Genese und wesentliche Inhalte der Österreichischen Strategie für Cyber Sicherheit (ÖSCS)

Helmut Habermayer und Josef Schröfl*

Abstract: Since the cyber attacks against Estonia in 2007, several initiatives within Austria were started by different national stakeholders, private as well as public. The following essay will briefly outline the history of origin of the Austrian National Cyber Security Strategy, which has been finalised at the end of 2012 and has been approved by the Council of Ministers with decision from March 20, 2013 (Decision No. 180/8). The Strategy has already been published in German and English.

The content of the Strategy is as follows: *"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 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."* [1]

Keywords: Austrian strategy for cyber security, cyberattacks, security
Österreichische Cyber Sicherheitsstrategie, Cyberangriffe, Sicherheit

1. Vorwort

Bedingt durch die rasche technologische Entwicklung auf dem Gebiet der Informations- und Kommunikationstechnologie wurde mit dem Ende des 20. Jahrhunderts das Industrie- vom Informationszeitalter abgelöst. Die Infrastruktur der Informations- und Kommunikationstechnologie (IKT) hat sich somit zu einer höchst kritischen Infrastruktur für Wirtschaft, Verwaltung und Gesellschaft Österreichs gewandelt. Insbesondere der Cyberraum und hier das Internet haben sich zu einer allumfassenden Plattform für Staat, Wirtschaft und Forschung entwickelt. Wirtschaftlicher Erfolg und die Aufrechterhaltung staatlicher und weiterer strategischer Infrastrukturen und Dienste hängen zunehmend von der Verfügbarkeit und der Sicherheit der IT-Infrastrukturen und der elektronischen Kommunikationsmedien ab. Die Informations- und Kommunikationstechnologien bilden zudem die Grundlage für die Bereitstellung anderer kritischer Infrastrukturen wie zum Beispiel Energie und Notfalldienste und sind gleichzeitig von ihnen abhängig.

Das Internet stellt somit gemeinsam mit der Stromversorgung und der Sprach- und Datenübertragung die „Cyberinfrastruktur" dar, die aufgrund ihres starken Hebels auch ein guter Ansatzpunkt für die asymmetrische Kriegführung (Cyberwar) ist. Durch Kettenreaktionen (Dominoeffekte – große Hebelwirkung) können weitreichende Störungen ausgelöst werden. Dies wurde bereits kurz nach der Einführung des Internets erkannt. Bereits 1993, also ca. zehn Jahre nach der erstmaligen Erwähnung des Wortes „Cyberspace" veröffentlichten zwei Wissenschaftler der RAND Corporation einen Artikel unter dem Titel „Cyber War is coming"[2]. Nach weiteren zehn Jahren wurden erste ernste Vorfälle im Bereich der kritischen Infrastruktur mit dem Internet in Verbindung gebracht: Im August 2003 brach die Stromversorgung in New York, Detroit, Ottawa und Toronto zusammen, weil die computer– und internetbasierten Steuerungssysteme von 21 Kraftwerken nicht mehr funktionierten[3].

Am 27. April 2007 begannen die Internetangriffe auf Estland, die sich gegen das Parlament, Banken, Ministerien und Rundfunksender (Teil der strategischen/kritischen Infrastrukturen eines Landes[4]) richteten[5]. Der Angriff war eine sogenannte Denial-of–Service-Attacke (DoS), bei der Internetzugänge und/oder Betriebssysteme mit einer größeren Anzahl von Anfragen befasst werden, als diese verarbeiten können, was zu einer Fehlfunktion (einem Absturz) der Systeme führen kann, wie es in Estland auch der Fall war.

Ausgangsbasis waren Botnetze, vernetzte Rechner (Server), auf denen ohne Wissen der Eigentümer von einer nach eigenen Angabe „patriotischen" Gruppe russischer Hacker Schadprogramme installiert worden waren, die selbstständig versucht hatten, weitere Rechner zu infizieren.

* Helmut Habermayer, Mag, MSC, Leiter Gruppe Strukturen/Organisation und Chief Information Officer im BMLVS. Josef Schröfl, Mag., Oberst des höheren militärfachlichen Dienstes, Abteilung Militärstrategie (MilStrat) im BMLVS.

1 ÖSCS, englische Version, S. 4; Die ÖSCS liegt sowohl in gedruckter (Eigenpublikation des BKA, Abteilung IV/6-Sicherheitspolitische Angelegenheiten, März 2013) als auch digitaler Form auf (http://www.bka.gv.at/DocView.axd?CobId=50748), die diesbezügliche Abfrage erfolgte letztmalig am 23.01.2014. In weiterer Folge wird innerhalb der Fußnoten auf die explizite Angabe der Fundstelle als Nachweis verzichtet und nur mehr die Seitenangabe innerhalb der ÖSCS genannt.

2 John Arquilla, David Ronfeldt: RAND/Comparative Strategy, Vol. 12, No. 2, Spring 1993, S. 141-165.

3 J.R. Minkel: "The 2003 Northeast Blackout-Five Years Later", in Scientific American, 13.8.2008, Internet edition (http://www.scientificamerican.com/article/2003-blackout-five-years-later, (22.1.2014).

4 Lt. EPCIP (European Programme for critical Infrastructure Protection), – veröffentlicht in den Mitteilungen der EU-Kommission über ein Europäisches Programm für den Schutz kritischer Infrastrukturen, Brüssel, 12.12.2006, KOM(2006) 786.

5 Walter Unger: „Cyber War and the Protection of Strategic Infrastructure" in: Schröfl/Rajaeed/Muhr: "Cyber and Hybrid War as consequences of the Asymmetrie", 2011, Peter Lang, New York, S. 145ff.

Spätestens nach diesem Angriff, der beinahe zwei Wochen die wesentlichsten kritischen Infrastrukturen des Landes lahmlegte, war weltweit Sicherheitsexperten und -planern klar, dass die Aufrechterhaltung des Betriebs der strategischen bzw. kritischen Infrastrukturen, wie eben jene am Beispiel Estlands, kritisch für das Funktionieren des Staates als Ganzes ist. Der Cyberraum wird sowohl von nichtstaatlichen Akteuren, zu denen auch die Organisierte Kriminalität oder terroristische Vereinigungen gehören, als auch von staatlichen Akteuren für ihre Zwecke genutzt.

Die globale Vernetzung sowie die räumlich und zeitlich fast uneingeschränkte Verfügbarkeit von Informationen aus dem Cyberraum haben zu einer Erhöhung der Lebensqualität beigetragen. Gleichzeitig entstand aber eine starke Abhängigkeit und damit eine erhöhte Verwundbarkeit der Gesellschaft von den für den Cyberraum erforderlichen Infrastrukturen. Informationsoperationen in Form von Propaganda und/oder der Verbreitung von Desinformation zur Beeinflussung eines Gegners sowie zur Schaffung eines günstigen Meinungsumfelds finden regelmäßig – nicht nur auf strategischer Ebene – statt. Internetbasierte soziale Netzwerke und die weit verbreitete Verfügbarkeit von Mobilkommunikation bieten auch nichtstaatlichen Akteuren die Möglichkeit von diesen Mitteln Gebrauch zu machen.

