Cyber Security Strategy for Germany

Contents:

Introduction

Cyberspace includes all information infrastructures accessible via the Internet beyond all territorial boundaries. In Germany all players of social and economic life use the possibilities provided by cyberspace. As part of an increasingly interconnected world, the state, critical infrastructures, businesses and citizens in Germany depend on the reliable functioning of information and communication technology and the Internet.

Malfunctioning IT products and components, the break-down of information infrastructures or serious cyber attacks may have a considerable negative impact on the performance of technology, businesses and the administration and hence on Germany's social lifelines. 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 thus turned into a central challenge for the state, business and society both at national and international level. The Cyber Security Strategy is intended to improve the framework conditions in this area.

IT threat assessment

In recent years attacks against information infrastructures have become ever more frequent and complex, while at the same time perpetrators have become more

professional. Cyber attacks are launched both from Germany and abroad. Given the openness and extent of cyberspace it is possible to conduct covert attacks and misuse vulnerable systems as tools for an attack. In view of technologically sophisticated malware the possibilities of responding to and retracing an attack are rather limited. Often attacks give no clue as to the identity and the background of the attacker. Criminals, terrorists and spies use cyberspace as a place for their activities and do not stop at state borders. Military operations can also be behind such attacks. The trend to develop information systems for industry on the basis of standard components and connect them to cyberspace, which is motivated mainly by economic concerns, entails new vulnerabilities. Experience with the Stuxnet virus shows that important industrial infrastructures are no longer exempted from targeted IT attacks.

Given the increasing complexity and vulnerability of information infrastructures the cyber security situation will remain critical also in the future. In Germany, the public and the private sector as well as society at large are all equally affected by targeted or coincidental IT failures.

Framework conditions

Ensuring cyber security, enforcing rights and protecting critical information infrastructures require major efforts by the state both at national level and in cooperation with international partners. Given the shared responsibilities of the state, the industry and the society a cyber security strategy will only be successful if all players act as partners and fulfil their tasks together. The same applies to the international context.

Since IT systems are interconnected in global networks, incidents in other countries' information infrastructures may also indirectly affect Germany. For this reason, strengthening cyber security also requires the enforcement of international rules of conduct, standards and norms. Only a mix of domestic and external policy measures will be appropriate for the dimension of the problem. Cyber security can be improved by enhancing the framework conditions for drawing up common minimum standards (code of conduct) with allies and partners. Fighting the rapid growth of cybercrime requires close cooperation between law enforcement authorities worldwide.

Basic principles of the Cyber Security Strategy

The Federal Government aims at making a substantial contribution to a secure cyberspace, thus maintaining and promoting economic and social prosperity in Germany. Cyber security in Germany must be ensured at a level commensurate with the importance and protection required by interlinked information infrastructures, without hampering the opportunities and the utilization of the cyberspace. In this context the level of cyber security reached is the sum of all national and international measures taken to protect the availability of information and communications technology and the integrity, authenticity and confidentiality of data in cyberspace. Cyber security must be based on a comprehensive approach. This requires even more intensive information sharing and coordination. The Cyber Security Strategy mainly focuses on civilian approaches and measures. They are complemented by measures taken by the Bundeswehr[1] to protect its capabilities and measures based on mandates to make cyber security a part of Germany's preventive security strategy. Given the global nature of information and communications technology, international coordination and appropriate networks focusing on foreign and security policy aspects are indispensable. This includes cooperation not only in the United Nations, but also in the EU, the Council of Europe, NATO, the G8, the OSCE and other multinational organizations. The aim is to ensure the coherence and capabilities of the international community to protect cyberspace.

Strategic objectives and measures

With the present Cyber Security Strategy the Federal Government adapts measures to the current threats on the basis of the structures established by the CIP implementation plan and the implementation plan for the federal administration. The Federal Government will specifically focus on ten strategic areas:

1. Protection of critical information infrastructures

The protection of critical information infrastructures is the main priority of cyber security. They are a central component of nearly all critical infrastructures and become increasingly important. The public and the private sector must create an enhanced strategic and organizational basis for closer coordination based on intensified information sharing. To this end, cooperation established by the CIP implementation plan is systematically extended, and legal commitments to enhance the binding nature of the CIP implementation plan are examined. With the participation of the National Cyber Security Council (cf. objective 5), the integration of additional sectors is examined and the introduction of new relevant technologies is

[1] German Army

considered to a greater extent. Whether and where protective measures have to be made mandatory and whether and where additional powers are required in case of specific threats have to be clarified, too. Furthermore we will examine the necessity of harmonizing rules to maintain critical infrastructures during IT crises.

