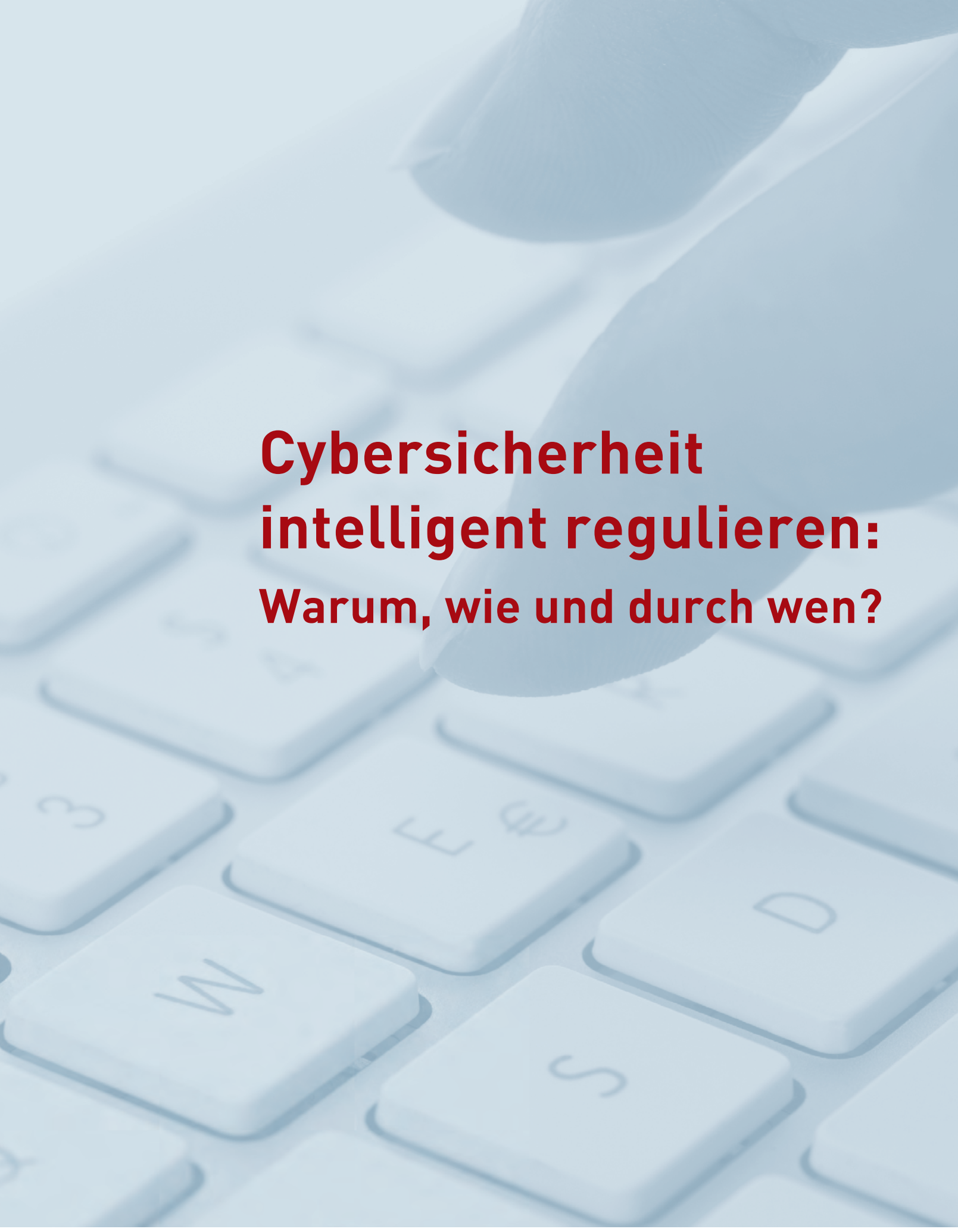


Cybersicherheit intelligent regulieren:

Warum, wie und durch wen?

BM.I
BUNDESMINISTERIUM FÜR INNERES

KURATORIUM SICHERES ÖSTERREICH

Impressum

KSÖ - Kuratorium Sicheres Österreich
Generalsekretär Christian Kunstmann
Herrengasse 7
Postfach 100
A-1014 Wien
Email: kunstmann@dasmachichsicher.at
ZVR-Zahl: 444 913 001

DRUCK: BM.I

FOTOS
Kuratorium Sicheres Österreich
Bundesministerium für Inneres

Cobyright © 2012 BM.I

Mir ist deutlich geworden, dass wir beim Thema Cybersecurity
ein stärkeres, neues „Miteinander“ entwickeln müssen.
Wir stehen vor Aufgaben, die wir gemeinsam bewältigen müssen.
Und die wir nur gemeinsam bewältigen können.

Mag.ª Johanna Mikl-Leitner, Bundesministerin für Inneres
Cybersecurity-Konferenz, Wien, 20. September 2011

Mit der Veranstaltung „Freiwillige Selbstverpflichtung versus staatliche Regulierung" startete das Kuratorium Sicheres Österreich (KSÖ) in Kooperation mit dem BM.I im Februar 2012 seine Cyberplattform, auf der sich Politik, Verwaltung, Wirtschaft und Wissenschaft auch in Zukunft zu Themen der Cybersicherheit austauschen können. Das vorliegende White Paper beleuchtet die Diskussion zum Veranstaltungsthema und gibt zusätzliche Denkanstöße.

Cybersicherheit ist eine Verbundaufgabe von Staat, Wirtschaft und Bürgern. Daher müssen Ansätze zur Verbesserung der Cybersicherheit bestehende Organisations- und Zuständigkeitsgrenzen überschreiten – das gilt auch für mögliche regulatorische Maßnahmen.

Zu klären ist: Was sind die Rahmenbedingungen, die Staat, Wirtschaft und Gesellschaft für den Umgang mit Cyberrisiken benötigen? Dafür sind verschiedene Aspekte von Bedeutung: Soll der Staat für die Cybersecurity spezifische Vorschriften erlassen? Und falls ja, in welcher Form? Oder soll sich der Staat nicht einmischen, weil Cybersecurity im Interesse der Unternehmen liegt und diese ohne entsprechende Vorkehrungen ihre Kunden ohnehin nicht bedienen können? Die Beantwortung dieser Fragen ist nicht einfach und kann nur in enger Zusammenarbeit zwischen Politik, Behörden und Wirtschaft erfolgen. Denn mögliche Antworten können direkt in die individuellen Freiheiten der Bürgerinnen und Bürger, in die Geschäftsmodelle der Unternehmen oder in den Handlungsspielraum der staatlichen Behörden eingreifen.

Ich begrüße daher den Ansatz des partnerschaftlichen Dialogs zwischen Behörden und Wirtschaft, den das BM.I hier verfolgen möchte. Aus Sicht der Wirtschaft ist klar: Regelungen müssen im internationalen Gleichklang festgelegt werden, um die Wettbewerbsfähigkeit Österreichs hier im internationalen Vergleich nicht einzuschränken. Und auch innerhalb Österreichs müssen sie für alle wettbewerbsneutral gestaltet werden – Verpflichtungen müssen für alle gelten und von allen eingehalten werden.

Sehr positiv ist: Die österreichischen Unternehmen kritischer Infrastruktur bekennen sich zu einem starken Sicherheitsbewusstsein. Auch die Formulierung konkreter Sicherheitsziele für Unternehmen und mögliche Sanktionsmechanismen wird in diesem Zusammenhang offen diskutiert. Vorhandene Expertise dazu wird Behörden und Politik gerne zur Verfügung gestellt. Ich bin daher zuversichtlich, dass wir auf dem richtigen Weg sind, um Österreich gemeinsam Schritt für Schritt cyber-sicherer zu machen.

GD Mag. Erwin Hameseder
Präsident Kuratorium Sicheres Österreich

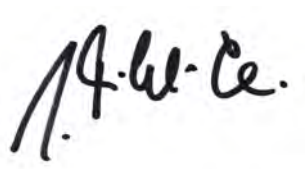
Cybersecurity ist zu einem zentralen Thema der inneren Sicherheit geworden. Attacken aus dem Cyberspace bedrohen einzelne Bürgerinnen und Bürger genauso wie Unternehmen und ganze Staaten. Wir alle profitieren von den Vorzügen des Internets, sind aber auch von den Gefahren, die der global vernetzte Informationsaustausch mit sich bringt, in gleicher Weise bedroht. Um dem zu begegnen, müssen wir uns entsprechend rüsten. Als Sicherheitsministerin sehe ich es als meine Aufgabe, Österreich im Cyberspace sicherer zu machen. Das können wir nur durch eine enge Vernetzung und Zusammenarbeit zwischen Politik, Verwaltung, Wirtschaft und Wissenschaft erreichen.

Dafür brauchen wir klare Spielregeln, die wir in einem Dialog mit der Wirtschaft festlegen wollen. Wir benötigen hier eine Kultur des vertrauensvollen Austausches – was bei der Vielzahl an beteiligten Akteuren und der Komplexität ihres Zusammenspiels durchaus eine Herausforderung darstellt. Sehr wichtig ist mir auch, dass die Aktivitäten in Kooperation mit dem Bundeskanzleramt, dem Verteidigungsministerium und dem Außenministerium erfolgen.

Ich bin sehr dankbar, dass das Kuratorium Sicheres Österreich als Plattform für den Dialog zur Verfügung steht und die Vernetzung und den Austausch weiter vorantreibt. Bei der ersten Cyberplattform-Veranstaltung des KSÖ konnten wir verschiedene Facetten des Spannungsfeldes zwischen staatlich festgesetzten Spielregeln auf der einen und der freiwilligen Selbstverpflichtung von Unternehmen auf der anderen Seite diskutieren. Dabei ist mir klar geworden: Diese Diskussion ist noch lange nicht abgeschlossen. Wir stehen erst am Anfang eines Verständnisprozesses, der deutlich macht, wie vielschichtig die Aufgabe ist, der wir uns gegenüber sehen.

Ich möchte eines betonen: Bei der Wahl regulatorischer Mittel muss der Staat auf jeden Fall mit Augenmaß und unter Gesichtspunkten der Verhältnismäßigkeit agieren. Wir dürfen das Internet weder als rechtsfreien noch in erster Linie als „kriminellen“ Raum sehen. Wir müssen uns klar am Nutzen für Bürger und Wirtschaft orientieren.

In der Kooperation mit nicht-staatlichen Akteuren setzen wir daher auf „regulierte Selbstverpflichtung“. Das bedeutet: Der Staat und nicht-staatliche Partner verständigen sich gemeinsam über die zu erreichenden Ziele und darauf, wie die Zielerreichung überprüft wird. Das Internet ist zu einer Basisinfrastruktur unserer Gesellschaft geworden. Lassen Sie uns gemeinsam daran arbeiten, es ein Stück weit sicherer zu machen.



Mag.[a] Johanna Mikl-Leitner
Bundesministerin für Inneres

Cybersicherheit intelligent regulieren: Warum, wie und durch wen?

