Germany: Report on “Developments in the field of information and telecommunications in the context of international security” (GA Resolution 71/28)

General appreciation of the issues of information security

The evolution of information and communication technologies (ICT) offers widespread economic, social and scientific opportunities. At the same time, access to the internet and IT technology and the integrity, authenticity and confidentiality of data in cyberspace have become vital issues of the 21st century.

Progress in international cyber security is a priority of German cyber policy. Working with partners around the globe, the objective is to find common solutions and strategies to prevent a malicious use of ICTs and cyber-attacks that carry the danger of uncontrolled escalation. Germany has also taken initiatives, together with partners, to ensure that human rights, including the right to privacy, are protected “online” as much as they are protected “offline”.

In an increasingly interconnected world, states, critical infrastructures, businesses and individuals depend on the reliable functioning of ICT. The consequences of a misuse of ICT may not be limited to cyberspace. They can cause social, economic, political and other damage. Attacks targeting state institutions or democratic and political processes can affect public order and safety.

Germany is addressing these challenges by promoting international law-abiding, norm-adhering and confidence-building state use of ICT.

Efforts taken at the national level to strengthen information security and promote international cooperation in the field of information and telecommunications in the context of international security

Core aspects of Germany’s national cyber security policy are the protection of critical infrastructure and ensuring the integrity and confidentiality of data. The 2015 Information Technology Security act obliges public and private institutions to report significant ICT incidents.

With a view to supporting international peace and security in the context of ICT use, Germany has established national points of contact for both technical and political coordination in the field of cyber security. They are part of the Federal Ministry of the Interior and the Federal Foreign Office, respectively.
Efforts at the regional and global levels to strengthen information security and promote international cooperation in the field of information and telecommunications in the context of international security

Germany maintains bilateral cyber dialogues or cyber consultations with multiple partners.

Germany’s 2016 National Cyber Security Strategy emphasizes, inter alia, support for building cyber capacities in other countries. To this end, the Federal Government has decided to work toward establishing a German Institute for International Cyber Security, which will also be an independent partner for the private sector, academia and civil society organizations.

Building on established partnership relations, Germany already supports cyber security capacity building efforts in third countries, as well as efforts in regional organizations around the globe that aim at increasing security in and of ICT use.

At the regional level, the focus is on confidence-building measures (CBMs) that help address the risk of ICT incidents escalating into political or even military crisis. During Germany’s chairmanship-in-office of the Organization for Security and Cooperation in Europe in 2016, implementation of the CBMS agreed in 2013 made good progress, and OSCE participating States agreed additional such measures. The 2016 OSCE Ministerial Council in Hamburg approved these and gave directions not only for their implementation, but also for further work to be undertaken. Security in and of the use of ICT needs to expand beyond politico-military aspects to other dimensions of security as well.

Globally, Germany is supporting efforts at agreeing how existing international law applies to State use of ICT, and at developing voluntary non-binding norms, rules or principles of responsible state behavior which aim at an open, secure, stable, accessible and peaceful ICT environment. Of particular importance in this context is the work of successive United Nations Groups of Governmental Experts. German experts have actively participated in these groups, and Germany is committed to promoting their recommendations. Now is the time to universalize the work and engage the wider UN membership. Germany supports a lead United Nations’ role and a strengthening of UN capacities to this end. Issues to be explored further include international information-sharing and cooperation on attributing cyber-attacks. Clear and universally respected rules should address the malicious use of cyber capabilities as well as online espionage for economic purposes.
The content of the concepts aimed at strengthening the security and global information and telecommunication systems

Germany is committed to implementing the recommendations offered by the 2015 Group of Governmental Experts (GGE), including the voluntary non-binding norms, rules or principles of responsible state behavior that aim at promoting an open, secure, stable, accessible and peaceful ICT environment. These norms can enhance international transparency and predictability, thereby contributing to peace and stability. Germany looks forward to the results of the 2016/2017 GGE.

Continued international cooperation in developing and implementing measures to increase stability and security in ICT use is vital. At the same time, and fully recognizing that certain challenges of attribution in the ICT environment remain, Germany sees a need for clarity on the consequences of attributable breaches of international law through ICT use, and for building an international consensus on how existing international law applies to state use of ICT.

Possible measures that could be taken by the international community to strengthen information security at the global level

The discussion on ICT use in the context of international security needs to include the wider UN membership. At the same time, the need for continued expert discussion on the basis of consensus decision making remains. Germany supports building a UN architecture to this end, including the strengthening of the Secretariat’s capacities and the establishment of a special adviser to the Secretary-General on developments in the field of information and telecommunications in the context of international security.

Beyond states, other actors share in the responsibility for establishing and maintaining a secure ICT environment: The IT industry, the academic and science communities as well as users. Any measures that taken by the international community to strengthen information security at the global level should ensure that these stakeholders’ input is taken, within their respective roles and responsibilities. One possible measure could be to establish an advisory board for the Secretary-General that represents a variety of stakeholder communities.