2. Secure IT systems in Germany

Infrastructure protection requires more security with regard to IT systems used by citizens and small and medium-sized businesses. Users need appropriate and consistent information on risks related to the use of IT systems and on security measures they can take to use cyberspace in a secure manner. We will organize joint initiatives with groups from society to pool information and advice consistently. Furthermore we will examine whether providers may have to assume greater responsibility and make sure that a basic collection of appropriate security products and services are made available to users by providers. We want to provide specific incentives and funds for basic security functions certified by the state (e.g. electronic proof of identity or De-mail) to be used by the vast majority of citizens.
To support small and medium-sized businesses in the secure use of IT systems, the Federal Ministry of Economics and Technology has set up a task force on “IT security in industry” with the participation of industry.

3. Strengthening IT security in the public administration

The public administration will further enhance the protection of its IT systems. State authorities have to serve as role models for data security. We will create a common, uniform and secure network infrastructure in the federal administration (“federal networks”) as a basis for electronic audio and data communication. We will continue to press ahead with the implementation plan for the federal administration. Should the IT security situation get worse, this plan may be aligned accordingly. Effective IT security requires powerful structures in all federal authorities. For this reason resources must be deployed appropriately at central and local level. To facilitate implementation through uniform action by authorities, joint investments into the Federal Government’s IT security will be made regularly in line with budgetary possibilities. Operational cooperation with the federal *Länder*, particularly with regard to CERTs (computer emergency response teams), will be further intensified by the IT planning council.

4. National Cyber Response Centre

To optimize operational cooperation between all state authorities and improve the coordination of protection and response measures for IT incidents we will set up a National Cyber Response Centre. It will report to the Federal Office for Information Security (BSI) and cooperate directly with the Federal Office for the Protection of the Constitution (BfV) and the Federal Office of Civil Protection and Disaster Assistance (BBK). Cooperation in the National Cyber Response Centre will strictly observe the statutory tasks and powers of all authorities involved on the basis of cooperation agreements. The Federal Criminal Police Office (BKA), the Federal Police (BPOL), the Customs Criminological Office (ZKA), the Federal Intelligence Service (BND), the Bundeswehr and authorities supervising critical infrastructure operators all participate in this centre within the framework of their statutory tasks and powers.

Quick and close information sharing on weaknesses of IT products, vulnerabilities, forms of attacks and profiles of perpetrators enables the National Cyber Response Centre to analyse IT incidents and give consolidated recommendations for action. The interests of the private sector to protect itself against crime and espionage in cyberspace should also be adequately taken into account. At the same time respective responsibilities must be observed. Every stakeholder takes the necessary measures in its remit on the basis of the jointly developed national cyber security assessment and coordinates them with the competent authorities as well as partners from industry and academia.
Since security preparedness is best achieved by early warning and prevention, the Cyber Response Centre will submit recommendations to the National Cyber Security Council both on a regular basis and for specific incidents. If the cyber security situation reaches the level of an imminent or already occurred crisis, the National Cyber Response Centre will directly inform the crisis management staff headed by the responsible State Secretary at the Federal Ministry of the Interior.

5. National Cyber Security Council

The identification and removal of structural causes for crises are considered an important preventive tool for cyber security. For this reason we want to establish and maintain cooperation within the Federal Government and between the public and the private sector within the responsibility of the Federal Government Commissioner for Information Technology more visible and set up a National Cyber Security Council. The Federal Chancellery and a State Secretary from each the Federal Foreign Office, the Federal Ministry of the Interior, the Federal Ministry of Defence, the Federal Ministry for Economics and Technology, the Federal Ministry of Justice, the Federal Ministry of Finance, the Federal Ministry of Education and Resarch and

representatives of the federal *Länder* will participate. On specific occasions additional ministries will be included.
Business representatives will be invited as associated members. Representatives from academia will be involved, if required. The National Cyber Security Council is intended to coordinate preventive tools and the interdisciplinary cyber security approaches of the public and the private sector. The National Cyber Security Council will complement and interlink IT management at federal level and the work of the IT Planning Council in the area of cyber security at a political and strategic level.

6. Effective crime control also in cyberspace

The capabilities of law enforcement agencies, the Federal Office for Information Security and the private sector in combating cyber crime, also with regard to protection against espionage and sabotage, must be strengthened. To improve the exchange of know how in this area we intend to set up joint institutions with industry with the participation of the competent law enforcement agencies, which will act in an advisory capacity. Projects to support partner countries with structural weaknesses will also serve the aim of combating cyber crime. To face up to the growing challenges of global cyber crime activities we will make a major effort to achieve global harmonization in criminal law based on the Council of Europe Cyber Crime Convention. Furthermore, we will examine whether additional conventions in this area may be necessary at UN level.

