperation

In 2014, Interpol opened the doors of a major second hub for its operations in Singapore. The Global Complex for Innovation is a research and development hub for international policing operations with a focus on the use of new technologies. Its Cyber Fusion Centre is an operational capability that assesses, analyses and shares information about new and emerging cybercrime threats.

ASEAN is a natural area of focus for Interpol for international police cooperation in the area of cybercrime. Starting in 2016, Interpol initiated a project to strengthen the capabilities of ASEAN police forces in preventing and fighting cybercrime. In 2018, in parallel, a dedicated operational desk was established to provide ASEAN member states with cybercrime threat intelligence, investigative support and operational coordination.

Highlights of ASEAN member states' collaborative efforts with Interpol include the following:

National Cybercrime Reviews. Interpol conducted in-country assessments with all ASEAN member states. The resulting national cybercrime review reports looked at governments' capabilities to prevent, investigate and prosecute cybercrime and at potential areas for capacity-building.

National Cybercrime Strategy Guidebook. Informed by national cybercrime assessments that Interpol conducted in various ASEAN countries, a general guidebook was developed to help countries develop, review or enhance their national cybercrime strategies.[7]

Specialised training. To strengthen investigative and forensic skills, Interpol has been providing technical training and assistance for local cybercrime units across the ASEAN region.

The ASEAN cyber threat assessment. To help protect the region's digital economies, the ASEAN cyber threat assessment report offers analysis and insight into the current cyberthreat landscape, while also highlighting strategies for moving forward.[8]

Operation Night Fury (2019–2020). Interpol facilitated a multi-country operation against a strain of malware targeting e-commerce websites in Southeast Asia, leading to the arrest of three individuals in Indonesia suspected to be the administrators of seized command and control servers. The ASEAN desk disseminated cyber activity reports to six affected ASEAN countries to support their national investigations.[9]

Operation Goldfish Alpha (2019). Interpol facilitated a region-wide operation against cryptojacking targeting routers. It included collaboration between cybercrime investigators and all ASEAN-10 national CERTs to locate infected routers, alert victims and assist with the patching of identified devices.[10]

Annual planning cycle for ASEAN joint operations. Interpol is establishing a systematic approach to joined-up regional operations informed by the annual threat assessment and through standard tactical plans that are to be executed by national law enforcement authorities / cybercrime units.

United Nations

General Assembly

GUIDANCE FROM THE UN MEMBER STATES

Agreed text

States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

Additional guidance

This norm reminds States to respect and protect human rights and fundamental freedoms, both online and offline, in accordance with their respective obligations.

Requiring special attention in this regard is the right to freedom of expression, including the freedom to seek, receive and impart information regardless of frontiers and through any media, and other relevant provisions provided for in the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and as set out in the Universal Declaration of Human Rights.

Observance of this norm can also contribute to promoting non-discrimination and narrowing the digital divide, including with regard to gender. State practices such as arbitrary or unlawful mass surveillance may have particularly negative impacts on the exercise and enjoyment of human rights, particularly the right to privacy.

Observance of this norm implies the following:

a. States should consider specific guidance contained in the cited resolutions. They should also take note of new resolutions adopted since the 2015 UNGGE report and contribute to new resolutions that may need to be advanced in light of ongoing developments.

b. States participate in dedicated forums within the UN that specifically address human rights issues.

c. Engaging a variety of stakeholders in policymaking processes relevant to ICT security can support efforts for the promotion, protection and enjoyment of human rights online and help clarify and minimise potential negative impacts of policies on people, including those in vulnerable situations.

Questions to help your thinking

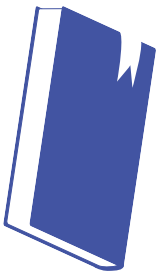
When you are considering implementation efforts to give effect to this norm, answers to the following questions can guide you:

- Is the government enabling freedom of expression and rights of privacy online, domestically, regionally and globally?
- Does the government have sufficient means and capabilities to protect human rights online and privacy?
- Has the government affirmed in policies and other frameworks that human rights apply online as they do offline?
- Is the government addressing recommendations by the UN Human Rights Council and/or regional human rights instruments?
- Is the government making an effort to ensure that citizens have adequate understanding of their human rights and how those rights can be exercised and protected online?

Summary of UN resolutions

The resolutions of the UN General Assembly and the UN Human Rights Council to which norm #5 refers contain the following:

1. The same rights that people have offline must also be protected online, including freedom of expression, which is applicable regardless of frontiers and through any media of one's choice.
2. Access to the internet and international cooperation aimed at the development of media and information and communication facilities and technologies should be promoted and facilitated.
3. Security concerns on the internet should be addressed in accordance with international human rights obligations to ensure the protection of freedom of expression, freedom of association, privacy and other human rights online.
4. Advocacy of hatred that constitutes incitement to discrimination or violence on the internet should be combated in accordance with international human rights laws and standards.
5. The global and open nature of the internet is a driving force in accelerating progress towards economic, social and cultural development.



Further reading

- DigitalReach, **Digital rights in Southeast Asia 2020/2021**, online.
- Manushya, **Thailand's Cybersecurity Act: towards a human-centered act protecting online freedom and privacy while tackling cyber threats**, 2019, online.
- ASEAN Telecommunications and IT Ministers, **ASEAN Framework on Personal Data Protection**, 2016, online.

