REPUBLIK ÖSTERREICH

Austrian Cyber Security Strategy

BUNDESKANZLERAMT ÖSTERREICH

Bundesministerium für europäische
und internationale Angelegenheiten

BM.I REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES

Bundesministerium
für Landesverteidigung
und Sport

Austrian Cyber Security Strategy

Vienna, 2013

Publishing information:

Media owner, publisher, editor:
Federal Chancellery of the Republic of Austria
Department IV - Coordination
Division IV/6 – Security Policy Affairs
Ballhausplatz 2, 1014 Vienna

Graphic design: Federal Chancellery | ARGE Grafik
Vienna, March 2013

Table of Contents

1 Introduction

The digital revolution has been gaining ground in all spheres of life of the modern world. And more than ever, post-industrial societies and highly developed countries are taking advantage of cyber space for their technological, economic, social, cultural, scientific and political development. Digital infrastructures are becoming the backbone of a successful economy, a vibrant research community, a transparent state as well as a free society. The development of modern information and communication technologies – above all the Internet – has transformed our social and economic life radically. In Austria about three quarters of the population use the Internet regularly, and half of this group does so on a daily basis.

The economy depends increasingly on effective digital infrastructures with regard to its technological further development and the efficiency of internal procedures. The public administration does no longer rely exclusively on traditional channels of service delivery but considers the Internet indispensable for reaching out to the general public.

The citizens must have confidence that their data will be received by the addressees fast and reliably. An open and free Internet, the protection of personal data as well as the integrity of interconnected networks are the basis for global prosperity, security and the promotion of human rights.

Effective digital infrastructures are a prerequisite for providing services of general interest such as energy, water and transport to the population. To allow citizens to realise the benefits promised by our globalised and digitised world, digital infrastructures must function reliably and securely.

Attacks from cyber space[1] pose a direct threat to our safety and the proper functioning of the state, economy, science and society. They may have a profound negative impact on our daily lives. Non-state actors (e.g. criminals, organised crime or terrorists) as well as state actors (e.g. secret services and the military) may misuse cyber space for their own purposes and interfere with its proper functioning. Both the threats in cyber space and the productive use of cyber space are practically infinite. It is therefore a top priority of Austria to help make cyber space sufficiently safe and secure at national and international level. The term “cyber security” stands for the security of infrastructures in cyber space, of the data exchanged in cyber space and above all of the people using cyber space.

It is a paramount common concern of the state, the economy and society to ensure cyber security in national and international contexts. The Austrian Cyber Security Strategy/ ACSS (Österreichische Strategie für Cyber Sicherheit/ÖSCS) is a comprehensive and proactive concept for protecting cyber space and the people in virtual space while guaranteeing human rights. It will enhance the security and resilience of Austrian infrastructures and services in cyber space. Most importantly, it will, however, build awareness and confidence in the Austrian society.

[1] The terms “cyber space” and “virtual space” are used synonymously.

Austria's Cyber Space Security Strategy has been developed on the basis of the Security Strategy[2] and is guided by the principles of the Austrian Programme for Critical Infrastructure Protection[3].

[2] Decision of the Council of Ministers of 1 March 2011

[3] Decision of the Council of Ministers of 2 April 2008

2 Opportunities and risks in cyber space

2.1 Opportunities

Cyber space has developed into a vital area of activity for the state, the economy, science and society. It is important for all of them as a(n):

Information and communication space: Cyber space makes it possible to disseminate and transmit different sets of data and information resources. It is growing at a rapid pace: worldwide every minute about 204 million e-mails are sent, more than two million Google searches are conducted, Facebook is logged in six million times and more than 70 new domains are registered[4].

Space for social interaction: Cyber space is a space of general social interaction which is used by people for socialising. Today there are more than two billion Internet users globally.

Economic and trade space: Cyber space has developed into a market place of strategic importance in a relatively short period of time. Based on estimates, the global e-commerce volume could almost double between 2012 (US $ 572 billion) and 2014.

Space for political participation: Cyber space has an impact on the relationship between the government and society. The state reaches the citizens through e-government, offering facilitated access to government services. Digital forms of interaction open up new opportunities for political participation and political expression. The prerequisite for achieving this goal is to guarantee all human rights – both in virtual space and offline.

Control space: The role of cyber space as a control space is closely connected to its function as an information space. By using this control space, it is practically possible to monitor, operate and maintain all infrastructures of the transport, economic, industrial, health and educational sectors. Based on estimates, up to 50 billion devices will be able to communicate with one another (“Internet of Things“) by 2020. It will therefore be all the more important to ensure the security of this communication.

2.2 Risks and threats

Cyber space as well as the security and safety of people in cyber space are exposed to a number of risks and threats as cyber space is also a space of criminal misuse. These risks and threats range from operating errors to massive attacks by state and non-state actors using cyber space as a venue for their activities, which is not limited by national borders; military operations may also be behind these attacks. The spectrum of these risks and threats is presented in the Cyber Risk Matrix in Annex 1. Cyber crime, identity fraud, cyber attacks or misuse of the Internet for extremist purposes are serious new challenges facing all the stakeholders affected, requiring broad cooperation of governmental and non-governmental bodies at national and international level.