Grundsatzüberlegungen im Spannungsfeld zwischen staatlichen Vorgaben, privatwirtschaftlicher Selbstverpflichtung und individuellen Grundrechten

Heiko Borchert

Inhaltsübersicht

1. Zusammenfassung 8
2. Einführung 13
3. Begriffliche Grundlagen 15
4. Ziele: Warum und wozu soll reguliert werden? 18
5. Risiken und Chancen: Was soll reguliert werden? 24
6. Zuständigkeiten: Wer soll regulieren? 29
7. Adressaten: Wer soll reguliert werden? 32
8. Regime: Wie soll reguliert werden? 36
9. Rahmenordnung: Welche Begleitmaßnahmen soll es geben? 42
10. Autorenhinweis 48

1. Zusammenfassung

Der Cyberspace, verstanden als jener Raum, der durch die weltumspannende Nutzung der Informations- und Kommunikationstechnologie (IKT) sowie die darüber transportierten Daten entsteht, verspricht seinen Nutzern beinahe ungeahnte Möglichkeiten. Dem großen Potenzial stehen Risiken gegenüber. Um das Eintreten der Risiken zu vermeiden und damit das vorhandene Potenzial zu nutzen, sind Rahmenbedingungen erforderlich. Diese Rahmenbedingungen dienen dazu, erwünschtes Verhalten zu fördern und unerwünschtes Verhalten einzudämmen.

Regulierung für Cybersicherheit hat die Aufgabe, diese Rahmenbedingungen zu schaffen. Allerdings kommt es entscheidend darauf an, aus welcher ordnungspolitischen Leitvorstellung Ansätze zur möglichen Regulierung abgeleitet werden. Die Entscheidung darüber ist Sache der Politik. Die vorliegende Ausarbeitung will dazu einen unterstützenden Beitrag leisten und verfolgt drei Zielsetzungen: Sie zeigt (1) das gesamte Spektrum der bei der Regulierung zu berücksichtigenden Aspekte auf, (2) illustriert anhand ausländischer Beispiele, wie diese Aspekte umgesetzt werden können, und regt (3) mit weiterführenden Fragen die Diskussion zur Förderung der Cybersicherheit in Österreich an. Dabei stehen die folgenden sechs Fragestellungen im Mittelpunkt:

Frage 1: Warum und wozu soll reguliert werden?

Verschiedene Akteure nutzen den Cyberspace in unterschiedlicher Form. Innerhalb kürzester Zeit hat er sich zu einem zentralen Marktplatz für Unternehmen und Konsumenten entwickelt und wird zur Pflege sozialer Beziehungen genutzt. Der Cyberspace dient als beinahe unerschöpfliches Informationsreservoir, erleichtert den Zugang zu staatlichen Dienstleistungen, eröffnet neue Wege der politischen Partizipation und ermöglicht den Betrieb sowie die Steuerung industrieller Prozesse, erlaubt aber auch kriminellen Akteuren die Ausübung von Straftaten. Je nachdem, welche dieser Entwicklungen gefördert, beschränkt oder verboten werden soll, können regulatorische Maßnahmen unterschiedlich begründet werden, nämlich mit dem

- Eindämmen der Risiken, die die Sicherheit des Cyberspace und die öffentliche Sicherheit gefährden können **(Gefahrenabwehr)**
- Bereitstellen der für den Cyberspace maßgeblichen Informations- und Kommunikationstechnologien und -komponenten **(Versorgungssicherheit)**
- Gewährleisten, dass Verbraucherinnen und Verbraucher den Cyberspace sicher, d.h. beispielsweise ohne Verlust der Privatsphäre, nutzen können **(Verbraucherschutz)**

- Sicherstellen des Vorhandenseins der erforderlichen Infrastrukturen **(Infrastrukturgewährleistung)**
- Beheben mangelnder, nicht ausreichender oder fehlender Steuerungsimpulse des Marktes **(Marktversagen)**

Frage 2: Was soll reguliert werden?

Mit einem **risikoorientierten** Regulierungsansatz sollen die Schwachstellen behoben werden, die die Cybersicherheit gefährden können:

- Diesem Ziel dienen **verhaltensorientierte Maßnahmen,** die Aspekte der individuellen Nutzung des Cyperspace ebenso zum Gegenstand haben wie beispielsweise strafrechtliche Normen, die der Gefahrenabwehr dienen. Immer wichtiger wird im Bereich der verhaltensorientierten Maßnahmen auch die Analyse der Motive, die Investoren veranlassen, sich an strategisch bedeutenden Betreibern der nationalen IKT-Infrastruktur zu beteiligen.
- Im **technischen Bereich** geht es um die eingesetzte Hard- und Software sowie deren Zusammenwirken. Bewusst herbeigeführte Verwundbarkeiten durch die Konfiguration der entsprechenden Komponenten sind dabei ebenso relevant wie Risiken, die sich aus global arbeitsteiligen Wirtschaftsprozessen und der damit einhergehenden Abhängigkeit von ausländischen Komponentenlieferanten ergeben.
- In **organisatorischer Hinsicht** geht es darum, Prozesse und Strukturen sowie damit verbunden Zuständigkeiten, Kompetenzen und Verantwortlichkeiten für die Cybersicherheit festzulegen.
- Regulatorische Maßnahmen können sich schließlich auch auf die Inhalte der elektronischen Daten- und Kommunikationsübertragung **(Content-Regulierung)** erstrecken sowie die Auswirkungen **natürlicher Umwelteinflüsse** (z.B. Hochwasser, Lawinen) auf die IKT-Infrastruktur berücksichtigen.

In Ergänzung dazu steht der **chancenorientierte** Regulierungsansatz, der positive Nutzeneffekte schaffen will:

- Denkbar sind Maßnahmen, die dem Aufbau, dem Erhalt und der Förderung der benötigten Expertise des Erkennens, Abwehrens und Bewältigens von Cyberrisiken dienen **(Capacity Building)**.
- Hinzu kommt das Bestreben, mit der Entwicklung von Cybersicherheitslösungen auch die Wirtschaft zu unterstützen und mit geeigneten Produkten und Lösungen ausländische Märkte zu erschließen **(Wirtschaftsförderung)**.

Frage 3: Wer soll regulieren?

Regulierung im Sinne der Verhaltenssteuerung ist im Cyberspace nicht mehr ausschließliche Kompetenz des Staates. Es bedarf neuer Wege, um die Anliegen verschiedener Anspruchsgruppen zu berücksichtigen:

- Auf **Ministerien und Behörden** fällt traditionellerweise der Blick, wenn es um Regulierung geht. Angesichts der zu lösenden Herausforderungen fällt auf, dass gerade in Ländern, die bislang der Wirtschaft einen großen Handlungsspielraum bei Fragen der nationalen Sicherheitsvorsorge eingeräumt haben, eine stärkere Rolle des Staates angemahnt wird.
- Neben Ministerien und Behörden spielen **Gerichte** eine wichtige Rolle, auch weil sie mit ihren Entscheidungen den Rahmen staatlichen Handelns direkt beeinflussen können.
- Daneben verfolgt die **Industrie** über Verbände und normierende Gremien eigene Interessen und bringt diese in regulatorische Prozesse ein.
- Angesichts des Mobilisierungspotenzials, das der Cyberspace mit sich bringt, sollte schließlich auch die Rolle der **Bürgerinnen und Bürger** nicht vernachlässigt werden – wie das jüngste Beispiel um den Widerstand gegen das Urheberrechtsabkommen ACTA deutlich macht.

Frage 4: Wer soll reguliert werden?

Der Kreis der Akteure, an die sich regulatorische Maßnahmen richten, ist umfassend:

- **Produzenten der Hardware- und Softwareprodukte** bzw. relevanter Komponenten und die **Eigentümer und Betreiber strategischer IKT-Infrastrukturen** bilden das eigentliche Rückgrat der digitalen Wirtschaft. Fehler und Schwächen, die auf diesen Ebenen auftreten, beeinflussen die Leistungsfähigkeit aller anderen nachgelagerten Akteure.
- Das Vordringen der IKT in **andere strategische Infrastruktursektoren** führt zur Entstehung konvergenter Infrastrukturnetzwerke, die komplexe Fragen der regulatorischen Zuständigkeiten aufwerfen.
- Auch in der **allgemeinen Wirtschaft** sind IKT-Anwendungen inzwischen allgegenwärtig. Umfassend verstandene Ansätze der Unternehmenssicherheit und des Risikomanagements können helfen, die IKT-spezifischen Risiken zu berücksichtigen.
- **Behörden** sind ebenfalls Teil der strategischen Infrastruktur. Sie können durch spezifische Vorschriften zur Sicherheit ihrer IKT-Anwendungen eine Vorbildfunktion übernehmen.

- Zur Aufklärung der **Bürgerinnen und Bürger** sind Kampagnen der Bewusstseinsbildung und -förderung von Nutzen. In vielen Ländern werden für die jüngsten Nutzer des Cyberspace auch spezifische Schulungsprogramme angeboten.

Frage 5: Wie soll reguliert werden?

Um die Frage zu beantworten, welche Inhalte konkret Gegenstand einer möglichen Regulierung für Cybersicherheit sein können, sind vier Aspekte von Bedeutung:

- **Modelle der Regulierung:** Zwischen den idealtypischen Ansätzen staatlicher Vorschriften auf der einen und privatwirtschaftlicher Selbstregulierung auf der anderen Seite stehen partnerschaftliche Ansätze, an denen sich Akteure aus beiden Sektoren beteiligen. Wichtig ist dabei, wie sich die jeweiligen Akteure organisieren, um innerhalb eines Sektors und sektorübergreifend zusammenzuarbeiten, und wie diesbezüglich koordiniert wird.
- **Vorgaben:** Vorgaben können in Form von Gesetzen, Verordnungen, Normen, Standards und freiwilligen Selbstverpflichtungen erfolgen und dabei organisationsspezifische, verhaltensorientierte sowie technische Aspekte abdecken.
- **Anreize und Sanktionen:** Diese sind wichtig, um ein bestimmtes Verhalten zu bewirken. Als Anreize kommen z.B. steuerliche Vergünstigungen, haftungsrechtliche Erleichterungen oder Anpassungen bei der Unternehmensbewertung in Frage. Bußen, die zeitweise Einschränkung und die vollständige Einstellung des Betriebs auf Anordnung stellen mögliche Sanktionen dar.
- **Monitoring:** Hier geht es um die Frage, wie überprüft wird, ob Vorgaben zur Cybersicherheit eingehalten werden. Diese Überprüfungen können von staatlichen Stellen, durch Unternehmen oder durch unabhängige (und zertifizierte) Dritte vorgenommen werden.

Frage 6: Welche Begleitmaßnahmen soll es geben?

Die Wirkung regulatorischer Maßnahmen kann verstärkt werden durch Begleitmaßnahmen, die Verbindungen zu anderen Politikfeldern ermöglichen. Drei Ansatzpunkte erweisen sich als besonders interessant:

- **Informationsaustausch:** Dieser unterstützt regulatorische Vorgaben zur Cybersicherheit und ist gleichzeitig auch Voraussetzung dafür. In einem partnerschaftlichen Regulierungsmodell spielt der Informationsaustausch zwischen den Behörden, den Behörden und der Privatwirtschaft sowie auf privatwirtschaftlicher Seite eine zentrale Rolle. Wichtige Aspekte des Informationsaustauschs sind die Rechtssicherheit, die Klärung der Frage, ob Informationen freiwillig oder verpflichtend weitergegeben werden sollen, sowie die Struktur und die Inhalte des Informationsaustauschs.

