"net fragmentation" see a greatly increased amount of geopolitical tension in cyberspace, with espionage attacks and preparations for all-out warfare blending together in a seamless conflict area of constant "war of the webs". This geopolitical tension is somewhat offset by a marginal decrease in cybercrime, as the new borders and alliances in cyberspace makes global cybercrime more difficult. At the same time, the effective freeze of the free movement of ideas and news means that globalization – at least as a cultural quality – goes into reverse.

4.4. **"Muddling On":** In this scenario group, not much seems to change. The Internet muddles on, security remains an afterthought, and the development of standards and services continues at light-speed. Most scenario variants here revolve around the occurrence of specific geopolitical events, such as crises between individual countries, or the continuing spying and surveillance scandals. In both cases, the increased insecurity of the average consumer may prompt a drive towards commercial "walled gardens" that seek to simplify and secure the user experience, reducing the Internet to a series of apps, or even less. This trend is somewhat offset by the burgeoning "Internet of Things" that requires a certain amount of interconnectivity to be successful and is especially conducive to "generative" technology. This continuation of the rapid technology development means that cyber-attack options will continue to greatly outstrip defense options, encouraging concepts such as resilience and redundancy instead. Similarly, the unceasing media coverage on cyber espionage and, increasingly, cyber activism/terrorism means that there is a higher awareness in the population for the geopolitical dimension of cyber security.

As said previously, all attempts to look into the cyber crystal ball will be completely contingent on the observer's point of view. Equally, the devil is in the details – some of the scenarios within the individual groups differ starkly from each other in outcome, even if they have been assigned the same scenario group. A persistent theme in those groups, as well as this essay as a whole, is the difference in perception of the value of information in general as well as the role of the Internet in particular. The views and aims of liberal democracies and authoritarian governments do have some commonality, but in essence are so very much divergent that, in the view of this author, they are incompatible with each other on a very basic level. The main difference between any "liberal democracy" – including those outside of the OECD – and an "authoritarian state" is the overriding focus of the latter on regime stability, to the detriment of all other considerations. That also means that liberal democracies are particularly challenged when engaging with those nations on such issues as Internet governance – for these issues may very well be considered as "existential" issues for an authoritarian regime, and something that is worth a maximum level of effort. It can be doubted that most liberal democracies see the stakes as being quite so high. But they should.

Cyber Defence – eine nationale Herausforderung

Walter J. Unger*

Abstract: Facing the increasing dependence on cyber infrastructures and vulnerability of the current information society through cyber attacks, this article defines various risks within cyberspace, potential scenarios and challenges of such an attack, as well as in the context of international law and international humanitarian law. The article focuses on questions of responsibility – getting more complex given the non-governmental aspects of cyberspace –, constant protection of critical infrastructure and Europeanization of those aspects which are as relevant as Austria's role, implementing the EU's policies. Finally, it discusses the tasks of the Austrian Armed Forces within cyberspace in the context of defending the sovereignty of Austria in case of an attack.

Keywords: Informations- und Kommunikationstechnologie, Infrastrukturschutz, Internetkriminalität, Internetsicherheit; Information and communication technology, security of infrastructure, cybercrime, cybersecurity.

1. Einleitung

Der Cyberraum[1][2] (englisch Cyberspace)[3] ist jener virtuelle Raum, der durch die Vernetzung von Computern entstanden ist. Derzeit sind bereits mehr als zwei

* Mag. Walter J. Unger, Oberst des Generalstabsdienstes. 2006-2008 Leiter der Interministeriellen Arbeitsgruppe Strategie „IKT-Sicherheit", 2009 Leiter der Abteilung IKT-Sicherheit, seit Mai 2013 Leiter der Abteilung Cyber Defence & IKT-Sicherheit im Abwehramt im Bundesministerium für Landesverteidigung und Sport.

Der Autor dankt Frau Ella-Maria Moritz für ihre wertvolle Unterstützung.

1 Gem. BKA, Österreichische Strategie für Cyber Sicherheit, (ÖSCS), Wien 2013, S. 21 ist der „Cyber Raum der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab. Dem Cyber Raum liegt als universelles und öffentlich zugängliches Verbindungs- und Transportnetz das Internet zugrunde, welches durch beliebige andere Datennetze ergänzt und erweitert werden kann. Im allgemeinen Sprachgebrauch bezeichnet Cyber Space auch das weltweite Netzwerk von verschiedenen unabhängigen IK-Infrastrukturen, Telekommunikationsnetzen und Computersystemen. In der sozialen Sphäre kann bei Benutzung dieses globalen Netzwerkes zwischen Individuen interagiert werden, Ideen ausgetauscht, Informationen verteilt, soziale Unterstützung gewährt, Geschäfte getätigt, Aktionen gelenkt, künstlerische und mediale Werke geschaffen, Spiele gespielt, politisch diskutiert und vieles mehr getan werden. Cyber Space ist ein Überbegriff für Alles mit dem Internet verbundenes und für die verschiedenen Internet Kulturen geworden. Viele Staaten betrachten die vernetzte IKT und die unabhängigen Netzwerke, die über dieses Medium operieren als Teil ihrer Nationalen Kritischen Infrastrukturen".
Vgl. auch Cyber-Sicherheitsstrategie für Deutschland, Bundesministerium des Inneren (Stand: Februar 2011), S.14.

2 Der „virtuelle" Raum beginnt und endet im physischen Raum und umfasst Endgeräte, Netzwerkgeräte, Leitungen,...

Milliarden Menschen und zirka fünf Milliarden Geräte Teil dieses Cyberraumes. Die Vernetzung nimmt nach wie vor stark zu, bis 2020 werden Schätzungen zufolge etwa fünf Milliarden Menschen und 20 Milliarden Geräte vernetzt sein.

Hochentwickelte Staaten stützen sich im Rahmen ihrer technischen, wirtschaftlichen, sozialen, kulturellen, wissenschaftlichen und politischen Entwicklung mehr denn je auf den Cyberraum ab. Viele Bereiche sind mittlerweile von der Verfügbarkeit, Vertraulichkeit und Integrität der Cyberinfrastruktur abhängig[4].

Die Bedrohung durch Angriffe im Cyberraum ist in den letzten Jahren so stark angestiegen, dass zahlreiche Staaten sich veranlasst sahen, mit strategischen Konzepten darauf zu reagieren. Auch Österreich hat zunächst mit der IKT-Sicherheitsstrategie 2012[5] und mit der Österreichischen Strategie Cyber Sicherheit (ÖSCS)[6] 2013 nach einem aufwendigen Analyseprozess reagiert. Die ÖSCS fußt auf der Österreichischen Sicherheitsstrategie (ÖSS)[7] und orientiert sich an den Prinzipien des Programms zum Schutz kritischer Infrastrukturen (APCIP)[8].

Mit dem Ministerratsbeschluss vom März 2013[9] wurde dem BMLVS die Aufgabe Cyber Defence zugeordnet. Damit wurde der grundsätzliche militärische Auftrag zur Landesverteidigung auch auf den Cyberraum erweitert. Der Cyberraum ist dabei als eine Erweiterung des physischen Raumes zu begreifen und nimmt in militärischen Planungen neben Erdboden, Wasser, Luft und Weltraum als 5. Dimension einen in der Bedeutung steigenden Platz ein.

Cyber Defence wurde definiert als „die Summe aller Maßnahmen zur Verteidigung des Cyber-Raumes mit militärischen und speziell dafür geeigneten Mitteln zur Erreichung militärstrategischer Ziele. Cyber Defence ist ein integriertes System und besteht in seiner Gesamtheit aus der Umsetzung der Maßnahmen zur IKT-Sicherheit und der Informationssicherheit, aus den Fähigkeiten des ‚militärischen Computer Emergency Readiness Teams' (milCERT), der Computer Network Operations (CNO) und der Unterstützung durch die physischen Fähigkeiten der Streitkräfte"[10].