[4] Sources of all the data contained in this chapter: Intel and KSÖ White Paper – Cybersicherheit intelligent regulieren; warum, wie und durch wen?“

3 Principles

State-of-the-art cyber security policy is a cross-cutting issue which has to be taken into account in many spheres of life and policy. It must be modelled based on a **comprehensive** and **integrated** approach, allow for **active** participation and must be implemented in the spirit of **solidarity**.

A **comprehensive cyber security policy** means that external and internal security as well as civilian and military security aspects are closely interlinked. Cyber security goes beyond the purview of traditional security authorities and comprises instruments of numerous other policy areas.

An **integrated cyber security policy** must place emphasis on task-sharing between the state, the economy, academia and the civil society. It comprises measures in the following areas: political-strategic management, education and training, risk assessment, prevention and preparedness, recognition and response, limitation of effects and restoration as well as the development of governmental and non-governmental capabilities and capacities. An integrated cyber security policy has to be based on a cooperative approach both at national and international level.

A **proactive cyber security policy** means to work towards preventing threats to cyber space and the people in cyber space or mitigating their impact (configuring security).

A **cyber security policy based on solidarity** takes account of the fact that – due to the global nature of cyber space – today the cyber security of Austria, the EU and the entire community of nations is interconnected very closely. Intensive cooperation based on solidarity at European and international level is therefore required to ensure cyber security.

The universal **Principles of ICT Security for a Digital Austria** are fully applicable to cyber security: **confidentiality, integrity, mandatory application, authenticity, availability as well as privacy and data protection**[5].

The following **fundamental principles** are in any case applicable to the area of cyber security:

The rule of law: Governance in the area of cyber security has to meet the high standards of the rule of law of the Austrian administration and guarantee **compliance with human rights,** in particular privacy and data protection as well as the freedom of expression and the right to information.

Subsidiarity: Cyber security is a legal asset. Therefore the state pledges it strong commitment to the protection of this legal asset. However, it cannot and should not assume sole responsibility for protecting cyber space. The owners and operators of information and communication technology (ICT) are primarily responsible for protecting their systems. The following principle shall apply: “Self-commitment if possible, regulation if necessary“.

Self-regulation: Efforts should in general be made to increase the level of protection through the actors’ own initiatives on the basis of code of conducts, standardisation and certification.

[5] See:http://www.digitales.oesterreich.gv.at/site/5743/default.aspx#a2

However, it remains the task of the state to create the regulatory framework for protecting the ICT of enterprises and private persons and to support self-regulation in the private sphere.

Proportionality: Measures to increase the level of protection and the respective costs have to be proportionate to the respective risk and to the possibilities of limiting these threats.

Based on these principles, a comprehensive and coherent **cyber security policy** is developed, which comprises all measures at national, European and international level

- to help shape cyber space in a positive way in the interest of the citizens, academia and the state,
- to prevent threats to cyber space and the people in cyber space from emerging or becoming effective ("prevention") as well as
- to protect the legal asset "cyber security" against threats as well as to cope with them.

4 Strategic goals

As Austria continues to develop into a **digital society**, it is vital to ensure compatibility with the **fundamental values of an open society**. A dynamic virtual space facilitates social prosperity and economic benefits in the framework of e-government and e-commerce. Moreover, it serves as a **basis for information exchange as well as social and political participation**.

In the framework of its Cyber Security Strategy, Austria pursues the following **strategic goals**:

- Availability, reliability and confidentiality of data exchange as well as the integrity of data themselves are guaranteed only in a **secure, resilient and reliable cyber space**. Therefore the virtual space must be capable of resisting risks, absorbing shocks and adjusting to a changed environment. The design of crucial ICT systems should be as redundant as possible.
- Based on the **national approach of the competent federal ministries**, Austria will ensure that its **ICT infrastructures** are secure and resilient to threats. The governmental bodies will cooperate closely and as partners with the private sector.
- The **legal asset "cyber security"** is protected by the Austrian authorities – in cooperation with non-governmental partners – by taking effective and proportionate measures in the field of political-strategic control, recognition and response as well as limitation of effects and restoration.
- By taking a number of **awareness measures**, Austria is building a **"culture of cyber security"**.
- In the framework of a national dialogue on cyber security, existing cooperation is strengthened and new initiatives are supported and interlinked by building knowledge, capabilities and capacities. Thanks to this approach, Austria is acting as a **pioneer in implementing measures to secure the digital society**. Offering high levels of availability, integrity and confidentiality of required ICT infrastructures, Austria's attractiveness as a business location is also enhanced.
- Austria will play an **active role in international cooperation** at European and global level, particularly by exchanging information, formulating international strategies, developing voluntary schemes and legally binding regulations, prosecuting criminal cases, holding transnational exercises and conducting cooperation projects.
- The Austrian administration's **e-government** is secure and continuously further developed; the security measures of the Federal Republic of Austria, the federal provinces, cities and municipalities will be strengthened.
- All **Austrian enterprises** will protect the integrity of their own applications as well as the identity and privacy of their customers. The close and systematic cooperation among enterprises plays a crucial role in this process.
- The **Austrian population** should be aware of the individual's personal responsibility in cyber space. All citizens should ensure adequate protection of their online activities and have the necessary capabilities for electronic authentication and signature.