- **Übungen:** Übungen sind ein geeignetes Mittel, um zu überprüfen, ob vorhandene Konzepte, Verfahren, Instrumente und Fähigkeiten geeignet sind, Ereignisse zu bewältigen. Das gilt auch für regulatorische Vorgaben, insoweit sie beispielsweise Bestimmungen zu spezifischen Koordinationsmechanismen, Verfahrensabläufen oder Reaktionszeiten enthalten.
- **Forschung und Entwicklung:** Die Förderung der Forschung und Entwicklung im Umgang mit Cyberrisiken dient gleichzeitig der Innovations-, Wirtschafts- und Sicherheitspolitik.

2. Einführung

Wie kaum ein zweites Thema haben es Fragestellungen rund um die Nutzung des Cyberspace in kürzester Zeit geschafft, die politische, unternehmerische und gesellschaftliche Diskussion zu prägen, mitunter auch zu dominieren. Es scheint, als ob sich kein Lebensbereich der Anziehungskraft des Cyberspace entziehen kann. Bei näherem Blick auf das Phänomen Cyberspace wird klar, dass unser Umgang damit einen Kernaspekt des modernen Lebens betrifft – **Vertrauen**:

- Vertrauen in die Infrastruktur, die für die Übermittlung von Daten und Kommunikation benötigt wird;
- Vertrauen in die Personen, die die Produkte und Komponenten entwickeln, damit der Cyberspace überhaupt entsteht und genutzt werden kann;
- Vertrauen in die Anwendungen, mit denen Bürgerinnen und Bürger online Bestellungen aufgeben, Zahlungen abwickeln und kommunizieren;
- Vertrauen, mit Hilfe des Cyberspace seine Meinung frei von staatlicher Kontrolle äußern zu können;
- Vertrauen in die Erfolgsaussichten, die sich Unternehmen versprechen, wenn sie ihre Produkte digital vermarkten und vertreiben;
- Vertrauen in die Rolle der staatlichen Behörden, dass sie im Fall möglicher Verletzungen von Rechtsbestimmungen in der Lage sind, die Täter zu fassen und zu bestrafen.

Cyberunsicherheit kann dieses Vertrauen zerstören! Das verdeutlicht den Stellenwert des Themas: Wer sagt, dass er sich ein Leben ohne Internet – als Kurzformel der Nutzung des Cyberspace – nicht mehr vorstellen kann, der trifft den Kern der Herausforderung, denn diese ist gesellschaftspolitischer Natur. Es geht um nichts weniger als die Frage, wie ein Instrument, das den Lebensstil eines Großteils der Bürgerinnen und Bürger prägt, sicher, zuverlässig, leistungsfähig und vertrauenswürdig gestaltet werden kann.

Wie dieses Ziel erreicht werden kann, ist Gegenstand der Arbeiten, die in den nächsten Monaten zu einer Cybersicherheitsstrategie für Österreich führen werden. Die vorliegende Ausarbeitung ist Teil dieses Prozesses. Sie greift den zentralen Aspekt der Spielregeln auf, die benötigt werden, um Risiken für die Cybersicherheit abzuwehren. Es handelt sich hierbei jedoch nicht um ein politikgestaltendes Dokument. Die Definition der Inhalte einer künftigen nationalen Cybersicherheitsstrategie ist Aufgabe der Ministerien. Die Ausarbeitung leistet hierzu einen Impuls, indem sie in einer Bestandsaufnahme aufzeigt, welche Aspekte zu berücksichtigen sind, wenn Spielregeln für die Cybersicherheit erarbeitet werden sollen. Dabei werden Beispiele aus anderen Ländern des OECD-Raums angeführt, um zu zeigen, welche

Ansätze denkbar sind. Hinweise auf diese Beispiele nehmen keine Entscheidungen in Österreich vorweg. Vielmehr sollen sie anregen zum Nachdenken darüber, welche Maßnahmen in Österreich bereits ergriffen wurden und welche Schritte noch folgen könnten.

Zu diesem Zweck beleuchtet die Ausarbeitung nach der Definition wesentlicher Grundbegriffe sechs Aspekte der Regulierung von Cybersicherheit. In jedem Abschnitt werden die grundsätzlichen konzeptionellen Herausforderungen beschrieben und anhand von Beispielen aus der Praxis illustriert. Jeder Abschnitt schließt mit Grundsatzfragen für den künftigen Umgang mit Cybersicherheit in Österreich. Diese Fragen sind nicht abschließend, sondern sollen zur Diskussion in Österreich beitragen.

Cybersicherheit ist ohne Zweifel ein zentrales Thema – aber sie ist nicht die einzige Herausforderung für die nationale Sicherheitsvorsorge. In der weiteren Folge geht es daher immer darum, Ansätze zur Verbesserung der Cybersicherheit aus dem umfassenderen Blickwinkel der nationalen Sicherheitsvorsorge zu betrachten. Vier grundlegende Gedanken seien deshalb den folgenden Ausführungen vorangestellt:

- Erstens muss **abgewogen** werden zwischen dem, **was schon erreicht** wurde, und dem, was **noch zu tun** ist, um die Cybersicherheit aus österreichischer Sicht zu verbessern. Dabei geht es besonders um die Frage der Ausgewogenheit der Maßnahmen, die mehrheitlich zwar vom Staat angeordnet werden könnten, jedoch nur teilweise von diesem umgesetzt werden müssen. Diejenigen Akteure, die im Kern für die Sicherheit des Cyberspace verantwortlich sind, sind die Unternehmen und die Bürger. In dieser Feststellung liegt die Bedeutung partnerschaftlicher Ansätze, die in der eingangs zitierten Beobachtung der Bundesinnenministerin zum Ausdruck kommt.

- Zweitens gibt es vor dem Hintergrund des breiten Aufgabenspektrums der nationalen Sicherheitsvorsorge eine große **Berührungsfläche** zwischen dem Bestreben nach Cybersicherheit, dem Schutz strategischer Infrastrukturen[1] und weiteren Sicherheitsaufgaben (z.B. Abwehr der Wirtschaftsspionage). Das Vorhandensein dieser Berührungsfläche erleichtert die Bemühungen zur Förderung der Cybersicherheit, weil auf vorhandenen Ansätzen aufgebaut werden kann. Die Berührungsfläche bedeutet aber auch, dass mit Vor-

1 Strategische Infrastrukturen sind „jene Infrastrukturen oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl der Bevölkerung oder die effektive Funktionsweise von Regierungen haben würde“. Zit. nach: Masterplan Österreichisches Programm zum Schutz Kritischer Infrastruktur (Wien: Bundeskanzleramt, 2008), S. 5. Die Begriffe „strategische“ und „kritische“ Infrastruktur werden in der Praxis oftmals synonym verwendet. Hier wird die Bezeichnung „strategisch“ bevorzugt, um die Bedeutung der entsprechenden Infrastrukturbetreiber für die Prosperität und die Sicherheit Österreichs zu unterstreichen.

sicht und Bedacht vorgehen muss, wer beispielsweise den Betreibern strategischer Infrastrukturen zusätzliche Verpflichtungen für die Cybersicherheit übertragen will. Dies vor allem deshalb, weil der Einsatz der IKT, der die Nutzung des Cyberspace überhaupt erst ermöglicht, eines **querschnittlichen Ansatzes** bedarf, der über Organisationsgrenzen und Aufgabenzuständigkeiten deutlich hinausreicht. Der Wille der Akteure in Politik, Administration, Wirtschaft, Wissenschaft und Gesellschaft, diese Grenzen zu überschreiten, ist daher maßgeblich für den Erfolg der angedachten Maßnahmen.

- Drittens sind Fragen der Cybersicherheit vorwiegend technisch getrieben. Sie unterliegen daher stärker als Fragen in anderen Politikfeldern einer **hohen Dynamik.** Diese Dynamik steht in einem Spannungsverhältnis zum klassischen Politikbetrieb. Um mit technischen Veränderungen Schritt zu halten, bedarf es daher neuer Formen des Zusammenwirkens der Akteure.

- Viertens sind diese Formen des Zusammenwirkens und die Maßnahmen zur Stärkung der Cybersicherheit **prozessorientiert** zu betrachten. Handlungen sind in einen auf kontinuierliche Verbesserungen ausgerichteten Ablauf zu bringen. Dieser reicht von der Risikoanalyse über die Definition von Schutzzielen und die Identifizierung sowie die Umsetzung von Schutzmaßnahmen bis zur laufenden Überprüfung dieser Maßnahmen vor dem Hintergrund der erkannten Risiken. Auf jeder Stufe dieses Regelkreises ist die enge Abstimmung zwischen Partnern aus dem öffentlichen und privaten Sektor unerlässlich.

3. Begriffliche Grundlagen

Cybersicherheit und Regulierung sind zwei Begriffe, die oft verwendet, aber nur selten konkret definiert werden. Die relative Unbestimmtheit der beiden Begriffe ist in der Diskussion von Vorteil, denn sie erlaubt es den verschiedenen Akteuren, ihre Interessen in den Diskussionsprozess einzubringen. Die begriffliche Unklarheit wird jedoch dann zum Problem, wenn es konkret darum geht, Zielsetzungen, Maßnahmen und Zuständigkeiten zu bestimmen. Daher ist es unerlässlich, für die vorliegende Ausarbeitung zu definieren, wie Cybersicherheit und Regulierung verstanden werden.

In einer ersten Annäherung können wir Regulierung im politisch-wirtschaftlichen Umfeld als Steuerung im Hinblick auf ein (oder mehrere) Ziel(e) verstehen. Demzufolge geht es darum, das Verhalten von Akteuren, ihre Interaktion und möglicherweise auch ihre Organisation so zu beeinflussen, dass eine erwünschte Wirkung erzielt wird. Regulierung zieht daher **zielorientiertes Einwirken** nach sich. Welche Form des Einwirkens erforderlich und verhältnismä-

ßig ist, wer dieses wie vornimmt und wer die Einhaltung der Vorgaben prüfen soll, ist abhängig von den **ordnungspolitischen Leitvorstellungen.** Diese definieren die allgemeinen Rahmenbedingungen des politisch, gesellschaftlich und wirtschaftlich wünschenswerten Handelns. Wichtig ist in diesem Zusammenhang die Feststellung, dass die angesprochenen Eingriffe nicht ausschließlich mit gesetzgeberischem Handeln des Staates gleichgesetzt werden. Vielmehr sollte unter dem Begriff der Regulierung ein breites Spektrum von Maßnahmenansätzen verstanden werden, das in der Folge noch näher betrachtet wird.