Um dieser Aufgabe gerecht zu werden, ist die Verwundbarkeit unserer Informationsgesellschaft und deren Bedrohung durch Cyberangriffe zu analysieren. Aus den Analyseergebnissen sind die Herausforderungen und erforderlichen Maßnahmen zur Verteidigung im Kriegsfall abzuleiten. Da der Cyberraum über nationale Grenzen hinweg den ganzen Globus umfasst, kommt der internationalen Zusammenarbeit bei der Abwehr von Angriffen eine hohe Bedeutung zu. Für Österreich sind die Maßnahmen der EU richtungsweisend. Auf internationaler und nationaler Ebene besteht auch die Herausforderung, adäquate Rechtsgrundlagen zu schaffen.

2. Bedrohungsbild

Zur Veranschaulichung des Bedrohungsbildes ist die Verwundbarkeit unserer Informationsgesellschaft, das Cyberrisikospektrum sowie ein potenzielles Cyberwar-Angriffsszenario darzustellen.[11]

2.1 Verwundbare Informationsgesellschaft

Der Armeechef der Schweiz hat im September 2010 Cyberangriffe als die „aktuell gefährlichste Bedrohung" bezeichnet. „Wenn es jemandem gelingt, unsere Kommunikations- und Stromnetze lahmzulegen, dann müssen wir über den Einsatz unserer Systeme gar nicht mehr diskutieren."[12]

Seit jeher gilt, dass Staaten von ihren strategischen Infrastrukturen[13] abhängig sind. Diese Infrastrukturen oder Teile davon haben eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen. Ihre Störung oder Zerstörung hat schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl der Bevölkerung oder die effektive Funktionsweise von staatlichen Einrichtungen.

Bisherige „Industriegesellschaften" sind auf dem Weg „Informationsgesellschaften" zu werden. Sie basieren (noch immer) auf der industriellen Produktion, aber mittlerweile sind der Wirtschaftsstandort und die Daseinsvorsorge erheblich vom Funktionieren der Informations- und Kommunikationsflüsse abhängig.[14] Damit wird ein Staat aber auch gegenüber einer

3 Cyberspace wird in diesem Aufsatz als Synonym zu Cyberraum genutzt.
4 Laut Studie BitKom vom 02.12.2011, „WIRTSCHAFT DIGITALISIERT, Wie viel Internet steckt in den Geschäftsmodellen deutscher Unternehmen?", sind 50% der deutschen Unternehmen vom Internet abhängig und nur 18% kommen ohne Internet aus.
5 Nationale IKT-Sicherheitsstrategie, Bundeskanzleramt, Wien, 2012 unter http://www.kiras.at/uploads/media/IKT_Sicherheitsstrategie.pdf.
6 Beschluss der Bundesregierung vom 18.03.2013; Bundeskanzleramt, Wien März 2013 unter http://www.bundeskanzleramt.at/DocView.axd?CobId=50748.
7 Entschließung des Nationalrates vom 3. Juli 2013, Österreichische Sicherheitsstrategie, Sicherheit in einer neuen Dekade – Sicherheit gestalten; Wien, Juli 2013.
8 Vgl. Gemeinsamer Bericht des Bundeskanzlers und des Bundesministers für Inneres betreffend das österreichische Programm zum Schutz kritischer Infrastrukturen; Masterplan APCIP (= Austrian Program for Critical Infrastructure Protection); Beschluss des Ministerrates vom 2. April 2008.
9 MINISTERRATSBESCHLUSS 180/8 vom 20.03.2013; Gemeinsamer Bericht des Bundeskanzlers, der Bundesministerin für Inneres, des Bundesministers für europäische und internationale Angelegenheiten und des Bundesministers für Landesverteidigung und Sport betr. Österreichische Strategie für Cyber Sicherheit (ÖSCS).
10 ÖSCS, Wien, März 2013, S. 21.
11 Auszug aus Unger Walter, Cyber Defence – eine militärische Herausforderung, ÖMZ 6/2012, S.698 ff.
12 Vgl. „Armeechef sieht Cyberwar als gefährlichste Bedrohung", NZZ online (www.nzz/ch/aktuell/startseite/armeechef-sieht-cyberwar -als-gefährlichste-bedrohung) vom 06. September 2010.
13 Im EPCIP (European Program for Critical Infrastructure Protection) werden 11 Sektoren kritischer Infrastrukturen angeführt: Energie, Nuklearindustrie, IKT, Wasser, Lebensmittel, Gesundheit, Finanzen, Transport, Chemische Industrie, Raumfahrt und Forschungseinrichtungen. Auf der Basis des Europäischen Programms für den Schutz kritischer Infrastrukturen wurde der Masterplan zur Erstellung des österreichischen Programms zum Schutz kritischer Infrastrukturen (APCIP) auf nationaler Ebene festgelegt. Der Masterplan beschreibt die Grundsätze des Programms, beinhaltet die Auflistung der vorrangig zu untersuchenden Sektoren, definiert Kriterien für die Einstufung kritischer Infrastrukturen, benennt die Risikofaktoren und die Akteure, listet die Maßnahmen zum Schutz kritischer Infrastrukturen auf und entwickelt einen Aktionsplan mit detaillierten Teilzielen. Die Schwerpunkte bei der nationalen österreichischen kritischen Infrastruktur sollen hingegen auch die verfassungsmäßigen Einrichtungen, die Aufrechterhaltung des Sozialsystems und der Verteilungssysteme sowie die Hilfs- und Einsatzkräfte umfassen.
14 Vgl. Deutscher Bundestag, Bericht des Ausschusses für Bildung, Forschung und Technologiefolgenabschätzung zum TA-Projekt: „Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung", Drucksache 17/5672 vom 27. April 2011, S. 44, grafische Darstellung der massiven Abhängigkeiten anderer Infrastrukturen von der Stromversorgung, Telekommunikation und den Informationssystemen und -netzen gem. einer Studie des Schweizer Bundesamtes für Bevölkerungsschutz.

Störung dieser Flüsse anfällig. Diese zunehmende Abhängigkeit der Informationsgesellschaft von ihren Informations- und Kommunikationssystemen einerseits und die Verwundbarkeit dieser Systeme andererseits schaffen Angriffspunkte, die gezielt genutzt werden könnten, um eine Informationsgesellschaft oder Teile davon zu schwächen oder seine Funktionalität dauerhaft und massiv zu stören. Österreich ist, wie andere postmoderne Staaten, in erheblichem Ausmaß vom Funktionieren seiner kritischen Informationsinfrastrukturen abhängig.

Die Zentralen, Kommunikationsknoten und Steuerungssysteme dieser, einer modernen Gesellschaft zu Verfügung stehenden, kritischen Infrastrukturen basieren auf Informations- und Kommunikationstechnologie oder sind für die IKT von erheblicher Bedeutung.

Das Funktionieren der strategischen Infrastrukturen ist von vitaler Bedeutung für einen technologisch hochentwickelten Staat. Sie sind damit kritisch für das Überleben eines Staates und werden zu vorrangigen Angriffszielen in einem Cyberwar.

Ein massiver Angriff auf die IKT-Systeme eines Staates oder einer Gesellschaft hat damit unter Umständen ähnliche Wirkungen wie ein massiver Angriff auf die industrielle Basis und könnte zu einem politisch verwertbaren Ergebnis führen. Dies ist die Grundlage für die nachfolgenden Überlegungen zu einem möglichen Cyberwar-Szenario.

2.2 Cyber-Risikospektrum

Das Cyberrisikospektrum beschreibt Gefahren und Bedrohungen, die den einzelnen Menschen ebenso wie Organisationen, Behörden, Unternehmen und Staaten treffen können. Der Risikobogen spannt sich dabei von der Übertretung von Bestimmungen über den subversiven Hacktivismus[15] auf das breite Feld der Cyberkriminalität, einschließlich der politischen Kriminalität wie Cyberspionage und Cyberterrorismus bis zum Cyberwar[16].