Observed examples of regional good practice

This page lists examples of good practice that have been observed in the ASEAN region.

This list gives an idea of what concrete measures of implementation are and what states can demonstrate as their practices of implementation.

Actions

- Provide support for civil society organisations that promote digital freedoms, domestically or regionally.
- Conduct human rights dialogues with other states, businesses and civil society organisations.
- Make efforts to protect citizens (users), particularly vulnerable groups such as children, indigenous people and the elderly, in terms of e-safety awareness.
- Make efforts to provide relevant advice on e-safety and cybersecurity for human rights defenders, privacy watchdogs and whistleblowers.
- Assign social and due diligence responsibilities to the IT industry, social media platforms and other internet service providers in accordance with international human rights standards.
- Sponsor or co-sponsor relevant cyber and ICT-related resolutions at the UN Human Rights Council as a consequence of ratifying existing human rights conventions.

Institutional capabilities

- Establishment and provision of sufficient resources for oversight bodies such as national human rights commissions, data protection authorities and other relevant oversight instruments.
- Offer access to, and contributions to, the ASEAN Intergovernmental Commission on Human Rights.
- Ability to participate in UN human rights forums such as the Human Rights Council and implement relevant outcomes, such as the recommendations of the Universal Periodic Review.

Laws and policy

- Legislation or legislative measures that address privacy, personal data protection, access to information and human rights online in accordance with international human rights standards.
- Endorsement of the ASEAN Declaration on Human Rights (2012).
- Endorsement of the ASEAN Framework on Personal Data Protection (2016).

United Nations

General Assembly

GUIDANCE FROM THE UN MEMBER STATES

Agreed text

A State should (1) not conduct or knowingly support ICT activity contrary to its obligations under international law that (2) intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

Additional guidance

(2) ICT activity that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public can have cascading domestic, regional and global effects. It poses an elevated risk of harm to the population and can be escalatory, possibly leading to conflict.

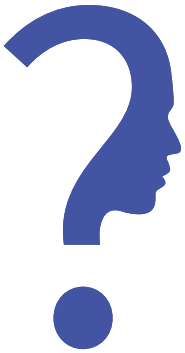
Critical infrastructure is of fundamental importance as a national asset since this infrastructure forms the backbone of a society's vital functions, services and activities. If these were to be significantly impaired or damaged, the human costs as well as the impact on a State's economy, development, political and social functioning and national security could be substantial.

Observance of this norm implies the following:

a. States take appropriate measures to protect their critical infrastructure. In this regard, each State determines which infrastructure or sectors it deems critical within its jurisdiction, in accordance with national priorities and methods of categorisation of critical infrastructure.

- Examples of critical infrastructure sectors that provide essential services to the public include:
  - healthcare and medical infrastructure and facilities
  - energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes
  - technical infrastructure essential to the general availability or integrity of the internet.

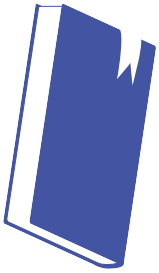
b. States put in place relevant policy and legislative measures at the national level to ensure that ICT activities conducted or supported by a State and that may impact the critical infrastructure of or the delivery of essential public services in another State so that they meet international legal obligations and are subject to comprehensive review and oversight.



Questions to help your thinking

When you are considering implementation efforts to give effect to this norm, answers to the following questions can guide you:

- Do state security agencies possess or have access to potentially offensive cyber capabilities? Are their cyber operations or decisions to deploy cyber capabilities guided by principles of international law and international humanitarian law?
- Do state security agencies impose professional standards for their CERTs, cyber units or third-party units operating under the government's direction and guidance?
- Do state security agencies that possess cyber capabilities have the skills, tools and knowledge to ensure that any operations do not lead to damage to critical infrastructure in other jurisdictions?
- Has the government articulated how international law and international humanitarian law apply to state conduct in cyberspace?



Further reading

- Tom Uren, Bart Hogeveen, Fergus Hanson, **Defining offensive cyber capabilities**, Australian Strategic Policy Institute, 2018, online.
- UN Group of Governmental Experts 2019–2021, **Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies**, 2021, online.

Observed examples of regional good practice

This page lists examples of good practice that have been observed in the ASEAN region.

This list gives an idea of what concrete measures of implementation are and what states can demonstrate as their practices of implementation.

Actions

- Acknowledge that the state possesses, or wishes to acquire, sovereign cyber capabilities, of a defensive and/or offensive nature, including the mandate and command and control relations of relevant domestic agencies.
- State organisations that possess sovereign cyber capabilities participate in national, regional and international (military) cyber exercises.

Institutional capabilities

- State organisations that possess cyber capabilities develop, enact and publish operational policies or doctrines guiding the use and deployment of those capabilities.
- State organisations that possess cyber capabilities can demonstrate a clear division of responsibilities and command and control depending on the type of operation, such as for intelligence-gathering, military (domestic or cross-border) or defensive purposes, and between strategic, operational and tactical capabilities.
- An ability to coordinate, deconflict and command cyber operations, for instance through a cyber defence operations centre.
- An ability to train and equip staff working on cyber operations up to professional standards, such as through (military) cyber defence schools and/or cyber operations testing ranges.