Dieser Zugang macht deutlich, dass sich die Frage, wie Cybersicherheit erreicht werden kann, in den grundsätzlichen Ordnungsrahmen einfügt, den ein Gemeinwesen für sich als maßgeblich definiert. Diese Feststellung erscheint auf den ersten Blick trivial. Auf den zweiten Blick macht sie allerdings deutlich, dass Regulierung zur Cybersicherheit gleichermaßen alle normativen Vorgaben dieses Gemeinwesens berücksichtigen muss. Und genau daraus ergibt sich das **Spannungsfeld** für mögliche Regulierungsansätze, die neben dem gesellschaftlichen Interesse an Stabilität, Ruhe und Ordnung das wirtschaftliche Streben nach Innovation, Wettbewerbsfähigkeit und Prosperität genauso beachten müssen wie den individuellen Wunsch nach dem Schutz der Privatsphäre und den verfassungsmäßig gewährleisteten Grundrechten.

Cyber Security is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be comprised of a limitation of the availability and reliability of the ICT, breach of the confidentiality of information stored in ICT or damage to the integrity of that information

The National Cyber Security Strategy (The Hague: Ministry of Security and Justice, 2011), S. 3.

Cyber-Sicherheit in Deutschland ist (...) der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des deutschen Cyber-Raums auf ein tragbares Maß reduziert sind. Cyber-Sicherheit (in Deutschland) entsteht durch die Summe von geeigneten und angemessenen Maßnahmen.

Cyber-Sicherheitsstrategie für Deutschland (Berlin: Bundesministerium des Innern, 2011), S. 15.

In our approach, we will use the term „cyber security" as the need to prevent from, prepare for, detect, respond to and recover from any hazard or illicit content in the cyberspace, covering networked infrastructures, including internet.

Towards a concerted EU approach to cyber security (Brussels: European Organisation for Security, 2010), S. 8.

Cyber security embraces both the protection of UK interest in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers.

Cyber Security Strategy of the United Kingdom (London: Cabinet Office, 2009), S. 9.

Cybersecurity policy includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communication infrastructure.

Cyberspace Policy Review (Washington, DC: The White House, 2010), S. 2.

Box 1: Cybersicherheitsdefinitionen ausgewählter OECD-Staaten

Dieses bewusst breit angelegte ordnungspolitische Verständnis ist auch deshalb sinnvoll, weil ein Grundkonsens über die Definition des Begriffs der Cybersicherheit bislang weitgehend fehlt (siehe Box 1). Das gilt für die nationale Debatte in Österreich genauso wie für die internationale Diskussion. Je nach Betrachtungsweise stehen eher technische Fragen im Vordergrund, werden Aspekte der Strafverfolgung betont, standort- und wettbewerbspolitische Überlegungen in den Mittelpunkt gestellt oder verbraucher- und datenschutzrechtliche Argumente angeführt, um den Begriff zu definieren. Vor diesem Hintergrund können regulatorische Ansätze zur Förderung der Cybersicherheit, je nachdem, aus welcher Perspektive sie entwickelt werden, ganz unterschiedlich ausfallen. Den weiteren Ausführungen liegt daher folgendes Begriffsverständnis zugrunde:

Cybersicherheit

- beschreibt den Schutz eines zentralen Rechtsgutes mit geeigneten rechtsstaatlichen Mitteln,
- vor akteursbezogenen, technischen, organisations- und naturbedingten Gefahren,
- die die Sicherheit des Cyberspace (inklusive Infrastruktur- und Datensicherheit) und die Sicherheit der Nutzer im Cyberspace gefährden,
- in einem vernetzten und partnerschaftlichen Ansatz, der die relevanten staatlichen bzw. nicht-staatlichen Akteure einbezieht und damit dazu beiträgt,
- die Gefährdungen zu erkennen, zu bewerten und zu verfolgen sowie
- die Fähigkeit zu stärken, Störungen im und aus dem Cyberspace zu bewältigen, die damit verbundenen Folgen zu mindern sowie die Handlungs- und Funktionsfähigkeit der davon betroffenen Akteure, Infrastrukturen und Dienste wieder herzustellen.

Regulierung zum Zweck einer verbesserten Cybersicherheit soll vor diesem Hintergrund klären,

- **warum** und **wozu** regulatorische Maßnahmen erforderlich sind (Abschnitt 4);
- welche **Risiken** und **Chancen** Gegenstand regulatorischer Maßnahmen sein sollen (Abschnitt 5);
- **wer** die entsprechenden regulatorischen Maßnahmen ergreifen kann (Abschnitt 6);
- an **wen** sich die regulatorischen Maßnahmen richten (Abschnitt 7);
- in welchem **institutionellen Rahmen** die Regulierung erfolgt (Abschnitt 8) und
- welche **Begleitmaßnahmen** sinnvollerweise vorzusehen sind (Abschnitt 9).

4. Ziele: Warum und wozu soll reguliert werden?

Die Begründung einer regulatorischen Maßnahme ist für ihre Wirksamkeit und für ihre Legitimität aus Sicht der Betroffenen von zentraler Bedeutung. Weshalb Regulierung gefordert wird, hängt wesentlich von den im vorangehenden Abschnitt diskutierten ordnungspolitischen Grundvorstellungen ab. Diese ordnungspolitischen Grundvorstellungen stehen in engem Zusammenhang mit den individuellen und kollektiven Vorstellungen darüber, was der Cyberspace ist und wie dieser genutzt wird. Mindestens sechs verschiedene Vorstellungen können unterschieden werden:

- **Wirtschafts- und Handelsraum**

  In verhältnismäßig kurzer Zeit hat sich der Cyberspace zu einem Marktplatz von strategischer Bedeutung entwickelt. Schätzungen zufolge könnte sich der Wert des weltweiten E-Commerce-Geschäfts von heute 572 Milliarden $ bis 2014 nahezu verdoppeln. Betrachtet man zudem das Geschäftsvolumen, das Unternehmen untereinander auf elektronischem Weg abwickeln, könnte sich dieses 2013 auf geschätzte 16 Billionen $ belaufen.[2] Bis 2014 wird mit dem weltweiten Download von über 70 Milliarden Apps gerechnet, womit ein geschätzter Umsatz von beinahe 60 Milliarden $ erzielt wird.[3]

- **Sozialer Interaktionsraum**

  Darüber hinaus ist der Cyberspace ein allgemeiner sozialer Interaktionsraum, den die Menschen zur Pflege sozialer Beziehungen nutzen. Weltweit gibt es schätzungsweise mehr als zwei Milliarden Internetnutzer.[4] Wäre Facebook ein Staat, läge dieser mit über 800 Millionen „Einwohnern“[5] auf Platz 3 der bevölkerungsreichsten Nationen – gleich nach China bzw. Indien und noch deutlich vor der Europäischen Union. Über den Online-Nachrichtendienst Twitter werden täglich gut 350 Millionen Tweets ausgetauscht, und während des Tsunamis/Erdbebens im Frühjahr 2011 in Japan waren es pro Sekunde 5.530 Tweets.[6]

- **Informationsraum**

  Der Cyberspace ist zusätzlich auch Informationsraum, der die Verbreitung und Übertragung unterschiedlicher Daten- und Informationsbestände ermöglicht. Als Informationsraum wächst der Cyberspace mit rapider Geschwindigkeit: Pro Minute werden gut 168

---

2 The New Digital Economy. How it will transform business (Oxford: Oxford Economics, 2011), S. 9.

3 „Das Smartphone als Verkaufsplattform“, Neue Zürcher Zeitung, 24. November 2011, S. 35.

4 Internet matters: The Net’s sweeping impact on growth, jobs, and prosperity (o.O.: McKinsey Global Institute, 2011), S. viii.

5 <http://www.socialnetworkingwatch.com/all_social_networking_statistics/index.html> (Zugriff: 5. März 2012).

6 <http://www.jeffbullas.com/2011/09/21/11-new-twitter-facts-figures-and-growth-statistics-plus-infographic/> (Zugriff: 5. März 2012).

Millionen E-Mails versandt, knapp 700.000 Suchabfragen bei Google eingegeben oder mehr als 70 neue Domains registriert (Abbildung 1).

Abbildung 1: Was in 60 Sekunden alles im Internet geschieht

Quelle: <http://www.go-gulf.com/blog/60-seconds> (Zugriff: 5. März 2012).

- **Politischer Partizipationsraum**

  Als Handels-, Interaktions- und Informationsraum beeinflusst der Cyberspace auch das Verhältnis zwischen Staat und Bevölkerung. Mit digitalen Angeboten des E-Government baut der Staat seine Dienstleistungsfunktion zugunsten der Bürgerinnen und Bürger aus und ermöglicht diesen vereinfachte Wege, um staatliche Leistungen in Anspruch zu nehmen.[7] Der verstärkte Rückgriff auf digitale Formen der Interaktion eröffnet darüber hinaus auch neue Möglichkeiten der politischen Partizipation und der politischen Meinungsäußerung.[8]

7 Zum Stand der diesbezüglichen Anstrengungen im europäischen Vergleich: Europe's Digital Competitiveness Report (Luxembourg: Publications Office of the European Union, 2010), S. 85–94.

8 Zur Frage der politischen Partizipation im Allgemeinen: Ulrike Wagner, Peter Gerlicher und Niels Brüggen, Partizipation im und mit dem Social Web. Herausforderungen für die politische Bildung. Expertise für die Bundeszentrale für politische Bildung (München: JFF – Institut für Medienpädagogik in Forschung und Praxis, 2011), <http://pb21.de/files/2012/01/bpb-Expertise_Partizipation_im_Social_Web.pdf> (Zugriff: 6. März 2012). Zur Förderung der politischen Meinungsäußerung mit besonderem Bezug zu den Unruhen im Frühjahr 2011 in Nordafrika: Evgeny Morozov, The Net Delusion: The Dark Side of Internet Freedom (New York: Public Affairs, 2011); Nadia Idle and Alex Nunns (eds.), Tweets from Tahir: Egypt's Revolution as it Unfolded, in the Words of the People Who Made It (New York: OR Books, 2011).

