Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Hermann Kaponig, *Connections QJ* 19, no. 1 (2020): 21-37
https://doi.org/10.11610/Connections.19.1.03

Policy Article

Austria's National Cyber Security and Defense Policy: Challenges and the Way Forward

Major General Hermann Kaponig

ICT & Cyber Security Center, Austrian Armed Forces

Abstract: The article presents Austria's cybersecurity policy, set in a whole-of-government context. It is comprehensive, integrated, proactive, and based on solidarity and cooperation within and beyond the European Union. Transparent governance, the cooperation between public agencies, businesses, research institutes, and the citizens, investments in awareness, research and development are expected to protect effectively vital information and critical infrastructures. The Ministry of Defense and the Austrian Armed Forces contribute to the national policy primarily through the Joint Forces Command, the Communication and Information Systems & Cyber Defense Command, and the two intelligence services.

Keywords: cyber defense, critical infrastructure, whole-of-government, interagency cooperation, cybersecurity platform.

Policy Highlights: Austria's National Military Cyber Defense Policy Within a Whole-of-Government Context

The "Austrian Security Strategy: Security for a New Decade – Shaping Security," adopted by the Austrian National Council in 2013 (ÖSS 2013) [1] was followed in the same year by the "Austrian Cyber Security Strategy" (ÖSCS 2013),[2] which was

[1] "Österreichische Sicherheitsstrategie: Sicherheit in einer neuen Dekade – Sicherheit gestalten," Vienna, July 2013, https://www.bmi.gv.at/502/files/130717_Sicherheitsstrategie_Kern_A4_WEB_barrierefrei.pdf.

[2] "Austrian Cyber Security Strategy," Vienna, 2013, https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf.

produced in accordance with the ÖSS. Both documents were developed at the national level.

The ÖSS 2013 describes new challenges, risks, and threats, including cyber threats (attacks against the security of IT systems, or "cyberattacks") based on analysis of the Austrian security environment. In addition, the ÖSS 2013 distinguishes between two key areas in terms of required policy development.

The chapter "Security policy at the national level: *Internal security*" discusses cybercrime, cyberattacks, and the misuse of the Internet for extremist purposes as well as network security posing new and specific challenges for all actors concerned. Moreover, this chapter points out that *broad cooperation based on a comprehensive concept* is required. In the same chapter, under "*Defense policy*," it posits that managing sub-conventional threats and new hazards resulting from cyberattacks may create a new area of military activity. From these two subchapters, one can infer that the ÖSS recognizes modern cyber threats but does not elaborate explicit countermeasures.

The military is required to expand its cyber capabilities following the national cybersecurity concept. This means that the military must be capable of providing cyber support and assistance comparable to military assistance in the case of disaster relief.

On 3 July 2013, the National Council passed a resolution requesting that the Federal Government develop Austria's security policy along with certain principles. The guideline for cybersecurity states:

> Threats caused by state and non-state actors in cyberspace are constantly on the rise. This is why cybersecurity is becoming more and more important. Measures to increase the security of computer systems, as well as Internet security, shall be intensified.

The Austrian Cyber Security Strategy of 2013 must be implemented and updated regularly following current developments. This means that the ÖSCS 2013 is to be implemented at the national level and developed further. Currently, national plans for an ÖSCS 2.0—which will be based on already accomplished ÖSCS 2013 objectives as well as developments and requirements that have occurred since then—are being developed.

The introduction to the ÖSCS 2013 explains that attacks from cyberspace pose a direct threat to the safety and the proper functioning of the state, the economy, science, and society. They can have a profound negative impact on our daily lives. Non-state actors like criminals, organized crime, or terrorists, as well as state actors like secret services and the military, may misuse cyberspace for their purposes and interfere with its proper functioning. Both the threats in cyberspace and the productive use thereof are practically infinite. It is, therefore, *Austria's top priority to work towards securing cyberspace at the national and international levels*. Cybersecurity means the security of cyberspace infrastructure, the security of data exchange in cyberspace, and above all, the protection of the people using cyberspace.

It is a joint, core task of the state, the economy, and society to ensure cybersecurity nationally and internationally. The ÖSCS 2013 is a comprehensive and proactive concept for protecting cyberspace and the people in cyberspace while guaranteeing human rights. The strategy is expected to contribute to the security and resilience of Austrian infrastructures and services in cyberspace. Most importantly, it will build awareness and confidence in Austrian society.

The chapter on "Risks and threats" states that cyberspace and the security and safety of people in cyberspace are exposed to a number of risks and threats since cyberspace is also a space of criminal activity. Risks and threats span the spectrum from operating errors to massive attacks by state actors and non-state groups using cyberspace as operational fora not limited by national borders. *Foreign military organizations may also be behind these attacks*.