Laws and policy

- The ASEAN Treaty of Amenity and Cooperation in Southeast Asia commits the member states to mutual respect for their independence, sovereignty, territorial integrity and national identity; to non-interference in the international affairs of one another; and to the peaceful settlement of differences or disputes.
- Cabinet ministers or senior officials publicly declare their commitment to upholding international law, international humanitarian law and other international obligations in the conduct of cyber operations, such as through the ADMM Plus framework.
- A national defence strategy / white paper / policy describes the state's interests in cyberspace, its broader defence policy and its cyber capabilities.

United Nations

General Assembly

GUIDANCE FROM THE UN MEMBER STATES

Agreed text

States should take (1) **appropriate measures to protect their critical infrastructure** from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.

Additional guidance

This norm reaffirms the commitment of all States to protect critical infrastructure under their jurisdiction from ICT threats and the importance of international cooperation in this regard.

(1) Appropriate measures include:

- actions listed in General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructure
- measures to ensure the safety and security of ICT products throughout their life cycle
- measures to classify ICT incidents in terms of their scale and seriousness.

Some States serve as hosts of infrastructure that provides services regionally or internationally. States in such arrangements are encouraged to engage in cross-border cooperation with relevant infrastructure owners and operators to enhance the ICT security measures accorded to such infrastructure and strengthen existing or develop complementary processes and procedures to detect and mitigate ICT incidents affecting such infrastructure.

Observance of this norm implies that:

a. State designates an infrastructure or sector as critical, which can be helpful for protecting that infrastructure or sector

b. State determines the structural, technical, organisational, legislative and regulatory measures necessary to protect its critical infrastructure and restore functionality if an incident occurs.

Questions to help your thinking

When you are considering implementation efforts to give effect to this norm, answers to the following questions can guide you:

- Has the government listed critical infrastructure?
- Does the government have cybersecurity resources in place to support the protection of critical infrastructure?
- Does the government have mechanisms in place to coordinate between the government and critical infrastructure operators?
- Has the government issued guidelines on minimal requirements for critical infrastructure protection against cyberattacks and the division of responsibilities between the government and critical infrastructure operators?

A global culture of cybersecurity

UNGA resolution 58/199 recommends that states do the following:

1. Have emergency warning networks regarding cyber vulnerabilities, threats and incidents.
2. Raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them.
3. Examine infrastructures and identify interdependencies among them, thereby enhancing their protection.
4. Promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information to prevent, investigate and respond to damage to or attacks on such infrastructure.
5. Create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergencies.
6. Ensure that data availability policies take into account the need to protect critical information infrastructure.
7. Facilitate the tracing of attacks on critical information infrastructure and, where appropriate, the disclosure of tracing information to other states.
8. Conduct training and exercises to enhance response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack and encourage stakeholders to engage in similar activities.
9. Have adequate substantive and procedural laws and trained personnel to enable the state to investigate and prosecute attacks on critical information infrastructure and to coordinate such investigations with other states, as appropriate.
10. Engage in international cooperation, when appropriate, to secure critical information infrastructure, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats and incidents, and coordinating investigations of attacks on such infrastructure, following domestic laws.
11. Promote national and international research and development and encourage the application of security technologies that meet international standards.

Observed examples of regional good practice

This page lists examples of good practice that have been observed in the ASEAN region.

This list gives an idea of what concrete measures of implementation are and what states can demonstrate as their practices of implementation.

Actions

- Conduct a mapping of critical national infrastructure and critical information systems.
- Organise regular incident exercises or cybersecurity drills involving government agencies, critical infrastructure organisations and IT security partners.
- Perform sectoral cyber risk assessments.
- Organise cybersecurity awareness campaigns, including materials, activities and other resources.

Institutional capabilities

- National cybersecurity centres or CERTs have the ability and mandate to support critical infrastructure sectors in case of incidents.
- Sectoral CERTs or company incident response teams exist and are connected to the national CERT.
- Best practice cybersecurity guidelines are available and endorsed by the government.
- Education facilities develop and train a qualified and skilled cybersecurity workforce.
- A culture and practice of public–private collaboration on ICT security and cybersecurity response mechanisms.

Laws and policy

- Legislation outlines the cybersecurity responsibilities of government and critical infrastructure sectors in terms of information security, data protection and reporting obligations.
- Legislation or policy identifies and lists which sectors the government considers to be critical infrastructure and/or critical information infrastructure.
- Operational advice, guidance or recommendations are issued to provide critical infrastructure sectors with adequate technical IT security instructions.

OVERVIEW: Cybersecurity capacity building in Southeast Asia

Southeast Asia possesses several capabilities that enable ASEAN member states to lift their cybersecurity skills and competences. Key cybersecurity capacity-building initiatives include the following:

ASEAN–Singapore Cybersecurity Centre of Excellence (ASCCE)

ASCCE was launched in 2019 as a physical training and policy research facility in Singapore for the benefit of all ASEAN countries. The centre offers training, workshops and exercises in areas such as international law, cyber strategy, legislation, cyber norms and other cybersecurity policy issues, as well as CERT-related technical training. It also facilitates the exchange of open-source information on cyber threats and attacks and best practices and organises virtual cyber defence training and exercises.