- **Steuerungsraum**

  Eng mit der Funktion als Informationsraum verbunden ist die Rolle des Cyberspace als Steuerungsraum, mit dessen Hilfe zum Beispiel industrielle Prozesse und Anlagen überwacht, betrieben und gewartet werden können. Schätzungen zufolge könnten im Jahre 2020 bis zu 50 Milliarden Geräte[9] miteinander kommunizieren. Umso wichtiger wird es, dass auch diese Kommunikation sicher erfolgt, um Zwischenfälle zu vermeiden.[10]

- **Tatraum**

  Schließlich wird der Cyberspace von kriminellen Akteuren auch als Tatraum genutzt, in dem Straftaten begangen werden. Statistisch gesehen, so der aktuelle Norton Cybercrime Report, wurden im letzten Jahr über 430 Millionen Erwachsene Opfer krimineller Handlungen im Internet – das sind täglich mehr als 42.000 Nutzer. Der Schaden, der ihnen auf diesem Weg zugeführt wurde, beläuft sich auf gut 114 Milliarden $.[11] Zu den charakteristischen Eigenschaften des Cyberspace als Tatraum zählt auch der Umstand, dass illegal erworbene Informationen über diesen in kürzester Zeit global zugänglich gemacht werden können (Stichwort: Wikileaks). Gerade aus Sicht der inneren Sicherheit zunehmend bedeutend ist auch der Umstand, dass Konflikte aus dem Cyberspace auf die reale Welt überschwappen können. Das zeigte jüngst die Auseinandersetzung zwischen den Online-Aktivisten von Anonymous und Drogengangs in Mexiko.[12]

Jede dieser verschiedenen Formen der Nutzung des Cyberspace ist mit individuellen Chancen und Risiken (Abschnitt 5) verbunden. Daraus können wiederum unterschiedliche Motive zur Regulierung abgeleitet werden – je nachdem, ob es darum geht, eine spezifische Entwicklung zu fördern, zu beschränken oder gar zu verbieten:

- **Gefahrenabwehr**

  Gefahrenabwehr zum Schutz der öffentlichen Ordnung und Sicherheit sowie von Leib und Leben[13] ist ein klassisches Regulierungsmotiv. Dabei gilt der Grundsatz „What is illegal

---

9 Bob Emmerson, „M2M: The Internet of 50 billion devices“, Win-Win, Januar 2010, S. 19–22.

10 Siehe zur Verwundbarkeit von Steuerungsanlagen generell: Nicolas Falliere, Liam O. Murchu, and Eric Chien, W32.Stuxnet Dossier (Cupertino: Symantec, 2011); Global Energy Cyberattacks: „Night Dragon“ (Santa Clara: McAffee, 2011); In the Dark. Crucial Industries Confront Cyberattacks (Santa Clara/Washington, DC: McAffee/CSIS, 2011); Protecting Industrial Control Systems. Recommendations for Europe and Member States (Heraklion: ENSIA, 2011).

11 <http://us.norton.com/cybercrimereport/promo> (Zugriff: 5. März 2012).

12 „Anonymous vs Zetas Amid Mexico's Cartel Violence“, Stratfor, 3. November 2011.

13 Zu beachten ist allerdings, dass Leib und Leben durch zahlreiche cyberrelevante Risiken nicht oder nur indirekt tangiert werden. Siehe auch: Gerald Spindler, „Haftung im IT-Recht“, in: Egon Lorenz (Hrsg.), Karlsruher Forum 2010: Haftung und Versicherung im IT-Bereich (Karlsruhe: Verlag Versicherungswirtschaft GmbH, 2011), S. 3–112, hier S. 69.

offline is illegal online".[14] Daraus lässt sich für den Bereich der Kriminalitätsbekämpfung auf der staatlichen Seite zwar eine grundsätzliche Zuständigkeit der Innenministerien ableiten. Aber nicht immer reichen die vorhandenen Kompetenzen der staatlichen Behörden aus, um in geeigneter Weise aktiv zu werden. Hinzu kommt, dass die Gefahrenabwehr im Cyberspace über strafrechtsrelevante Tatbestände hinausreicht und weitere Dimensionen der nationalen Sicherheitsvorsorge erfasst. Dazu zählen beispielsweise der Schutz strategisch bedeutender Infrastrukturen, die für die Daseinsvorsorge[15] relevant sind, sowie die Abwehr von Gefahren, die in ihrer Wirkung einem bewaffneten Angriff gleichgesetzt werden könnten. Der Umgang mit diesen Risiken erfordert neue Wege der öffentlich-privaten Koordination und des Informationsaustauschs (Abschnitt 9).

- **Versorgungssicherheit**

  Versorgungssicherheit spielt im Zusammenhang mit Cybersicherheit eine zentrale Rolle. Dabei können zwei Perspektiven unterschieden werden. Einerseits geht es um die Gewährleistung der entsprechenden Dienste, z.B. durch die Sicherstellung der erforderlichen IKT-Infrastrukturen. In Schweden steht dem zuständigen Regulator PTS (Swedish Post and Telecoms Agency) ein Jahresbudget von mehreren Millionen Euro zur Verfügung, um Sicherheitsmaßnahmen wie Notstromversorgung und mobile Basisstationen zu unterstützen.[16] Andererseits geht es um die Verfügbarkeit kritischer Komponenten, die für die Funktionsfähigkeit der IKT-Infrastruktur benötigt werden. So verfügt die National Emergency Supply Agency in Finnland über ein eigenes Budget, aus dem beispielsweise auch IKT-Backup-Systeme beschafft werden können.[17] Die jüngsten Erdbeben- und Hochwasserkatastrophen in Japan und Thailand, die sich auf die weltweite Chipproduktion ausgewirkt haben, aber auch Drohungen Chinas, den Export von seltenen Erdenmetallen einzuschränken, die für die Chipherstellung relevant sind, verdeutlichen darüber hinaus noch ganz andere Gefahren für die Funktionsfähigkeit der IKT-Infrastrukturen. Ob und in welchem Umfang die Industrieländer als Antwort darauf Ansätze wie Pflichtlager für IKT-relevante Bauteile in Betracht ziehen, dürfte vor allem eine Frage der Substitutionsmöglichkeiten und der Kostenfolgen sein.

---

14 The UK Cyber Security Strategy. Protecting and Promoting the UK in a digital world (London: Cabinet Office, 2011), S. 29.

15 Als Rechtsbegriff wird die Daseinsvorsorge mit dem Budgetbegleitgesetz 2012 und der damit verbundenen Änderung des Außenhandelsgesetzes 2011 eingeführt. Er umfasst auch den Bereich der Telekommunikation. Siehe: Artikel 21 des Budgetbegleitgesetzes 2012 zur Änderung des Außenwirtschaftsgesetzes 2011, § 25a Abs. 2 Ziffer 2, in: Bundesgesetzblatt vom 7. Dezember 2011, S. 22.

16 Peter Wallström, „Swedish Public-Private Partnerships for Resilience in the Electronic Communications Sector", Presentation, Meeting of the Working Groups of the European Public-Private Partnership for Resilience, Brussels, 6 July 2011, S. 1.

17 Finland Country Report (Heraklion: ENISA, 2011), S. 28.

- **Verbraucherschutz**

  Regulatorische Maßnahmen der Gefahrenabwehr und des Verbraucherschutzes liegen gerade im Cyberspace nahe beieinander. So sieht das niederländische Telekommunikationsgesetz vor, dass der Post- und Telekommunikationsregulator OPTA sich im Zeichen des Verbraucherschutzes auch der Internetsicherheit annimmt. Zu den Aufgaben von OPTA zählen deshalb die Überwachung des Verbots der Zustellung unerlaubter Werbung per E-Mail (Spam) sowie der Kampf gegen Schadsoftware.[18] In ähnlicher Weise sieht auch das finnische Gesetz zum Schutz der Privatsphäre in der Telekommunikation eine Rolle für den Regulator FICORA vor, der durch die Telekommunikationsbetreiber über Verstöße der Informationssicherheit informiert werden muss. Gestützt darauf hat FICORA Ausführungsbestimmungen erlassen, wonach die Telekommunikationsbetreiber ein umfassendes Managementsystem zur Gewährleistung der Informationssicherheit erarbeiten, dokumentieren und umsetzen müssen.[19] Eine solche Maßnahme empfiehlt auch das Bundesamt für Kommunikation in der Schweiz, das sich dabei auf ISO 27001 bezieht.[20]

- **Infrastrukturgewährleistung**

  Bei der Regulierung verschiedener Infrastruktursektoren ist ein Trend ersichtlich, der neben den grundlegenden Fragen des Zugangs z.B. zu Telekommunikations- oder Energienetzen verstärkt auch Aspekte der künftigen Ausgestaltung und des Ausbaus dieser Infrastrukturen regelt.[21] So erklärt das deutsche Telekommunikationsgesetz die „Sicherstellung einer flächendeckenden Grundversorgung mit Telekommunikationsdiensten zu erschwinglichen Preisen“ explizit zum Regulierungsziel.[22] Auch wenn die praktische Bedeutung dieser Vorgabe noch unklar ist, deutet sie an, dass regulatorische Vorstellungen und Vorgaben immer stärker auch in die Infrastrukturorganisation eingreifen. Die Relevanz dieser Entwicklung für die Cybersicherheit zeigt sich besonders deutlich an der Forderung nach Netzneutralität, also der Frage, „was eine angemessene Steuerung des Datenverkehrs darstellt“.[23] Wettbewerbspolitisch mag es Gründe geben, weshalb derjenige, der die relevante Infrastruktur für die Datenübertragung bereitstellt, nicht oder nur eingeschränkt

---

18 <http://www.opta.nl/en/about-opta/regulatory-areas/internet-safety/> (Zugriff: 5. März 2012).

19 Regulation on Information Security Management of Telecommunications Operators, FICORA 47C/2009M, Helsinki, 27. August 2009, <http://www.ficora.fi/attachments/englantiav/5k8y6zm5w/FICORA47C2009M.pdf> (Zugriff: 5. März 2012).

20 Richtlinien zur Sicherheit und Verfügbarkeit von Fernmeldeinfrastrukturen und -diensten (Biel: Bundesamt für Kommunikation, 2009), S. 6–7.

21 Josef Ruthig, „Europäisierte Regulierungsstrukturen und -netzwerke als Basis einer künftigen Infrastrukturvorsorge“, in: Ludwig Gramlich und Cornelia Manger-Nestler (Hrsg.), Europäisierte Regulierungsstrukturen und -netzwerke. Basis einer künftigen Infrastrukturvorsorge (Baden-Baden: Nomos, 2011), S. 11–24, hier S. 14.

22 § 2 Abs. 2 Ziff. 5 Telekommunikationsgesetz vom 22. Juni 2004, zuletzt geändert am 24. März 2011, <http://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf> (Zugriff: 8. März 2012).

23 Offenes Internet und Netzneutralität in Europa, KOM (2011) 222, Brüssel, 19. April 2011, S. 4. Siehe hierzu auch: Cyber-security: The vexed question of global rules. An independent report on cyber-preparedness around the world (Brussels: SDA, 2012), S. 18.

in der Lage sein soll, auf den Datenverkehr Einfluss zu nehmen. Sicherheitspolitisch mag dagegen das Interesse an genau dieser Steuerung überwiegen, insbesondere dann, wenn es darum geht, schädliche Inhalte aus dem Datennetz fernzuhalten oder das Verhalten straffälliger Nutzer aufzuklären.

- **Marktversagen**

  Marktversagen ist ordnungspolitisch ein klassischer Grund für regulatorische Intervention, sei es, um einen Strukturfehler des Marktes zu beheben (z.B. Schwächung der Stellung des Monopolisten gegenüber neuen Anbietern) oder Verzerrungen in der Preisbildung zu korrigieren (z.B. Internalisierung von Umweltschutzkosten). Unzureichende Sicherheit von Hardware und Software kann in diesem Sinne als Marktversagen interpretiert werden: Offenbar ist es nämlich einfacher, Anwendungen auf den Markt zu bringen und nachträglich durch Sicherheitspakete zu ergänzen, als die notwendige Sicherheit von Beginn an zu berücksichtigen. So wird denn auch aus juristischer Sicht kritisch angemerkt, dass IKT zwar als strategisch bedeutende Infrastruktur betrachtet wird, es jedoch nicht ausreichend griffige Bestimmungen zur Sicherheit der dazu benötigten Hard- und Software gibt. Anknüpfungspunkte, um mit dieser Problematik umzugehen, werden im Haftungs- und im Produktsicherheitsrecht gesehen.[24] Auf dieser Grundlage werden auf europäischer Ebene gegenwärtig Ansätze eines IT-Haftungsrechts entwickelt.