Die deutschen verteidigungspolitischen Richtlinien sagen hiezu: *„Informations- und Kommunikationsinfrastrukturen gehören heute zu den strategischen Infrastrukturen, ohne die das private und öffentliche Leben zum Stillstand käme. Komplexe und zielgerichtete Angriffe darauf können auf Grund der Interdependenz der Infrastrukturen und einem daraus resultierenden Kaskadeneffekt eine ernstzunehmende Bedrohung für die nationale Sicherheit eines Staates darstellen. Die Geschwindigkeit und Nichtvorhersehbarkeit von Angriffen machen es nahezu unmöglich, den Gegner, seine Herkunft und seine Motive in ein eigenes vorbereitendes Handeln einzubeziehen. Die Möglichkeit, „Cyber-Angriffe" im Nachhinein zu bestreiten, gehört bereits heute zum strategischen Kalkül einer neuen, computergestützten Auseinandersetzung auch zwischen Staaten.*[6]*"* Um den deutschen Richtlinien Folge zu tragen, ist somit die positive Nutzung des Cyberraumes, sind aber auch dessen Gefahren praktisch unbegrenzt.

Die im Fokus dieser Ausarbeitung stehende ÖSCS formuliert hiezu: *„Es gehört somit zu den obersten Prioritäten der Staatenwelt, national und international an der Absicherung des Cyberraums zu arbeiten. Cybersicherheit bedeutet Sicherheit der Infrastruktur des Cyberraums, der im Cyberraum ausgetauschten Daten und vor allem der Menschen, die den Cyberraum nutzen*[7]*"*.

Die Gewährleistung von Cybersicherheit wurde somit zu einer zentralen Herausforderung für Staat, Wirtschaft und Gesellschaft im nationalen und internationalen Kontext und es begannen weltweit die Ausarbeitungen nationaler Cyberstrategien, um der neuen Herausforderung zu begegnen[8].

Die ersten Nationen, die relativ rasch nach dem erwähnten Angriff auf Estland bereits diesbezügliche Strategien verfügten, waren verständlicherweise Estland noch 2007, gefolgt von Kanada und Frankreich bereits 2009. Seitdem erließ die NATO ihre diesbezüglichen strategischen Ausarbeitungen (2011) und weitere Nationen wie Deutschland, Großbritannien, die Niederlande, Tschechien, die Schweiz, Finnland und die USA folgten[9]. Die EU stellte am 7. Februar 2013 den Entwurf des "Cybersicherheitsplans der EU für ein offenes, freies und chancenreiches Internet" vor, der Mitte 2014 beschlossen werden soll[10].

Nach mehrjährigen Vorarbeiten wurde am 20. März 2013 die Österreichische Strategie für Cyber Sicherheit (ÖSCS) vom Ministerrat mit Beschluss 180/8 verabschiedet. Die nachfolgenden Abschnitte sollen die Entwicklungsgeschichte kurz skizzieren.

2. Ein Forschungsprojekt als Initialzündung (BMLVS)

In den Jahren 2007-2009 wurden verstärkt österreichische Experten, hauptsächlich von den im nationalen Sicherheitsrat vertretenen Ressorts[11], zu entsprechenden Symposien bzw. Lessons-Learned-Fachtagungen entsandt. Außerdem wurde die diesbezügliche Forschungstätigkeit verstärkt. 2010 erfolgte als erste Initiative zur Ausarbeitung einer nationalen Cyberstrategie durch das BMLVS der Gedankenanstoß zur Etablierung einer gesamtstaatlichen Forschungsplattform. So lud das BMLVS zum ersten Informationsaustausch zwischen den relevanten Ressorts am 17. Juni 2010 ein (BKA, BMLVS, BM.I, BMEIA, BMVIT).

Grundlage stellte das Regierungsprogramm der XXIV. Gesetzgebungsperiode betreffend die Bildung eines gesamtstaatlichen Sicherheitsclusters zur Schaffung von Synergien im Sicherheitsbereich dar. Im Punkt Sicherheitspolitik-Umfassende Sicherheitsvorsorge wird dort formuliert: *„ … insbesondere zur Gewährleistung einer qualitativ hochwertigen Vernetzung von Aus- und Weiterbildungseinrichtungen für Entscheidungsträger, Experten und Einsatzkräfte aus den verschiedenen sicherheitsrelevanten Bereichen (Polizei, Bundesheer, Katastrophenhilfeeinrichtungen, Blaulichtorganisationen, Wirtschaft, Wissenschaft und Forschung)"*.[12] Dies sollte unter möglichst guter Einbeziehung und Nutzung bestehender Einrichtungen erfolgen, die entsprechend zu vernetzen und weiter zu entwickeln wären. Dabei sollte das österreichische Programm zum Schutz kritischer Infrastrukturen (APCIP) genutzt bzw. entsprechend weiterentwickelt werden.

Von Seiten des BMLVS wurde daher ein nationaler Forschungsbedarf mit folgender Forschungsfrage eingebracht:

Wie kann in Bezug auf Interdependenzen die kritische Informationsinfrastruktur in Österreich angegriffen werden bzw.

6 Verteidigungspolitische Richtlinien des deutschen Bundesministeriums der Verteidigung vom 27.5.2011, S. 3

7 ÖSCS, S. 4.

8 Das Risiko- und Bedrohungsbild bzw. auch die Ableitungen wurden auszugsweise der ÖSCS, dem Militärstrategischen Konzept (MSK) des Österreichischen Bundesheeres bzw. dem derzeit noch in Ausarbeitung befindlichem Konzept des ÖBH „Cyber-Verfahren und -Handlungen" entnommen.

9 Vgl. hiezu auch die Ausarbeitungen des NATO-CCDCoE (Cooperative Cyber Defence Center of Excellence) „National Strategies & Policies", https://ccdcoe.org/328.html (23.01.2014).

10 http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security ((23.01.2014).

11 Bundeskanzleramt (BKA), Bundesministerium für Verteidigung und Sport (BMLVS), Bundesministerium für Inneres (BM.I), Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) sowie Bundesministerium für Justiz (BMJ).

12 Vgl. hiezu auch das Regierungsprogramm der XXIV. Gesetzgebungsperiode, www.bka.gv.at (23.01.2014) S. 139.

wodurch kann ihr wirtschaftlicher und politischer Schaden zugefügt werden, sodass Österreich nicht mehr handlungsfähig ist?

Es sollten zumindest folgende Aspekte der Informationsinfrastruktur-Sicherheit behandelt werden:

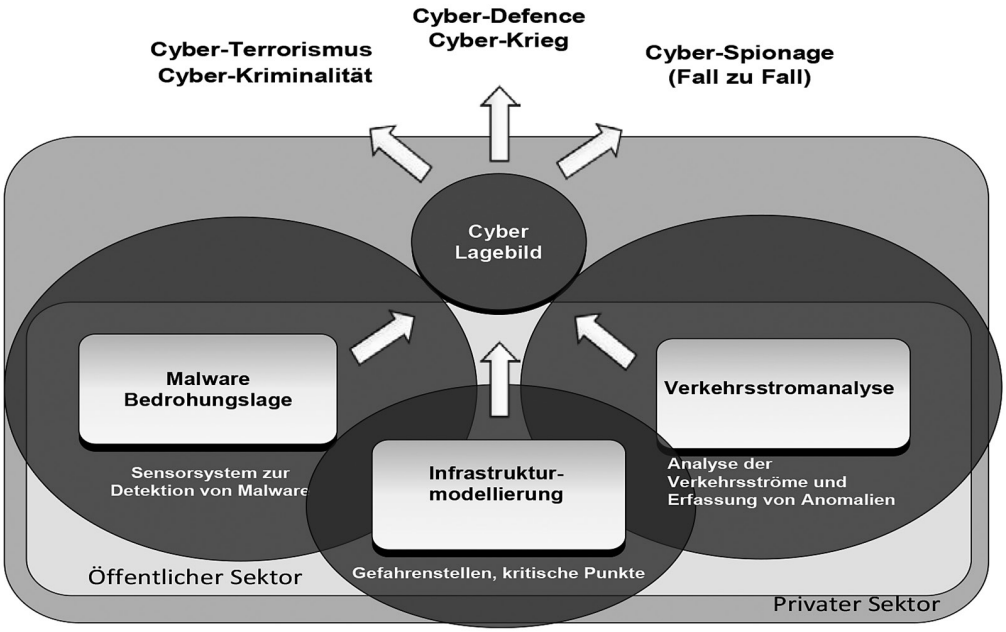
- Die Ermittlung und Ausweisung kritischer nationaler Informationsinfrastrukturen,
- Analyse und Evaluation der vorhandenen Sicherheitsprobleme und Interdependenzen in der österreichischen IKT-Infrastruktur und deren Bedarfsträger,
- Schaffung einer Vernetzung und eines Dialogs zwischen den staatlichen Stellen und den Bedarfsträgern mit den Eigentümern/Betreibern kritischer Informationsinfrastrukturen,
- Ermittlung sektorspezifischer Abhängigkeiten,
- Ausarbeitung von Notfallplänen für die nationale Informationsinfrastruktur.