The spectrum of risks and threats was presented in a specific Cyber Risk Matrix (effective 2011).[3] The Risk Matrix was revised and updated in 2016.[4] Cybercrime, identity fraud, cyberattacks, or misuse of the Internet for extremist purposes are new serious challenges that require broad cooperation between governmental and non-governmental agencies at the national and international levels. This is a clear indication that countering cyber challenges is a top priority on the national agenda and that all forces need to join in a whole-of-government cooperative approach, and that national and international cooperation and interaction are essential.

The chapter on "Principles" continues with the following definitions:

State-of-the-art cybersecurity policy is a cross-cutting issue that impacts many spheres of life and policy. It must be developed in terms of a comprehensive and integrated approach, to allow for active participation and has to be implemented in the spirit of solidarity.

Comprehensive cybersecurity policy means that external and internal security, as well as aspects of civilian and military security, are closely interlinked. Cybersecurity goes beyond the purview of traditional security authorities and comprises instruments of numerous policy areas.

Integrated cybersecurity policy emphasizes task-sharing between the state, economy, academia, and civil society. It comprises measures in the following areas: political-strategic control, education and training, risk assessment, prevention and preparedness, detection and response, mitigation and restoration, as well as the development of governmental and non-governmental capabilities and capacities. An integrated cybersecurity policy must be based on a cooperative approach both at national and international levels.

Proactive cybersecurity policy means that efforts are made to prevent threats to cyberspace and the people in cyberspace as well as to mitigate the impact of incidents (shaping security).

---

[3] "Cyber-Risikomatrix 2011," https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2015/02/KSO_Cyber_Risikomatrix.pdf, accessed March 12, 2020.

[4] "Cyber-Risikomatrix 2011."

Cybersecurity policy based on solidarity takes into account that due to the global nature of cyberspace today, the cybersecurity of Austria, the EU, and the entire community of nations is strongly interconnected. Ensuring cybersecurity requires intensive cooperation based on solidarity at European and international levels.

Austria's Main Policy Challenges and Key Priority Areas

Based on strategic objectives, the ÖSCS 2013 identifies seven fields of action and a total of 15 measures:

- Field of action 1 – Structures and processes
- Field of action 2 – Governance
- Field of action 3 – Cooperation of government, economy, and society
- Field of action 4 –Critical infrastructure protection
- Field of action 5 – Awareness-raising and training
- Field of action 6 – Research and development
- Field of action 7 – International cooperation.

Field of Action 1 – Structures and Processes

Objective: There are numerous structures and stakeholders active in cyberspace that are working separately from each other to ensure cybersecurity. Several organizations specializing in cybersecurity (e.g., Computer Emergency Response Teams, CERTs) are already playing an important role in cyber crisis management. Overarching cybersecurity procedures have not been defined formally so far. Therefore, it is necessary to define processes and structures to provide for overall coordination at the political-strategic level, as well as at the operational level by involving all relevant public and private stakeholders.

Measures:

1) Establishing a Cyber Security Steering Group

In 2012, the Austrian Council of Ministers formed a *Cyber Security Steering Group*. Under the leadership of the Federal Chancellery, the group is responsible for coordinating measures related to cybersecurity at the political-strategic level, monitoring and supporting the implementation of the ÖSCS 2013, drafting an annual Cyber Security Report, and advising the federal government in all matters relating to cybersecurity. The Steering Group includes liaison officers working with the National Security Council and cybersecurity experts from the ministries represented in the National Security Council. The Chief Information Officer of the Federal Republic of Austria (National CIO) is also a member of this body. In case of specific issues, representatives of other ministries and the Austrian federal provinces may be included in the Steering Group as required. This holds especially for agencies dealing with organizations and enterprises that are subject

to or affected by control measures. Representatives of other relevant enterprises become included on an appropriate, case-specific basis.

2) Creating a structure for coordination at the operational level

An *Operational Coordination Structure* will be created on the basis of existing operational structures to serve as a platform for preparing incident-related and periodic cybersecurity reports and for deliberations on measures to be taken at the operational level. Thus, it will provide a continuously updated overview of cyber developments by collecting, compiling, evaluating, and passing on relevant information. The economic sector should be involved in an appropriate manner and on an equal footing. The joint and permanently updated overview report will indicate the current cyber status and serve as a basis for planning preventive and response measures. The operators of critical infrastructure will be supported at the operational level and particularly in cases of failures of information and communication structures. Besides, they will be provided with information on dangers to the Internet. The Operational Coordination Structure must be designed so that it can be used as an operational executive body of cyber crisis management leaders.