Leitfragen für die Diskussion in Österreich

- *Welche allgemeinen Ziele sollen mit der Regulierung von Cybersicherheit in Österreich erreicht werden?*
- *Welche konkreten Schutzziele der Cybersicherheit sind in Österreich erstrebenswert?*
- *Inwieweit soll zwischen übergreifenden und spezifischen, auf bestimmte Akteure ausgerichteten Cyberschutzzielen unterschieden werden (Abschnitt 7)?*
- *Wer ist in den Prozess der Zieldefinition eingebunden?*
- *Wie priorisiert Österreich mögliche Schutzziele für die Cybersicherheit?*
- *Wie und durch wen werden mögliche Zielkonflikte zwischen Cybersicherheit und den Zielsetzungen in anderen Politikfeldern behoben?*
- *Wer stellt in welcher Form sicher, dass die Zielsetzungen in unterschiedlichen Politikfeldern aufeinander abgestimmt werden?*

24 Spindler, „Haftung im IT-Recht“.

5. Risiken und Chancen: Was soll reguliert werden?

Angesichts der gegenwärtigen Diskussionen über die Gefahren des Cyberspace ist es naheliegend, bei der Frage nach dem Gegenstand der Regulierung zuerst an einen risikoorientierten Ansatz zu denken. Dieser dient dazu, Schwachstellen, die die Cybersicherheit gefährden können, zu erkennen und zu beheben. Wichtig ist dabei allerdings auch mit Blick auf andere Sicherheitsaufgaben, dass ein umfassendes Risikoverständnis zugrunde gelegt wird. Dieses sollte akteurs-, technik, organisations- und naturbedingte Risiken gleichermaßen umfassen. Vor diesem Hintergrund können folgende Cybersicherheitsrisiken als mögliche Anknüpfungspunkte für regulatorische Maßnahmen unterschieden werden:

- **Verhalten**

  Bei diesem Aspekt geht es beispielsweise um das Verhalten des Nutzers, wenn er bzw. sie online agiert (z.B. Preisgabe persönlicher Daten), um strafrechtlich relevante Handlungen (Abschnitt 4 → Gefahrenabwehr) oder den Umgang mit Verstößen gegen die Informationssicherheit.

  Um die Privat- und Intimsphäre der Nutzer zu schützen, sind Telekommunikationsbetreiber und Online-Dienste-Anbieter in vielen Ländern zu entsprechenden Schutzvorkehrungen verpflichtet. Kommt es zu Verstößen gegen diese Schutzvorkehrungen, besteht in einigen Ländern eine Informationspflicht (Abschnitt 9 → Informationsaustausch). Zunehmende Bedeutung erhält in diesem Zusammenhang die rapide steigende Zahl von Nutzern in sozialen Netzwerken. Die Nutzung und das Angebot medialer Inhalte werden dadurch vermischt. Hinzu kommt, dass es sich bei den Betreibern dieser Netzwerke meist um international tätige Unternehmen handelt. Daher lässt beispielsweise der Schweizer Bundesrat untersuchen, ob nationale Gesetze und Grundrechte ausgehebelt werden könnten und deswegen möglicherweise entsprechender Regelungsbedarf besteht.[25] Das deutsche Innenministerium setzt demgegenüber auf die Selbstregulierung der Anbieter und hat im November 2011 einen Prozess lanciert, um einen allgemeinen Kodex für soziale Netzwerke zu erarbeiten.[26]

  Wie sich Nutzer verhalten sollten, wenn die Informationssicherheit verletzt wird, ist in den USA Gegenstand einer Vorlage, die im Juli 2011 in den US-Kongress eingebracht wurde. Sie sieht unter anderem vor, wann und auf welchem Wege Nutzer über Verletzungen der Informationssicherheit informiert werden und wie sich diese in solchen Fällen an die An-

25 „Bundesrat sieht sich Gefahren von Facebook & Co. näher an. Bericht über mögliche Gesetzeslücken angekündigt“, NZZ Online, 24. November 2011, <http://www.nzz.ch/nachrichten/politik/schweiz/bundesrat_will_sich_der_gefahren_von_facebook__co_annehmen_1.13409713.html> (Zugriff: 6. März 2012).

26 „Kodex für soziale Netzwerke: Dialog verläuft konstruktiv“, Pressemitteilung, Bundesministerium des Innern, 7. März 2012.

bieter von Online-Diensten oder Kreditkartenagenturen wenden können.[27] In ähnlicher Absicht haben Finnland und die Schweiz Vorschriften bzw. empfehlende Richtlinien erlassen, dass Telekommunikationsbetreiber ein Managementsystem zur Informationssicherheit aufbauen müssen bzw. sollten (Abschnitt 4 → Verbraucherschutz).

Neueren Datums ist ein weiteres Risiko, das sich aus dem Verhalten von Investoren ergeben kann, die sich an Unternehmen des IKT-Sektors beteiligen. Dahinter steht die Sorge, dass Investoren z.B. durch ihren Einfluss auf die Geschäftsstrategie, die Standortwahl oder die Supply-Chain-Strategie Sicherheitsprobleme verursachen könnten. Österreich hat ähnlich wie Deutschland und Frankreich mit einer gesetzlichen Maßnahme auf dieses Risiko reagiert. Mit der Änderung des Außenwirtschaftsgesetzes wurden Vorschriften für Investoren erlassen, die sich an Unternehmen beteiligen wollen, die für die innere und äußere Sicherheit sowie für die Daseins- und Krisenvorsorge relevant sind.[28]

Nationale Bemühungen werden zusätzlich ergänzt durch internationale Initiativen. Das Spektrum reicht von der Diskussion zu Normen des zulässigen Verhaltens im Cyberspace[29] über die Frage der Vereinbarkeit spezifischer Maßnahmen und Operationen mit bestehendem Völkerrecht bis hin zur internationalen Unterstützung der Bekämpfung der Cyberkriminalität.[30]

- **Technik**

  Technische Risiken ergeben sich in erster Linie aus der eingesetzten Hard- und Software sowie aus deren Zusammenwirken. Der Umstand, dass IKT-Komponenten immer stärker auch in anderen strategisch bedeutenden Infrastruktursektoren eingesetzt werden, führt zu zunehmend konvergenten Infrastrukturnetzwerken, die durch das Cloud Computing

---

27 S. 1408 Data Breach Notification Act of 2011 vom 22. Juli 2011, <http://www.gpo.gov/fdsys/pkg/BILLS-112s1408is/pdf/BILLS-112s1408is.pdf> (Zugriff: 6. März 2012).

28 Budgetbegleitgesetz 2012 zur Änderung des Außenwirtschaftsgesetzes 2011; Außenwirtschaftsgesetz vom 28. April 1961, zuletzt geändert am 15. Dezember 2011, < http://www.gesetze-im-internet.de/bundesrecht/awg/gesamt.pdf> ; Décret no. 2005-1739 du 30 décembre 2005 réglementant les relations financières avec l'étranger et portant application de l'article L. 151-3 du code monétaire et financier, <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000268021&dateTexte= > (Zugriff: 6. März 2012).

29 Hierzu zählen Grundprinzipien wie die Verhältnismäßigkeit des Handelns durch Regierungen, freier Zugang zum Cyberspace für jedermann, Toleranz und Respekt gegenüber Dritten und der Schutz der Privatsphäre. Siehe hierzu: UK Cyber Security Strategy, S. 22.

30 Hierzu weiterführend: Cyber-security: The vexed question of global rules; Sandro Gaycken, Cyberwar. Das Internet als Kriegsschauplatz (München: Open Source Press, 2011), S. 196–205; Gutachten über Rechtsgrundlagen für Computernetzwerkooperationen durch Dienststellen des VBS, Verwaltungspraxis des Bundes, 3/2009, S. 141–177; Jeffrey T.G. Kesley, „Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", Michigan Law Review, 106:7 (May 2008), S. 1427–1452; Karl Frederick Rauscher and Andrey Kortokov, Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace (New York: EastWest Institute, 2011); Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cyber crime. Working paper prepared by the Secretariat, Twelfth United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.213/9, 22 January 2010, <http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf> (Zugriff: 8. März 2012).

grenzüberschreitend miteinander verbunden sein können. Konvergente Infrastrukturnetzwerke stellen eine besondere Herausforderung für die Frage der regulatorischen Zuständigkeit dar (Abschnitt 8 → Modelle der Regulierung).

Zwei besondere Ausprägungen technischer Risiken gewinnen jüngst verstärkt an Aufmerksamkeit, nämlich die bewusst herbeigeführte Verwundbarkeit für Angriffe aus dem Cyberspace durch entsprechende Konfiguration der Hard- und Software sowie die Abhängigkeit von ausländischen Lieferanten. Beide Risiken sind eine direkte Folge global arbeitsteiliger Wirtschaftsprozesse. Diese führen allerdings im Ergebnis dazu, dass heute kaum noch jemand weiß, welche Bauteile auf welcher Stufe der jeweiligen Wertschöpfungskette eingebaut werden und ob diese Bauteile wirklich nur jene Funktionen ausführen, die vorgesehen sind.[31]

Die USA haben darauf mit einer nicht nur auf Aspekte der Cybersicherheit ausgerichteten nationalen Strategie zur Sicherheit globaler Wertschöpfungsketten reagiert.[32] Damit verbunden sind auch erste gesetzgeberische Vorstöße zum Aufbau eines Risikomanagementsystems für öffentliche Beschaffungen, um Risiken in der IKT-bezogenen Wertschöpfungskette zu erkennen und diesbezügliche Informationen mit der Privatwirtschaft auszutauschen.[33] Mit vergleichbarer Absicht wurden in Deutschland die Kompetenzen des Bundesamts für Sicherheit in der Informationstechnik (BSI) erweitert.[34] Die britische Regierung erwartet entsprechende Sicherheitsvorkehrungen insbesondere von den Lieferanten im besonders sensiblen Bereich der Rüstungsgüter.[35]

Die Abhängigkeit von ausländischen Lieferanten strategisch bedeutender IKT-Komponenten verstärkt Risiken, die aus einer unsicheren Wertschöpfungskette resultieren. Ob und in welcher Form dieses Problem bearbeitet wird, ist auch eine Frage der Industriepolitik, und damit letztlich der Mittel, die Staat und Wirtschaft hierfür einsetzen können. Die 14 Thesen des Bundesinnenministeriums zur deutschen Netzpolitik sprechen diesen Punkt direkt an und rufen zur Wahrung der „technologischen Souveränität“ auf. Ohne diese, so das Thesenpapier, könnten „unsere Freiheiten und unsere Verfassungsidentität“ gefähr-

---

31 Siehe zu den grundsätzlichen Herausforderungen anstelle vieler: Cyber Threats to National Security. Countering Challenges to the Global Supply Chain (Washington, DC: CACI, 2010).