5 Fields of action and measures

Field of action 1 – structures and processes

Objective:

Within cyber space there are numerous structures and stakeholders which are working individually to ensure cyber security. Several organisations specialised in cyber security (e.g. CERTs[6]) are already playing an important role in cyber crisis management. Overarching cyber security procedures have not yet been defined formally. It is therefore necessary to define processes and structures which will ensure overall coordination both at the political-strategic level and the operational level by involving all relevant stakeholders of the public and private sectors.

Measures:

1) Establishing a Cyber Security Steering Group

- The **Cyber Security Steering Group** was set up based on a decision of the Council of Ministers of 11 May 2012. Under the leadership of the Federal Chancellery, it is responsible for coordinating measures relating to cyber security at a political-strategic level, monitoring and supporting the implementation of the ACSS, preparing an annual Cyber Security Report and advising the federal government in all matters relating to cyber security. The Steering Group is composed of liaison officers for the National Security Council[7] and cyber security experts of the ministries represented in the National Security Council. The Chief Information Officer of the Federal Republic of Austria is also a member of this body. Representatives of other ministries (particularly those competent for organisations and enterprises which are subject to or affected by control measures) and of the Austrian federal provinces will join the Steering Group as required to address specific issues. Representatives of relevant enterprises will be involved in an appropriate manner.

2) Creating a structure for coordination at operational level

- Building on and taking advantage of existing operational structures, a **structure for coordination at operational level** will be created. It will serve as a platform for preparing a periodic and incident-related **Cyber Security Picture** and for deliberations on measures to be taken at operational level. Furthermore, it will provide an overview of the status quo in cyber space by collecting, compiling, evaluating and passing on relevant information. The economic sector should also be involved appropriately and on an equal footing. The survey of the situation in cyber space will be prepared in a joint and ongoing process and will serve as a basis for the planning, preventive and response measures to be taken. The operators of critical infrastructures will be supported at operational level and particularly in the event of failures of information and communication structures. In addition, they will be provided with information on the dangers of the Internet. The Operational Coordination Structure must be designed in such a way that it can be used as an operational executive body of the overall cyber crisis management.

[6] Computer Emergency Response Team

[7] Federal Act on the Establishment of a National Security Council, Section 5(1)

- The tasks performed in the framework of the **Operational Coordination Structure** are coordinated by the Federal Ministry of the Interior (PPP model) by involving the ministries and the operational structures of the business and research sectors. In carrying out its coordination tasks, it is supported at operational level by the Federal Ministry of Defence and Sports, to which coordination tasks will be transferred if a cyber defence incident occurs. All operational organisation-/ sector-/ or target-group-specific structures will remain within the purview of the respective organisation. Institutions dealing with security issues of computer systems and the Internet as well as the protection of critical infrastructures will cooperate in the framework of the Operational Coordination Structure. At state level, these organisations are in particular: GovCERT (Government Computer Emergency Response Team), MilCERT (Military Cyber Emergency Readiness Team) and the Cyber Crime Competence Center (C 4). Other governmental institutions are involved by forming a second circle. An additional circle comprises private CERTs (CERT.at, BRZ-CERT, banks, ...) as well as the economic and research sectors.
- The Cyber Security Steering Group will set up a **working group**. It will be in charge of preparing proposals for processes and structures for permanent coordination at operational level. Representatives of relevant enterprises will be involved in the appropriate manner.

3) Establishing a Cyber Crisis Management

- Austria's **Cyber Crisis Management** consists of representatives of the state and of operators of critical infrastructures. As far as its composition and work procedures are concerned, it is modelled on the Governmental Crisis and Civil Protection Management (Krisen- und Katastrophenmanagement/SKKM). As its responsibility goes beyond ICT and to ensure internal security, the Federal Ministry of the Interior will be responsible for coordinating it in respect of overarching threats. As far as external security is concerned, the Federal Ministry of Defence and Sports will play the leading role in coordinating measures to protect sovereignty in the framework of military national defence (cyber defence).
- **Crisis management and continuity plans** are prepared and updated regularly on the basis of risk analyses for sector-specific and cross-sectoral cyber threats in cooperation with public institutions and the operators of critical infrastructures.
- Regular **cyber exercises** will be held to test the Cyber Crisis Management as well as crisis and continuity plans.

4) Strengthening existing cyber structures

- The role of **GovCERT** (operated by the Federal Chancellery as the government's CERT) will be enhanced and strengthened. To this end, it will be necessary to lay down in detail its responsibilities, powers and spheres of action, its institutional embedding within the public administration, its role in the event of crisis as well as its interaction with the Operational Coordination Structure. In addition, new requirements will have to be defined.
- To avoid and prevent cyber crime as well as to facilitate operational international cooperation in this area, the role of the **Cyber Crime Competence Center** (**C 4**) of the Federal Ministry of the Interior will be enhanced. The Center is Austria's central body in charge of exercising security and criminal police duties in the area of cyber security.
- As a basis of operational capabilities for the prevention of cyber attacks, **MilCERT** (set up within the Federal Ministry of Defence and Sports) will be strengthened to protect its own networks and to further develop the Cyber Security Survey. By taking advantage of these capabilities, capacities for providing assistance in the ICT area will inter alia have to be established.

- The Austrian **CERT Association** will be expanded and **CERT.at** will be strengthened to facilitate national cooperation among Austrian CERTs. This will help to promote the establishment of CERTs in all sectors on the one hand and to intensify the exchange of information and experience on CERT-specific issues on the other hand.