The *Operational Coordination Structure* engages ministries and operational structures of business and research sectors. The tasks performed within the Operational Coordination Structure are coordinated by the Federal Ministry of the Interior (in a public-private partnership, or PPP arrangement). In carrying out its coordination task, the Federal Ministry of the Interior (BMI) is supported by the Federal Ministry of Defense (BMLV), to which coordination tasks will be transferred if a cyber defense incident occurs. All operational, organizational, sectoral, or target group-specific structures will remain within the purview of the respective organization. Institutions with responsibilities for security issues of computer systems, the Internet, and the protection of critical infrastructure, will cooperate within the framework of the Operational Coordination Structure. At the national level, these organizations comprise the GovCERT (Government Computer Emergency Response Team), MilCERT (Military Computer Emergency Readiness Team), and the Cyber Crime Competence Center (C4). Other government institutions are involved by forming a second circle. The additional circle comprises private CERTs (CERT.at, BRZ-CERT, banks, etc.), as well as economic sectors and research institutes.

The Cyber Security Steering Group will establish a *working group* in charge of preparing proposals for necessary processes and structures for permanent coordination at the operational level. Representatives of relevant enterprises will be involved appropriately.

3) Establishing a Cyber Crisis Management system

Austria's *Cyber Crisis Management* consists of state representatives and operators of critical infrastructure. In terms of composition and working procedures, it is modeled on the National Crisis and Civil Protection Management (Austrian

abbreviation: SKKM) arrangements. Since its responsibilities go beyond information and communications technology (ICT) and to ensure internal security in case of overarching threats, the Federal Ministry of the Interior will be responsible for cyber crisis management coordination. As far as external security is concerned, the Federal Ministry of Defense will play the leading role in coordinating measures to protect sovereignty by ensuring national defense (cyber defense). *Crisis management and continuity plans* will be prepared and updated regularly in cooperation with public institutions and the operators of critical infrastructure based on risk analyses for sector-specific and cross-sectoral cyber threats.

Further, *regular cyber exercises* will be held to test Austria's Cyber Crisis Management System as well as crisis and continuity plans.

4) Strengthening of existing cyber structures

The role of the *GovCERT* operated by the Federal Chancellery as the government's CERT will be strengthened. Towards that purpose, it will be necessary to describe in detail its powers, responsibilities, and spheres of action, its institutional place within the public administration, role in the event of a crisis, and the modalities of interaction with the Operational Coordination Structure. Further, new requirements will have to be defined.

To avoid and prevent cybercrime as well as to facilitate operational international cooperation, the role of the *Cyber Crime Competence Center (C4)* of the Federal Ministry of the Interior will be enhanced. This Center is Austria's central body in charge of exercising security and criminal police duties in the area of cybersecurity.

The *MilCERT*, operated by the Federal Ministry of Defense, will be expanded to provide operational capabilities for preventing cyberattacks, to protect its own networks, and to further develop the Cyber Security Overview. These capabilities will, inter alia, also lead to the creation of capacity for providing ICT assistance to other state agencies.

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

Field of Action 2 – Governance

Objective: The aim concerning governance is to define the role, responsibilities, and powers of state and non-state actors in cyberspace and to create adequate framework conditions for cooperation among all players.

Measures:

5) Establishing a modern regulatory framework

With the support of the *Cyber Security Steering Group*, a comprehensive report analyzing the need to establish additional *legal principles*, *regulatory measures*, and *voluntary self-commitment* (codes of conduct) for guaranteeing cyber secu-

rity in Austria will be prepared and submitted to the Federal Government. This report will cover the following issues: the establishment of necessary organizational structures, tasks and powers of authorities, information exchange between authorities and private entities, reporting duties, obligation to adopt protective measures as well as supply chain security.

Balancing incentives and sanctions should be considered when determining obligations for non-state actors.

6) Defining minimum standards

All relevant stakeholders should cooperate and define *minimum security standards* in order 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 conduct, and best practices, will be compiled in the Austrian *Information Security Management Handbook*, which will be updated regularly.

7) Preparing an annual report on cybersecurity

The Cyber Security Steering Group will prepare an annual report entitled "Cyber Security in Austria."

Field of Action 3 – Cooperation of Government, Economy, and Society

Objective: Many tasks and responsibilities of public administration agencies, economic entities, and the world at large are based on the information and communications technology (ICT). The responsibility of using digital technologies in a prudent way rests with each organizational unit. However, it is only a broad cooperation between all sectors and permanent exchange of information that will facilitate the transparent and safe use of ICT. Therefore, existing cyber capacities and processes in the administration, the economy and within the population must be strengthened and new opportunities must be created through cooperation.