32 National Strategy for Global Supply Chain Security (Washington, DC: The White House, 2012).

33 SEC. 601 S. 2105 Cyber Security Act of 2012 vom 14. Februar 2012, <http://thomas.loc.gov/cgi-bin/query/z?c112:s2105:>. Der von Senator Joseph Lieberman und anderen Abgeordneten vorgebrachte Vorstoß wurde kontrovers aufgenommen, weil er umfangreiche neue Maßnahmen einführt und im Urteil verschiedener Kommentatoren auch die Rolle des Department of Homeland Security deutlich stärkt. Gleichwohl ist der Vorschlag für die vorliegende Ausarbeitung relevant, weil darin zahlreiche, hier thematisierte Fragestellungen aufgegriffen werden. Anfang März 2012 hat eine andere Gruppe von Abgeordneten um John McCain einen abgeschwächten Gegenvorschlag eingebracht. Siehe: Strengthening and Enhancing Cybersecurity by Using Research, Education, Information and Technology Act of 2012 (SECURE IT) vom 1. März 2012, <http://commerce.senate.gov/public/?a=Files.Serve&File_id=e1244f6d-24ac-44b0-872e-61e1ce6509e6> (Zugriff: 7. März 2012).

34 § 4 Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 14. August 2009, <http://www.gesetze-im-internet.de/bundesrecht/bsig_2009/gesamt.pdf> (Zugriff: 6. März 2012).

35 The UK Cyber Security Strategy, S. 33.

det werden.[36] Daraus resultieren entsprechende Maßnahmen, die unter dem Stichwort „Wirtschaftsförderung“ gleich im Anschluss illustriert werden.

- **Organisation**

  Hierbei geht es um die Frage, wie öffentliche und privatwirtschaftliche Institutionen aufbau- und ablauforganisatorisch zu strukturieren sind, um mögliche Cybersicherheitsrisiken abzuwehren und zu bewältigen. Ein Beispiel hierfür sind die jüngst veröffentlichten ICT Continuity-Empfehlungen, die der Verband Schweizerischer Elektrizitätsunternehmen auf Initiative des Bundesamts für wirtschaftliche Landesversorgung in Zusammenarbeit mit der Branche erarbeitet hat. Sie sehen technische und physische Organisationsmaßnahmen in verschiedenen Bereichen, wie z.B. der Netzführung oder bei Rechenzentren, vor.[37] Vergleichbar tiefgreifende regulatorische Organisationsvorgaben im Umgang mit IKT durch staatliche Behörden gibt es im Energiebereich beispielsweise auch für den Betrieb von Kernanlagen.[38]

- **Inhalte (Content)**

  Regulatorische Maßnahmen können sich auf die Inhalte der elektronischen Daten- und Kommunikationsübertragung erstrecken. Anliegen des Verbraucher- und Urheberrechtsschutzes stehen dabei oft im Vordergrund. In Abschnitt 4 (→ Verbraucherschutz) wurde dargestellt, dass die für den Telekommunikationssektor zuständigen Regulatoren in Finnland und in den Niederlanden teilweise mit entsprechenden Aufgaben betraut sind. Diese Aufgabenzuweisung deckt sich mit Teilen der Literatur, die Content-Regulierung als geeignetes Mittel zur Bekämpfung der Cyberkriminalität betrachtet.[39] Allerdings ist nicht jede Maßnahme der Content-Regulierung geeignet, die schutzwürdigen Interessen zu wahren. So entschied der Europäische Gerichtshof kürzlich, dass eine Verpflichtung der Internetanbieter zur Überwachung des Datenverkehrs unvereinbar sei mit der europäischen Richtlinie über den elektronischen Geschäftsverkehr sowie der EU-Grundrechtscharta.[40]

- **Umwelteinflüsse**

  Einflüsse der natürlichen Umwelt können in Form von Hochwasser, Lawinen und anderen Ereignissen die Funktionsfähigkeit relevanter IKT-Komponenten sowie anderer Versor-

---

36 Lothar de Maizière, 14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft (Berlin: Bundesministerium des Innern, 2010), S. 4.

37 ICT Continuity. Handlungsempfehlungen zur Sicherstellung der Versorgung (Aarau: Verband Schweizerischer Elektrizitätsunternehmen, 2011).

38 Siehe beispielsweise: HSK-R-46/d Anforderungen für die Anwendung von sicherheitsrelevanter rechnerbasierter Leittechnik in Kernkraftwerken (Villigen: Hauptabteilung für die Sicherheit der Kernanlagen, 2005).

39 Trends in Telecommunication Reform 2010/11. Enabling Tomorrow’s Digital World (Geneva: International Telecommunication Union, 2011), S. 217.

40 Urteil des Europäischen Gerichtshofs vom 24. November 2011, Rechtssache C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM).

gungsinfrastrukturen beeinträchtigen. Damit stellen sie auch eine Gefahr für die Cybersicherheit dar. In dem Maße, wie nationale Telekommunikationsgesetze die Betreiber dieser Infrastrukturen verpflichten, die Sicherheit ihrer Netze zu gewährleisten, kann diese Risikokategorie berücksichtigt werden.[41] Einen hinsichtlich Regulierungsumfang und -tiefe deutlichen Schritt weiter geht Finnland. Die Ausführungsbestimmungen des Regulators FICORA sehen umfangreiche Schutzmaßnahmen zur Abwehr verschiedener, auch naturbedingter Umweltrisiken vor. Dabei werden Schutzmaßnahmen für die Bereiche Stromversorgung, Zugangskontrolle, Gebäudestruktur und Alarmierung auf die Kritikalität verschiedener Komponenten der Telekommunikationsinfrastruktur abgestimmt.[42]

Neben der risikoorientierten gibt es auch die chancenorientierte Regulierung. Diese zielt auf positive Nutzeneffekte und die Stimulierung von Anreizen (Abschnitt 8) ab. Zwei Ansatzpunkte lassen sich unterscheiden:

- **Kapazitätsaufbau (Capacity Building)**

  Individuelle Fähigkeiten eines jeden Nutzers sowie der gezielte Aufbau und die Bewirtschaftung von Fachexpertise sind wichtige Erfolgsfaktoren der Cybersicherheit. Vielerorts wird allerdings im Bereich der Cyberfachkräfte ein Mangel beklagt. In den USA wurden daher von mehreren Abgeordneten Gesetzesvorschläge mit dem Ziel eingebracht, staatlich geförderte Programme zur Aus- und Weiterbildung von Cybersicherheitsexperten aufzubauen bzw. weiterhin zu fördern.[43] In die gleiche Richtung zielen auch Vorschläge zur Durchführung nationaler Wettbewerbe, mit deren Hilfe spezifische Fähigkeiten (z.B. Ethical Hacking, Cyberforensik, offensive und defensive Operationen) gefördert werden sollen, sowie Vorstöße zur Definition von Ausbildungsstrategien für die Mitarbeitenden des öffentlichen Dienstes.[44]

- **Wirtschaftsförderung**

  Im Streben nach „technologischer Souveränität“ bemühen sich Regierungen darum, durch die Entwicklung von Cybersicherheitslösungen auch die Wirtschaft zu unterstützen. So spricht die britische Regierung in ihrer neuen Cybersicherheitsstrategie die Erwartung

41 So der Ansatz in der Schweiz mit Artikel 90 Verordnung über Fernmeldedienste (SR 784.101.1) vom 9. März 2007 (Stand am 1. März 2012) <http://www.admin.ch/ch/d/sr/7/784.101.1.de.pdf> und in Deutschland mit § 1 und § 5 des Gesetzes zur Sicherstellung von Postdienstleistungen und Telekommunikationsdiensten in besonderen Fällen vom 24. März 2011, <http://www.gesetze-im-internet.de/bundesrecht/ptsg_2011/gesamt.pdf> (Zugriff: 8. März 2012).

42 Regulation on Priority Rating, Redundancy, Power Supply and Physical Protection of Communications Networks and Services, FICORA 54/2008 M vom 14. Februar 2008, <http://www.ficora.fi/attachments/englantiav/5wJbOLb5P/FICORA542008.pdf> (Zugriff: 6. März 2012).

43 H.R. 76 Cybersecurity Education Enhancement Act vom 5. Januar 2011, <http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.76:>; H.R. 2096 Cybersecurity Enhancement Act of 2011 vom 6. Februar 2011, <http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.2096:> (Zugriff: 6. März 2012).

44 SEC. 403 S. 2105 Cyber Security Act of 2012.

aus, dass bis zu 25 % des Volumens der Regierungsaufträge für Cybersicherheitslösungen an Klein- und Mittelunternehmen gehen. Gleichzeitig will sie sich mit den Wirtschaftsverbänden dafür einsetzen, dass mit britischen Cybersicherheitslösungen internationale Märkte erschlossen werden können.[45] In Deutschland und in Frankreich unterstützen die Regierungen Initiativen der Wirtschaft zum Aufbau sicherer Cloud-Computing-Lösungen.[46] In Frankreich wurde hierfür ein öffentlich-privates Gemeinschaftsunternehmen gegründet. Der französische Staat investiert darüber hinaus gezielt in nationale Unternehmen, die Lösungen für die legale elektronische Daten- und Kommunikationsüberwachung entwickeln, während die deutsche Bundesregierung die Entwicklung sicherer IKT-Komponenten unterstützt (Abschnitt 9 → Forschung & Entwicklung).[47]

Leitfragen für die Diskussion in Österreich

- *Welche Aspekte der risiko- und chancenorientierten Regulierung werden bei den Vorgaben für Cybersicherheit berücksichtigt?*
- *Wo liegen diesbezüglich die Schwerpunkte, und welche Aspekte wurden eher am Rande betrachtet?*
- *Welche Überlegungen führten zu den heutigen Schwerpunkten?*
- *Gibt es bezüglich der aktuellen Schwerpunktverteilung Unterschiede zwischen den einzelnen strategischen Infrastruktursektoren sowie zwischen diesen und anderen Adressaten bestehender Vorgaben für die Cybersicherheit?*

6. Zuständigkeiten: Wer soll regulieren?

In der historischen Betrachtung hat sich der Staat die Entscheidungskompetenz zur Steuerung durch Regulierung von anderen Akteuren (z.B. Kirche, Adel) abgerungen. Zur Umsetzung dieser Entscheidungskompetenz hat er nach und nach eigene Verwaltungsapparate aufgebaut. Im Ergebnis schuf sich der Staat durch die Kombination dieser beiden Entwicklungen eine eigene Legitimationsquelle.[48] Im Zeitalter der Globalisierung ist Regulierung im Sinne von Verhaltenssteuerung allerdings nicht mehr ausschließliche Kompetenz des Staates. Seine eigenen Entscheidungen und arbeitsteilige Wirtschaftsprozesse haben dazu bei-

45 The UK Cyber Security Strategy, S. 33.

46 Jürgen Berke, „Innenminister Friedrich will Bundes-Cloud aufbauen“, Wirtschaftswoche, 17. Dezember 2011, <http://www.wiwo.de/politik/deutschland/it-sicherheit-innenminister-friedrich-will-bundes-cloud-aufbauen/5965544.html> (Zugriff: 6. März 2012); Romain Gueugneau, „Le projet de ‚cloud computing’ à la française prêt à fonctionner malgré la défection de Dassault Systèmes“, Les Echos, 30. Januar 2012, S. 24.