Trotz einiger Widerstände, die primär auf Zuständigkeitsfragen zurückgingen, formierte sich eine Expertengruppe unter Führung des AIT (Austrian Institute of Technology), welche im Rahmen des nationalen Sicherheitsforschungsprogrammes „KIRAS" Mitte 2011 mit den Ausarbeitungen beauftragt wurde. Das Forschungsprojekt erhielt den Namen „Cyber Attack Information System" (CAIS). Ziel des Projekts war die Entwicklung und Evaluation von Tools zur Analyse und Simulation von Bedrohungen im Cyberraum. Das AIT formulierte damals: *„Das Ausnutzen von Schwachstellen in IKT-Systemen hat sich zu einem profitablen Geschäftsmodell entwickelt. Um besser mit diesen Bedrohungen umgehen zu können, ist eine verstärkte Zusammenarbeit aller Beteiligten notwendig. Das Projekt CAIS beschäftigte sich deshalb mit der Implementierung eines Cyberangriffsinformationssystems auf nationaler Ebene mit dem Ziel, die Widerstandsfähigkeit der heutigen vernetzten Systeme zu stärken und ihre Verfügbarkeit und Vertrauenswürdigkeit zu erhöhen. Hauptziele dieses Projekts waren die Identifizierung der erwarteten künftigen Cyberrisiken und -bedrohungen, die Untersuchung neuartiger Techniken zur Anomalieerkennung, die Entwicklung modularer Infrastrukturmodelle und agentenbasierter Simulationen zur Risiko- und Bedrohungsanalyse und schließlich die Untersuchung von Umsetzungsmöglichkeiten eines nationalen „Cyber Attack Information System"*.[13]

Das Projektkonsortium bestand aus einer ausgewogenen Mischung aus Forschungsinstituten, Partnern aus der Industrie sowie Regierungsbehörden, die eine solide wissenschaftliche Basis, eine anspruchsvolle technische Umsetzung sowie die praktische Anwendbarkeit und Validierung der Ergebnisse gewährleisten sollten.

Der Abschluss erfolgte im vierten Quartal 2013 und lässt sich kurz in untenstehender Graphik skizzieren[14]. Das hierbei entwickelte Tool soll innerhalb der noch zu generierenden staatlichen Struktur zur permanenten Koordination auf operativer Ebene Verwendung finden:

Graphik 1: Funktionsweise CAIS



In der Graphik wird dargestellt, welche Instrumente notwendig sind, um ein staatliches Cyberlagebild generieren zu können. Zunächst muss für die Sicherheit im staatlichen Bereich ein Sensorsystem angelegt werden, das in der Lage ist, sowohl in Mails, auf Websites, in Programmen usw. Schadsoftware zu erkennen, als auch Anomalien im Datenverkehr zwischen den Usern zu erfassen. Um diese Funktionalitäten einrichten zu können, müssen diese idealerweise bereits bei der Erstellung der IT-Architektur von kritischen Infrastrukturen an den jeweiligen Gefahrenstellen (z.B. Schnittstellen) berücksichtigt werden. Die bereitgestellten Sensorinformationen ermöglichen in automatisierter Form die Generierung eines z.B. regional referenzierten Lagebilds, das Auskunft über den Zustand der österreichischen Netze gibt (z.B. Server von kritischen Infrastrukturen in Wien und ihre Verbindungen). Aufgrund dieser Informationen ist es möglich, bei Auftreten von Unregelmäßigkeiten nach einer Lagebeurteilung durch Experten den entsprechenden Akteuren (z.B. Einrichtungen von BKA, BM.I, BMLVS) die richtigen Handlungsanweisungen zu geben, um Gegenmaßnahmen einzuleiten. Dem Betreiber muss dieser

13 Aus der Projektausschreibung des AIT. Nachzulesen unter: http://www.ait.ac.at/research-services/research- services-safety-security/ict-security/referenzprojekte/cais-cyber-attack-information-system (23.01.2014).

14 Die Graphik entstammt einem Vortrag von Obst Schröfl, welchen dieser erstmalig im Mai 2012 anlässlich eines Vortrages über die Erwartungshaltung der Bedarfsträger am Forschungsprojekt vor den Abteilungsleitern der SII/BMLVS, hielt. Die Graphik basiert auf einer Ablaufanalyse AIT.

Vorfall zu diesem Zeitpunkt noch nicht einmal bekannt sein. Der Vorteil für den Betreiber liegt auf der Hand: Durch die staatliche Überwachung des Datenflusses (nicht der Inhalte!) entsteht eine zusätzliche Absicherung seiner Netze. In weiterer Folge kann dieses Modell auch auf jene Unternehmen ausgeweitet werden, die bereit sind, ihre Netze in das Sensorsystem einzubinden.

Es wurde damit der erste Abschnitt zur Erarbeitung der ÖSCS beendet.

3. Die Initiative zur Ausarbeitung einer Informations-, Kommunikations- und Technologie-Sicherheitsstrategie (BKA)

Am 16. November 2011 startete die Ausarbeitung einer nationalen IKT-Sicherheitsstrategie mit dem Kickoff mit ca. 200 Teilnehmern aus allen wichtigen Cybersicherheitsbereichen, initiiert durch das BKA. Zwei Drittel der Teilnehmer sagten sofort eine aktive Teilnahme bei der Entwicklung der Strategie zu.