Complementing the ASCCE campus is the Cyber Range facility at Temasek Polytechnic. By the end of 2021, ASCCE had delivered more than 30 programs attended by more than 900 senior officials from ASEAN and collaborated with more than 40 partners from governments, the private sector, academia and non-government organisations.

ASEAN–Japan Cybersecurity Capacity Building Centre (AJCCBC)

AJCCBC was established in 2018 as a physical training facility in Bangkok. Funded through the Japan–ASEAN Integration Fund, the initiative aims to develop a cybersecurity workforce of 700 by December 2022. So far, 500 people from national CERTs, cybersecurity agencies and telcos from all ASEAN member states have participated.

Guided by the ASEAN–Japan cybersecurity policy meeting, the centre offers training in network forensics, malware analysis, incident response and threat hunting, and the annual CYDER (Cyber Defence Exercise with Recurrence) exercise. Trainers and instructors are from JP-CERT.

Cybersecurity Alliance for Mutual Progress (CAMP)

Launched in 2016 by the Korean Internet and Security Agency, CAMP offers a network platform to lift the overall level of cybersecurity of its members. Members engage in activities (annual meetings, regional forums) that aim to share development experiences and trends in cybersecurity to catalyse mutual growth and to contribute to the development of global cybersecurity.

ASEAN members: Cambodia, Vietnam, Indonesia, Lao PDR, Malaysia, Philippines, Thailand.

Global Forum on Cyber Expertise (GFCE)

Launched in 2015, the GFCE is a permanent global multistakeholder forum of more than 140 community members and partners. The GFCE intends to drive international collaboration, share global and regional good practices and initiate research to address knowledge gaps. The forum facilitates member-driven working groups on cybersecurity policy and strategy, cybercrime, incident management, critical infrastructure protection and cybersecurity culture and skills.

ASEAN members: Singapore, Malaysia, Philippines, Vietnam.

This overview lists global and regional platforms for states to participate in joint cyber capacity-building efforts in an effort to lift local, national and regional cyber maturity levels.

For the purpose of implementing norm #7, states could check and assess their own cyber maturity levels and identify capacity shortfalls. States can check what skills, resources and assistance they can offer to—and request from—the regional community through bilateral, multilateral and multistakeholder platforms for collaboration.

United Nations

General Assembly

GUIDANCE FROM THE UN MEMBER STATES

Agreed text

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

Additional guidance

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

Observance of this norm implies the following:

a. Upon receiving a request for assistance, States should offer any assistance they have the capacity and resources to provide and that is reasonably available and practicable in the circumstances.

b. A State may choose to seek assistance bilaterally or through regional or international arrangements. States may also seek the services of the private sector to assist in responding to requests for assistance.

c. A State has the necessary national structures and mechanisms in place to detect and mitigate ICT incidents with the potential to threaten international peace and security. Such mechanisms complement existing mechanisms for day-to-day ICT incident management and resolution.

d. A State wishing to request assistance from another State would know whom to contact and the appropriate communication channel to use.

e. A State receiving a request for assistance needs to determine, in as transparent and timely a fashion as possible and respecting the urgency and sensitivity of the request, whether it has the capabilities, capacity and resources to provide the assistance requested.

f. States from which assistance is requested are not expected to ensure a particular result or outcome.

g. States engage in cooperative mechanisms that define the means and mode of crisis communications and of incident management and resolution.

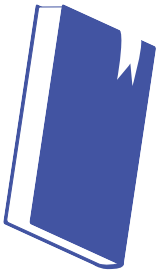
Common and transparent processes and procedures for requesting assistance from another State and for responding to requests for assistance can facilitate the cooperation described by this norm. In this regard, common templates for requesting assistance and responding to such requests can ensure that the State seeking assistance provides as complete and accurate information as possible to the State from which it seeks the assistance, thereby facilitating cooperation and the timeliness of the response.

A common template for responding to assistance requests could include elements that acknowledge receipt of the request and, if assistance is possible, an indication of the time frame, nature, scope and terms of the assistance that could be provided.

Questions to help your thinking

When you are considering implementation efforts to give effect to this norm, answers to the following questions can guide you:

- Does the government have the capability to take immediate incident-response action against perpetrators operating from its territory?
- Does the government have a 24/7 capability to receive and send requests for information and to receive and provide technical assistance?
- Are relevant government agencies integrated and engaged in multinational networks at the policy and operational levels? Has the government submitted up-to-date information for the ARF Points of Contact Directory?
- Has the government expressed an in-principle willingness to respond to requests for information, requests for assistance and requests for mitigating actions?



Further reading

- Forum of Incident Response Teams, **Computer Security Incident Response Team (CSIRT) Services Framework**, version 2.1, online.
- Bart Hogeveen (ed.), **Sydney recommendations: practical futures for cyber confidence building in the ASEAN region**, Australian Strategic Policy Institute, 2018, online.

Observed examples of regional good practice

This page lists examples of good practice that have been observed in the ASEAN region.

This list gives an idea of what concrete measures of implementation are and what states can demonstrate as their practices of implementation.