7. Effective coordinated action to ensure cyber security in Europe and worldwide

In global cyberspace security can be achieved only through coordinated tools at national and international level.
At EU level we support appropriate measures based on the action plan for the protection of critical information infrastructures, the extension and moderate enlargement of the mandate of the European Network and Information Security Agency (ENISA) in view of the changed threat situation in ICT and the pooling of IT competences in EU institutions. The EU Internal Security Strategy and the Digital Agenda provide guidance for further activities.
We will shape our external cyber policy in such a way that German interests and ideas concerning cyber security are coordinated and pursued in international organizations, such as the United Nations, the OSCE, the Council of Europe, the OECD and NATO. An increasingly multilateral approach must be brought in line with the necessity of sovereign evaluation and decision-making powers. In this context, a code for state conduct in cyberspace (cyber code) should be established, which is

signed by as many countries as possible and includes confidence-building security measures. In the G8 framework we are currently working on intensifying anti-botnet activities.

NATO serves as the basis of transatlantic security. Hence, NATO must take cyber security appropriately into account in its entire range of responsibilities. We are in favour of the alliance's commitment to establishing uniform security standards, which Member States may also use for civilian critical infrastructures on a voluntary basis, as foreseen in NATO's new Strategic Concept.

8. Use of reliable and trustworthy information technology

The availability of reliable IT systems and components must be ensured on a permanent basis. The development of innovative protection plans for improved security which take into account social and economic aspects is strongly supported. To this end, we will continue and intensify research on IT security and on critical infrastructure protection. Furthermore we will strengthen Germany's technological sovereignty and economic capacity in the entire range of core strategic IT competences, include them in our political strategies and develop them further. Wherever it makes sense, we will pool our resources with those of our partners and allies, particularly in Europe. We are in favour of diversity in technology. Our aim is to use components in critical security areas which are certified against an international recognized certification standard

9. Personnel development in federal authorities

Given the strategic importance of cyber security, it must be examined as a priority whether additional staff is necessary in authorities in the interest of cyber security. Furthermore, intensified personnel exchange between federal authorities and appropriate further training measures will enhance interministerial cooperation.

10. Tools to respond to cyber attacks

If the state wants to be fully prepared for cyber attacks, a coordinated and comprehensive set of tools to respond to cyber attacks must be created in cooperation with the competent state authorities. We will continue to assess the threat situation regularly and take appropriate protection measures. If necessary, we have to examine whether additional statutory powers must be created at federal or *Länder* level. Above all, the aims, mechanisms and institutions mentioned above must be internalized through a permanent exercise process with the relevant federal and *Länder* authorities as well as businesses.

Sustainable implementation

With the implementation of the strategic objectives and measures the Federal Government contributes to ensuring cyber security and thus to freedom and prosperity in Germany.

A lot will depend on whether we succeed at international level in taking effective measures to protect cyberspace.

The information technologies used are subject to short innovation cycles. This means that the technical and social aspects of cyberspace will continue to change and bear not only new opportunities, but also new risks. For this reason the Federal Government will regularly review whether the aims of the Cyber Security Strategy have been achieved under the overall control of the National Cyber Security Council and will adapt the strategies and measures to the given requirements and framework conditions.

Abbreviations

BBK	Federal Office of Civil Protection and Disaster Assistance
BfV	Federal Office for the Protection of the Constitution
BKA	Federal Criminal Police Office
BMI	Federal Ministry of the Interior
BND	Federal Intelligence Service
BPOL	Federal Police
BSI	Federal Office for Information Security
CERT	Computer Emergency Response Team
ENISA	European Network and Information Security Agency
EU	European Union
G8	Group of leading industrialized nations in the world (Germany, USA, Japan, United Kingdom, Canada, France, Italy and the Russian Federation)
IT	Information technology
CIP	Critical infrastructure protection
NATO	North Atlantic Treaty Organization
OSCE	Organization for Security and Co-operation in Europe
ZKA	Customs Criminological Office

End of Cabinet decision

Definitions
(Explanations and terminology used in this document)

Definition: “Cyberspace”
Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace.

Definitions: “Cyber attack”, “cyber espionage” and “cyber sabotage”
A cyber attack is an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability may all or individually be compromised. Cyber attacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services, are called cyber espionage. Cyber attacks against the integrity and availability of IT systems are termed cyber sabotage.

Definitions: “Cyber security” and “civilian and military cyber security”
(Global) cyber security is the desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum. Hence, cyber security in Germany is the desired objective of the IT security situation, in which the risks of the German cyberspace have been reduced to an acceptable minimum. Cyber security (in Germany) is the sum of suitable and appropriate measures.
Civilian cyber security focuses on all IT systems for civilian use in German cyberspace. Military cyber security focuses on all IT systems for military use in German cyberspace.

Definition: “Critical infrastructures”
Critical infrastructures are organizations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences.

At federal level, the following areas have been identified:

- Energy
- Information technology and telecommunication
- Transport

- Health
- Water
- Food
- Finance and insurance sector
- State and administration
- Media and culture