Der Cyberraum ist die Spielwiese für Script Kiddys, der Aktionsraum für Aktivisten und Wutbürger, der Tatort für Kriminelle und Terroristen und kann zum Operationsgebiet/Kriegsgebiet für staatliche Cyberwarrior werden. Die Akteure unterscheiden sich nach ihrer Motivation, Zielsetzung, verfügbaren Ressourcen und Fähigkeiten.

In dieser Arbeit soll nur die Ebene des Cyberwar beleuchtet werden. Denn nur für diese extensive Form der Bedrohung sind militärische Verteidigungsmaßnahmen (Cyberdefence) erforderlich.[17]

15 *Hacktivismus* (Kofferwort aus Hack und Aktivismus, engl. *Hacktivism*), ist die Verwendung von Computern und Computernetzwerken als Protestmittel, um politische Ziele zu erreichen. Die erste Verwendung erfuhr der Begriff im Juli 2004 von Mitgliedern eines Hacker-Kollektivs namens *Omega* unter http://de.wikipedia.org/wiki/Hacktivismus.

16 In diesem Spektrum ist Vandalismus ebenso enthalten wie die Veröffentlichung vertraulicher Daten zur Bloßstellung von Personen oder Organisationen ohne Bereicherungsmotiv oder politischer Aktivismus.

17 Alle darunterliegenden Bedrohungen sind durch die Strafverfolgungsbehörden zu bekämpfen.

3. Cyberwar – Analyse der Bedrohung

Nach Clausewitz ist Krieg „eine bloße Fortsetzung der Politik mit anderen Mitteln". Er meint, „dass der Krieg nicht bloß ein politischer Akt, sondern ein wahres politisches Instrument ist, eine Fortsetzung des politischen Verkehrs, ein Durchführen desselben mit anderen Mitteln. Was dem Kriege nun noch eigentümlich bleibt, bezieht sich bloß auf die eigentümliche Natur seiner Mittel". Der Krieg wäre also ein Akt der oder die Androhung von Gewalt, um den Feind wehrlos zu machen und zur Erfüllung des Willens des Aggressors zu zwingen.[18]

Cyberwar wäre demnach die kriegerische Auseinandersetzung zur Fortsetzung der Politik im und um den Cyberraum vorwiegend mit Mitteln aus dem Bereich der Informationstechnik.

Die ÖSCS definiert Cyberwar als „die kriegerische Auseinandersetzung im und um den virtuellen Raum mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. In einem weiteren Sinne ist damit auch die Unterstützung militärischer Aktionen in den klassischen Operationsräumen Boden, See, Luft, Weltraum durch Maßnahmen aus dem virtuellen Raum angesprochen. Ganz allgemein werden darunter auch die hochtechnisierten Formen des Krieges im Informationszeitalter verstanden, die auf einer weitgehenden Computerisierung, Elektronisierung und Vernetzung fast aller militärischer Bereiche und Belange basieren"[19].

Für Joseph S. Nye, dem ehemaligen stellvertretenden US-Verteidigungsminister, ist der „Cyberkrieg, auch wenn er derzeit erst in den Kinderschuhen steckt, die dramatischste aller potenziellen Bedrohungen. Große Staaten mit hoch entwickelten technischen und menschlichen Ressourcen könnten im Prinzip durch Cyber-Angiffe auf militärische und zivile Ziele enorme Störungen und physische Zerstörungen anrichten."[20]

Es ist davon auszugehen, dass etliche Staaten[21] sich mit der systematischen Vorbereitung von Cyberattacken beschäftigen; einerseits, um im Rahmen eines Verteidigungsfalles Cybergegenangriffe starten zu können, andererseits, um in einem Konflikt zur raschen Erreichung eines politischen Zieles offensiv agieren zu können.

Diese Annahme bestätigte Ehud Barak[22], der ehemalige Ministerpräsident und Verteidigungsminister Israels, im Plenum des europäischen Cyber-Security-Gipfels am 11. November 2013 in Bonn, als er sagte, dass eine Armee die Landesinteressen im Web nur dann wahren könne, wenn sie die Möglichkeit habe, sich in die Computersysteme seiner Gegner zu hacken.

Im Weiteren soll unter Vernachlässigung des politischen Motivs ein Angriffsszenario beschrieben und die hierfür erforderlichen Mittel und Methoden dargestellt werden.

18 Vgl. Carl von Clausewitz, "Vom Kriege", 1832, Ullstein-Verlag 1980, S. 27-29.

19 Vgl. CYBERWAR: Konzept, Stand und Grenzen; Center for Security Studies (CSS), ETH Zürich, CSS Analysen zur Sicherheitspolitik, Nr. 71, April 2010, S. 2 und auch ÖSCS, S. 22.

20 Vgl. „Cyberkrieg: Die Bedrohung, die aus dem Netz kommt", Joseph S. Nye, ehem. stellvertretender US-Verteidigungsminister in der Tageszeitung „Die Presse" vom 16. April 2012, S. 26-27.

21 Watts, Sean, Combatant Status and Computer Network Attacks, Virginia Journal of International Law 50 (2010), 391, unter: http://ssrn.com/abstract=1460680 (4.10.2011).

22 Ehud Barak, der ehemalige Ministerpräsident und Verteidigungsminister Israels im Plenum des europäischen Cyber-Security-Gipfels in Bonn, Vgl. „Die Schweiz wappnet sich"; unter: http://www.sonntagszeitung.ch/ vom 17.11.2013 (4.12.2013).

4. Szenario Cyberwar

Mutmaßliche Angriffsziele im Cyberwar sind die Verfügbarkeit, Vertraulichkeit und Integrität der strategischen, auf IKT basierenden Infrastrukturen eines Staates. Ein Cyberwar-Szenario entstünde bei gleichzeitigen Cyberangriffen gegen die Verfügbarkeit und Integrität mit dem Effekt des nachhaltigen Zusammenbruchs von z.B. folgenden kritischen, strategischen Infrastrukturen:

- Versorgung mit elektrischer Energie
- Telekommunikationsdienstleistungen
- Internet
- Banken und Geldversorgung
- Militär, Sicherheits- und andere Behörden
- Kraftwerk- und Staubeckensteuerungen
- Krankenhäuser und Notfalleinrichtungen
- Österreichischer Rundfunk (ORF), andere Medien
- Luftverkehrskontrollzentren, Flughäfen
- Lebensmittel- und Wasserversorgung, Abwasserentsorgung
- Bundesbahn- und andere Logistikunternehmen…

Auch wenn mit Cyberangriffen direkt keine physische Gewalt angewendet wird, ist indirekt mit Opfern in erheblichem Ausmaß zu rechnen.[23] Maßnahmen zur Beeinflussung des Willens der Bevölkerung und Regierung über neue und herkömmliche Medien (Manipulation von Internetauftritten, etc.) könnten die Angriffe begleiten. Diplomatische, ökonomische feindselige Akte, verdeckte Operationen sowie eine Eskalation und der Übergang in offene militärische Maßnahmen sind zu verschiedenen Zeitpunkten des Konflikts nicht auszuschließen.[24]

4.1 Mittel und Methoden, Vorteile für den Angreifer

Zur Durchführung komplexer Cyberangriffe eignen sich Bot-Netze[25], bösartige, schadenverursachende Software[26], die Einbringung von schadhafter Hardware ebenso wie Methoden zur Störung bzw. Lähmung der IKT, z.B. DDoS-Attacken[27]. Die Vorteile für den Angreifer liegen darin, dass die Mittel preiswert sind, die Wahrscheinlichkeit entdeckt zu werden gering ist, eine juristischen Strafverfolgung kaum möglich ist und die Angriffe unabhängig von Zeit und Ort sind.