Actions

- Participate in regional points of contact schemes, such as the ARF cyber points of contact directory, and the member lists of APCERT and OIC-CERT.
- Contribute to mutual exchange of threat intelligence and information, for instance through platforms such as the MISP.
- Participate in the ASEAN Cyber Incident Drill and other incident-response tabletop exercises organised under the ARF program of work.

Institutional capabilities

- States participate in various networks and have nominated points of contact for their national CERT, police and law enforcement, critical infrastructure and foreign policy / international security agencies.
- An ability and willingness to provide and accept technical assistance when responding to ICT incidents of a regional nature.
- The national CERT has working arrangements with subnational, sectoral and other CERTs, such as the security operations centres of major telcos.

Laws and policy

- Endorsement of the recommended confidence-building measures from the 2015 UNGGE report.
- Endorsement of the ARF Work Plan on ICT Security (2015) and participation in subsequent meetings, such as the intersessional meetings.
- Endorsement of the ARF Point of Contract Directory.

EXPLAINED: ASEAN's participation in the ARF's Points of Contact Directory

Communicating requests for assistance between states requires government authorities to know whom to contact in their own country and in other countries. In 2019, ARF ministers agreed to the establishment of a cyber points of contact directory. The directory is an online resource that contains names and contact details for each ARF member country's authorised and competent diplomatic, national security policy, law enforcement and technical agencies, and specifies their office hours and English-language competency.

The directory provides a means of direct communication to prevent miscalculation and escalation, as well as to manage potential responses in the event of cybersecurity incidents with the potential to affect regional security. The details contained in the directory are available only to the authorities of ARF member countries. The following government bodies of ASEAN member states are involved:

Brunei

Diplomatic: Ministry of Foreign Affairs
National cybersecurity policy: Prime Minister's Department
Technical: BruCERT (https://www.brucert.org.bn/)
Law enforcement: Royal Brunei Police Force

Myanmar

Diplomatic: Ministry of Foreign Affairs
National cybersecurity policy: Ministry of Interior
Technical: mmCERT (Ministry of Communications and Information Technology; https://www.mmcert.org.mm)
Law enforcement: Myanmar Police, Criminal Investigation Department

Cambodia

Diplomatic: Ministry of Foreign Affairs and International Cooperation
National cybersecurity policy: Ministry of Interior
Technical: CamCERT (Ministry of Post and Telecommunications, ICT Security Department; https://www.camcert.gov.kh/en/)
Law enforcement: National Police, Anti-Cybercrime Department

Philippines

Diplomatic: Department of Foreign Affairs
National cybersecurity policy: National Security Council Secretariat
Technical: CERT PH (Department of ICT; https://www.brucert.org.bn/)
Law enforcement: PNP-ACG

Indonesia

Diplomatic: Ministry of Foreign Affairs, Directorate of Disarmament and International Security

National cybersecurity policy: Coordinating Ministry for Political, Legal and Security Affairs (Polhukam)

Technical: Badan Siber dan Sandi Negara (https://bssn.go.id)

Law enforcement: POLRI

Lao PDR

Diplomatic: Ministry of Foreign Affairs

National cybersecurity policy: Ministry of Public Security

Technical: LaoCERT (Ministry of Post and Telecommunications; https://www.laocert.gov.la/en/)

Law enforcement: Ministry of Public Security, General Police Department

Malaysia

Diplomatic: NACSA

National cybersecurity policy: National Cyber Security Agency

Technical: Cybersecurity Malaysia

Law enforcement: Royal Malaysian Police

Singapore

Diplomatic: Cybersecurity Agency (CSA)

National cybersecurity policy: CSA, as part of the Prime Minister's Office

Technical: SingCERT (CSA; https://www.csa.gov.sg/singcert)

Law enforcement: Singapore Police Force Cybercrime Command

Thailand

Diplomatic: Ministry of Foreign Affairs

National cybersecurity policy: Prime Minister's Department

Technical: ThaiCERT (Electronic Transactions Development Agency; https://www.thaicert.or.th)

Law enforcement: Royal Thai Police, Cybercrime Investigations Bureau

Vietnam

Diplomatic: Ministry of Foreign Affairs

National cybersecurity policy: Ministry of Public Security

Technical: VNCERT (National Cybersecurity Centre; http://www.vncert.gov.vn/)

Law enforcement: Ministry of Public Security

United Nations

General Assembly

GUIDANCE FROM THE UN MEMBER STATES

Agreed text

States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products (**Part A**). States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions (**Part B**).

Additional guidance

This norm recognises the need to promote end-user confidence and trust in an ICT environment that is open, secure, stable, accessible and peaceful. Ensuring the integrity of the ICT supply chain and the security of ICT products and preventing the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions are increasingly critical in that regard, as well as to international security and digital and broader economic development.

