Norms of responsible State behaviour in the use of ICTs

A INTERSTATE CO-OPERATION ON SECURITY

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 CONSIDER ALL RELEVANT INFORMATION

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 PREVENT MISUSE OF ICTS IN YOUR TERRITORY

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

D COOPERATE TO STOP CRIME AND TERRORISM

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 RESPECT HUMAN RIGHTS AND PRIVACY

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 DO NOT DAMAGE CRITICAL INFRASTRUCTURE

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 PROTECT CRITICAL INFRASTRUCTURE

States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199.

H RESPOND TO REQUESTS FOR ASSISTANCE

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 ENSURE SUPPLY CHAIN SECURITY

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 REPORT ICT VULNERABILITIES

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 DO NO HARM TO RESPONSE TEAMS

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.

This material was prepared by DiploFoundation for educational purposes only.

OEWG CONFIDENCE-BUILDING MEASURES
NATIONAL POINTS OF CONTACT
EXCHANGING NATIONAL VIEWS
SHARING INFORMATION ON A VOLUNTARY BASIS
COOPERATIVE EXERCISE OF CBMs
CAPACITY BUILDING IN ICT SECURITY
REGULAR SEMINARS, WORKSHOPS AND TRAINING PROGRAMMES ON ICT SECURITY
EXCHANGING INFORMATION ON THE PROTECTION OF CI AND CII
PUBLIC-PRIVATE PARTNERSHIPS ON ICT SECURITY

Annex B

to the third Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025:

Initial List of Voluntary Global Confidence-Building Measures

The following is an initial, non-exhaustive list of voluntary global Confidence-Building Measures. These global CBMs are drawn from the Final Report of the 2021 Open-ended Working Group and the first and second APRs of the OEWG. Additional global CBMs may be added to this list over time, as appropriate, reflecting discussions within the OEWG.

CBM 1. Nominate national Points of Contact to the Global POC Directory, and operationalize and utilize the Global POC Directory

a) States agree to establish, building on work already done at the regional level, a global, intergovernmental, points of contact directory. At the fourth and fifth sessions of the OEWG, States to engage in further focused discussions on the development of such a directory, on a consensus basis, as well as engage in discussions on initiatives for related capacity building, taking into account available best practices such as regional and sub regional experiences where appropriate.

[First APR of the OEWG, CBM section, Recommended Next Steps, paragraph 2]

b) States, which have not yet done so, consider nominating a national Point of Contact, inter alia, at the technical, policy and diplomatic levels, taking into account differentiated capacities. States are also encouraged to continue to consider the modalities of establishing a directory of such Points of Contact at the global level.

[2021 OEWG report, paragraph 51]

c) States are encouraged to operationalize and utilize the Global POC Directory in the following ways:

i) Communication checks in the form of “Ping” tests;
ii) Voluntary information-sharing, including in the event of an urgent or significant ICT incident, facilitated through the Global POC Directory;
iii) Tabletop exercises to simulate practical aspects of participating in a Global POC directory; and
iv) Regular in-person or virtual meetings of POCs to share practical information and experiences on the operationalization and utilization of the Global POC Directory on a voluntary basis.
v) Utilize the POC directory to establish communication between POCs, in accordance with the modalities of the Global POC Directory.

CBM 2. Continue exchanging views and undertaking bilateral, sub-regional, regional, cross-regional and multilateral dialogue and consultations between States

a) States concluded that the dialogue within the Open-ended Working Group was in itself a CBM, as it stimulates an open and transparent exchange of views on perceptions of threats and vulnerabilities, responsible behaviour of States and other actors and good practices, thereby ultimately supporting the collective development and implementation of the framework for responsible State behaviour in their use of ICTs.

[2021 OEWG report, A/75/816, paragraph 43]

b) States explore mechanisms for regular cross-regional exchanges of lessons and good practices on CBMs, taking into account differences in regional contexts and the structures of relevant organizations.

[2021 OEWG report, A/75/816, paragraph 52]

ac) States continue to consider CBMs at the bilateral, regional and multilateral levels and encourage opportunities for the cooperative exercise of CBMs.
[2021 OEWG report, paragraph 53]

d) States continued to emphasize that the OEWG itself served as a CBM.

[First APR of the OEWG, paragraph 16(e)]

CBM 3. Share information, on a voluntary basis, such as national ICT concept papers, national strategies, policies and programmes, legislation and best practices, on a voluntary basis

a) States, on a voluntary basis, continue to inform the Secretary-General of their views and assessments and to include additional information on lessons learned and good practice related to relevant CBMs at the bilateral, regional or multilateral level.

[2021 OEWG report, paragraph 48]

b) States voluntarily engage in transparency measures by sharing relevant information and lessons in their chosen format and fora, as appropriate, including through the Cyber Policy Portal of the United Nations Institute for Disarmament Research.
[2021 OEWG report, paragraph 50]

c) States are encouraged to continue, on a voluntary basis, to share concept papers, national strategies, policies and programmes, as well as information on ICT institutions and structures with relevance to international security, including through the report of the Secretary-General on developments in the field of information and communication technologies in the context of international security as well as the UNIDIR Cyber Policy Portal as appropriate.

[First APR of the OEWG, CBM section, Recommended Next Steps, paragraph 5]

CBM 4. Encourage opportunities for the cooperative development and exercise of CBMs

a) States voluntarily identify and consider CBMs appropriate to their specific contexts, and cooperate with other States on their implementation.

[2021 OEWG report, paragraph 49]

b) States continue to consider CBMs at the bilateral, regional and multilateral levels and encourage opportunities for the cooperative exercise of CBMs.

[2021 OEWG report, paragraph 53]

c) States continue exchanging views at the OEWG on the development and implementation of CBMs, including on the potential development of additional CBMs .

[First APR of the OEWG, CBM section, Recommended Next Steps, paragraph 1]

In addition to the Global CBMs listed above States have included the following as additional voluntary global CBMs:

CBM 5. Promote information exchange on cooperation and partnership between States to strengthen capacity in ICT security and to enable active CBM implementation

Capacity-building programmes are an important avenue of collaboration which could strengthen relationships as well as build trust and enhance confidence between States.

CBM 6. Engage in regular organization of seminars, workshops and training programmes on ICT security

The regular organization of seminars, workshops and training programmes on relevant issues related to ICT security with the inclusive representation of States could increase communication and mutual understanding and contribute to confidence-building.

CBM 7. Exchange information and best practice on, *inter alia*, the protection of critical infrastructure (CI) and critical information infrastructure (CII), including through related capacity-building.

Exchange of information and best practice on, inter alia, the protection of critical infrastructure (CI) and critical information infrastructure (CII), including through related capacity -building could build trust and enhance confidence between States.

CBM 8. Strengthen public-private sector partnerships and cooperation on ICT security

A range of technical capabilities and knowledge are required to detect, defend against and respond to and recover from ICT incidents. In this regard, public-private sector partnerships and cooperation, including regular dialogue and the exchange of good practice, could contribute to confidence-building.