Entwicklung und Tests von Cyberwaffen können in abgeschotteten Laboren erfolgen. Maßnahmen zur Aufklärung potenzieller Ziele unterscheiden sich nicht von den Methoden krimineller Hacker. Die Platzierung von Schadware auf Zielsystemen kann gut getarnt werden. Ein konzentrierter Angriff lässt sich ohne Vorwarnung mit hoher Geschwindigkeit rund um die Uhr auslösen und fortführen. Angriffsziele könnten in sehr kurzer Zeit erreicht werden und in Hinblick auf eine eventuell beabsichtigte Folgenutzung könnte der physische Zerstörungsgrad beim Angegriffenen begrenzt werden.

4.2 Ableitungen

Aus dem Szenario und bisher bekannten Cyberangriffen lässt sich Folgendes ableiten:

Da technische Vorbereitungsaktivitäten für einen Cyberangriff frühzeitig nur schwer bzw. gar nicht direkt erkennbar sind, könnten Attacken überraschend ohne Vorwarnung beginnen. Allenfalls können Indizien für die Aufklärung potenzieller Ziele erkannt werden. Jedoch laufen permanent Aktivitäten zur Auskundschaftung von Servern und Netzen, wobei die Zuordnung zur Vorbereitung eines kriegerischen Aktes ohne zusätzliche Erkenntnisse aus anderen Bereichen zunächst unmöglich ist.[28]

Das Einschleusen von Schadprogrammen, die erst zu einem späteren Zeitpunkt aktiviert werden sollen, kann aufgrund deren technischer Eigenschaften ebenfalls kaum entdeckt und nicht eindeutig zugeordnet werden. Moderne Schadware wird erst auf „Befehl" nach Nachladung zusätzlicher Elemente aktiv. Bei einem Angriff muss damit gerechnet werden, dass Systeme für eine zeitverzugslose Kommunikation ausfallen oder/und der Abruf von gespeichertem Wissen nicht mehr möglich ist.

Dies bedeutet, dass potenzielle Angriffsziele – strategische Infrastrukturen – auch im tiefsten Frieden optimal geschützt werden müssen. Systeme und Organisationen, die nicht vorbereitet sind, könnten enorme Schäden erleiden. Daraus folgt, dass die erste „Verteidigungslinie" zunächst einmal präventive Maßnahmen sind. Diese Sicherheitsmaßnahmen und die eingesetzte IKT müssen permanent auf aktuellem Stand gehalten, auditiert sowie an geänderte Bedrohungslagen angepasst werden

23 Vgl. Deutscher Bundestag, Bericht des Ausschusses für Bildung, Forschung und Technologiefolgenabschätzung zum TA-Projekt: „Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung", Drucksache 17/5672 vom 27. April 2011.

24 Wie großangelegte Angriffe ablaufen könnten, ist in Ansätzen an den Beispielen Estland 2007 und Georgien 2008 zu studieren. Hierzu ist umfangreiche Literatur verfügbar, z.B. Robert Knake: Cyber War: The Next Threat to National Security and What to Do About It. Ecco, April 2010.

25 Bot, Botnet: Unter einem Bot (vom Begriff robotic abgeleitet) versteht man ein Computerprogramm, das weitgehend autonom ständig gleichen, sich wiederholenden Aufgaben nachgeht. Es handelt sich dabei meist um ein eher simples, aber effektives Programm. Gebräuchlich ist die Bezeichnung auch für quasi-selbständige Programme im Bereich der künstlichen Intelligenz. Kommunizieren Bots untereinander in einem fernsteuerbaren Netzwerk, so spricht man von einem Botnet (robotic network). Vgl. http://de.wikipedia.org/wiki/Bot und http://de.wikipedia.org/wiki/Botnet.
Dabei infiziert in der Regel ein Angreifer zahlreiche Rechner mit einem Bot, der sich dann zu einem IRC-Server verbindet, einen bestimmten Channel betritt und dort auf Befehle des Botnet-Besitzers, des sogenannten Botmasters, wartet, wie beispielsweise das Starten eines DDoS-Angriffs oder das Versenden von Spam. Unter http://forum.computerbetrug.de/threads/vorsicht-mails-mit-rechnung-zip-enthalten-trojaner.25594/page-2, zuletzt am 25.01.2014.

26 Im Jahr 2012 sind ca. 37 Millionen neuer Schadprogramme im Internet beobachtet worden (ca. 100.000 pro Tag), vgl. Dr. Isselhorst Hartmut, Bundesamt für Sicherheit in der Informationstechnik, Vortragsunterlage der Cybersecurity 2013, Berlin 10.06.2013.

27 DoS, DDoS: Als Denial of Service (DoS, zu Deutsch etwa: Dienstverweigerung) bezeichnet man einen Angriff auf einen Host (Server) oder sonstigen Rechner in einem Datennetz mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen. In der Regel geschieht dies durch Überlastung. Erfolgt der Angriff koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von verteilter Dienstblockade bzw. DDoS (Distributed Denial of Service). Unter http://www.chanology-wiki.info/anonymous/hintergrund/ddos; zuletzt am 25.01.2014.

28 Ein potenzieller Aggressor sollte jedoch nicht übersehen, dass auch einfache Maßnahmen der Aufklärung (Computer Network Exploitation) tendenziell zur Eskalation eines schwelenden Konflikts beitragen können. Da die verbleibende Reaktionszeit extrem kurz sein könnte, könnten beobachtete Aufklärungsversuche einen „Erstschlag" im Sinne eines präemptiven Vorgehens provozieren.

(Patch-Management[29], Verstärken physischer Sicherheitsmaßnahmen, etc.). Darüber hinaus sind Vorkehrungen für eine rasche Warnung und Alarmierung zu treffen.

Die Nachrichtendienste sind besonders gefordert, einen Beitrag zur strategischen Frühwarnung zeitgerecht zu liefern. Potenzielle Cyberangreifer sind mit nachrichtendienstlichen und Cybermitteln und -methoden zu beobachten, um die allgemeine Lage durch ein konkretes Feindlagebild zu ergänzen. Diese Aufgaben sind als Schwergewichtsaufgaben von allen Nachrichtendiensten zu betreiben. Im Kontext eines schwelenden oder eskalierenden politischen Konflikts sind politische, diplomatische, wirtschaftliche und militärische Entwicklungen genau zu beobachten und zu analysieren. Hinweise auf einen Konflikt und technische Erkenntnisse müssen in das Lagebild einfließen und sind die Grundlage für ein Cyber-Frühwarnsystem. Ein Verbund der Elemente, die permanent die Cyberlage beobachten, und die Zusammenführung zu einem gesamtstaatlichen Lagebild sind zwingend erforderlich. Darüber hinaus muss diese „Feindlage" permanent mit dem Sicherheitszustand der zu schützenden Systeme korreliert werden.

Da die kritischen, von IKT abhängigen Infrastrukturen überwiegend in privatem Besitz sind, müssen alle Betreiber selbst in hohem Ausmaß für die Sicherheit ihrer Systeme vorsorgen. Darüber hinaus sollten die Betreiber den konkreten Bedarf an Unterstützung durch staatliche Stellen analysieren und bei der zuständigen Behörde einbringen. Nur so können staatliche Stellen in die Lage versetzt werden, eine bedarfsgerechte Ressourcenplanung und -bereitstellung vorzunehmen. Hierzu braucht es eine detaillierte Analyse der Kritikalität, des potenziellen Bedarfs sowie der sonstigen Notwendigkeiten.

Während eines großflächigen Angriffs werden die Sicherheitsorganisationen der kritischen Infrastrukturbetreiber mit der Abwehr bzw. der Wiederherstellung des Betriebs voll ausgelastet oder mutmaßlich sogar überlastet sein. Es ist daher nicht zu erwarten, dass Schlüsselpersonal verschoben werden kann („Nachbarschaftshilfe"). Dies zwingt zum Vorhalten von Reservekräften bei staatlichen Stellen, um überforderten Sicherheitsorganisationen rasch Hilfe leisten zu können. Diese Hilfe kann durch Remote-Beratung oder durch die Entsendung von Unterstützungsteams erfolgen.