Field of action 2 - governance

Objective:

The aim is to define the role, responsibilities and powers of state and non-state actors in cyber space and to create adequate framework conditions for cooperation among all players.

Measures:

5) Establishing a modern regulatory framework

- Under the auspices of the **Cyber Security Steering Group**, a comprehensive report analysing the need to establish an additional **legal basis, regulatory measures** and voluntary **self-commitment** (Code of Conduct) for guaranteeing cyber security in Austria will be prepared and submitted to the federal government. This report will inter alia cover the following issues: the establishment of necessary organisational structures, the tasks and powers of authorities, the information exchange between authorities and private persons, reporting duties, the duty of adopting protection measures as well as supply chain security.
- A **balance between incentives and sanctions** must be ensured in defining the duties of non-state actors.

6) Defining minimum standards

- Based on the interaction of all relevant stakeholders, **minimum security standards** must be defined to ensure effective prevention and to achieve a common understanding of current requirements. These requirements will be applied to all components and services used in all security-relevant ICT areas. The applicable norms, standards, codes of conducts, best practises and the like will be compiled in the Austrian **Information Security Management Handbook**, which will be updated regularly.

7) Preparing an annual report on cyber security

- The **Cyber Security Steering Group** will prepare the **annual report "Cyber Security in Austria"**.

Field of action 3 - cooperation between the government, economy and society

Objective:

Many tasks and responsibilities of public administrations, the economy and population are based on information and communication technologies. The responsibility of using digital technology in a prudent way rests with each individual organisational unit. But it is only broad cooperation between all sectors and a permanent mutual exchange of information that will make the use of ICT transparent and safe. It is therefore important to strengthen existing capacities and processes in the administration and economy as well as among citizens through cooperation and to create new opportunities.

Measures:

8) Establishing a Cyber Security Platform

- The **Austrian Cyber Security Platform** shall bee established as a public private partnership to facilitate ongoing communication with all stakeholders of the administration, economy and academia. In parallel, existing initiatives (e.g. Austrian Trust Circle, Cyber Security Austria, Kuratorium sicheres Österreich, A-SIT[8], …) will be carried on and taken advantage of. The Austrian Cyber Security Platform will provide the institutional framework for a permanent exchange of information within the public administration as well as between the public administration and representatives of the economy, science and research. All stakeholders will participate on an equal footing. The Cyber Security Platform advises and supports the Cyber Security Steering Group.
- **Cooperation with private operators of critical infrastructures and other economic sectors** is of crucial importance for Austria's cyber security. The respective details will be discussed in further talks between the Cyber Security Steering Group and the economic sector.
- Extensive **cooperation** will be initiated **between the partners participating** in the Cyber Security Platform on issues such awareness-raising, training as well as research and development.
- To promote the mutual understanding of challenges and opportunities for action of all partners involved in cyber security issues, **exchanges** of experts should be intensified between the participating governmental, private and academic organisations. Under the leadership of the Cyber Security Steering Group and with the support of the Austrian Cyber Security Platform, a programme will be developed for this purpose.

9) Strengthening support for SMEs

- **Priority programmes on cyber security** will be launched to raise the awareness of SMEs and to prepare them for hazardous situations. Interest representations are to be encouraged to publish online information tailored to the needs of SMEs on the new Internet portal ICT Security[9] and to initiate cyber security campaigns for SMEs. With the support of governmental bodies, sector-specific information platforms such as the Austrian Trust Circles should develop sector-specific cyber risk management plans; regulatory authorities and interest representations will be involved in this dialogue. These risk management plans will be coordinated with governmental crisis and continuity management plans. Cross-sectoral cyber exercises for SMEs will be organised and held at periodic intervals. Specific sectors of SMEs should be allowed to participate in governmental cross-sectoral cyber exercises upon request.

10) Preparing a Cyber Security Communication Strategy

- With a view to optimising communication between stakeholders in the administration, economy, academia and society, all websites set up or planned by governmental bodies have to be coordinated in the framework of a Cyber Security Communication Strategy. This **Cyber Communication Strategy** is prepared by the Cyber Security Steering Group by involving all relevant stakeholders.

[8] Secure Information Technology Centre Austria

[9] Compare: Measure 12

Field of action 4 – protection of critical infrastructures

Objective:

Today almost all infrastructures increasingly depend on specialised ICT systems, which are expected to guarantee operations that are as smooth, reliable and continuous as possible. It is therefore a top priority to improve the resilience of these information systems against threats. Under the Austrian Programme for Critical Infrastructure Protection (Programm zum Schutz kritischer Infrastrukturen/APCIP), enterprises operating critical infrastructures are encouraged to implement comprehensive security architectures. The aim of the ACSS is to supplement and intensify these measures in the field of cyber security. Cooperation with operators of critical information infrastructures should be given priority.

Measures:

11) Improving the resilience of critical infrastructures

- The operators of critical infrastructures should be involved in all **processes of national cyber crisis management**. These strategic enterprises should set up a **comprehensive security architecture** (risk and crisis management), update it according to the threats arising and appoint a security officer. **Crisis communication** should be further developed and intensified. Moreover, **cyber security standards** should be defined for these enterprises based on a partnership approach.
- The operators of critical infrastructures should have a duty to report **severe cyber incidents**. The appropriate legal basis has to be established after comprehensive consultations with the relevant stakeholders.
- Existing arrangements for the **protection of critical infrastructures (APCIP)** and the **Governmental Crisis and Civil Protection Management** should be reviewed on an ongoing basis to ensure that they continue to meet new cyber challenges and to modify them if required.

