Germany: "Report on Developments in the Field of Information and Telecommunications in the Context of International Security" (RES 68/243),

General appreciation of the issues of information security

The accelerating digitalization of economic, administrative and private use of information and communication technology offers unprecedented opportunities for industrialized and developing countries alike. At the same time, an increasing dependency on information and communications technologies, as well as the trend toward an interconnectivity of machines ("web 3.0"), creates vulnerabilities and systemic weaknesses.

There is a trend towards hard-to-detect, sophisticated malicious activities, targeting high-value objectives. The motivation for such attacks varies: it may be profit; it may be the search for information on or it may even be an attempt to control critical assets, systems and infrastructures. Severe consequences for Governments, private industry and civil organizations may result, including for the providers of critical infrastructure services. The process control systems for critical infrastructures have proven particularly vulnerable to malicious information and communications technology operations. As a consequence, the risks of uncontrollable collateral damage on a global scale are high, including the infection of industrial control systems with potentially physical destructive effects. A single cyber-attack against core telecommunication infrastructure could cause more global disruption than a single physical attack.

Despite such risks, an all-out "cyber war" seems unlikely at present. In fact, the term "cyber war" is inadequate and misleading. It implies an extensive, existential threat to a state solely through targeted attacks by other states on computer systems and IT networks, or through other actions in cyberspace. This seems unrealistic for the foreseeable future. A more likely scenario may be the limited use of cyber capabilities as part of a larger warfighting effort. Modern conflict scenarios assume that military adversaries use functions and components of cyberspace. Consequently, cyberspace can be classified as an operational military domain, comparable to maritime, air or outer space. Finally, the dependence of the modern world on information and communication technologies carries the danger that cyber incidents may escalate into "real-life" conflict.

Traditional political-military strategies, predating modern information and communication technologies, account for these risks inadequately at best. This makes alternative approaches to enhancing security ever more important: increasing cyber-resilience, agreeing laws and rules that apply to the use of information and communication technology, and engaging in confidence -building measures.

Cyber-resilience often gets deferred or is even left entirely off the agenda. This may be the result of political priority-setting in light of scarce resources, of a more or less informed risk assessment, or of uncertainty on how to address risks associated with the use of modern information and communication technology. Work is needed on this front.

There has been welcome progress in 2013 concerning the laws and rules that apply to the use of information and communication technology: The last UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications (GGE), in its June 2013 report to the UN Secretary General, has made clear that international law, and in particular the UN Charter, is applicable to cyberspace and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. At the same time, the GGE found that state sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory. Germany is looking forward to how the new GGE will take this further.

Concerning confidence-building measures, the Organization for Security and Cooperation in Europe made important progress in December 2013, with the adoption of a first set of steps to increase interstate co-operation, transparency, predictability, and stability, with a view to reducing the risks of misperception, escalation, and conflict that may stem from the use of information and communication technologies. The OSCE agreement might be useful as a model for other regional organizations as well.

Efforts taken at the national level

In 1991, the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) was established as the first and foremost central information technology security service provider for the Federal Government. In this function, BSI publishes mandatory minimum information technology security standards for the federal administration and serves as its central information technology incident reporting office. It also operates as a neutral office for consultation and support in the field of information technology security. Major achievements of the work done by the office were, for example, the Information Technology Security Management Standard (IT-Grundschutz) and the establishment in 1994 of a computer emergency response team for federal agencies (CERT-Bund) as a platform for incident handling and information exchange. Since 2006, a Citizen's Computer Emergency Response Team (Bürger-CERT), serves as a cyber-security partner to society as a whole and works on raising awareness.. BSI also issues warnings on malware and security vulnerabilities in information technology products and services, informs concerned parties (including information technology vendors and the general public), and recommends countermeasures.