Als Ziele wurden festgelegt:

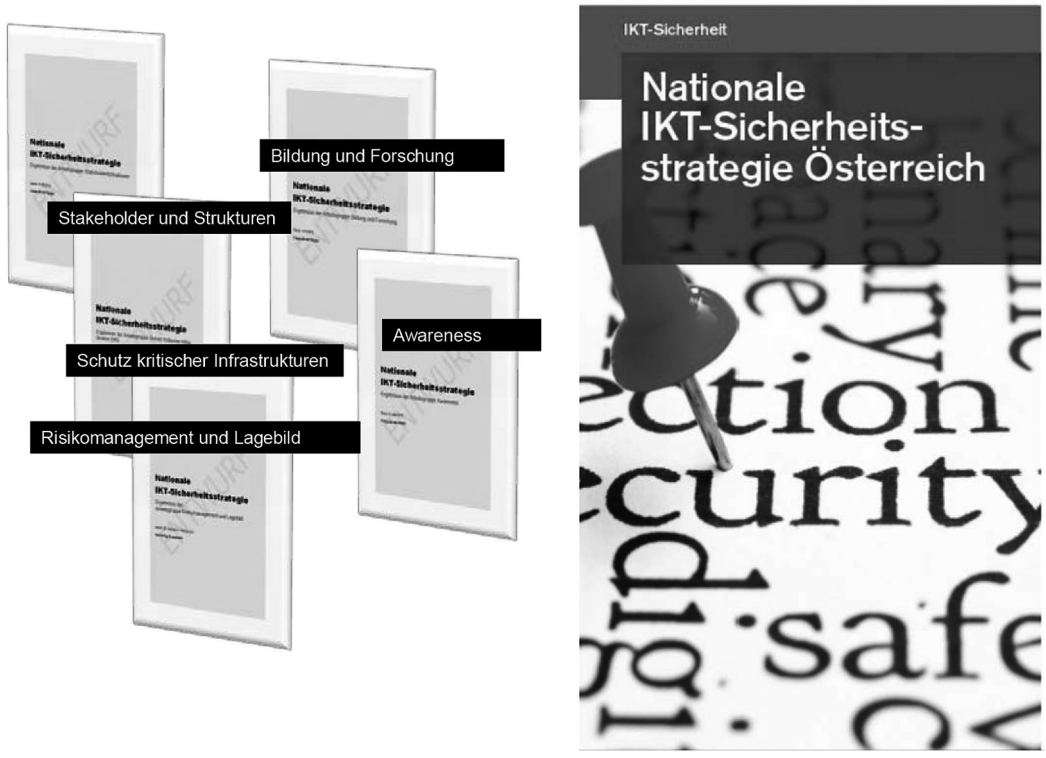
- Erarbeiten eines gemeinsamen Verständnisses von Cybersicherheit in Österreich für eine in weiterer Folge noch auszuarbeitende nationale Cyberstrategie.
- Erarbeiten eines Cybersicherheitsmaßnahmenkatalogs für alle relevanten Bereiche in Österreich.
- Erstellen eines detaillierten Aktionsplans zum Umsetzen der definierten Ziele.
- Beteiligung eines repräsentativen Querschnitts von Österreichs Cybersicherheits-Stakeholder aus Industrie, Akademien und öffentlicher Verwaltung.
- Enge Zusammenarbeit von Österreichs Cybersicherheits-Stakeholdern durch gemeinsames Erarbeiten einer Strategie zur Absicherung des Cyberraums.
- Erzeugen eines gemeinsamen Verständnisses zur Umsetzung der Ergebnisse der IKT-Sicherheitsstrategie[15].

Die strategischen Zielsetzungen und Maßnahmen präsentierten sich damit aus der Perspektive von fünf Kernbereichen, welche in der damaligen Sitzung festgelegt wurden und zugleich auch die Unterkapitel der Strategie darstellen sollten:

- Stakeholder und Strukturen,
- kritische Infrastrukturen,
- Risikomanagement und Lagebild,
- Bildung und Forschung,
- Bewusstseinsbildung (Awareness)

Zu jedem dieser Punkte wurde eine Arbeitsgruppe eingesetzt, welche die Ergebnisse erarbeiten sollte. Nach siebenmonatiger intensiver Ausarbeitungs- bzw. Konsultationsperiode präsentierte das BKA am 15. Juni 2012 schlussendlich das Dokument „Nationale IKT-Sicherheitsstrategie Österreich" im feierlichen Rahmen. Ein Anhang der Strategie stellte die erstmalige Ausarbeitung und Publizierung eines IKT-/Cyber-Lexikons dar, um eine gemeinsame Sprache und somit auch einen Rahmen für die Entwicklung, Erlangung und in weiterer Folge Aufrechterhaltung einer gemeinsamen IKT-Sicherheitswahrnehmung zu schaffen.

Graphik 2: Die IKT-Sicherheitsstrategie mit ihren Unterkapiteln



Der zweite Abschnitt zur Erarbeitung der Cyber Strategie Österreichs war somit beendet.

4. Die Initiative zur Ausarbeitung einer Cyberrisikomatrix durch das KSÖ (Kuratorium Sicheres Österreich) im Auftrag des BM.I

Im Herbst 2011 erfolgte der nächste Schritt, diesmal durch das BM.I. Seitens des mit der Ausarbeitung der Cyberrisikomatrix

15 Die Ziele wurden am 16.11.2011 im Rahmen der ersten Besprechung festgelegt und sind in Form einer Präsentation an die Teilnehmer versandt worden. Abrufbar unter: http://www.bka.gv.at/Docs/2013/3/11/Vock_vortrag.pdf (23.01.2014).

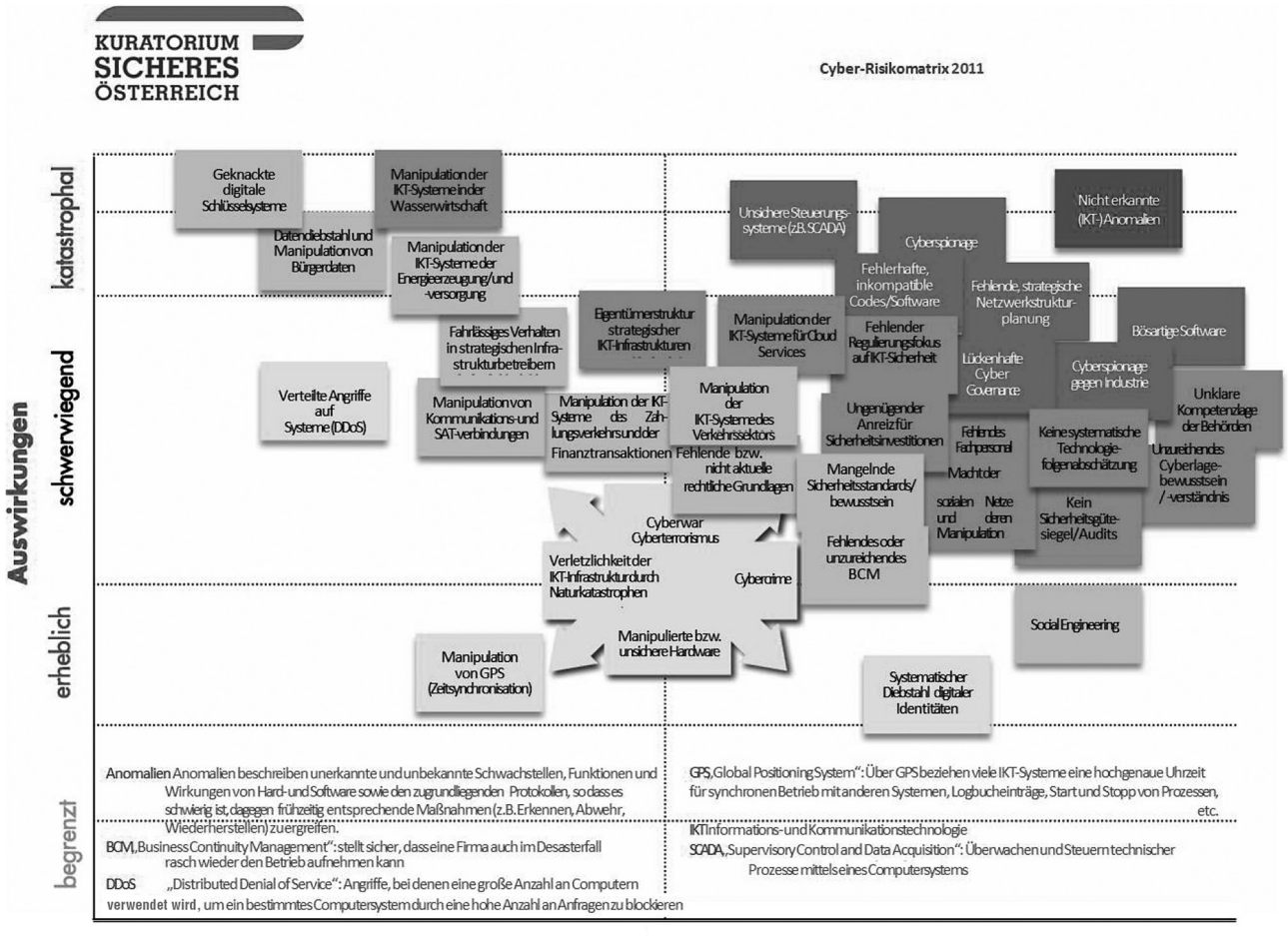
beauftragten KSÖ-Studienteams wurden in einer ersten Runde Vertreter der Wirtschaft und involvierte Behörden mittels eines Fragebogens über deren Einschätzung von Cyberbedrohungen befragt. Die diesbezüglichen Parameter wurden von Seiten des KSÖ folgendermaßen festgelegt[16]:

- *Sehr hohe Relevanz:* Das Risiko gefährdet die Funktionsfähigkeit der kritischen Systemelemente bzw. Geschäftsprozesse ihrer Organisation in umfassender Weise. Abwehr- und Bewältigungsmaßnahmen sind kaum oder nur mit sehr großem (zeitlichem, organisatorischem, personellem und finanziellem) Aufwand möglich und gehen über die vorgesehenen Sicherheitsmaßnahmen hinaus. Das Risiko ist für ihre Organisation existenzgefährdend.
- *Hohe Relevanz:* Das Risiko gefährdet die Funktionsfähigkeit ausgewählter kritischer Elemente und Geschäftsprozesse. Abwehr- und Bewältigungsmaßnahmen im Rahmen bestehender Sicherheitsvorkehrungen reichen gerade noch aus, um mit dem entsprechenden Risiko umzugehen.
- *Niedrige Relevanz:* Das Risiko gefährdet ausgewählte Systemelemente und/oder Geschäftsprozesse, die für die Funktionsfähigkeit Ihrer Organisation kritisch bzw. nicht kritisch sein können. Die vorgesehenen Sicherheitsvorkehrungen reichen vollständig aus, um das entsprechende Risiko zu bewältigen.
- *Sehr niedrige Relevanz:* Das Risiko gefährdet nur einzelne Systemelemente oder Geschäftsprozesse, die für die Leistungsfähigkeit Ihrer Organisation nicht kritisch sind. Die bestehenden Sicherheitsvorkehrungen reichen aus.

Die daraufhin ausgearbeitete Cyberrisikomatrix führte das Kuratorium sicheres Österreich einer vertiefenden Cyberrisikoanalyse in den Sektoren IKT, Energie, Verkehr, Finanzen/Versicherungen und öffentliche Behörden zu. Ziel war es, in Zusammenarbeit mit ausgewählten Vertretern der genannten Sektoren die in der Cyberrisikomatrix allgemein dargestellten Cyberrisiken aus sektorspezifischer Sicht zu bewerten sowie den Stand der sektorspezifischen Vorbereitung zum Umgang mit den entsprechenden Cyberrisiken zu erfassen. Weiters waren daraus entstehende Stärken und Schwächen der Cybersicherheit in ausgewählten Infrastruktursektoren abzuleiten; zu identifizieren, welche Maßnahmen geeignet sind, um bestehende Stärken auszubauen und vorhandene Schwächen zu überbrücken sowie Vorschläge für die künftige Zusammenarbeit der öffentlichen und privatwirtschaftlichen Bedarfsträger im Kontext der Cybersicherheit zu entwickeln.

Die finalisierte Cyberrisikomatrix wurde in Form einer Publikation Ende Juni 2012 vorgestellt[17].

Graphik 3: Akkordierte Fassung der Cyber-Risikomatrix vom Juni 2012



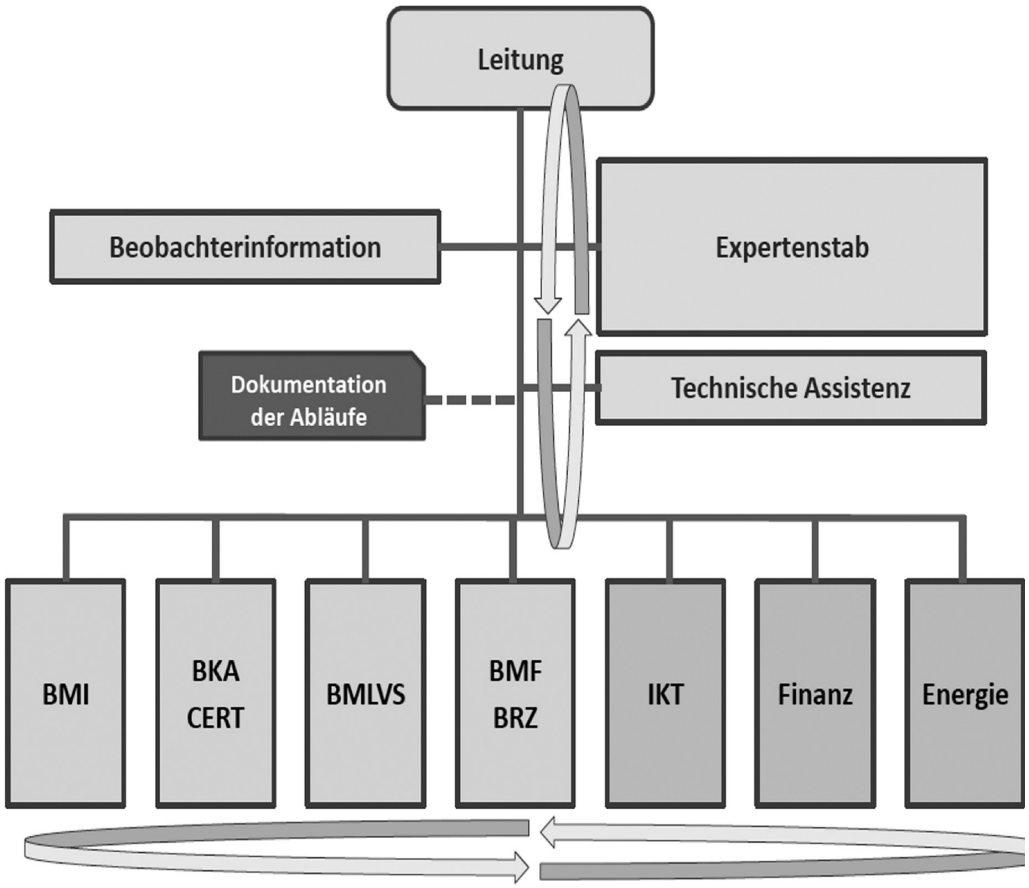
16 KSÖ-Fragebogen vom November 2011; Inhalte abrufbar unter: http://www.kuratorium-sicheres-oesterreich.at/themen/detail-ansicht/thema/ksoe-praesentiert-cyber-risikomatrix-fuer-oesterreich (23.01.2014).