Field of action 5 – awareness raising and training

Objective:

By sensitising all target groups, the necessary awareness of, personal interest in and attention paid to cyber security will be increased. These awareness-raising measures will help to create understanding for the need to ensure cyber security. By taking concrete and target-group-specific measures, the necessary knowledge about security-conscious behaviour and a responsible approach to using information and ICT as a whole will be imparted and promoted. A meaningful and adequate ICT competence level should be ensured by intensifying training in the field of cyber security and media competence in schools and other educational facilities as well as by developing national cyber security competence in the apprenticeship training system.

Measures:

12) Strengthening a cyber security culture[10]

- **Awareness-raising initiatives** are developed, coordinated and implemented on the basis of a common approach by taking into account existing programmes. In this context it is important to examine cyber security from different perspectives, to highlight relevant

[10] See: National ICT Security Strategy, chapter “Awareness”

dangers, to draw attention to possible effects and damages as well as to make recommendations for security measures.

- To give different target groups access to more in-depth customised advice, the existing **consulting programmes** should be further strengthened and expanded.
- An **ICT Security Internet Portal** will be set up in the form of a web platform. It will serve as an information and communication hub for awareness-raising measures. The Ministry of Finance, the Federal Chancellery and A-SIT will be in charge of coordinating the ICT Security Internet Portal. The strategic approach of the Portal will be guided by the principles and objectives of the ACSS.
- **Cyber crime prevention programmes** will be further developed.

13) Incorporating cyber security and media competence into all levels of education and training[11]

- Stronger integration of **ICT, cyber security and media competence into the school curriculum**. ICT and new media literacy has become part of the curriculum of all types of schools. Moreover, ICT security issues and cyber security should become **an integral part of a model for "digital competence"** – adjusted to the curriculum of the respective type of school – so as to create awareness for security issues and to help children learn a responsible use of ICT and new media. The aim is to ensure an adequate ICT competence level across all types of schools.
- ICT (security) competence should be taken into account in the **training programmes of pedagogical universities and other pedagogical institutions at tertiary level** as a prerequisite for teaching these skills at school as well as in adult education centres.
- The **training of experts** in the public sector responsible for improving cyber security will be intensified in cooperation with national and international training facilities.
- The ICT system administrators of the operators of critical infrastructures should receive cyber security training to enable them to **recognise cyber incidents**, to detect anomalies in their ICT systems and to report them to their security officers (**Human Sensor Programme**).

Field of action 6 – research and development

Objective:

To ensure cyber security, technical expertise is necessary, which must be based on state-of-the-art research and development results. To this end, cyber security issues must increasingly be taken into account in applied cyber research as well as in security research programmes such as KIRAS. Efforts should be made to achieve active thematic leadership in EU security research programmes.

Measures:

14) To strengthen Austria's research in the area of cyber security[12]

- In the framework of national and EU security research programmes, **cyber security must** be among the key **research priorities**. In joint projects, the relevant stakeholders in administration, economy and research will develop the conceptual framework and technological instruments to enhance Austria's cyber security standards. Special emphasis will be placed on measures helping to turn research and development findings speedily into marketable products. Existing research projects, such as those under A-SIT, will be further developed.

[11] See: National ICT Security Strategy, chapter "Education and Research"

[12] For more details see: National ICT Security Strategy, chapter "Education and Research"

- Austria should strive for an **active thematic leadership in EU security research programmes.** Austria should contribute themes which it considers important to international research programmes.

Field of action 7 – international cooperation

Objective:

Global networking and international cooperation are key factors of the ACSS. Security in cyber space may be achieved only through a coordinated policy mix at national and international level. Austria will therefore engage in an active "cyber foreign policy" and pursue its interests in the framework of the EU, UN, OSCE, Council of Europe, OECD and NATO partnerships based on a coordinated and targeted approach. Furthermore, the international aspects of Austria's cyber policy will be coordinated consistently in other policy areas.

Measures:

15) Effective collaboration on cyber security in Europe and worldwide

- Austria will make a substantial contribution to the development and implementation of an **EU Cyber Security Strategy**. It will fully participate in the strategic and operational work of the EU[13].
- The competent ministries will take the necessary measures to implement and to take full advantage of the **Convention on Cybercrime of the Council of Europe**.
- Austria advocates a free Internet at international level. The **free exercise of all human rights** must be guaranteed in virtual space, and particularly the right to freedom of expression and information must not be restricted unduly in the Internet. This is the position Austria will adopt in international forums. Hence, Austria will participate actively in developing and establishing a transnational code for governance in cyber space, which will include measures to build confidence and security.
- Austria will continue its bilateral cooperation which has been initiated in the framework of the **NATO Partnership for Peace** and actively support the preparation of a list of concrete confidence- and security-building measures in the **OSCE**.
- Austria participates actively in planning and implementing **transnational cyber exercises.** The experience gained will be used as a direct input for planning and further developing operational cooperation.
- **Foreign policy measures** relevant for cyber security are coordinated by the **Federal Ministry for European and International Affairs**. Where appropriate, the conclusion of bilateral or international agreements will be taken into consideration.