Observance of this norm (**Part A**: Reasonable steps to promote openness and ensure the integrity, stability and security of the supply chain) implies that States consider the following:

a. Putting in place at the national level comprehensive, transparent, objective and impartial frameworks and mechanisms for supply-chain risk management, consistent with a State's international obligations. Such frameworks may include risk assessments that take into account a variety of factors, including the benefits and risks of new technologies.

b. Establishing policies and programs to objectively promote the adoption of good practices by suppliers and vendors of ICT equipment and systems in order to build international confidence in the integrity and security of ICT products and services, enhance quality and promote choice.

c. Increased attention in national policy and in dialogue with States and relevant actors at the UN and other forums on how to ensure that all States can compete and innovate on an equal footing, so as to enable the full realisation of ICTs to increase global social and economic development and contribute to the maintenance of international peace and security, while also safeguarding national security and the public interest.

d. Cooperative measures such as exchanges of good practices at the bilateral, regional and multilateral levels on supply-chain risk management; developing and implementing globally interoperable common rules and standards for supply-chain security; and other approaches aimed at decreasing supply-chain vulnerabilities.

Observance of this norm (**Part B**: Prevent the development and proliferation of malicious ICT tools and techniques and the use of harmful hidden functions, including backdoors), implies that States at the national level put in place the following:

a. Measures to enhance the integrity of the supply chain, including by requiring ICT vendors to incorporate safety and security in the design and development and throughout the life cycle of ICT products. To this end, States may also consider establishing independent and impartial certification processes.

b. Legislative and other safeguards that enhance the protection of data and privacy.

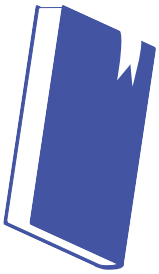
c. Measures that prohibit the introduction of harmful hidden functions and the exploitation of vulnerabilities in ICT products that may compromise the confidentiality, integrity and availability of systems and networks, including in critical infrastructure.

In addition to the steps and measures outlined above, States should continue to encourage the private sector and civil society to play an appropriate role in improving the security of and in the use of ICTs, including supply-chain security for ICT products, and thus contribute to meeting the objectives of this norm.

Questions to help your thinking

When you are considering implementation efforts to give effect to this norm, answers to the following questions can guide you:

- Does the government have laws, policies, regulations and guidelines in place to provide assurance that ICT products are secure?
- Does the government have laws, regulations and policies in place to deal with discovered software vulnerabilities?
- Does the government have means and capabilities to prevent discovered vulnerabilities from spreading?
- Does the government have an established practice of requiring minimum cybersecurity standards in public procurement processes?
- Does the government have laws and regulations in place that address potential obligations of ICT providers to collaborate with national security agencies?



Further reading

- Oleg Demidov, Giacomo Persi Paoli, **Supply chain security in the Cyber Age: sector trends, current threats and multi-stakeholder responses**, UN Institute for Disarmament Research, 2020, online.
- ISO/IEC, **Standard 27036-3 (2013): Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security**, online.
- Industrial Internet Consortium, **Software trustworthiness best practices**, white paper, 2020, online.

Observed examples of regional good practice

This page lists examples of good practice that have been observed in the ASEAN region.

This list gives an idea of what concrete measures of implementation are and what states can demonstrate as their practices of implementation.

Actions

- Provide guidance on how government, industry and others should manage risks in the ICT supply chain.
- Conduct a review of the national telecommunications or ICT supply chain.
- Introduce an IT security certification scheme, such as one based on ISO 15408 / Common Criteria.

Institutional capabilities

- National bodies that are technically equipped, skilled and mandated to advise on, assess and certify industry products and consumer goods, such as a national cybersecurity centre, universities or national scientific organisations.
- An ability to access industry transparency centres, such as those established in Southeast Asia by Huawei, Kaspersky and Microsoft.
- Promoting national research and development in the ICT domain and encouraging the building of local IT talent and the cybersecurity industry.
- Making use of international arrangements for mutual recognition of certified products and services, such as the Common Criteria initiative.

Laws and policy

- Legal prohibition of the deliberate introduction of systemic weaknesses or vulnerabilities in ICT products.
- Combating black markets in ICT products and the use of pirated software.
- Participation in the Wassenaar Arrangement on the transparency of dual-use goods and technologies.
- Introducing an approach to the security and integrity of the ICT supply chain, for instance through a risk-management approach and/or an approach based on testing and verification.
- Emerging practices in which ICT products and services are considered critical national security infrastructure, leading to deliberate decisions about market-entry requirements for specific products, services and suppliers.

CASE STUDY

Common Criteria initiative

The Common Criteria Recognition Arrangement (CCRA), an international agreement signed in 1998, provides a framework for the mutual recognition of IT security certifications. Currently, the arrangement has 31 members, 17 certificate-authorising members and 14 certificate-consuming members.

As security evaluations of IT products are complex and costly exercises for both certifiers and manufacturers, members of the CCRA recognise certificates issued by the certificate authorities, who rely on licensed laboratories. The evaluations are based on the Common Criteria, which are codified in ISO/IEC standard 15408.

From ASEAN, Singapore and Malaysia are certificate-authorising members, and Indonesia is a consuming member. Other ASEAN states, such as the Philippines and Vietnam, also make use of the Common Criteria standard despite not being members of the CCRA.

CASE STUDY

Industry transparency centres

Assuring the integrity of the IT supply chain is not a responsibility only of governments. The IT industry is also responsible for providing consumers and end users with reassurance about the confidentiality, integrity and availability of the industry's products and services.