Measures:

8) Establishing a Cybersecurity Platform

The *Austrian Cyber Security Platform* will be operated as a public-private partnership to facilitate ongoing communication with all stakeholders of the administration, economy, and academia. In parallel, existing initiatives (run by the Austrian Trust Circle, Cyber Security Austria, the Austrian independent non-profit security association *Kuratorium Sicheres Österreich* (KSÖ), the Austrian Center for Secure Information Technology (A-SIT), etc.) will be continued and leveraged. The Austrian Cyber Security Platform will serve as the institutional framework for continuous exchange of information within the public administration and between the administration and representatives of the business, academia, and

research institutes. All will participate on an equal footing in the Cyber Security Platform, advising and supporting the Cyber Security Steering Group.

Cooperation with private operators of critical infrastructure and other economic sectors is essential for Austria's cybersecurity. Details on this cooperation will be discussed in further talks between the Cyber Security Steering Group and the economic sector.

The Cyber Security Platform will be used to initiate extensive *cooperation between the participating partners* on issues like awareness-raising and training as well as research and development.

In order to promote a common understanding of challenges and opportunities for action among all partners involved in cybersecurity issues, an *exchange* of experts should be intensified between the participating governmental, private, and academic organizations. Under the leadership of the Cyber Security Steering Group and with the support of the Austrian Cyber Security Platform, a program will be developed for this purpose.

9) Strengthening support for small and medium-sized enterprises (SMEs)

Priority programs on cybersecurity will be launched to raise cybersecurity awareness among SMEs and to prepare them for hazardous situations. Interest groups should be encouraged to post tailored information for SME needs online on the new Internet portal, ICT Security, and to initiate cybersecurity campaigns for SMEs. Support by governmental bodies, sector-specific information platforms such as the Austrian Trust Circles will develop sector-specific cyber risk management plans. Regulatory authorities and interest representations should be involved in this dialog. These risk management plans will be harmonized with governmental crisis and continuity management plans. Cross-sectoral cyber exercises for SMEs will be organized and held at periodic intervals. SME sectors should also be allowed to participate in governmental cross-sectoral cyber exercises upon request.

10) Preparing a Cyber Security Communication Strategy

In order to optimize communication between stakeholders in the administration, economy, academia, and society, all existing and planned government websites must be harmonized as part of a *Cyber Security Communication Strategy*. This communication strategy will be prepared by the Cyber Security Steering Group and involve the input of all relevant stakeholders.

Field of Action 4 –Critical Infrastructure Protection

Objective: Almost all infrastructures increasingly depend on specialized ICT systems, which guarantee smooth, reliable, and continuous operations to the greatest possible extent. It is, therefore, a top priority to build and improve the threat resilience of information systems. Under the Austrian Program for Critical Infrastructure Protection (APCIP), enterprises operating critical infrastructure are urged to implement comprehensive security architectures. The ÖSCS aims to

supplement and intensify these measures in the field of cybersecurity. In this process, cooperation with operators of critical information infrastructures is of paramount importance.

Measures:

11) Improving the resilience of critical infrastructure

The operators of critical infrastructure should be involved in all processes of national cyber crisis management. These strategic enterprises are tasked to define a comprehensive security (risk and crisis management) architecture, update it according to current threats, appoint a security officer, and further prepare for *crisis communication*. Also, *cybersecurity standards* should be set up for these enterprises and implemented in a partnership approach.

The operators of critical infrastructure should have a duty to report *severe cyber incidents*. The appropriate legal basis must be established after comprehensive consultations with the relevant stakeholders.

Existing arrangements in the *Program for Critical Infrastructure Protection* (APCIP) and the *National Crisis and Civil Protection Management* (SKKM) should be reviewed on an ongoing basis to ensure the continuous countering of new cyber challenges and to effect modifications if required.

Field of Action 5 – Awareness-Raising and Training

Objective: All target groups should be sensitized to cybersecurity in order to increase the awareness of, personal interest in, and the attention paid to it. These awareness-raising measures will help create an understanding of the need to ensure cybersecurity. Concrete and target-group-specific measures will impart and promote the necessary knowledge about security-conscious behavior and responsible use of information and ICT tools at large. Increased training in cybersecurity and media literacy in schools and other educational facilities, as well as adding cybersecurity competence to teaching, should ensure a meaningful and adequate level of ICT competence level across the board.

Measures:

12) Strengthening a cybersecurity culture

Awareness-raising initiatives are developed, coordinated, and implemented in harmony with a common approach whilst taking into account existing programs. In doing so, it is important to examine cybersecurity from different perspectives, highlight relevant dangers, draw attention to possible impacts and damages as well as make recommendations for security measures.

