26/08/2019

Cyber Norm Initiative

Synthesis of Lessons Learned and Best Practices

On 6 April 2019, G7 Foreign Ministers met in Dinard, France, and launched a Cyber Norm Initiative dedicated to sharing best practices and lessons learned on the implementation of previously recognized voluntary, non-binding norms of responsible State behaviour. The norms that are presented in this document have notably emerged during the previous sessions of the United Nations Group of Governmental Experts (GGE) and are a subset of the international cyber stability framework. G7 countries are committed to continuing this work and to sharing views on the full range of important recommendations that have been underlined in GGE reports.

Norm 1 – 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 agreed to be harmful or that may pose threats to international peace and security.

G7 countries have taken a number of steps to increase stability and security in the use of ICTs and prevent the most harmful ICT practices. Such steps include:

- The promotion, at the international level, of a stability framework based notably on the application of existing international law and agreed voluntary norms of responsible State behavior, which this very initiative aims to strengthen;
- The establishment of confidence-building measures (notably at OSCE, OAS and ARF) and of strategic bilateral, trilateral or multilateral dialogues on cyber issues with a range of partners to build trust, capacities and cooperation mechanisms, which also reinforce the stability framework mentioned above;
- The development of cyber capacities at national and international levels, to increase the general level of resilience, protection and security of their own information systems and networks as well as those of partners. Importantly, G7 countries have all published comprehensive whole-of-government cybersecurity strategies, whose

development and effective implementation is seen as a crucial and useful step to ensure coherent effort and increased security;
- The continued development of industry standards on security of technology, which help to build cyber resilience globally and seek alignment at an international level.

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

G7 States have developed crisis-management procedures to deal with ICT incidents at the national level:

- These generally include, under different forms, regular information-sharing and enhanced cooperation between relevant administrations and agencies;
- After an attack has been detected, technical agencies have the responsibility to come up with an assessment of the nature of the incident which then paves the way for a whole-of-government response, if required;
- G7 countries consider that attribution is sovereign political decision, taken on a case-by-case basis with due consideration for all relevant information;
- Some G7 countries have found it useful to establish incident categorization frameworks to help officials and decision-makers in their analysis and action.

Norm 3 – States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

In order to ensure their territory is not used to commit internationally wrongful acts, G7 countries have:

- Increased the resources and capabilities of their respective national cybersecurity agencies;
- Strengthened cooperation with the private sector to promote effective cybersecurity standards, frameworks, and processes including on incident-reporting and the security of IoT devices (Internet of Things), to increase information-sharing on threats and to conduct cyber-awareness raising campaigns;
- Taken active measures to prevent and discourage cybercriminals from operating on their territories or through their digital infrastructures – including through the criminalization of wrongful acts using ICTs, such as unauthorized intrusions in information security systems of third parties.

Some G7 countries have taken measures to encourage responsible reporting of vulnerabilities and established national competence centres. Some have also chosen other approaches to reducing harm from commodity attacks.

Norm 4 – 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.

G7 countries have developed an array of measures to increase cooperation with their partners to prevent and prosecute terrorist and criminal use of ICTs, such as:

- Ratifying the 2001 Council of Europe Convention on Cybercrime (Budapest Convention) which provides for effective, flexible and modern means of international cooperation in the fight against cybercrime;
- Establishing strong partnerships with public and private partners, including at the technical and operational level through exchanges between CERTs and among law enforcement officers;
- Supporting other countries to develop their own cybercrime capabilities, bilaterally or working through and alongside European and international organizations.

Some G7 countries have also dedicated important resources to cooperation with the private sector and civil society to prevent terrorist use of the Internet and remove terrorist content.

Norm 5 – States, in ensuring the secure use of ICTs, should respect Human Rights Council Resolutions A/HRC/RES/20/8 and A/HRC/RES/26/13 (The promotion, protection and enjoyment of human rights on the Internet), as well as General Assembly Resolutions A/RES/68/167 and A/RES 69/166 (The right to privacy in the digital age) to guarantee full respect for human rights, including the right to freedom of expression;

All G7 countries share a commitment to a free, open and secure Internet, where the rights that people have offline are also protected online. They take an active role in defending and promoting this approach, including by:

- Ensuring applicable domestic legislation to protect, *inter alia*, privacy, freedom of expression and personal data and to prevent online harms;
- Supporting international and, when applicable, European initiatives on the protection of human rights online (such as the Council of Europe's Guide to Human Rights for Internet Users, relevant United Nations Human Rights Council resolutions, the EU General Data Protection Regulation, etc.).

Norm 6 – A State should not conduct or knowingly support any ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of a critical infrastructure to provide services to the public.

As responsible States, G7 countries have reaffirmed support to this norm and promoted it at the international level. Several of them have made clear that the use of sovereign offensive cyber capabilities must be governed in accordance with international law, including humanitarian law.

Norm 7 – States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account, *inter alia*, General Assembly Resolution 58/199 (2003) "Creation of a global culture of cybersecurity and the protection of critical information infrastructure", and other relevant resolutions.

To protect their critical infrastructure from ICT threats, G7 countries have:

- Established effective regulatory frameworks, requiring companies to increase their level of protection, have appropriate cyber resilience and report cyber incidents – this has notably entailed strengthened cooperation between the public and private sector, especially with operators and systems deemed essential or critical;
- Promoted regional and international cooperation on this issue, including through the sharing of best practices, information on specific threats and incidents, and the development of confidence-building measures between States;
- Developed education, training and cooperation programmes and activities to increase their capabilities and resources in this field.

Norm 8 - 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 another State's critical infrastructure emanating from their territory, taking into account due regard for sovereignty.

To facilitate the response to appropriate requests for assistance, G7 countries have established clear and operational permanent points of contact. These are usually located within the national CERT/CSIRT and available 24/7. They are shared with other members of

relevant regional and international organizations, such as the OSCE, the EU CSIRT network or the parties to the Budapest Convention.

Norm 9 – States should take reasonable steps to ensure the integrity of the supply chain, so 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.

G7 countries have taken a series of steps to ensure the integrity of the supply chain and to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions, such as:

- Developing and promoting frameworks, recommendations, codes of conduct, norms and standards for industry, to improve awareness of supply chain security and help companies establish effective control and oversight of their supply chain – these can also include labelling, evaluation and certification schemes;
- Establishing procedures to ensure ICT procurement by the public sector helps drive improvements in security and resilience;
- Supporting the proper and effective use of export-control regimes to prevent the proliferation of malicious ICT tools and techniques.

Norm 10 – States should encourage responsible reporting of ICT vulnerabilities and share related information on available remedies to such vulnerabilities, in order to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

G7 countries have established procedures, mechanisms and sometimes legal frameworks that facilitate and encourage responsible disclosure of vulnerabilities by and to their national cybersecurity agencies. They have increased cooperation with public and private partners to better share information on vulnerabilities, mitigation and recovery measures and developed programmes to assist partners in creating vulnerability disclosure processes.

Norm 11 – States should not conduct or knowingly support activity to harm the information systems of another State's authorized emergency response teams (sometimes known as CERTS or CSIRTS). A State should not use authorized emergency response teams to engage in malicious international activity.

As a principle, and as responsible States, all G7 countries have strongly reaffirmed that they will not conduct or knowingly support activity to harm another State's CERT, nor use their own CERT to engage in malicious international activities./.