INTRODUCTION TO THE COMMITTEE

Established in 1945 under the Charter of the United Nations1, the General Assembly occupies a central position as the chief deliberative, policymaking and representative organ of the United Nations. Comprising all 193 Members of the United Nations2, it provides a unique forum for multilateral discussion of the full spectrum of international issues covered by the Charter. It also plays a significant role in the process of standard-setting and the codification of international law3. The Assembly is empowered to make recommendations to States on international issues within its competence. It has also initiated actions—political, economic, humanitarian, social and legal—which have benefited the lives of millions of people throughout the world. The landmark Millennium Declaration, adopted in 2000, and the 2005 World Summit Outcome Document, reflect the commitment of Member States:

● to reach specific goals to attain peace, security and disarmament along with development and poverty eradication;

● to safeguard human rights and promote the rule of law; ● to protect our common environment;

● to meet the special needs of Africa; and

● to strengthen the United Nations.

 OVERVIEW OF AGENDA

The exponential pace of technological change has shaken the very foundations of traditional security understanding. Over the past 50 years, international conflict has morphed into a shape beyond our wildest imaginations It is our mandate to oversee frameworks and solutions to issues that lead to a destabilization of peace and security to both individualsand states alike. Cyberspace has long been a blind spot for the international system, where criminal and inter-state threats jeopardize the trust and readiness of collective security in both the developed and developing world. Over the past two years, actors such as China, the USA, the E.U., and Great Britain all shifted their view on cyberspace to include not only a matter of information security/C4-infrastructure but also the Fifth Domain of Warfare. The problem with classifying cyber-attacks as the fifth domain of warfare is that cyberspace differs radically from other domains (land, sea, air, and space). A key tenant of international peace & security is deterrence, which involves parties to a potential conflict dissuading each other via credit mutual threats. In cyber, however, parties can strike with a certain degree of anonymity and deliver crippling blows without technically inflicting “kinetic” (or physical) violence. Cyber deterrence proponents like Nigel Inkster and the U.S. Department of Homeland Security generally agree that states are vulnerable to attacks but tend to branch into two camps: those who argue for an offensive strategy in which leading countries assert dominance in cyberspace early on, and those who believe in defensive bandwagoning, which includes collaboration between states and the private sector.

 BLOC POSITIONS

In December 2018, the United Nations General Assembly (UNGA) approved the creation of two distinct groups to further explore issues related to responsible state behaviour in cyberspace: an Open-Ended Working Group (OEWG) and a new Group of Governmental Experts (GGE)

This decision was preceded by the submission of [two draft resolutions by Russia and the United States](http://russiancouncil.ru/analytics-and-comments/analytics/rossiya-i-ssha-dva-raznykh-vzglyada-na-kiberbezopasnost/) to the UNGA First Committee, the Disarmament and International Security Committee (DISEC). In November 2018, both drafts were [approved by a vote](https://undocs.org/A/73/505) for submission to the General Assembly as resolutions.

On 5 December 2018, a vote was taken on the Russian revolution and the document was adopted by a large majority: 119 votes to 46, with 14 abstentions. The resolution [A/RES/73/27](http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27), originally titled ‘Developments in the field of information and telecommunications in the context of international security, proposed the establishment of the OEWG to discuss further cyber norms for state behaviour. The text of the document has undergone significant changes in comparison with its first [draft](http://undocs.org/A/C.1/73/L.27/Rev.1). The number of proposed norms of responsible behaviour of states has been reduced from 25 to 13. They are still based on earlier reports of the GGE, but there is a norm that stands out on the list. It says that all charges against states regarding organising and/or conducting illegal activities with the use of ICT need to be substantiated. The norm also touches on the problem of attribution, and the need to study all available information and the broader context of an incident. Some of the removed norms were partially included in the preamble of the resolution: new paragraphs indicate the growing concern of Russia and other countries with the issue of ‘dissemination of false or distorted news, which can be interpreted as interference in the internal affairs of other states. Reference is also made to the need to assist states in bridging the capacity gap in ICT security. Provisions on the necessity to limit human rights and freedoms online and offline to a certain extent for national security reasons, as well as on the internationalisation of Internet governance and the establishment of ‘multilateral, transparent and democratic international mechanisms’ to guarantee the stable and secure functioning of the Internet and the equitable distribution of resources, have disappeared from the list of norms.