In recent years, several global IT companies have started to establish transparency centres. These physical labs offer clients an opportunity to review product source code and to access technical documentation and security data and apply other relevant procedures and processing practices.

Examples include:

Microsoft	• Transparency Centre (Singapore) • Government Security Program (Vietnam) • Asia Pacific Public Sector Cyber Security Executive Council (Malaysia, Thailand, Brunei, Indonesia, Philippines, Singapore)
Kaspersky	• Transparency Centre (Kuala Lumpur, Malaysia)
Huawei	• 5G Cybersecurity Lab (Kuala Lumpur, Malaysia)

United Nations

General Assembly

GUIDANCE FROM THE UN MEMBER STATES

Agreed text

States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

Additional guidance

This norm reminds States of the importance of ensuring that ICT vulnerabilities are addressed quickly in order to reduce the possibility of exploitation by malicious actors. Timely discovery and responsible disclosure and reporting of ICT vulnerabilities can prevent harmful or threatening practices, increase trust and confidence, and reduce related threats to international security and stability.

Vulnerability disclosure policies and programs, as well as related international cooperation, aim to provide a reliable and consistent process to routinise such disclosures. A coordinated vulnerability disclosure process can minimise the harm to society posed by vulnerable products and systematise the reporting of ICT vulnerabilities and requests for assistance between countries and emergency response teams. Such processes should be consistent with domestic legislation.

Observance of this norm implies the following:

a. At the national, regional and international levels, States put in place impartial legal frameworks, policies and programs to guide decision-making on the handling of ICT vulnerabilities and curb their commercial distribution as a means to protect against any misuse that may pose a risk to international peace and security or human rights and fundamental freedoms.

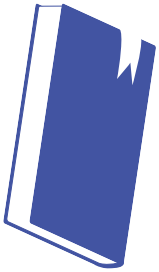
b. States put in place legal protections for researchers and penetration testers.

c. States, in consultation with relevant industry and other ICT security actors, develop guidance and incentives, consistent with relevant international technical standards, on the responsible reporting and management of vulnerabilities and the respective roles and responsibilities of different stakeholders in reporting processes; the types of technical information to be disclosed or publicly shared, including the sharing of technical information on ICT incidents that are severe; and how to handle sensitive data and ensure the security and confidentiality of information.

Questions to help your thinking

When you are considering implementation efforts to give effect to this norm, answers to the following questions can guide you:

- Does the government have laws, regulations and policies in place that describe how IT security vulnerabilities can be reported?
- Does the government have capabilities, or access to capabilities, to manage the process of disclosing and remedying IT security vulnerabilities?
- Does the government have or promote a national policy on vulnerability disclosures? Does it promote such mechanisms with industry?
- If state security agencies discover a zero-day vulnerability, does the government have the means and capabilities to process that zero-day vulnerability responsibly?



Further reading

- Global Forum on Cyber Expertise, **GFCE global good practices: coordinated vulnerability disclosure**, 2020, online.
- US Government, **Vulnerabilities equities policy and process**, 2017, online.
- National Cyber Security Centre, **Understanding vulnerabilities**, UK Government, 2015, online.

Observed examples of regional good practice

This page lists examples of good practice that have been observed in the ASEAN region.

This list gives an idea of what concrete measures of implementation are and what states can demonstrate as their practices of implementation.

Actions

- Organise or endorse the organisation of legitimate hacking sessions, such as Indonesia's 'Everybody can hack' and the US's 'Hack the Pentagon' competition.
- Accept the practice of legitimate bug bounty programs by private-sector companies and cybersecurity industry and security researchers, such as CyberArmyID and HackerOne.

Institutional capabilities

- Establish a vulnerability equities process whereby discovered vulnerabilities are carefully weighted, assessed and reported to the manufacturer.
- Offer support to government agencies and private-sector companies to conduct vulnerability assessments and access penetration-testing solutions.
- The national CERT is able to issue designated advisories (patches) to known and resolved vulnerabilities (common vulnerabilities and exposures; CVEs).

Laws and policy

- Endorse relevant ISO standards (such as ISO 29147) and, for instance, the GFCE's global good practices on CVD.
- Acknowledge and endorse public vulnerability reporting policies for, and by, government and private-sector organisations.
- Provide adequate legal protections to support, encourage and protect responsible reporters.

United Nations

General Assembly

GUIDANCE FROM THE UN MEMBER STATES

Agreed text

(**Part A**) States should not conduct or knowingly support activity to harm the information systems of the authorised emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. (**Part B**) A State should not use authorised emergency response teams to engage in malicious international activity.

Additional guidance

This norm reflects the fact that CERTs/CSIRTs or other authorised response bodies have unique responsibilities and functions in managing and resolving ICT incidents, and thereby play an important role in contributing to the maintenance of international peace and security.

The teams are essential in effectively detecting and mitigating the immediate and long-term negative effects of ICT incidents. Harm to emergency response teams can undermine trust and hinder their ability to carry out their functions and can have wider, often unforeseen, consequences across sectors and potentially for international peace and security.

It is important to avoid the politicisation of CERTs/CSIRTs and respect the independent character of their functions.

Observance of this norm (**Part A**) implies the following:

a. In recognition of their critical role in protecting national security and the public and preventing economic loss deriving from ICT-related incidents, states categorise CERTs/CSIRTs as part of their critical infrastructure.