Nebst der Unterstützung der Sicherheitsorganisationen sind Maßnahmen zur Identifizierung der Angreifer und Unterbindung laufender Angriffe offensiv einzusetzen (active defence, aktive Verteidigung). Dazu zählen beispielsweise die Identifizierung und Maßnahmen zur Abschaltung bzw. Blockierung von Botmaster-Servern und die Rückverfolgung bis zu den Tätern hinter einem Bot-Netz. Hierzu sind IT-forensische Maßnahmen zur Spurensicherung und nachrichtendienstliche Anstrengungen erforderlich. Damit können die Voraussetzungen für Reaktionen im diplomatischen, politischen oder gegebenenfalls sogar militärischen Bereich geschaffen werden.

Nach Abwehr der unmittelbaren Angriffe sind unverzüglich alle Maßnahmen zur Wiederherstellung des ordnungsgemäßen Betriebs zu treffen und eventuell aktive Maßnahmen im Sinne der Gesamtstrategie wahrzunehmen.

Außerdem sind unverzüglich Maßnahmen zur Härtung der IKT-Systeme umzusetzen. Das Postulat, Angriffe seien nicht wiederholbar[30], stimmt nur dann, wenn beobachtete Angriffe/Schadware mit Reverse-Engineering-Methoden analysiert, die eigenen Systeme gepatcht und das Personal fortgebildet werden. Ein permanenter Lessons-Learned-Prozess auf der Basis aktualisierter unterstützender Wissensdatenbanken ist unabdingbar.

4.3 Herausforderungen

Großangelegte gegen den Gesamtstaat gerichtete Cyberangriffe stellen sowohl die politisch-strategische Ebene als auch die militärische Landesverteidigung vor neue Herausforderungen, auf die im Folgenden näher eingegangen werden soll.

Da sowohl kriminelle Täter als auch Terroristen und staatliche Cyberwarrior mit ähnlichen bzw. gleichen Mitteln und Methoden attackieren, stellt sich zunächst die Frage der Zuständigkeit für die Abwehrmaßnahmen. Gemäß derzeitiger Kompetenzlage ist die Verantwortung für den Schutz kritischer Infrastrukturen vom Bundeskanzleramt an das Bundesministerium für Inneres delegiert worden. Für die Verfolgung der Cyberkriminalität einschließlich des Cyberterrorismus sind die Strafverfolgungsbehörden zuständig (Justiz-, Innenministerium). Das BMLVS kann zur Unterstützung im Wege der Assistenz oder Amtshilfe beigezogen werden.

Bei einem Angriff von außen auf den Gesamtstaat geht die Zuständigkeit an das Verteidigungsministerium über, wobei die Strafverfolgungsbehörden nicht von ihren Aufgaben entbunden werden. Die Entscheidung dazu ist selbstverständlich auf politischer Ebene zu treffen. Die Aufbereitung der Entscheidungsgrundlagen kann nur auf der Basis eines aktuellen rund um die Uhr verfügbaren, umfassenden Lagebilds erfolgen. Es sind daher Ressourcen für die permanente Lagebeobachtung, -analyse und Aufbereitung zur Verfügung zu stellen.

Da der Wechsel der Verantwortlichkeit während eines laufenden Angriffs eine erhebliche Schwachstelle darstellen würde, sind Vorkehrungen zu treffen, die einen reibungslosen und zeitverzugslosen Übergang ermöglichen. Dazu wird es notwendig sein, schon im Frieden einen Cyberkrisenstab, bestehend aus Experten aller zuständigen Ressorts, einzurichten und im Anlassfall frühzeitig zu aktivieren.

Die Betreiber von strategischer Infrastruktur müssen permanent Eigenschutz auf aktuellem Stand der IKT-Sicherheit gewährleisten. Da diese Infrastrukturen überwiegend in privater Hand sind, muss ein Modell zur Sicherstellung eines hohen Standards entwickelt werden. Verschiedene Ausprägungen wären denkbar, z. B. eine freiwillige Selbstverpflichtung. Vorgaben von Standards, regelmäßige Audits und Kontrollen wären die erforderlichen Begleitmaßnahmen. Ein Beispiel hierfür könnten die Bestimmungen des Telekommunikationsgesetzes

29 Ein Patch ist eine Korrekturauslieferung für Software oder Daten aus Endanwendersicht, um Sicherheitslücken zu schließen, Fehler zu beheben oder bislang nicht vorhandene Funktionen nachzurüsten. Unter http://de.wikipedia.org/wiki/Patch_%28Software%29; zuletzt am 25.01.2014.

30 Beispielsweise verbreitete und verursachte das Schadprogramm „Conficker" erhebliche Schäden, z.B. wurde die Landesverwaltung von Kärnten zur Gänze im Januar 2009 lahmgelegt, obwohl schon Monate zuvor ein Sicherheitspatch mit entsprechenden Warnhinweisen zur Verfügung gestellt wurde.

sein. Die Rundfunk- und Telekom-Regulierungsbehörde kann demnach Sicherheitsstandards vorschreiben und regelmäßig überprüfen.

Anreize zur Implementierung und Optimierung von Sicherheitsmaßnahmen könnten die Durchführung kostenloser Sicherheitsberatungen, Unterstützung bei Bedrohungs- und Risikoanalysen und der Entwicklung von Sicherheitskonzepten sein. Die Durchführung von Audits durch eine staatliche Behörde sollten durch die Auszeichnung von „sicheren" Unternehmen mit einem Sicherheitszertifikat („Gütesiegel") honoriert werden. Gemeinsame, von staatlicher Seite vorbereitete Übungen könnten der Verbesserung der Zusammenarbeit, dem Test von Abläufen ebenso wie der Überprüfung von Alarm-, Notfall- und Krisenplänen dienen.

Eine weitere Herausforderung ist es, die richtigen Ressourcen für den Anlassfall bei staatlichen Organisationen bereit zu halten. Die dynamische Entwicklung der IKT zwingt zu technisch hochqualifiziertem Personal, das permanent fortgebildet werden muss. Dieses Personal ist grundsätzlich Mangelware und kann mit steigender Qualifizierung nur unter erheblichen Anstrengungen bei staatlichen Organisationen vorgehalten werden.

Redundante Systeme für Regierungstätigkeit und Kommunikation können nicht erst im Anlassfall aufgebaut werden. Diese müssen bereits im Frieden errichtet, routinemäßig betrieben und in Übungen getestet werden. Der Bedarf wäre daher umgehend zu erheben, vorhandene Systeme wären auszubauen und die erforderlichen Ressourcen zuzuordnen.

Ein internationales Problem ist die Frage der Identifizierung der tatsächlichen Angreifer. Die Zuordnung (Attribution) eines Angriffs zu physischen Angreifern/Tätern[31] ist derzeit nicht einmal technisch gelöst.[32] Außerdem wäre zu klären, wie man Staaten, über deren Cyberspace (Transitländer; wo endet der nationale Cyberspace?) Angriffe laufen, behandelt. Sind diese Staaten Mittäter? Welche Pflichten haben Neutrale?[33] Politik und Diplomatie sollten auf die Beantwortung dieser Fragen und die Entwicklung internationaler Instrumente bei der Zusammenarbeit zum Schutz vor Cyberangriffen hinarbeiten. Maßnahmen zur Vertrauensbildung (Verbot von Cyberwaffen, Open Cyber Space in Anlehnung an das Open Sky Abkommen), zur verpflichtenden Zusammenarbeit im Falle von laufenden Angriffen, zur Rückverfolgung sowie bei der Ermittlung von Tätern sind zu entwickeln und vertraglich zu vereinbaren.