17 Cyberrisikomatrix, diesbezügliche Erläuterungen sowie die Publikation in elektronischer Form sind abrufbar unter: http://www.kuratorium-sicheres-oesterreich.at/themen/detail-ansicht/thema/ksoe-praesentiert-cyber-risikomatrix-fuer-oesterreich (23.01.2014).

Gleichzeitig erfolgte am 22. Juni 2012 im Rahmen eines Planspiels die Evaluierung der Matrix. Planspielziele waren:

- praktisches Erleben eines realitätsnahen, komplexen Bedrohungsszenarios,
- möglichst realistische Nachstellung (Echtzeitablauf so weit als möglich),
- Bewältigung des Szenarios durch Spieler von Behörden und aus der Wirtschaft (Ansprechen, Bewerten, Folgern),
- Fokus auf Kommunikation und organisatorische Abläufe, nicht auf technische Bewältigung der Bedrohung,
- Feststellen von Verbesserungspotenzial und Abstimmungsbedarf,
- Optimierung der Zusammenarbeit/Kommunikation der Spieler.

Graphik 4: Spielaufbau des ersten gesamtstaatlichen Cyber-Planspiels



Spielinhalt stellte der Ausfall von Kerninfrastruktur des Internets eines Landes dar. Die Ausmaße des Ausfalls sollten durch Kooperation der teilnehmenden Spieler innerhalb und außerhalb ihrer Organisation erkannt werden. Dies führte zur teilweisen Lösung der Probleme durch Anordnung technischer Maßnahmen; die Lage eskalierte allerdings durch einen gezielten Angriff auf die Infrastruktur des Landes, was zur Befassung durch die Computer Emergency Response Teams (CERT) und Meetings des nationalen Einsatz- und Kontrollcenters (EKC) zur Koordination führte.

Dies stellte den Abschluss der dritten Initiative zur Ausarbeitung der Cyber Strategie Österreich dar.

5. Die Initiative zur Etablierung eines IKT-Sicherheitsportals in Österreich durch das BKA und das Bundesministerium für Finanzen (BMF)

Eine der strategischen Zielsetzungen der IKT-Sicherheitsstrategie war die Etablierung eines IKT-Sicherheitsportals in Form eines konzertierten Internetauftritts. Die Umsetzung hierfür erfolgt bereits ab Herbst 2012[18].

Das IKT-Sicherheitsportal fungiert in Form einer Web-Plattform für alle Zielgruppen in Österreich als zentrale Anlaufstelle für Themen der IKT-Sicherheit und als grundlegende Informations- und Kommunikationsbasis aller Awareness-Maßnahmen. Zu den Zielgruppen zählen sowohl IKT-AnwenderInnen als auch IKT-AuftraggeberInnen und IKT-DienstleisterInnen (in Handel, Entwicklung und Betrieb).

Das Informationsangebot des IKT-Sicherheitsportals soll mit einem breiten Themenumfang sowohl Laien als auch Experten zielgruppenspezifische Informationen über bestehende IKT-Gefährdungen sowie konkrete Handlungsempfehlungen für ein sicherheitsbewusstes Handeln bereitstellen. Die verfügbaren Portalinhalte, die in Form von zielgruppenspezifischen Inhalten, Portalservices und redaktionellen Beiträgen verfügbar sind, sollen eine effiziente Nutzung des Portals ermöglichen und das Auffinden sicherheitsrelevanter Informationen sowie zuständiger Behörden und Institutionen im Internet wesentlich erleichtern[19].

18 So nachzulesen auf dem inzwischen im Netz befindlichen Portal: www.onlinesicherheit.gv.at. Dort ist auch explizit erwähnt: *„Das IKT-Sicherheitsportal ist eine interministerielle Initiative in Kooperation mit der österreichischen Wirtschaft und fungiert als zentrales Internetportal für Themen rund um die Sicherheit der Informations- und Kommunikationstechnologie“* (23.01.2014).

19 Zusammenfassung des Ausschreibetextes von Seiten des BMF. Nachzulesen auf: „IKT-Sicherheitsportal-Umsetzungskonzept.doc“ lt. www.onlinesicherheit.gv.at (23.01.2014).

Auftraggeber des IKT-Sicherheitsportals waren BMF sowie BKA, wobei das BMF den Ausschreibetext formulierte und im November 2012 aussandte[20]. Die redaktionelle Gesamtverantwortung wird durch das Zentrum für sichere Informationstechnologie – Austria (A-SIT) wahrgenommen.

Die Struktur des IKT-Sicherheitsportals sieht folgende Kernelemente vor:

1. Navigationsbereich – Abbildung der Portal-Zielgruppen,
2. Infobox – Kurzbeschreibung des IKT-Sicherheitsportals,
3. Contentbereich – zielgruppenspezifische Aufbereitung der Portalinhalte,
4. Portal-Services – themenspezifische Abfragemöglichkeiten,
5. Redaktionelle Beiträge durch Kooperationspartner sowie weiterführende Informationen und Aktuelles.

Das Portal ist jederzeit im Internet unter www.onlinesicherheit.gv.at oder über den Suchbegriff IKT-Sicherheitsportal zu finden und stellt den Abschluss der vierten Initiative zur Ausarbeitung der Cyber Strategie Österreich dar. Parallel zu den Initiativen erfolgte auch der Beginn der ressortinternen Bearbeitungen innerhalb BKA (Cyber Security), BMLVS (Cyber Defence), BM.I (Cyber Crime) und BMeiA (Cyber Diplomacy).

Graphik 5: Portalinhalte für Portalservices und Zielgruppen

Portalservices
Gefährdungstrends
Compliance- und Sicherheits-Checks
Sicherheitshandbuch
Publikationsabfrage
Behörden- und Institutionssuche
Sicherheitswarnungen
News / Newsletter
Veranstaltungen
IKT-Sicherheitslexikon
Hilfe / Sitemap
Impressum
Zielgruppen
Kinder & Jugendliche
Eltern
Lehrende
Konsument/innen
Generation 60plus
Arbeitnehmer/innen
Forscher/innen
Unternehmer/innen
öffentliche Verwaltung
nationale Sicherheitsinitiativen

6. Die Erarbeitung der österreichischen Strategie für Cybersicherheit (ÖSCS)

Ziel aller bisher erwähnten Initiativen war die Erstellung einer österreichischen Cyberstrategie. Am 11. Mai 2012 erfolgte nun der Startschuss für die Erarbeitung der ÖSCS. mittels Ministerratsvortrag (MRV) durch BKA, BMLVS, BM.I und BMEIA. Die Eckpunkte des MRV stellten sich wie folgt dar[21]:

- Gefordert wird ein breites Zusammenwirken aller betroffenen Akteure im Rahmen eines Gesamtkonzepts.
- Die Initiativen der Ministerien BKA, BM.I, BMLVS und BMeiA sind Beiträge für das Cyber-Security-Gesamtkonzept. Deren Ergebnisse werden in den gesamtstaatlichen Prozess zur Erstellung und Umsetzung der Cyberstrategie einfließen. Alle Initiativen und Aktivitäten sollen fortgesetzt werden.
- Die Strategie ist vom BKA gemeinsam mit einer neuen Cybersecurity-Steuerungsgruppe (nationaler Sicherheitsrat + Cyberexperten) vorzubereiten.
- Bereits aufgesetzte Aktivitäten im operativen Bereich sollen eigenverantwortlich weitergeführt werden. Nutzung von Synergien sowie notwendige Strukturen sind in der Cyber Security Strategie festzulegen.
- Bei übergreifenden Cyber-Security-Herausforderungen soll das das BM.I – ähnlich dem staatlichen Krisen- und Katastrophenmanagement – die Federführung übernehmen. Es wird bei der entsprechenden Koordination auf der operativen Ebene vom BMLVS unterstützt, auf das die Federführung im Cyber-Defence-Fall übergehen würde. Die im Bereich Cyber Security relevanten außenpolitischen Maßnahmen werden vom BMeiA koordiniert.
- Zur laufenden Kommunikation mit allen Stakeholdern aus Verwaltung, Wirtschaft und Wissenschaft soll gemeinsam von Bundeskanzleramt, Bundesministerium für Inneres, Bundesministerium für Landesverteidigung und Sport und Bundesministerium für europäische und internationale Angelegenheiten eine Cyber Security Plattform betrieben werden.