Observance of this norm (**Part B**) implies the following:

b. States publicly declare or put in place measures affirming that they will not use authorised emergency response teams to engage in malicious international activity.

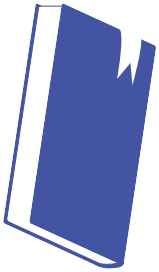
c. States acknowledge and respect the domains of operation and ethical principles that guide the work of authorised emergency response teams.

d. States put in place other measures such as a national ICT-security incident management framework that includes policies, regulatory measures or procedures that clarify the status, authority and mandates of CERTs/CSIRTs and that distinguish the unique functions of CERTs/CSIRTs from other functions of government.

Questions to help your thinking

When you are considering implementation efforts to give effect to this norm, answers to the following questions can guide you:

- Does the government have a defined and assigned national CERT with described roles and responsibilities? Does the CERT follow professional standards?
- Is the national CERT represented in relevant multilateral and regional networks of incident response agencies? Is it known and recognised by other CERTs?
- Is the national CERT well connected in the domestic ecosystem of sectoral, industry and non-government CSIRTs?
- Does the government clearly separate the national CERT role from other cybersecurity functions of government, such as the state's security agencies' cyber capabilities?



Further reading

- International Committee of the Red Cross, **Avoiding civilian harm from military cyber operations during armed conflicts**, 2021, online.
- Pablo Hinojosa, **Bridging the policy and technical communities on international cybersecurity discussions**, APNIC, 2019, online.

Observed examples of regional good practice

This page lists examples of good practice that have been observed in the ASEAN region.

This list gives an idea of what concrete measures of implementation are and what states can demonstrate as their practices of implementation.

Actions

- Establish and assign the authorised national CERT.
- Authorised national CERTs participate in regional and international networks such as FIRST, APCERT and OIC-CERT.
- Authorised national CERTs participate in international cybersecurity exercises and challenges, such as the ASEAN Cyber Incident Drill.
- National security cyber operators participate in training on the application of international humanitarian law in cyberspace, for instance in collaboration with the International Committee of the Red Cross and local Red Cross and Red Crescent organisations.

Institutional capabilities

- States engage in national, regional and global incident response capacity-building.
- States ensure that their CERT staff follow professional standards and are adequately certified, for instance by Carnegie Mellon.
- States ensure that their national security cyber operators follow professional standards and are adequately certified.

Laws and policy

- States ensure a separation of roles and responsibilities of the authorised national CERT from other arms of government (in particular those involved in national security) and from industry-led CERTs.
- When acknowledging that they develop, possess and/or potentially use military or offensive cyber capabilities, states make public statements and commitments to the legal and legitimate use of sovereign cyber capabilities and their adherence to international law and the norms.

Acronyms and abbreviations

ARF	ASEAN Regional Forum
ASEAN	Association of Southeast Asian Nations
ASPI	Australian Strategic Policy Institute
CAMP	Cybersecurity Alliance for Mutual Progress
CCRA	Common Criteria Recognition Arrangement
CERT	computer emergency response team
CSCAP	Council for Security Cooperation in the Asia Pacific
CSIRT	computer security incident response team
DNS	Domain Name System
FIRST	Forum of Incident Response Security Teams
GFCE	Global Forum on Cyber Expertise
ICT	information and communications technology
IEG	Intergovernmental Expert Group
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISP	internet service provider
IT	information technology
ITU	International Telecommunication Union
JCLEC	Jakarta Centre for Law Enforcement Cooperation
MISP	Malware Information Sharing Platform
OEWG	Open-ended Working Group
UN	United Nations
UNGA	UN General Assembly
UNGGE	UN Group of Governmental Experts
UNODC	UN Office on Drugs and Crime

Notes

1. UN General Assembly, Group of Government Experts on Developments in the field of ICTs in the context of international security, A/70/174, 22 July 2015, paragraph 10.
2. UN General Assembly, Group of Government Experts on Advancing responsible state behaviour in cyberspace in the context of international security, A/76/135, 14 July 2021, paragraph 15; UN General Assembly, Open-ended working group on developments in the field of ICTs in the context of international security, A/75/816, 18 March 2021, paragraph 24.
3. UN General Assembly, Group of Government Experts on Developments in the field of ICTs in the context of international security, A/70/174, 22 July 2015, paragraphs 26-28.
4. It is important to distinguish between 'norms of responsible state behaviour' (that is, the UN norms) and what are called 'norms of international law'. In this document, the term 'norms' refers only to the former.
5. UN International Law Commission, *Responsibility of states for internationally wrongful acts*, 2001, article 2.
6. Howard, Jessica, 'Invoking State responsibility for aiding the commission of international crimes—Australia, the United States and the question of East Timor', *Melbourne Journal of International Law*, link.
7. Interpol, *National Cybercrime Strategy Guidebook*, online.
8. Interpol, *ASEAN Cyber Threat Assessment 2021*, online.
9. Interpol, *Twitter*, 24 January 2020, online.
10. Interpol, 'Interpol-led action takes aim at cryptojacking in Southeast Asia', news release, 8 January 2020, online.

www.aspi.org.au/cybernorms