Maßnahmen zur aktiven Verteidigung sind durch entsprechende Rechtsgrundlagen zu ermöglichen. Damit Gegenmaßnahmen nicht Unbeteiligte schädigen, wären handhabungssichere Methoden zu entwickeln. Hierzu sollte die Forschung forciert, Netzwerkanalyse- und Forensikspezialisten mit smarter Software zur Just-in-time-Forensik und zur Unterbrechung von Angriffen befähigt werden.

31 Es stellt sich daher die Frage, wie z. B. ein DDoS-Angriff auf der Basis eines großen Bot-Netzes mit Zombie-Rechnern in 150 Staaten oder eines eingeschleusten Schadprogramms (Beispielsweise STUXNET) einem konkreten Angreifer zugeordnet werden könnte.

32 Siehe den Beitrag von Thomas Reinhold in diesem Heft mit Vorschlägen dazu.

33 Eine weiterführende Analyse findet sich bei: Sigmar Stadlmeier und Walter Unger, Cyber War und Cyber Terrorismus aus völkerrechtlicher Sicht, in: Kirsten Schmalenbach (Hrsg.), Aktuelle Herausforderungen des Völkerrechts, Beiträge zum 36. Österreichischen Völkerrechtstag (2011), Wien 2012, S. 63 ff.

5. Cyber Defence – europäische und nationale Strategien

Im Februar 2013 hat die EU im Rahmen der Digitalen Agenda 2020 ihre Cybersecurity-Strategie[34] festgelegt. In der Cybersicherheitsstrategie legt die EU ihre Vorstellungen für einen „offenen, sicheren und geschützten Cyberraum" vor. Ziel ist es, die europäischen Werte durch konkrete Maßnahmen zur Erhöhung der Widerstandsfähigkeit der Informationssysteme im Cyberraum, zur Eindämmung der Cyberkriminalität und zur Stärkung der internationalen Cybersicherheitspolitik und Cyberverteidigung der EU zu fördern. Die Cybersicherheit soll durch **fünf Prioritäten erreicht werden:**

1. Widerstandsfähigkeit gegenüber Cyberangriffen,
2. drastische Eindämmung der Cyberkriminalität,
3. Entwicklung einer Cyberverteidigungspolitik und von Cyberverteidigungskapazitäten im Zusammenhang mit der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP),
4. Entwicklung der industriellen und technischen Ressourcen für die Cybersicherheit,
5. Entwicklung einer einheitlichen Cyberraumstrategie der EU auf internationaler Ebene und Förderung der Grundwerte der EU.

5.1 Die Entwicklung einer Cyberverteidigungspolitik

Um die Robustheit der Kommunikations- und Informationssysteme zu erhöhen, die dem Schutz der Verteidigungs- und Sicherheitsinteressen der Mitgliedstaaten dienen, sollte der Schwerpunkt bei der Entwicklung der Cyberverteidigungskapazitäten auf der Erkennung komplexer Cyberbedrohungen, der Reaktion darauf und der Wiederherstellung danach liegen.

Synergien zwischen dem Vorgehen auf ziviler und auf militärischer Ebene sind beim Schutz kritischer Cyberanlagen und -daten (cyber assets) verstärkt zu nutzen. Diese Bemühungen sollten durch Forschungs- und Entwicklungsmaßnahmen sowie durch eine engere Zusammenarbeit zwischen Behörden, Privatsektor und Hochschulen in der EU gestützt werden. Um Doppelarbeit zu vermeiden wird die EU Möglichkeiten prüfen, wie sich die Maßnahmen der EU und der NATO zur Stärkung der Robustheit kritischer staatlicher, verteidigungsrelevanter und sonstiger Informationsinfrastrukturen, von denen beide Organisationen abhängen, gegenseitig ergänzen könnten.

Die Hohe Vertreterin legte den Schwerpunkt auf folgende wichtige Maßnahmen und bittet die Mitgliedstaaten und die Europäische Verteidigungsagentur um ihre Mitarbeit:[35]

34 Vgl. Cybersecurity Strategy of the European Union, unter: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security bzw. http://eeas.europa.eu/policies/eu-cyber-security/index_de.htm (08.12.2013).

35 Cybersecurity Strategy of the European Union, unter: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security; S.13.

- Prüfung der operativen Anforderungen an die Cyberverteidigung der EU und Förderung der Entwicklung von Cyberverteidigungskapazitäten und -technologien auf EU-Ebene, wobei alle Aspekte des Kapazitätsaufbaus zu behandeln sind (u.a. grundlegende Ziele, Leitung, Organisation, Personal, Schulung, Technologie, Infrastruktur, Logistik und Interoperabilität);
- Entwicklung eines EU-Rahmens für die Cyberverteidigungspolitik, um die Netze bei GSVP-Missionen und -Operationen zu schützen, unter Einbeziehung eines dynamischen Risikomanagements, einer besseren Bedrohungsanalyse der Bedrohungen und des Informationsaustauschs; Verbesserung der Möglichkeiten der militärischen Seite (im europäischen und multinationalen Kontext), Cyberverteidigungsschulungen und -übungen zu besuchen bzw. durchzuführen (u. a. durch Einbeziehung von Cyberverteidigungsaspekten bei bestehenden Übungen);
- Förderung des Dialogs und der Koordinierung zwischen zivilen und militärischen Beteiligten in der EU, wobei der Schwerpunkt vor allem auf dem Austausch empfehlenswerter Vorgehensweisen, dem Informationsaustausch, der frühzeitigen Warnung, der Reaktion auf Sicherheitsvorfälle, der Risikobewertung, der Sensibilisierung bzw. der Herstellung der Cybersicherheit insgesamt liegen sollte;
- Pflege des Dialogs mit den Partnern auf internationaler Ebene, u.a. mit der NATO, anderen internationalen Organisationen und multinationalen Exzellenzzentren, um effektive Verteidigungskapazitäten zu gewährleisten, Bereiche einer möglichen Zusammenarbeit zu ermitteln und Doppelarbeit zu vermeiden.

5.2 Sicheres und vertrauenswürdiges digitales Umfeld

Die vorgeschlagene NIS-Richtlinie (Netz- und Informationssicherheit) ist ein wichtiger Teil der Gesamtstrategie. Sie sieht für alle Mitgliedstaaten, aber auch für die Betreiber zentraler Internetdienste und kritischer Infrastrukturen (z. B. Plattformen des elektronischen Geschäftsverkehrs und soziale Netze) und für die Betreiber von Energie-, Verkehrs-, Bank- und Gesundheitsdiensten die Verpflichtung vor, in der gesamten EU ein sicheres und vertrauenswürdiges digitales Umfeld zu gewährleisten. Die vorgeschlagene Richtlinie enthält u. a. folgende Maßnahmen:[36]

- Jeder Mitgliedstaat muss eine NIS-Strategie annehmen und eine zuständige nationale Behörde mit ausreichender Finanz- und Personalausstattung für die Prävention von NIS-Risiken und -Vorfällen sowie den Umgang damit und die Reaktion darauf benennen.
- Ein Kooperationsmechanismus zwischen Mitgliedstaaten und Kommission muss geschaffen werden für den Austausch von Frühwarnungen vor Sicherheitsrisiken und -vorfällen über eine sichere Infrastruktur, für die Koordinierung und für die Durchführung regelmäßiger gegenseitiger Überprüfungen.
- Betreiber kritischer Infrastrukturen in bestimmten Bereichen (Finanzdienste, Verkehr, Energie und Gesundheitswesen), Betreiber zentraler Dienste der Informationsgesellschaft (vor allem App-Stores, eCommerce-Plattformen, Internet-Zahlungen, Cloud-Computing, Suchmaschinen, soziale Netze) und öffentliche Verwaltungen müssen Risikomanagementmethoden einführen und große Sicherheitsvorfälle in ihren Kerndiensten melden.