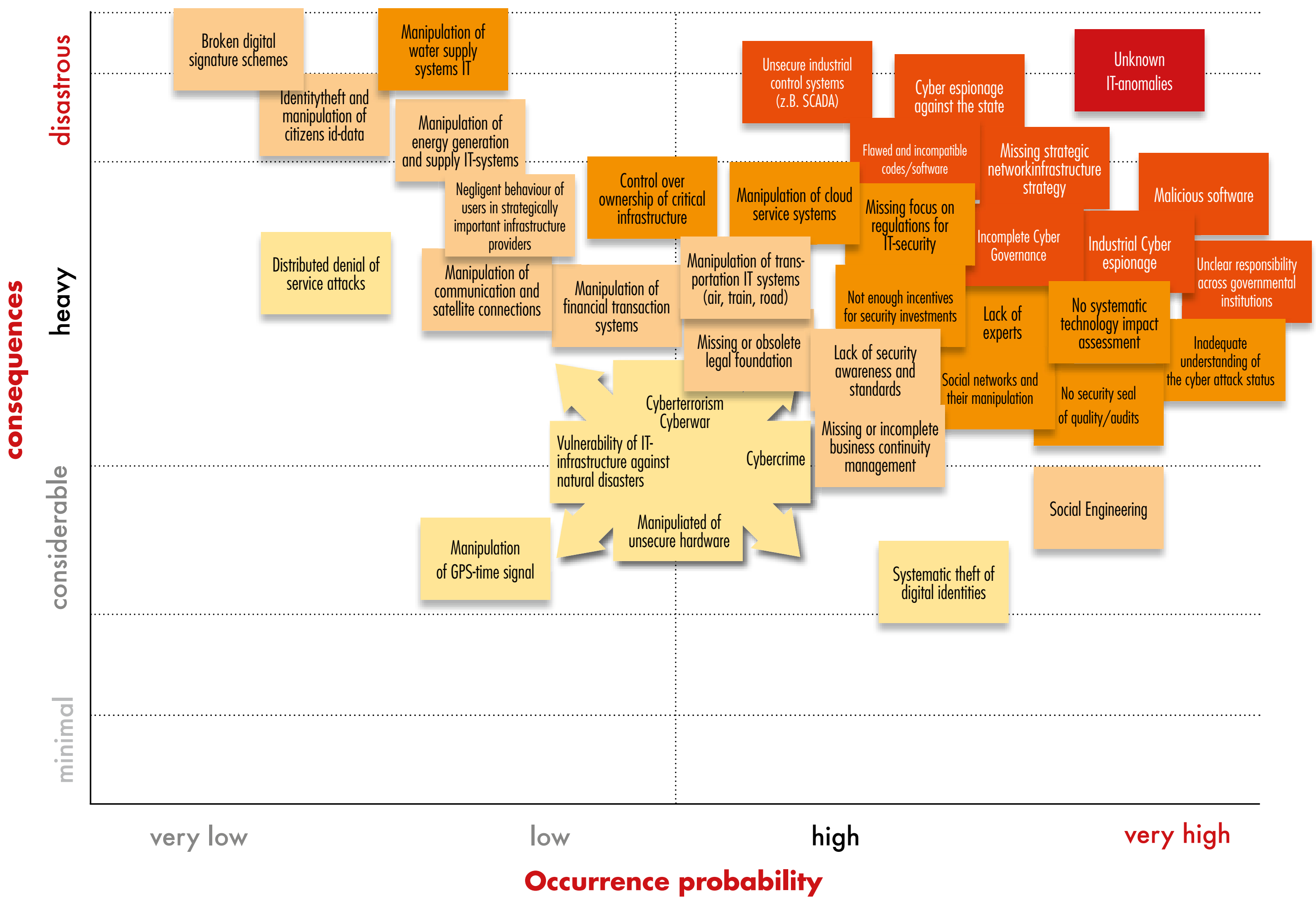
[13] On 7 February 2013 the European Commission presented drafts of the Cyber Security Strategy as well as of the Directive on Network and Information Security.

6 Implementation

The Steering Group develops an **Implementation Plan** to carry out the horizontal measures laid down in the Austrian Cyber Security Strategy within three months after adoption of the ACSS by the federal government. The competent bodies are responsible for **implementing** these measures within their respective mandate. The **implementation of measures** of the ACSS will be coordinated by the Cyber Security Steering Group. Based on the ACSS, the competent ministries will develop **sub-strategies** for their sphere of responsibilities. The ministries represented in the Cyber Security Steering Group will submit an **Implementation Report** to the federal government every two years. The preparation of the Implementation Report will go hand in hand with a review of the Austrian Cyber Security Strategy, which will be revised and updated if necessary. The strategic foundations will be further developed in cooperation with non-state partners.