The vote on the American document that asks for the creation of the next GGE, was postponed by the General Assembly due to a significant budget burden for the implementation of the proposed activities concerning the new GGE. According to a [document](https://undocs.org/ru/A/C.1/73/L.72) describing the financial implications of the resolution, the cost of the work of the group over three years is approximately USD$ 1 295 600. Meanwhile, the OEWG is estimated to [cost](https://undocs.org/ru/A/C.1/73/L.71) half as much – USD$ 603 100 – over two years. However, the financial justification was considered by the Fifth Committee, and on 22 December a vote was taken on the American resolution [A/RES/73/266](http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266) titled ‘Advancing responsible State behaviour in cyberspace in the context of international security. The document was approved with a larger majority of member states – 138 in favour, 12 against, and 16 abstentions.

INTERNATIONAL AND REGIONAL FRAMEWORK

The international community has been debating cybersecurity for the last two decades.95 The General Assembly, in particular, developed an elaborate international framework, adopting annual resolutions around the issue of ICTs and international security since 1999. The first, resolution 53/70, recognized the potential of ICTs for peoples’ development but also noted threats to international order and peace that may arise through the misuse of it. The General Assembly expanded on its original resolution by establishing a group of governmental experts in resolution 58/32 and addressing respect for human rights and fundamental freedoms regarding ICTs in resolution 70/237. In 2000, the General Assembly laid the foundations on “combating the criminal misuse of information technologies” highlighting effective legal regimes, prosecution, and information sharing and cooperation among the Member States to ensure that ICTs contribute to international development rather than undermining it.99 Another collection of noteworthy General Assembly resolutions, 57/239, 58/199, and 64/211, were adopted between 2003 and 2010 on the “creation of a global culture of cybersecurity” addressing Member States’ capacity to safeguard their critical information infrastructures from cyber attacks. These documents indicate an important shift from mere law enforcement practices and prosecution of cybercrimes to the prevention of attacks in the cybersphere and requested a more firm commitment from Member States to secure cyberspace and address growing cyber threats. In 2007, the International Telecommunications Union (ITU) introduced the Global Cybersecurity Agenda (GCA), which serves as a practical framework for all 193 Member States and more than 700 Sector Members to collaborate on cybersecurity. The GCA consists of five pillars. First, “legal measures” focuses on the persecution of unlawful cyber activities with an internationally consistent legislative approach. Second, “technical and procedural measures” looks at the security standards of ICT applications and systems and best practices of risk management. Third, “organizational structures” discusses national policies, and institutional setups allowing for effective prevention, response to, and crisis management of cyberattacks. Fourth, “capacity building” promotes awareness and technology sharing among all stakeholders. And the last pillar, “international cooperation,” promotes dialogue and coordinated action of the international community in dealing with cyber threats. In the context of the 2030 Agenda for Sustainable Development (2016), the usage of ICTs, and therefore their safeguarding, is critical considering their catalyst role for sustainable development.

FOR FURTHER STUDY

● “Developments in the field of information and telecommunications in the context of international security”, Report to the Secretary-General, United Nations General Assembly, 58th Session, Addendum, A/58/373, September 17, 2003

 ● “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”, Report to the Secretary-General, United Nations General Assembly, 60th Session, Addendum, A/60/202, August 5, 2005

● Resolution 64/211, March 2010, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures available at<http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211>

● Report of the Group of Governmental Experts on Development in the Field of Information and Telecommunication in the Context of International Security, submitted to the UN General Assembly 68th Session, June 24, 2013, available

<http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98>

\*DATA IS GATHERED FROM VARIOUS SOURCES ALL RIGHTS RESERVED TO ORIGINAL AUTHORS\*

BIBLIOGRAPHY

● UN Resolutions related to Cybersecurityhttps://www.itu.int/en/action/cybersecurity/Pages/un-resolution s.aspx ● UN FIRST COMMITTEE PROCESSES ON RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACEhttps://www.gp-digital.org/un-first-committee-processes-on-res ponsible-state-behaviour-i n-cyberspace-a-briefing/ ● Functions and Powers of the General Assemblyhttps://www.un.org/en/ga/about/background.shtml ● http://undocs.org/en/A/RES/70/1 ● https://www.un.org/en/ga/about/background.shtml ● http://www.un.org/fr/member-states/index.html ● http://www.un.org/en/sections/un-charter/chapter-iv/index.html ● 2015 GGE report, 2015 GGE report A/70/174 ● Principles of Personal Data Protection and Privacyhttps://www.unsystem.org/principles-personal-data-protection-and-priv acy ● https://dictionary.cambridge.org ● GGE: https://www.un.org/disarmament/group-of-governmental-experts/ ● Resolution adopted by the General Assembly on 22 December 2018:https://dig.watch/sites/default/files/Resolution%20A-RES-73-266%20-% 20Advancing% 20responsible%20State%20behaviour%20in%20cyberspace%20in%20the%20con text%2 0of%20international%20security.pdf

Individuals and