In order to give different target groups access to more in-depth customized advice, the existing *consulting programs* should be further enhanced and expanded.

A web-based *ICT Security Internet Portal* will be set up to serve as an information and communication hub for awareness-raising. The Ministry of Finance,

the Federal Chancellery, and A-SIT will be responsible for coordinating the ICT Security Internet Portal. The strategic approach of this portal will be guided by the principles and objectives of the ÖSCS.

Prevention programs safeguarding against cybercrime will be further developed.

13) Incorporating cybersecurity and media literacy into all levels of education and training

Austria will pursue stronger integration of ICT, cybersecurity, and media literacy into *school curricula*. ICT and new media literacy are part of the curriculum of all types of schools. ICT security issues and cybersecurity will eventually become an integral part of a model called *Digital Competence*. This model will be adjusted to the curriculum of the respective type of school and will create awareness for security issues and promote the safe and responsible use of the Internet. The aim is to ensure a certain level of ICT competence across all types of schools.

ICT (security) competence should be part of *academic training* at pedagogical universities as well as pedagogical institutes of higher education. Teachers will need to receive cyber education before they can teach cyber skills at the secondary school level as well as at adult education centers.

The *training of public sector experts* responsible for improving cybersecurity will be intensified in cooperation with national and international training facilities.

ICT system administrators working for operators of critical infrastructure should receive additional cybersecurity training in order to be able to recognize cyber incidents, detect anomalies in their ICT systems and report them to their security officers (*Human Sensor Program*).

Field of Action 6 – Research and Development

Objective: To ensure cybersecurity technical expertise, based on state-of-the-art research and development results. To this end, cybersecurity issues must be increasingly incorporated into applied cyber research as well as into security research programs such as the Austrian KIRAS program. Efforts should be invested to achieve active thematic leadership in EU security research programs.

Measures:

14) Strengthening Austria's cybersecurity research

Within the scope of national and EU security research programs, *cybersecurity* should be a *key research priority*. Through joint projects, relevant stakeholders from the administration, business, and research organizations will develop the conceptual framework and technological instruments to enhance Austria's cybersecurity capacity. Particular emphasis will be placed on measures helping to turn research and development findings speedily into marketable products. Existing research projects, such as those run by A-SIT, will be further developed.

Austria should strive for *active thematic leadership in EU security research programs*. In doing so, Austria should initiate the incorporation of cyber topics that are important for Austria into international research programs.

Field of Action 7 – International Cooperation

Objective: Global networking and international cooperation are vital factors in ÖSCS. Security in cyberspace can be achieved only through a coordinated policy mix at the national and international levels. Therefore, Austria will engage in an active cyber foreign policy and pursue its interests in a coordinated and targeted way within the framework of the EU, UN, OSCE, Council of Europe, OECD, and NATO partnerships. Furthermore, the international aspects of Austria's cyber policy will be harmonized consistently in other policy fields.

Measures:

15) Effective collaboration on cybersecurity in Europe and worldwide

Austria will make a substantial contribution to the development and implementation of the *EU Cyber Security Strategy*. It will participate fully in the strategic and operational work of the EU.

The relevant ministries will take the necessary measures to implement and to make full use of the *Convention on Cybercrime* of the Council of Europe.

Austria advocates for a free Internet at the international level, which will guarantee the free exercise of all *human rights in the virtual space*. In particular, the right to freedom of expression and information must not be restricted on the Internet without legal cause. This is the position that Austria shall adopt in international forums. Hence, Austria will participate actively in developing and establishing a transnational code of conduct for government activity in cyberspace, which will also include measures to build confidence and security.

Austria will continue its bilateral cooperation, initiated within the framework of NATO Partnership for Peace, and actively support the preparation of a list of concrete confidence and security-building measures in the framework of the OSCE.

Austria already participates actively in planning and implementing *transnational cyber exercises*. The experience gained from such exercises will be used as a direct input for planning and further developing operational cooperation.

Foreign policy measures that pertain to cybersecurity are coordinated by the Federal Ministry of Europe, Integration and Foreign Affairs (BMEIA). Where appropriate, the conclusion of bilateral or international agreements will be taken into consideration.

Implementing Policy Structures Within a Whole-of-Nation Context

In Austria, the coordinating structures for managing cyber challenges are as follows. At the highest level, which is the *political level*, the Austrian government defines its political and strategic objectives. The *National Security Council* (NSR)

functions as the national security advisory body at the *strategic level*. In case of a cyber incident, the NSR will draw on the *Cyber Security Steering Group* (CSSG). The CSSG coordinates cybersecurity measures at the political-strategic level under the leadership of the Federal Chancellery. It also monitors and supports the implementation of the ÖSCS, produces an annual report on cybersecurity and advises the federal government on cybersecurity issues.