Zur Erreichung dieser Ziele hat die Europäische Union mittlerweile die Kompetenzen der schon 2004 eingerichteten *Europäischen Agentur für Netz- und Informationssicherheit (European Union Agency for Network and Information Security, ENISA)*[37] und ihre Rolle als Beratungsorgan für EU-Mitgliedstaaten und EU-Institutionen ausgeweitet. Die Agenden der ENISA umfassen nun pan-europäische Kooperationen mit dem privatwirtschaftlichen Sektor, die Etablierung eines *Computer Emergency Response Teams (CERT)* für EU-Institutionen, die Abwicklung der *Telecommunication Framework Directive*, die Verantwortung im Bereich des europaweiten Informations- und Alarmsystem *(European Information-Sharing and Alert System, EISAS)* sowie eine stärkere Rolle im Sicherheitsbereich des EU-Telekommunikationssektors.

Auch das *Europäische Programm für den Schutz kritischer Infrastrukturen (EPSKI)*[38] mit den Richtlinien über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen sowie ein Warn- und Informationsnetz für kritische Infrastrukturen (*CI-WIN*) und die Identifikation und Reduktion von Systemschwächen ist für die Cybersicherheit von Bedeutung. Besonderer Wert wird auf den Schutz nationaler kritischer Infrastrukturen *(NCIs)* durch die Vereinbarung gemeinsamer politischer Ziele und die Verstärkung der Zusammenarbeit zwischen den Mitgliedstaaten gelegt.

6. Konsequenzen der EU-Vorgaben und ihre Umsetzung in Österreich

In Österreich sind in rascher Folge die IKT-Sicherheitsstrategie (2012)[39], die Österreichische Strategie Cyber Sicherheit (ÖSCS, 2013)[40] und die Österreichische Sicherheitsstrategie (2013)[41] abgeschlossen worden, während das Österreichische Programm zum Schutz Kritischer Infrastruktur (APCIP) bereits 2008 fertiggestellt wurde. Während die Sicherheitsstrategie die Evaluierung und Fortschreibung der Strategie aus dem Jahre 2001 darstellt, sind die anderen Dokumente die ersten ihrer Art in Österreich. In die ÖSCS sind alle wesentlichen Punkte der IKT-Sicherheitsstrategie eingearbeitet worden.

36 Unter http://www.eu-info.tradepress.eu/2013/07/31/neuen-richtlinie-zur-netz-und-informationssicherheit-meldung-machen-in-brussel/; (25.01.2014).

37 www.enisa.europa.eu (08.12.2013).
38 http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm (4.12.2013).
39 http://www.e-government.gv.at/DocView.axd?CobId=47986 (4.12.2013).
40 http://www.bka.gv.at/DocView.axd?CobId=50748 (4.12.2013).
41 http://www.bka.gv.at/DocView.axd?CobId=50748 (4.12.2013).

6.1 Österreichisches Programm zum Schutz Kritischer Infrastrukturen (APCIP)[42]

Das Programm umfasst die Definition österreichischer kritischer Infrastrukturen (ACI), die relevanten Ableitungen für Österreich im Vergleich zur europäischen Ebene (so z.B. ein starker Fokus auf die verfassungsmäßigen Einrichtungen, der Aufrechterhaltung des Sozialsystems sowie Hilfs- und Einsatzkräften zu nennen, unter besonderer Berücksichtigung der Prioritätensetzung auf Länder- und Regionalebene), die Kriterien für die Einstufung kritischer Infrastrukturen sowie strategische Ziele; sämtliche Maßnahmen der Europäischen Union zur ACI werden behandelt, so z.B. die Intensivierung des Informationsaustauschs, das Erstellen von Sicherheits- und Notfallplänen oder eine Public-Private-Partnership (PPP).

Besonders im Bereich der internationalen Kooperation werden bilaterale Abkommen mit für Österreich besonders relevanten Partnern in der Region, z.B. Deutschland, Tschechien und die Slowakei, hervorgehoben.

Die rechtliche Umsetzung sollte durch Anpassung des Aktiengesetzes (AktG), des Unternehmensgesetzesbuchs (UGB), des Sicherheitspolitikgesetzes (SPG), des Elektrizitätswirtschafts- und -organisationsgesetzes (EIWOG), des Geldwäschegesetzes (GWG) sowie des E-RBG (Energieregulierungsbehördengesetz) erfolgen. Eine Orientierung im Bereich der Umsetzung an unterschiedlichen internationalen Normen, darunter ISO 27001 (Information technology – security techniques), ist vorgesehen.

6.2 Österreichische Sicherheitsstrategie

In den allgemeinen Empfehlungen zum Entschluss des Nationalrats über eine neue Sicherheitsstrategie 2013 ist unter Punkt 3 die ständig steigende „Bedrohung im und aus dem Cyber-Raum durch staatliche und nicht staatliche Akteure“[43] beschrieben, ebenso wird auf die steigende Bedeutung der Cybersicherheit Bezug genommen.

Im Bereich der allgemeinen Herausforderungen werden unter Risiken und Bedrohungen Angriffe auf die Sicherheit der IT-Systeme („Cyber Attacks“) in einer Auflistung mit internationalem Terrorismus, der Verbreitung von Massenvernichtungswaffen und Drogenhandel genannt – nicht ohne hier bereits vorauszuschicken, dass es sich um „besondere neue Herausforderungen für alle betroffenen Akteure“ handelt, die „ein breites Zusammenwirken im Rahmen eines Gesamtkonzepts“ erfordern.

6.3 Österreichische Strategie für Cyber-Sicherheit (ÖSCS)

Als besonders relevant für die Umsetzung der europäischen Richtlinien in die österreichische politisch-rechtliche Sicherheitssituation stellt sich das *Kap. 5 der Strategie – Handlungsfelder und Maßnahmen* – dar. Eingeteilt in mehrere Handlungsfelder werden entsprechende Umsetzungsmechanismen dargelegt[44]:

Im Handlungsfeld „Strukturen und Prozesse“ werden die Steuerungsgruppe Cybersicherheit, die Struktur zur Koordination der operativen Ebene, das Cyberkrisenmanagement und die Stärkung bestehender Cyberstrukturen beschrieben.

Die Steuerungsgruppe Cybersicherheit wurde bereits mit dem Ministerratsbeschluss vom 11. Mai 2012 eingerichtet. Unter Leitung des Bundeskanzleramtes und der Einbeziehung des Nationalen Sicherheitsrats, Cybersicherheitsexperten und dem Leiter der Informationstechnologie des Bundes werden u.a. auf mehreren Ebenen die Maßnahmen zur Cybersicherheit koordiniert, ein jährlicher Bericht zur Cybersicherheit erstellt und die Bundesregierung beraten.[45]

Die noch zu schaffende Struktur zur Koordination der operativen Ebene soll unter Einbindung der Wirtschaft erfolgen. Hier soll das *Lagebild Cyber Sicherheit* erstellt, Beratungen über entsprechende Maßnahmen auf der operativen Ebene und eine regelmäßige Analyse der Situation im Cyberraum geleistet werden. Das BM.I, BMLVS und Einrichtungen zur Sicherheit von Computersystemen, des Internets und zum Schutz kritischer Infrastrukturen (u.a. staatliche Akteure wie GovCERT (*Government Computer Emergency Response Team*), milCERT (*militärisches Computer Emergency Readiness Team*) und das *Cyber Crime Competence Center* sowie private Akteure, Wirtschaft und Forschung) sind einbezogen.

Das Cyberkrisenmanagement und die Verantwortung liegen beim BM.I (Angelegenheiten der inneren Sicherheit) sowie beim BMLVS (äußere Sicherheit), welche unter Einbeziehung von staatlichen Vertretern und Betreibern von kritischen Infrastrukturen Krisenmanagements- und Kontinuitätspläne auf Basis von Risikoanalysen für Cyberbedrohungen und entsprechende Cyberübungen erarbeiten sollen.