Nach mehrjährigen Vorarbeiten wurde am 20. März 2013 nun die ÖSCS vom Ministerrat laut Beschluss 180/8 verabschiedet. Sie gliedert sich nach einer kurzen Einleitung in die Erörterung der Chancen, Risiken und Bedrohungen im Cyberraum, denen die Prinzipien, die strategischen Ziele, Handlungsfelder und Maßnahmen sowie die Umsetzung folgen.

Einleitend wird festgehalten, dass die ÖSCS[22]: *„ein umfassendes und proaktives Konzept zum Schutz des Cyberraums und der Menschen im virtuellen Raum unter Gewährleistung ihrer Menschenrechte darstellt. Sie soll die Sicherheit und Widerstandskraft der österreichischen Infrastrukturen und Leistungen im Cyberraum verbessern, vor allem aber soll sie Bewusstsein und Vertrauen in der österreichischen Gesellschaft schaffen. Die Strategie für Cybersicherheit leitet sich aus der Sicherheitsstrategie[23] ab und orientiert sich an den Prinzipien des Programms zum Schutz kritischer Infrastrukturen“*.[24]

Die Chancen werden als Informations- und Kommunikationsraum, sozialer Interaktionsraum, Wirtschafts- und Handelsraum, politischer Partizipationsraum und Steuerungsraum beschrieben, da sich der Cyberraum zu einem vitalen Aktionsraum für den Staat, die Wirtschaft, die Wissenschaft und die Gesellschaft entwickelt hat. Bei Risiken und Bedrohungen wird

20 Ebenda.
21 Zusammenfassung des MRV vom 11.05.2012, nachzulesen auf www.bka.gv.at/DocView.axd?CobId=507 (23.01.2014).
22 ÖSCS, S. 4 ff.
23 Ministerratsbeschluss vom 1. März 2011, inzwischen am 3. Juli 2013 vom Nationalrat beschlossen, vgl. hiezu auch www.bka.gv.at/DocView (23.01.2014).
24 Ministerratsbeschluss vom 2. April 2008, vgl. hiezu auch www.bka.gv.at/DocView (23.01.2014).

generell auf die der ÖSCS angeschlossene, bereits unter Teil 4 behandelte Cyberrisikomatrix verwiesen[25].

Für den Bereich Cybersicherheit sollen dieselben Prinzipien gelten wie für die IKT-Sicherheit: Vertraulichkeit, Integrität, Verbindlichkeit, Authentizität, Verfügbarkeit sowie Privatsphäre und Datenschutz. Darüber hinaus wird festgehalten, dass die: *„Umsetzung der Cybersicherheitspolitik ein Querschnittsthema darstellt, das in vielen Lebens- und Politikbereichen mitgedacht werden muss. Sie muss somit umfassend und integriert angelegt, aktiv gestaltet und solidarisch umgesetzt werden. Auf einen umfassenden (äußere und innere Sicherheit sowie zivile und militärische Sicherheitsaspekte sind aufs Engste verknüpft), integrierten, proaktiven und solidarischen Ansatz der Cybersicherheitspolitik, der auf den grundlegenden Prinzipien der Rechtsstaatlichkeit, Subsidiarität, Selbstregulierung und Verhältnismäßigkeit beruht, wird besonderer Wert gelegt"*.[26]

Die wesentlichsten strategischen Ziele lassen sich folgt beschreiben[27]:

- Sowohl Verfügbarkeit, Zuverlässigkeit und Vertraulichkeit des Datenaustauschs als auch Integrität der Daten selbst sind nur in einem sicheren, resilienten und verlässlichen Cyberraum gewährleistet. Deshalb muss der virtuelle Raum fähig sein, Risiken zu widerstehen, Schocks zu absorbieren und sich einem veränderten Umfeld anzupassen. Besonders wichtige IKT-Systeme sollen möglichst redundant ausgelegt werden.
- Österreich wird durch einen gesamtstaatlichen Ansatz der zuständigen Bundesministerien sicherstellen, dass seine IKT-Infrastrukturen sicher und resilient gegen Gefährdungen sind. Die staatlichen Stellen werden dabei eng und partnerschaftlich mit dem privaten Sektor zusammenarbeiten.
- Das Rechtsgut Cybersicherheit wird von den österreichischen Behörden in Zusammenarbeit mit nichtstaatlichen Partnern unter Einsatz wirksamer und verhältnismäßiger Mittel in den Bereichen der politisch-strategischen Steuerung, der Erkennung und Reaktion sowie der Folgenminderung und Wiederherstellung geschützt.
- Durch eine Vielzahl von Awareness-Maßnahmen wird eine „Kultur der Cybersicherheit" in Österreich implementiert.

An Maßnahmen wäre insbesondere das Handlungsfeld 1 „Strukturen und Prozesse" zu erwähnen, das festlegt: *„Es sind daher Prozesse und Strukturen festzulegen, die eine übergeordnete Koordination sowohl auf politisch-strategischer Ebene als auch auf operativer Ebene unter Einschluss aller relevanten Stakeholder im öffentlichen und privaten Bereich sicherstellen"*.[28]

Als einer der wesentlichsten Umsetzungsmaßnahmen wurden die Aufgaben der mit Ministerratsbeschluss vom 11. Mai 2012 eingerichteten Cyber Sicherheit Steuerungsgruppe (CSS) beschrieben. Die CSS koordiniert unter Federführung des BKA nicht nur wie bisher die Maßnahmen zur Cybersicherheit, sondern beobachtet und begleitet auch die Umsetzung der ÖSCS, erstellt einen Bericht und berät die Bundesregierung in allen Angelegenheiten der Cybersicherheit. Mitglieder der CSS sind die Ressorts BKA, BMLVS, BM.I, BMEIA sowie BMJ und hier die jeweiligen Verbindungspersonen zum Nationalen Sicherheitsrat[29] und Cybersicherheitsexperten. Auch der Chief Information Officer des Bundes gehört diesem Gremium an. Themenorientiert kann die CSS um Vertreter weiterer Ressorts sowie der Länder bzw. der Wirtschaft erweitert werden[30].