Annex 1

Cyber Risk Matrix 2011



Annex 2

List of Abbreviations

ACI	Austrian Critical Infrastructure / Österreichische kritische Infrastruktur
ACSS	Austrian Cyber Security Strategy / Österreichische Strategie für Cyber Sicherheit (ÖSCS)
APCIP	Austrian Programme for Critical Infrastructure Protection / Österreichisches Programm zum Schutz kritischer Infrastruktur
A-SIT	Secure Information Technology Centre - Austria / Zentrum für sichere Informationstechnologie – Austria
ASS	Austrian Security Strategy / Österreichischen Sicherheitsstrategie (ÖSS)
CERT	Computer Emergency Response Team
CERT.at	Computer Emergency Response Team - Austria
CII	Critical Information Infrastructures / Kritische Informationsinfrastrukturen
GovCERT	Governmental Computer Emergency Response Team / Staatliches Computer Emergency Response Team
ICT	Information and communication technology
MilCERT	Military Computer Emergency Response Team / Militärisches Computer Emergency Response Team
SCM	Submission to the Council of Ministers / Ministerratsvortrag (MRV)
SMEs	Small and medium-sized enterprises
PPP	Public Private Partnership

Annex 3

Cyber Security Glossary

Awareness

refers to the security awareness of all persons sharing responsibility for information security. Understanding and motivation are necessary to ensure that security rules are observed and implemented on a continuous basis. To remind employees regularly of the importance of their activities for information security, they must be supported through targeted awareness-raising measures.

CERT – Computer Emergency Response Team

refers to an emergency team which will prevent threats and restore ICT systems if security incidents occur.

Basically a CERT/CSIRT provides three types of services:
Emergency response services: making available emergency teams to prevent threats and restore ICT systems if security incidents occur (also referred to as CSIRT, i.e. Computer Security Incident Response Team).
Preventive services: the preventive tasks of a CERT are to observe developments of ICT security, to warn about weaknesses and recognised attack patterns, to provide support in assessing damage and to raise awareness within their sphere of responsibility, especially through training and consulting.
Security quality management: providing a pool of expert know-how, auditing capabilities and a lessons-learned cycle for their respective sphere of responsibility.

Critical infrastructure (CI), critical information infrastructure (CII)

Critical infrastructures are those infrastructures or parts thereof which are of crucial importance for ensuring important social functions. Their failure or destruction has severe effects on the health, security or the economic and social wellbeing of the population or the functioning of governmental institutions[14]. Critical infrastructure is often abbreviated as CI (Critical Infrastructure) even in the German-language area. CIP has become the abbreviation commonly used at international and national level, referring to Critical Infrastructure Protection, while CIIP stands for Critical Information Infrastructure Protection.

Cyber attack, cyber espionage, cyber sabotage

The term “cyber attack” refers to an attack through IT in cyber space, which is directed against one or several IT system(s). Its aim is to undermine the objectives of ICT security protection (confidentiality, integrity and availability) partly or totally. Cyber attacks directed against the confidentiality of an IT system are referred to as “cyber espionage”, i.e. digital spying. Cyber attacks directed against the integrity and availability of an IT system are referred to as cyber sabotage[15].

[14] Source of text: Austrian Programme for Critical Infrastructure Protection (APCIP)

[15] Source of text: definition AG “Cyber” based on: Federal Ministry of the Interior, “Cybersicherheitsstrategie für Deutschland”, Berlin, 2010 + KSÖ: Cyber Risik Matrix – Glossary (partly)

Cyber crime

Cyber crime comprises illegal attacks from cyber space on or through ICT systems, which are defined in penal or administrative laws. The term therefore covers all criminal offences committed with the aid of information technologies and communications networks and also encompasses Internet crime[16].

Cyber defence

The term “cyber defence” refers to all measures to defend cyber space with military and appropriate means for achieving military-strategic goals. Cyber defence is an integrated system, comprising the implementation of all measures relating to ICT and information security, the capabilities of milCERT and CNO (Computer Network Operations) as well as the support of the physical capabilities of the army.

Cyber security

Cyber security describes the protection of a key legal asset through constitutional means against actor-related, technical, organisational and natural dangers posing a risk to the security of cyber space (including infrastructure and data security) as well as the security of the users in cyber space. Cyber security helps to identify, assess and follow up on threats as well as to strengthen the ability to cope with interferences in or from cyber space, to minimise the effects as well as to restore the capacity to act and functional capabilities of the respective stakeholders, infrastructures and services.

Cyber space / virtual space

Cyber space is the virtual space of all IT systems interconnected at data level on a global scale. The basis for cyber space is the Internet as a universal and publicly accessible connection and transport network, which may be supplemented and expanded through other data networks[17]. In common parlance, cyber space also refers to the global network of different independent IC infrastructures, telecommunication networks and computer systems. In the social sphere the use of this global network allows individuals to interact, exchange ideas, disseminate information, give social support, engage in business, control action, create art and media works, play games, participate in political discussions and a lot more. Cyber space has become an umbrella term for all things related to the Internet and for different Internet cultures. Many countries regard networked ICT and independent networks operating through this medium as components of their “national critical infrastructures“.

Cyber terrorism / misuse of the Internet for extremist purposes

Cyber terrorism is defined as a politically motivated crime of state and/or non-state actors against computers, networks and the information stored therein. Its aim is to provoke a severe or long-term disruption of public life or to cause serious damage to economic activity with the intention of severely intimidating the population, of forcing public authorities or an international organisation to carry out, tolerate or omit an act or of profoundly unsettling or destroying the political, constitutional, economic or social foundations of a state or an international organisation. These acts constitute organised cyber sabotage (attacks) caused by political-fundamentalist groups or individual perpetrators; they are directed against states, organisations or enterprises[18].