The 2005 National Plan for the Protection of Information Infrastructures, directed at both government and industry, was followed by the national Cyber Security Strategy, which the Federal Government adopted in February 2011.
The Cyber Security Strategy proceeds from the assertion that the availability of cyberspace and the integrity, authenticity and confidentiality of data in cyberspace have become vital questions of the 21st century. Ensuring cyber security has turned into a central challenge for the state, business, and society. The Strategy goes on to explain that ensuring cyber security requires efforts by the state both at the national level and in cooperation with international partners. Given the shared responsibilities of the state, industry, and society, the Cyber Strategy will only be successful if all

stakeholders act as partners and fulfil their tasks together. The Cyber Security Strategy sets out the following objectives and measures:

- Protecting critical information infrastructures,
- Securing IT systems in Germany,
- Strengthening IT security in public administration,
- Running a national cyber response centre,
- Establishing a national cyber Security council,
- Effective crime control in cyberspace,
- Effective coordinated action to ensure cyber security in Europe and worldwide,
- Using reliable and trustworthy information technology,
- Personnel development in federal authorities, and
- Tools to respond to cyber-attacks.

Since 2008, the German Government and German critical infrastructure operators have been cooperating in a public private partnership. This “CIP Implementation Plan” (UP KRITIS) maintains working groups for different aspects of cyber security, such as crisis management, exercises and availability of critical services.

The National Information Technology Situation Centre (Nationales IT-Lagezentrum), operated by the BSI, keeps track of the national and global information technology security situation, in order to rapidly detect and analyze major information technology security incidents and recommend protective measures. In case of an information technology-related crisis, it expands its capacity and is transformed into the National Information Technology Crisis Reaction Centre (Nationales IT-Krisenreaktionszentrum). This center concentrates capabilities for handling information technology crises, covering all national aspects, including governmental networks and critical infrastructures.

In keeping with the 2011 Cyber Security Strategy, all Government authorities that deal with cyber security issues work closely and directly with each other and with the private sector within the National Cyber Response Centre (Nationales Cyber-Abwehrzentrum), which is led and hosted by BSI.

With regard to policy, the National Cyber Security Council (Nationaler Cyber-Sicherheitsrat) at the State Secretary level addresses key cyber security issues. This includes aspects of foreign, defense, economic and security policy. In support of this comprehensive policy, a platform for cooperation and information exchange was initiated in October 2012: The Alliance for Cyber Security (Allianz für Cybersicherheit) facilitates close cooperation between partners in the economic, academic and administrative fields and, in particular, with enterprises of special public interest.

Following the German general election in the fall of 2013 and according to the guidelines for the legislative period up to 2017 set out in the Coalition Agreement, cyber security is high on the government agenda. Technology continues to be a key topic. Data privacy standards will be on the rise and businesses are well advised to closely monitor and assess them. Lead topics for the next four years include a variety of government commitments such as: adoption of an EU General Data Protection Regulation; better consumer protection by mandatory reports from software providers in case they become aware of malicious codes affecting users’ IT systems; amendments to the criminal laws to better protect individuals against cyber mobbing,

cyber grooming and phishing; the passing of an IT security law with mandatory minimum IT security standards for critical infrastructures in order to improve their resilience; mandatory reporting of security incidents to the Federal Office for Information Security; and the obligation of all federal authorities to invest 10 percent of their IT budget to improve the security of their systems.

As a consequence of concerns about unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data by third parties, the German government strongly encourages IT service providers to encrypt telecommunication and not to forward telecommunication data to foreign intelligence services.

Confidence- and security-building measures in cyberspace

Since 2011, Germany has been supporting projects on international cyber security and confidence- and security-building measures carried out by the United Nations Institute for Disarmament Research (UNIDIR).