Weiters wurden die Tätigkeit einer operativen Koordinierungsstruktur erkannt und die Aufgaben im Wesentlichen beschrieben. *„Aufbauend auf bestehende operative Strukturen sowie unter deren Einbindung wird eine **Struktur zur Koordination auf der operativen Ebene** geschaffen. In ihrem Rahmen soll insbesondere ein periodisches und anlassbezogenes **Lagebild Cyber Sicherheit** erstellt und über zu treffende Maßnahmen auf der operativen Ebene beraten werden. Gewährleistet werden soll auch ein kontinuierlicher Überblick über die aktuelle Situation im Cyber Space durch Sammeln, Bündeln, Auswerten und Weitergeben von relevanten Informationen. Dabei ist auch die Wirtschaft in geeigneter Form auf Augenhöhe einzubinden. Der permanent und gemeinsam erarbeitete Status zur Situation im Cyberspace soll allen Beteiligten als Grundlage für zu treffende planerische, präventive und reaktive Maßnahmen dienlich sein. Die Betreiber von kritischen Infrastrukturen werden auf der operativen Ebene und insbesondere bei Störungen im Bereich der Informations- und Kommunikationsstrukturen unterstützt sowie über Gefahren im Netz informiert. Die Operative Koordinierungsstruktur ist so zu gestalten, dass es möglich ist, sie als operatives Ausführungsorgan des übergreifenden Cyber Krisenmanagement zu nützen, und sollen „unter Einbindung der Ressorts und operativer Strukturen aus Wirtschaft und Forschung vom BM.I koordiniert (PPP-Modell) werden. Es wird bei der entsprechenden Koordination auf der operativen Ebene vom BMLVS unterstützt, auf das die Federführung im Cyber Defence Fall übergeht. Die operativen organisations-, sektoren- bzw. zielgruppenorientierten Strukturen bleiben im jeweiligen Verantwortungsbereich. Im Rahmen der Operativen Koordinierungsstruktur sollen Einrichtungen zusammenarbeiten, die sich mit der Sicherheit von Computersystemen und des Internets sowie dem Schutz von kritischen Infrastrukturen beschäftigen. Es sind dies im staatlichen Bereich insbesondere GovCERT (Government Computer Emergency Response Team), MilCERT (Military Cyber Emergency Readiness Team) und das Cyber Crime Competence Center (C 4). Darüber hinaus werden in einem zweiten Kreis weitere staatliche Einrichtungen sowie in einem erweiterten Kreis private CERTs (CERT.at, BRZ-CERT, Banken, …), Wirtschaft und Forschung eingebunden."*[31]

Die ÖSCS legt auch detailliert fest, welche Maßnahmen im Anschluss der Beschlussfassung zu tätigen sind. So wurde beispielsweise auch festgehalten, dass die CSS innerhalb von drei Monaten nach Beschluss der ÖSCS durch die Bundesregierung einen Implementierungsplan für die in der Strategie angeführten horizontalen Maßnahmen erarbeitet. Der Implementierungsplan wurde im Juli 2013 von der Steuerungsgruppe beschlossen[32].

25 ÖSCS, S. 6.
26 Siehe http://www.digitales.oesterreich.gv.at bzw. S. 7 ff. der ÖSCS.
27 ÖSCS, S. 9.
28 ÖSCS, S. 10.
29 Bundesgesetz über die Errichtung eines Nationalen Sicherheitsrates § 5 Abs. 1.
30 Exakt beschrieben in der ÖSCS. S. 10.
31 ÖSCS, S. 10 ff.
32 Beschluss der CSS vom 6. Juni 2013, diesbezügliches Protokoll nur intern verteilt und aufliegend bei den Autoren des Artikels.

Darüber hinaus wurden bereits vom ÖSCS-Team (welches für die Sitzungsvorbereitung und die administrativ und organisatorische Umsetzung der ÖSCS verantwortlich zeichnet und sich aus Vertretern BKA, BM.I und BMLVS zusammensetzt) Projektaufträge für die wesentlichsten Umsetzungspunkte des Implementierungsplans erstellt.

Die derzeit behandelten Projektaufträge sollen spätestens Mitte 2014 abgeschlossen sein und beinhalten die folgenden im Rahmen des Umsetzungsprozesses von Seiten der CSS priorisierten Aktionen[33]:

1. Erarbeitung von Prozessen und Strukturen zur permanenten Koordination auf der operativen Ebene,
2. ordnungspolitischer Rahmen,
3. Cyber Sicherheitsplattform (CSP) und Konzept „Kritische Infrastrukturen“,
4. Cyber-Kommunikationsstrategie.

33 Ibid.

7. Schlussbemerkung

Abschließend lässt sich feststellen, dass Österreich in einem sehr gediegenen Prozess eine Cyberstrategie entwickelt hat, die auf die österreichischen Verhältnisse optimal zugeschnitten ist und insgesamt die gesamtstaatliche Zusammenarbeit erheblich verbessert hat. Durch die „Entgrenzung“ im Cyberraum ist die Unterscheidung zwischen Innen- und Außenangelegenheiten sowie zwischen kriminellen und (feindlichen) staatlichen Aktivitäten wesentlich schwieriger geworden. Dementsprechend sind auch die herkömmlichen Zuständigkeiten im Cyberraum nicht mehr zu halten und eine intensive Zusammenarbeit das Gebot der Stunde. Die Österreichische Cyber Sicherheitsstrategie setzt die Tradition der umfassenden Sicherheitsvorsorge weiter fort und gilt auch schon als Vorbild für ähnlich organisierte Staaten. Insgesamt kann ein sicheres Cyberumfeld auch zu einem Wettbewerbsvorteil für den österreichischen Wirtschaftsstandort beitragen.

BEITRÄGE AUS SICHERHEITSPOLITIK UND FRIEDENSFORSCHUNG

Sixty Minutes to Strike: Assessing the Risks, Benefits, and Arms Control Implications of Conventional Prompt Global Strike

Dennis M. Gormley[1]

Abstract: The United States faces the dilemma of reassuring the Russian Federation that America's "unrivaled superiority in conventional weapons" represents a stable future in which Russia would be willing to eliminate its own nuclear weapons. Russia has expressed concern about U.S. intentions to deploy new Conventional Prompt Global Strike (CPGS) delivery systems coupled with its growing arsenal of missile defenses and other advanced conventional systems. This article examines the risks, benefits, and arms control implications of CPGS systems, which are intended to strike targets any place on earth in roughly 60 minutes. Although I argue that the dangers and risks of deploying CPGS weapons greatly exceed the presumed benefits, and that more suitable, if less prompt, means exist of attacking such time-urgent targets, if the United States still proceeds to deploy these weapons, it will need to employ various arms control measures to allay legitimate Russian concerns about the threatening character of U.S. precision strike weapons.

Keywords: Conventional prompt global strike, nuclear reductions, U.S.-Russian arms control, treaty counting rules
Konventioneller globaler Sofortschlag, Nuklearwaffenabbau, US-russische Rüstungskontrolle, Vertragszählregeln

1. Introduction

Less than three months after he took office in 2009, President Barack Obama, speaking in historic Prague, asserted the right of all people to live free from the threat of nuclear devastation. To that end, Obama declared that the United States had a moral responsibility to move toward that goal, by leading a global quest "to seek the peace and security of a world without nuclear weapons."[2] The following year, the Obama administration

1 Dennis Gormley is Senior Research Fellow and Senior Lecturer at the Graduate School of Public and International Affairs, University of Pittsburgh. The author thanks Dr. Gregory DeSantis, Dr. Sonia Ben Ouagrham-Gormley, and Richard Grubb for their careful comments on an earlier version of this paper.
This article has been peer-reviewed.

2 "Obama Prague Speech on Nuclear Weapons: FULL TEXT," *Huffington Post,* first posted, May 6, 2009, updated April 25, 2011, http://www.huffingtonpost.com/2009/04/05/obama-prague-speech-on-nu_n_183219.html.