2015 GGE Norms
Excerpt from UN A/70/174*

The 2015 UN GGE committee consisted of experts from 20 representing Belarus, Brazil, China, Columbia, Egypt, Estonia, **France**, **Germany**, Ghana, Israel, **Japan**, Kenya, Malaysia, Mexico, Pakistan, the Republic of Korea, the Russian Federation, Spain, the **United Kingdom of Great Britain and Northern Ireland**, and the **United States of America**. The two G7 countries not represented are Canada and Italy.

"13. … (The) present Group offers the following recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment:

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

* Retrieved on April 3, 2018 from
https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement

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.

14. The Group observed that, while such measures may be essential to promote an open, secure, stable, accessible and peaceful ICT environment, their implementation may not immediately be possible, in particular for developing countries, until they acquire adequate capacity."

In addition, the 2015 GGE encouraged states to implement confidence-building measures to include a) identification of domestic technical and policy points of contact "to address serious ICT incidents," b) risk reduction measures, c) sharing of general threat information, known technological vulnerabilities, and best security practices, and d) identification of critical domestic infrastructures and the legal, technical and assessment steps that nations have taken to protect them. This GGE also encouraged states to exchange law enforcement and cybersecurity personnel as well as to facilitate exchanges between academic and research institutions. The creation of national computer emergency response teams is also encouraged along with exchanges of personnel between such groups.