Die bestehenden Cyberstrukturen, das GovCERT des BKA, das *Cyber Crime Competence Center* des BM.I (zur Vorbeugung und Prävention von Cyberkriminalität) sowie das vom BMLVS betriebene MilCERT (u.a. zum Schutz der eigenen Netze und als Basis operativer Fähigkeiten zur Abwehr von Cyber-Angriffen), sollen ausgebaut und verstärkt werden.[46]

Im Handlungsfeld „Governance“ soll die EU-Strategie unter Involvierung von staatlichen und nichtstaatlichen Akteuren durch die Schaffung eines zeitgemäßen ordnungspolitischen Rahmens, Festlegung von Mindestsicherheitsstandards für die Cybersicherheit und die Erstellung eines jährlichen Berichts zur Cybersicherheit umgesetzt werden.[47]

Im Handlungsfeld „Kooperation, Staat, Wirtschaft und Gesellschaft“ soll durch die Einrichtung einer Cybersicherheitsplattform, die Stärkung der Unterstützung für KMUs (Klein- und Mittelunternehmen) und die Ausarbeitung einer Cybersicher-

42 http://www.kiras.at/uploads/media/MRV_APCIP_Beilage_Masterplan_FINAL.pdf (4.12.2013).
43 Österreichische Sicherheitsstrategie unter: http://www.bka.gv.at/DocView.axd?CobId=52099 (4.2.2013).
44 Sämtliche Inhalte dieses Subkapitels sind der Österreichischen Strategie für Cyber-Sicherheit (ÖSCS) entnommen: http://www.bka.gv.at/DocView.axd?CobId=50748 (24.1.2014).
45 Vgl. Österreichische Strategie für Cyber-Sicherheit (2013), S.10.
46 Vgl. ebd., S.11.
47 Vgl. ebd., S.12.

heits-Kommunikationsstrategie die nationale Zusammenarbeit optimiert werden.[48]

Im Handlungsfeld „Schutz kritischer Infrastrukturen" soll die Resilienz kritischer Infrastrukturen durch die Einbindung der Betreiber in die Prozesse des Cyberkrisenmanagements, besonders durch Entwicklung einer Sicherheitsarchitektur, den Ausbau der Krisenkommunikation, die Definition von Cybersicherheitsstandards sowie die Meldepflicht von schweren Cybervorfällen erhöht werden.[49]

Im Handlungsfeld „Sensibilisierung und Ausbildung" soll die notwendige Aufmerksamkeit für Cybersicherheit durch eine Stärkung der Cybersicherheitskultur und die Verankerung von Cybersicherheit und Medienkompetenz auf allen Ebenen der Aus- und Weiterbildung erreicht werden.[50]

Im Handlungsfeld „Forschung und Entwicklung" sollen zentrale Forschungsschwerpunkte im Rahmen der nationalen und der EU-Sicherheitsforschungsprogramme gesetzt werden.[51]

Im Handlungsfeld „Internationale Zusammenarbeit" sollen die Beteiligung Österreichs an der Umsetzung der Cybersicherheitsstrategie der EU, der Europaratskonvention über Cyberkriminalität und der Gewährleistung von Menschenrechten im virtuellen Raum, besonders durch die Kooperation mit der OSZE und als Teil der NATO-Partnerschaft, die Beteiligung an der Planung und Durchführung von länderübergreifenden Cyberübungen sowie die Koordinierung entsprechender außenpolitischer Maßnahmen durch das BMeiA bearbeitet werden.[52]

7. Die Aufgaben des Österreichischen Bundesheeres im Cyberraum[53]

Die Aufgaben des Bundesheeres ergeben sich unmittelbar aus der Bundesverfassung (Art. 79 B-VG). Demnach obliegt dem Bundesheer als Kernaufgabe die militärische Landesverteidigung. Daneben sind zwei sog. „Assistenzfälle"[54] ausdrücklich vorgesehen. Damit sind alle Tätigkeiten des Bundesheeres umfasst, die im Rahmen der allgemeinen und unmittelbaren Einsatzvorbereitung und zur Wahrnehmung von Einsatzaufgaben einschließlich der notwendigen Abschlussmaßnahmen nach dessen Beendigung zu erbringen sind[55].

Mit „militärischer Landesverteidigung" ist grundsätzlich die „Abwehr von Gefahren von außen" gemeint; es kommt aber auch die Abwehr von Vorgängen im Staatsinneren in Betracht, insofern sie im Zusammenhang mit von außen drohenden Gefahren stehen und eine wirksame Abwehr nur mit militärischen Mitteln möglich ist".[56] Die militärische Landesverteidigung dient dem militärischen Neutralitäts- und Souveränitätsschutz. Alle anderen Angriffe sind Aspekte der „inneren Sicherheit", deren Abwehr den Sicherheitsbehörden des Bundes obliegt.[57]

Zusammenfassend ergibt sich, dass das Bundesheer im Rahmen allfälliger Maßnahmen der Österreichischen Strategie für Cyber Sicherheit immer im vollen Umfang und aus eigener Kompetenz tätig werden kann, sofern sich die zu beurteilende Maßnahme als ein Anlassfall der militärischen Landesverteidigung darstellt.

Ein Angriff stellt dann einen Anlassfall zur militärischen Landesverteidigung dar, wenn er durch Organe eines anderen Staates (insbesondere Militär o.Ä.) oder indirekt durch eine staatlich gelenkte Organisation mit dem Ziel erfolgt, die Souveränität Österreichs zur Gänze oder in Teilbereichen auszuschalten oder sich gegen militärische Rechtsgüter richtet (Abwehr im Rahmen des Militärbefugnisgesetzes / MBG)[58]. Ob ein solcher Anlassfall vorliegt, ist im jeweiligen Einzelfall nach dem „wer", „gegen wen" bzw. „in welcher Absicht"-Kalkül zu beurteilen.

Die dafür notwendigen Vorbereitungsmaßnahmen können im Rahmen der allgemeinen Einsatzvorbereitung in jenem Umfang, der ausschließlich nach militärfachlichen Gesichtspunkten zu beurteilen ist, durchgeführt werden.

Cyberangriffe, die sich nicht gegen die Souveränität Österreichs bzw. das Bundesheer selbst richten, können keinesfalls einen Aspekt der militärischen Landesvereidigung darstellen und fallen als Aspekt der „inneren Sicherheit" grundsätzlich in die Zuständigkeit der Sicherheitsbehörden. In diesen Fällen kann das Bundesheer nur im Rahmen eines sicherheitspolizeilichen Assistenzeinsatzes tätig werden.

48 Vgl. Österreichische Strategie für Cyber-Sicherheit (2013), S.12f.
49 Vgl. ebd., S.14.
50 Vgl. ebd., S.14f.
51 Vgl. ebd., S.15f.
52 Vgl. ebd., S.16.
53 Vgl. Stellungnahme des BMLVS/GrpRechtLeg vom 03.01.2013 zur ÖCSCS-Strategie; Ersuchen um rechtliche Würdigung – Stellungnahme GZ S91018/14-GrpRechtLeg/2012.
54 Zur Aufrechterhaltung der Ordnung und Sicherheit im Inneren, sofern die gesetzmäßige zivile Gewalt seine Mitwirkung in Anspruch nimmt; gem. Art. 79 Abs. 2 Z 1 lit. b B-VG. Die nähere Ausgestaltung auf einfachgesetzlicher Ebene erfolgt durch § 2 des Wehrgesetzes 2001 (WG 2001) BGBl. I Nr. 146, wobei gegenständlich insbesondere § 2 Abs. 1 lit. b WG 2001.
55 § 2 Abs. 2 bis 4a des Wehrgesetzes 2001 (WG 2001), BGBl. I Nr. 146.
56 VGH v 03.12.2007, GZ V6/07, Sammlungsnummer 18296, Pkt. 3.1, siehe https://www.ris.bka.gv.at/Dokumente/Vfgh/JFT_09928797_07V00006_00/JFT_09928797_07V00006_00.html.
57 aaO Stellungnahme des BMLVS/GrpRechtLeg, S. 2, Pkt. 2.
58 Siehe http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20000864.