The *Cyber Security Platform* (CSP) will also provide support in case of a cyber incident. The CSP is the primary platform for cooperation and exchange of information between business, science, research, critical infrastructure, and public administration entities.

Depending on the type of cybersecurity threat, it will be either the *Inner Circle of Operational Coordination* (IKDOK) or the Extended Circle of Operational Coordination (EKDOK) that will be tasked at the *operational level*.

The IKDOK is responsible for operational control and coordination in the area of cyber. It maintains contact with the operators of critical infrastructure, businesses, and ministry departments working in cyber and develops standards and operational measures to be implemented in case of a cyber crisis incident. The IKDOK also serves as an interagency platform for information exchange. It develops an intermittent incident-related Cyber Security Overview Report and discusses necessary operational measures. It provides a continuously updated overview of cyber developments by collecting, compiling, evaluating, and passing on relevant information. The IKDOK is comprised of representatives of the Federal Chancellery, the Ministry of the Interior (MoI), the MoD, and the BMEIA and also

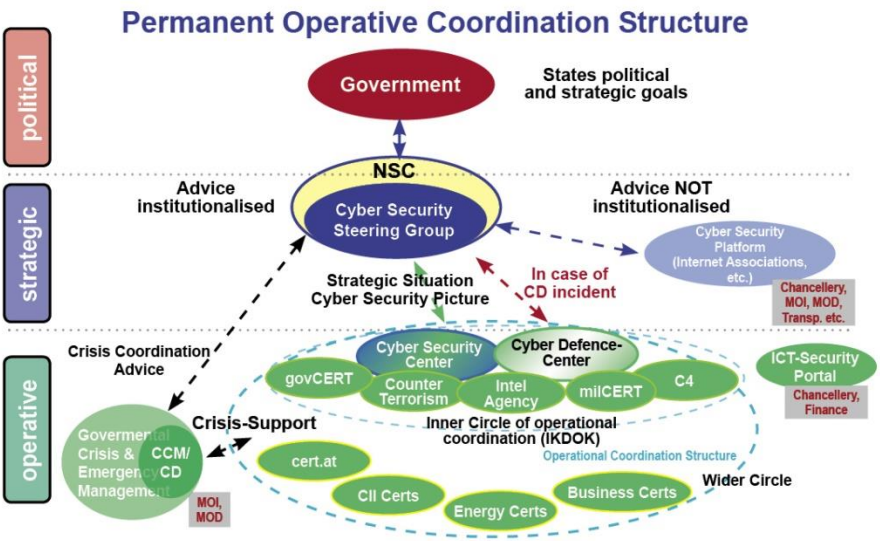

Figure 1: Permanent Operative Coordination Structure.

includes the Cyber Security Center (CSC; MoI) and the Cyber Defense Center (CDC; MoD), both of which chair the IKDOK, and involves other state actors/agencies as well. This means that all cyber assets in the national cyber community are included in the IKDOK: the CSC and the C4 of the MoI; the CDC and MilCert of the MoD; the GovCERT; etc.

As far as the *GovCert* is concerned, it is the superstructure of all state CERTs and plays a leading role in public administration.

The *EKDOK* is essentially the extended circle of IKDOK plus the CERT Association. The *CERT Association* enhances CERT structures at the national level. It intensifies cooperative efforts with sector-specific CERTs (engaging in defined critical infrastructure sectors).

At the national level, there are also civilian agencies with similar setups working alongside state CERTs. They serve first and foremost as crisis intervention teams in cases of cyberattacks against civilian companies or business sectors. These civilian agencies are organized in groups along sector-specific lines. The CERT.at serves as their superstructure and, in cooperation with the Federal Chancellery, has established the Austrian Trust Circle. The Austrian Trust Circle offers a formal framework for security information exchange between the CERT.at, the Federal Chancellery, and the GovCERT. Within the framework of this partnership, it is foreseen to link all Austrian CERTs to discuss standards, provide assistance to affected companies and business sectors, and to develop joint strategies in the event of a cyberattack.

Core Responsibilities

The MoI is responsible for *cybercrime* and the *protection of critical infrastructure*.

The MoD is primarily responsible for *cyber defense* and its three subcomponents: *cyber intelligence* (under the purview of the Armed Forces Protection Service and the Armed Forces Intelligence Service), *ICT security* (under the purview of the ICT & Cyber Security Center) and *cyber operations* (under the purview of the Armed Forces Command). In addition, in cases of cyber incidents, military forces will provide assistance to support the overall mission.