[16] Source of text: AG “Cyber” + KSÖ: Cyber Risk Matrix - Glossary

[17] Source of text: definition AG “Cyber“ based on: Federal Ministry of the Interior, “Cybersicherheitsstrategie für Deutschland” (Cyber Security Strategy for Germany), Berlin, 2010

[18] Source of text: AG “Cyber” + KSÖ: Cyber Risik Matrix – Glossary

Cyber war

Cyber war refers to acts of war in and around virtual space with means which are predominantly associated with information technology. In a broader sense, this implies the support of military campaigns in traditional operational spaces – i.e. ground, sea, air and outer space – through measures taken in the virtual space. In general, the term also refers to high-tech warfare in the information age based on the extensive computerisation, electronisation and networking of almost all military sectors and issues[19].

Data protection

Every individual has a right to secrecy of his/her personal data, especially in terms of respect for his/her private and family life, provided that they represent interests worthy of protection. Data protection interests are excluded if the respective data are not subject to confidential treatment due to their general availability or lack of traceability to the individual affected[20].

DDOS (Distributed Denial of Services)

Distributed Denial of Services: attacks for which a large number of computers are used to block a specific computer through numerous external communication requests.

Governmental Crisis and Civil Protection Management

The Governmental Crisis and Civil Protection Management is responsible for civil protection management in Austria. It covers all measures taken to prevent and combat threats and damages caused by disasters. Its aim is to protect public life or to restore it as fast as possible, particularly public order and security as well as the supply of necessities. It covers activities of authorities and institutions organised under a public mandate and those of all private disaster relief organisations[21].

ICT

ICT is an umbrella term for all computer- (IT) and network- (CT) based technologies as well as related economic sectors. Information and communication technology is also used as a blanket term for all communication instruments or communication applications, including radio, television, mobile telephones, hardware and software for computers and networks, satellite systems, etc. as well as different services and applications related to these items[22].

ICT security

ICT security is the protected state of information and communication technology and the information used therein which is appropriate to the type and level of sensitiveness as well as the type and intensity of a possible threat[23].

ICT system

An ICT system is a combination of forces, means and procedures for processing, transmitting and/or conveying information to fulfil a specific task. The products (ICT services) of an ICT system may be made available through interfaces or, if appropriate, through services outside the limits of the system.

[19] Source of text: ETH Zurich: "CSS No. 71/2010", Zurich, 2010 + KSÖ: Cyber Risik Matrix – Glossary + AG "Cyber"

[20] Data Protection Act DSG 2000, Art. 1, constitutional provision, fundamental right to data protection, Section 1(1)

[21] Guideline/Crisis and Civil Protection Management

[22] Source of text: Definition AG "Cyber" based on: Federal Ministry of the Interior "Cybersicherheitsstrategie für Deutschland" (Cyber Security Strategy for Germany), Berlin, 2010

[23] Internal definition AG "Cyber" (Federal Ministry of Defence and Sports/Federal Ministry of the Interior)

Information security / network security

Information security or network security are umbrella terms for ICT security, referring to the entire relevant information of an organisation or an enterprise, including information that has not been processed electronically. Hence, it describes the entirety of characteristics of an organisation ensuring the confidentiality, availability and integrity of information. Information may be available as spoken text, paper documents or other directly readable media or as electronically processed data in ICT systems.

Internet

The Internet is a worldwide system of interconnected computers which applies the same protocol standard (TCP/IP – Transmission Control Protocol/Internet Protocol) and is used by billions of people. It is a network of networks consisting of millions and millions of private, public, academic, business and administrative networks, which are interconnected through a tightly woven system of electronic, radio and optical network technologies both at local and global level. The Internet does not have any central instances, neither in terms of technical implementation nor with regard to the conditions of access and use. It applies only a general definition of the two principal name spaces, the Internet Protocol address spaces and the Domain Name System, which are administered by the Internet Corporation for Assigned Names and Numbers (ICANN). The Internet works across platforms and operational systems. Typical services on the Internet are the worldwide web (www) and e-mail.

Malware

Malware refers to computer programmes executing processes that are not desired by the owner of the ICT system and often cause damages. As a catch-all term, malware describes all types of malicious software such as viruses, worms, spyware, backdoors and the like.

Sensitive data

In accordance with the Austrian Data Protection Act, sensitive data are defined as the data of natural persons about their racial and ethnic origin, political opinion, trade union affiliation, religious or philosophical beliefs, health or sexuality[24].

Social engineering

In the context of IT security, this term is used for strategies of online fraudsters. It describes direct communication processes used by the attacker to obtain confidential information from the victim through manipulation or to draw benefits illegally. By approaching their victims individually, the attackers increase their success rates: phished data such as the user's browsing habits or names from the victim's personal environment are used, e.g. in phishing e-mails written in a personal style to inspire confidence in the recipient[25].

Worldwide web (www)

Name for the entirety of documents linked through hyperlinks on the Internet; often used as a synonym for the latter[26].

[24] www.sicherheitskultur.at, Information Security Glossary

[25] Source of text (partly): KSÖ: Cyber Risk Matrix - Glossary

[26] www.sicherheitskultur.at, Information Security Glossary