The first Berlin Cyber Conference, held in December 2011, provided a platform for international discussion on risks, strategies and confidence-building in international cyber security. The second Berlin Cyber Conference, held in September 2012, focused on the Internet and human rights. An important conclusion was that security, freedom and privacy online are complementary concepts. On 27 and 28 June 2013, the third Berlin Cyber Conference, held on the theme “Securing the Freedom and Stability of Cyberspace: The Role and Relevance of International Law”, and organized by the Federal Foreign Office in close cooperation with the University of Potsdam, endeavored to provide international legal assessments of cyber operations not transgressing the threshold of armed attack and thus not engaging the law of armed conflict. In December 2014, the German Foreign Office and the EastWest Institute, a non-governmental organization, will co-host the fifth “Cyber Cooperation Summit”. This event will bring together policymakers, business leaders, technical experts and civil society with the aim of identifying ways to mitigate the negative consequences of growing internet fragmentation, resulting from national policies on the flow of information and the handling of data, which is endangering economic growth and international security.

The Organization for Security and Cooperation in Europe has been discussing cyber security issues for several years, including in an informal working group established in 2012. Germany has actively participated in these activities from the outset. In December 2013, the OSCE Council of Ministers approved a first set of confidence-building measures. Participating States agreed, inter alia, on the following voluntary steps:

- Providing their national views on various aspects of national and transnational threats to and in the use of Information and Communication Technologies;
- Facilitating co-operation among the competent national bodies and exchanging information;
- Holding consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of Information and Communication Technologies;

- Sharing information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet , and on their national organization; strategies; policies and programs;
- Using the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building;
- Nominating contact points; and
- Providing a list of relevant national terminology.

OSCE Participating States also agreed that they will, at the level of designated national experts, meet at least three times each year, to discuss information exchanged and explore appropriate development of CBMs. Germany welcomes this agreement which demonstrates the OSCE's capacity to act in the field of security in the use of information and communication technology. It will be important now not just to implement faithfully what has been agreed upon, but to develop further confidence-building measures.

Military aspects of cyber security

As military forces, too, increasingly rely on information technology to master ever more complex scenarios at all levels of command, the protection of the information and the means to process it has become a primary task.

However, in military thinking, information security is challenged not only by a potential adversary, in an operational understanding, using weaponry for the physical destruction of information infrastructure, but also by irresponsible users, malfunctioning technology, criminals or simply accidents. Hence the efforts to be undertaken range from raising awareness of each single user and securing the trustworthiness of the supply chain for information technology, to responsive defenses to fend off cyber-attacks and establish an overall resilient information technology architecture. In essence, comprehensive risk management is required, with measures to strengthen information security on a national and global scale.

At an early stage, the German armed forces (Bundeswehr) established resilient command and control architectures, security techniques and procedures, and an information technology-security organization, encompassing all branches of the armed forces, and including an independent computer emergency response team with the capacity to intervene in case of critical disruptions to the operations of information technology. Adapting personal and technical abilities to the continually increasing level of threat is an ongoing task.

The German armed forces are collaborating closely with the Federal German Ministry of the Interior in its efforts. They strongly support the strengthening of information security in the North Atlantic Treaty Organization (NATO) and the European Union, and the formation of policies and better coordination of capacities to this end. Furthermore, the armed forces hold regular exchanges with a number of countries in the context of information security, both at the political and working levels.

The German armed forces welcome initiatives and work together with other departments of the Federal German Government on international efforts in order to better protect the utility of worldwide information networks.

Cyber defense in NATO

Cyber security has been identified by NATO as one of the key emerging security challenges. The strategic concept adopted by Heads of State and Government at the NATO summit held in November 2010 in Lisbon, stated that “cyber-attacks ... can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability”.

As tasked in the Summit Declaration, NATO Defense Ministers adopted a NATO policy on cyber defense and a cyber-defense action plan in June 2011. Since then, NATO has been continuously implementing the action plan.

The policy focuses on the protection of NATO networks and national networks of member States that are connected to NATO networks or process NATO information for core alliance tasks (including the development of common principles and criteria to ensure a minimum level of cyber defense in all member States). To reduce the global risks emanating from cyberspace, NATO intends to cooperate with partner nations, relevant international bodies such as the United Nations and the European Union, the private sector, and academia.

Germany welcomes the commitment of NATO regarding cyber security and actively supports these discussions.