The BMEIA is responsible for *cyber diplomacy*.

Responsibilities during Cyber Incidents

Austria distinguishes between *three cyber threat levels* determined by the degree of cyber risk escalation.

The first level pertains to *cyber standard operations*, where cybercrime, cyber espionage, and data theft must be managed appropriately. At this level, the MoI is responsible for response coordination. The MoI coordinates the close cooperation, exchange of information and mutual support between all stakeholders taking advantage of the IKDOK. The MoD must be able to take appropriate action within its scope of responsibilities and, as necessary, support other public institutions upon request for assistance.

The second level pertains to *cyber crisis* when incidents ranging from cyberattacks on critical infrastructure to blackouts caused by cyberattacks have to be

managed appropriately. At this level, it is also the MoI that is responsible for response coordination. The MoI coordinates close cooperation, exchange of information, and, if necessary, mutual assistance between all stakeholders. At the strategic level, the Cyber Security Steering Group will be activated and will take charge of the IKDOK and the CSC of the MoI. Again, the MoD must be able to take appropriate action within its scope of responsibilities and, if necessary, support other agencies upon request for assistance.

The third level pertains to *cyber defense* when politically motivated attacks pose a substantial threat to state sovereignty. In this case, response coordination is transferred to the MoD. At the strategic level, the Cyber Security Steering Group will be activated and will take charge of the IKDOK and use the CDC of the MoD for action at the operational level. The MoD will coordinate the close cooperation, exchange of information, and, if necessary, mutual support between all stakeholders.

It must be noted that the systematic transfer of authority from the MoI to the MoD cannot be effected categorically or preplanned in detail in the case of cyber crisis turning into cyber defense. A checklist was developed at the national level, which defines the preconditions for such a transfer. During an actual cyber incident, however, the transfer of authority will have to be determined based on a thorough situational assessment.

Policy Implementation in the Austrian MoD and Armed Forces

The ÖSCS 2013 has tasked the Federal Ministry of Defense (BMLVS) with performing important missions and measures. Also, the Ministry of Defense (MoD) is bound by the Defense Strategy 2014 (TV14) as well as by the Military Strategy 2017 (MSK17). Up to now, the MoD has worked with its existing concept papers. Currently, the MoD is developing a Cyber Defense Strategy (CDS) and a Concept for Military Cyber Operations (CyOps).

The national defense structural reform (LV21.1) of 2016 created the "Communication and Information Systems & Cyber Defense Command" (CIS & CD Command; KdoFüU&CD), which was a separate military branch exercising operational leadership and cyber capabilities. In doing so, almost all capabilities in the area of leadership support, ICT, electronic warfare, cyber defense, and navigation operations were packed into one command.

Due to budgetary reasons, this ambitious goal had to be abandoned, and in 2019 the CIS & CD Command was ultimately dissolved. The following military structures now exercise the responsibilities for merely cyber defense:

- The Joint Forces Command (JFC) is responsible for Cyber Operations (CyOps).
- The CIS & Cyber Security Center (CISCDC) is responsible for ICT defense.
- The two military intelligence services—the Armed Forces Security Agency (AFSA) and the Austrian Strategic Intelligence Agency (ASIA)—are responsible for the subdomain of cyber intelligence (CyInt).

Austrian military cyber defense focuses on network protection and will be expanded following medium and long-term armed forces' development goals.

Austria's Key National Initiatives and Policy Response Challenges

Currently, the main challenge is the full implementation at the national level of policies based on EU-wide legislation on cybersecurity known as the Directive on security of network and information systems (NIS Directive). This will set the course for increasing network and information system security in the long-term. Above all, it will enhance the security of particular critical infrastructures in various sectors.

Beyond this, as mentioned above, a new whole-of-nation Austrian Cyber Security Strategy is currently being developed at the national level.

Further, cooperative efforts are being intensified at all levels. On the one hand, cooperation at the national level between public and private business entities as well as cooperation between the military and the civilian sector is being strengthened. On the other hand, cooperative efforts between Austria and international organizations like NATO and the EU are being reinforced. As far as the EU is concerned, Permanent Structure Cooperation (PESCO) projects are also being initiated in the cyber area.

The Austrian Armed Forces (Österreichisches Bundesheer) also take advantage of the knowledge provided by the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE), a multinational and interdisciplinary cyber defense hub.

The Austrian Armed Forces also take part in joint international exercises to promote cyber capability development and cyber defense interoperability. Austria, Germany, and Switzerland belong to the trilateral cooperation of "D-A-CH" nations and hold interoperability exercises annually. Austria regularly participates in these exercises and also participated in the *Common Roof* 2018 interoperability exercise.

Austria regularly participates in major exercises such as *Locked Shields*, an international technical live-fire cyber defense exercise organized by the NATO CCDCOE, or the technically-oriented *KSÖ-Planspiele*, a cybersecurity simulation exercise organized nationally by the Kuratorium Sicheres Österreich (KSÖ), an Austrian independent non-profit association aiming at making Austria more secure), The Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX), a NATO interoperability event, Cyber.PHALANX 2018, an exercise designed for military planners and staff, and the Austrian Strategic Decision Making Exercise ASDEM18, to name just a few of the well-known exercises.

It is worth noticing that Austria is involved in a significant number of bilateral cooperative relations, primarily with other member states of the European Union, but is also engaging in a new cooperation with the Israel Defense Forces.

Moreover, every year Austria conducts the Austria Cyber Security Challenge, which is a contest to search nationally for talent. The winning team also represents Austria in the European Cyber Security Challenge.

Engaging the Austrian Private Sector and Academia

In the private sector, the research and technology activities of the Austrian Institute of Technology (AIT) and the work of the organization KSÖ are worth noting. In the academic sector, the Graz University of Technology and the Cybersecurity Campus Graz (a partnership between the Graz University of Technology and SGS), the Campus Hagenberg of the University of Applied Sciences Upper Austria and the St. Pölten University of Applied Sciences are worth noting.

Confronting Outstanding Limitations

The following limitations need to be considered in an Austrian context:

- The budgetary pressure on defense spending, which currently amounts to approximately 0.58% of the GDP.
- The legal framework, which currently allows for offensive cyber operations to be carried out only in incidents categorized as "national cyber defense." According to current law, cyberattacks below the cyber defense threat level (at the level of "cyber standard operations" or "cyber crisis") are not permitted.
- Recruiting cyber experts has become one of the most fundamental challenges. Currently, Austria's educational infrastructure does not produce the required amount of specialists to cover demands in the public sector, the military, and the private business sector. As a result, there is fierce competition for the best experts. Nevertheless, thanks to the conscript system, the Austrian Armed Forces have a certain advantage over other public agencies and the economy, since trained cyber and ICT specialists are available to the military on a regular or temporary basis. These cyber recruits receive additional training during their military service and their expertise is put to good use. Also, the Austrian militia system includes cyber specialists that are called upon as cyber experts for military purposes.

  As the next step in cyber education, Austria is considering establishing a separate military cyber & ICT training system. Developments towards cyber training, allowing for specialized career tracks for non-commissioned officers and officers, are underway. This will guarantee that the military can draw from its personnel to cover cyber and ICT expertise.
- It is a drawback in cyber defense that Austrian Armed Forces cyber experts are not part of the NATO Communications and Information Agency's Malware Information Sharing Platform community.

The Way Forward

Due to significant developments in military cyber affairs, it would be expedient to go even beyond the current, already ambitious EU efforts (for instance led by the European Defense Agency, the European Union Agency for Cybersecurity ENISA (formerly, European Union Agency for Network and Information Security), and computer emergency response teams for the EU institutions, agencies, etc.) and set up a central cyber office or cyber cell in the European Union Military Staff. It would be more than expedient if EU member states could manage developments both in a top-down and bottom-up approach.

The current Austrian government program foresees the establishment of a National Cyber Security Center for Austria, thereby engaging all major state players. Such a center is considered essential and, once available and operable, it will significantly improve effectiveness, the flow of information, situational awareness analysis, and response speed.

It would certainly be helpful if the NATO CCDCOE were to expand its task portfolio and develop into a central hub for all levels of cyber affairs (strategic, operational, tactical/technical, research).

Furthermore, it would be advisable if, under EU leadership, Europe could trigger significant cyber developments including measures such as developing *cyber technology clusters* (e.g., determining which nation is positioning itself or taking the lead in which research area or in which cyber industry) and increasing the technical security of networks and establishing European *standards* for various engineering solutions to create a higher degree of security by design and artificial intelligence in future ICT, weapon and sensor systems from the outset.

Disclaimer

The views expressed are solely those of the contributing author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgement

Journal *Connections: The Quarterly Journal*, Vol. 19, 2020 is supported by the United States government.

About the Author

Brigadier **Hermann KAPONIG** is the cyber coordinator of the Austrian Ministry of defense. Previously, he has served as head of the Command Support Center of the Austrian Armed Forces, head of the MOD Logistics Directorate, and head of the Planning and Armaments Section in the Cabinet of the Federal Minister of Defense and Sports.