47 „Sovereign fund has deep packets“, Intelligence Online, 29. September 2011, S. 5.

48 Marianne Beisheim, Tanja A. Börzel, Philipp Genschel und Bernhard Zangl, „Einleitung: der staatliche Beitrag zu Governance in Räumen konsolidierter und begrenzter Staatlichkeit“, in: dies. (Hrsg.), Wozu Staat? Governance in Räumen begrenzter und konsolidierter Staatlichkeit (Baden-Baden: Nomos, 2011), S. 11–34, hier S. 18–20.

getragen, dass sich der Staat diese Rolle mit anderen Akteuren teilen muss. Insbesondere im Infrastrukturbereich haben ordnungspolitische Vorstellungen der Privatisierung vormals staatlicher Aufgaben und der Liberalisierung der Märkte zu einer weitreichenden Aufsplitterung der Tätigkeiten geführt: „Consequently, infrastructures are separated from service, regulation is separated from implementation, short term transactions are separated from long term transactions and technical issues are separated from political issues".[49] Vor diesem Hintergrund kommen grundsätzlich vier Akteursgruppen als mögliche Förderer regulatorischer Maßnahmen zur Cybersicherheit in Frage:

- **Ministerien und Behörden**

  Die staatliche Regulierungszuständigkeit ist historisch begründet und nachgewiesen. Es scheint, als ob in der Folge der jüngsten Wirtschaftskrise und als Antwort auf die zunehmende Attraktivität staatlich gelenkter Volkswirtschaften in führenden Schwellenländern auch im OECD-Raum die Bereitschaft wieder zunimmt, die in den letzten Jahrzehnten in vielen Bereichen zurückgestutzte regulative Funktion des Staates wieder auszubauen. Symptomatisch dafür ist die gegenwärtige Diskussion in den USA. Gerade im „Mutterland" des weitgehend frei agierenden Unternehmertums werden die Rufe nach einer stärkeren staatlichen Rolle im Cyberkontext immer lauter. Davon zeugen die in der vorliegenden Ausarbeitung illustrativ erwähnten neuen Gesetzesverstöße. Aber auch von wissenschaftlicher Seite werden deutlicher als in der Vergangenheit Eingriffe des Staates gefordert. So stellte eine vom Center for Strategic and International Studies 2008 veröffentlichte Studie unmissverständlich fest: „It is undeniable that an appropriate level of cybersecurity cannot be achieved without regulation, as *market forces alone will never provide the level of security necessary to achieve national security objectives*".[50]

  Unabhängig von der ordnungspolitischen Präferenz für oder gegen eine robuste staatliche Regulierungsrolle ist darauf hinzuweisen, dass Regulierung in einem technologiegetriebenen Umfeld wie der Cybersicherheit auf Expertise angewiesen ist. Diese Expertise ist entscheidend, damit Regulatoren von der Wirtschaft als kompetente Partner betrachtet werden.[51] Hier könnte sich auch für den Staat eine natürliche Grenze abzeichnen: Staatliche Behörden mögen mit ihrem Sicherheitsapparat in der Lage sein, kriminelle Gruppierungen oder verdeckt operierende Nachrichtendienste aufzuklären. Ob staatliche Behörden jedoch in gleicher Weise in der Lage sind, mit dem technischen Fortschritt im Cyberkontext Schritt zu halten, diesen zu verstehen und daraus geeignete Schlussfolgerungen für ihr eigenes Handeln abzuleiten, muss gegenwärtig noch offen bleiben. Kritisch ist die-

49 Netherlands Scientific Council for Government Policy, Infrastructures. Time to Invest (Amsterdam: Amsterdam University Press, 2008), S. 36.

50 Securing Cyberspace for the 44th Presidency (Washington, DC: CSIS, 2008), S. 50. Hervorhebung nur hier.

51 Trends in Telecommunication Reform 2010/11, S. 216.

ser Punkt insofern, weil der Staat im Wettbewerb um die besten Talente mit anderen Nachfragern in Konkurrenz steht. Daher ist es mehr als naheliegend, dass in den USA bereits verschiedene Vorstöße in den Kongress eingebracht wurden, um Expertiseträger zu fördern (Abschnitt 5 → Kapazitätsaufbau).

- **Gerichte**

  Es empfiehlt sich, die regulatorische Wirkung von Gerichtsentscheidungen unabhängig von der Rolle der Ministerien und Behörden zu betrachten – vor allem auch deshalb, weil Gerichte in Auslegung und Anwendung bestehender Vorschriften den Rahmen staatlichen Handelns direkt beeinflussen können. So formulierte beispielsweise das deutsche Bundesverfassungsgericht in seinem Urteil zu Online-Durchsuchungen sehr hohe Hürden an die Zulässigkeit solcher Maßnahmen durch die staatlichen Behörden. Das Gericht hob dabei insbesondere hervor, dass die Überwachung informationstechnischer Systeme in ihrer Wirkung weit über die „telekommunikative Nutzung des (informationstechnischen) Systems" hinausgehen kann.[52] Von vergleichbarer Bedeutung ist das jüngste Urteil des Europäischen Gerichtshofs zur Überwachung des Datenverkehrs durch die Anbieter von Online-Diensten (Abschnitt 5 → Inhalte).

- **Industrie, Verbände, normierende Gremien**

  Die staatlichen Regulierungsinteressen werden ergänzt durch jene der Wirtschaft. Die regulatorischen Interessen der Wirtschaft gehen einher mit dem Streben nach attraktiven Rahmenbedingungen für unternehmerische Tätigkeiten. Sie ergeben sich aber auch aus dem eingangs angesprochenen Aspekt des Vertrauens, aus dem sich die Verantwortung der strategischen Infrastrukturbetreiber für das Funktionieren ihrer Betriebe logisch ableitet. Genauso wie es weder *den* Staat gibt, gibt es auch nicht *die* Wirtschaft. Ob und in welcher Form sich einzelne Unternehmen oder die Akteure eines strategischen Infrastruktursektors mit regulatorischen Vorstellungen und Vorschlägen zur Cybersicherheit äußern, hängt wesentlich von der direkten Betroffenheit, dem Risikoverhalten der einzelnen Unternehmen und auch von deren Organisationskultur ab.[53] Technische Early Adopter werden sich tendenziell mit anderen cybersicherheitsrelevanten Fragestellungen beschäftigen müssen als Unternehmen, die einige Jahre warten, bis entsprechende Anwendungen einen bestimmten Reifegrad aufweisen, um diese einzusetzen.

---

52 BVerfG, 1 BvR 370/07 vom 27. Februar 2008, <http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html> (Zugriff: 6. März 2012).

53 Unabhängig davon ist auf den allgemeinen Aspekt vertragsrechtlicher Beziehungen zwischen Unternehmen und ihren Kunden hinzuweisen. Durch konkrete vertragliche Vereinbarungen und allgemeine Geschäftsbestimmungen können Aspekte der Cybersicherheit ebenfalls geregelt werden.

- **Bürger**

  Wenn an dieser Stelle auf den Bürger als Akteur im Bereich der cyberrelevanten Regulierung hingewiesen wird, dann erfolgt dies aus zwei Überlegungen. Beide sind direkt mit den Interaktionsmöglichkeiten verbunden, die sich aus der Nutzung des Cyberspace ergeben. Die mit der weltweiten Verwaltung von Web-Adressen betraute Internet Corporation for Assigned Names and Numbers (ICANN) führt seit dem Jahre 2000 Internetwahlen zur Nominierung und Ernennung ihrer Verantwortungsträger durch. Sie zeigt damit, dass es auf globaler Ebene alternative Selektionsmechanismen zum klassischen Verfahren der politischen Wahl gibt.[54] Dieses Vorgehen könnte dereinst auch genutzt werden, um Entscheidungen über wünschenswerte oder ungewollte Regulierungen zur Cybersicherheit herbeizuführen. Dass dies keine Utopie ist, zeigt als zweite Überlegung die aktuelle Bürgerprotestbewegung gegen das Urheberrechtsabkommen ACTA, die sich auch weltweit online organisiert.[55] Dieses Beispiel illustriert das Mobilisierungspotenzial, das gegen staatliche Vorkehrungen im Internet aktiviert werden kann, und unterstreicht gleichzeitig, welche Sorgfalt künftig in diesem Bereich nötig sein wird.

Leitfragen für die Diskussion in Österreich

- *Gibt es ein Verständnis darüber, welcher Akteur für welche Form möglicher Regulierungsmaßnahmen am besten geeignet ist?*
- *Wie erarbeiten und erhalten die für die regulatorischen Vorgaben zuständigen Stellen die für Cybersicherheit benötigte Expertise?*
- *Besteht zu ausgewählten Aspekten der Regulierung der Cybersicherheit ein Bedarf an unabhängiger Expertise und wer könnte diese erbringen?*
- *Bedarf es neuer Verfahren, um die Interessen der von regulatorischen Maßnahmen betroffenen Adressaten frühzeitig in den Regulierungsprozess einzubinden?*

7. Adressaten: Wer soll reguliert werden?

Da IKT heute beinahe in jeder Lebenslage eingesetzt wird, erstreckt sich der Kreis der potenziellen Adressaten möglicher Vorgaben zur Cybersicherheit ins Uferlose. Mit Blick auf das Risikopotenzial, das von der Schwächung bestimmter Akteure durch Cyberrisiken für die nationale Sicherheitsvorsorge ausgeht, erscheint es sinnvoll, zwischen folgenden Kategorien zu unterscheiden:

54 Hans Klein, „The feasibility of global democracy: understanding ICANN's at-large election", Info, 3:4 (August 2001), S. 333–345.

55 <http://wiki.stoppacta-protest.info/Main_Page> (Zugriff: 6. März 2012).

- **Produzenten von Hard- und Softwareprodukten sowie relevanter Komponenten**
  Sie bilden das eigentliche Rückgrat der digitalen Wirtschaft. Fehler, Funktionsstörungen oder gezielt eingebaute Schwächen, die auf dieser Ebene entstehen, beeinflussen die Sicherheit aller anderen Akteure, die mit ihren Leistungen auf diesen Bausteinen aufsetzen. Umso überraschender ist es, dass die regulativen Anreize für diese Akteursgruppe nach wie vor zu schwach sind, um Sicherheit ebenso wie Komfort oder Benutzerfreundlichkeit zu einem integralen Bestandteil der jeweiligen Produkte zu machen (Abschnitt 4 → Marktversagen). Welchen Beitrag die zunehmende Diskussion über die notwendige Sicherheit der globalen Cyberwertschöpfungsketten (Abschnitt 5 → Technik) zur Überwindung dieses Problems leisten kann, bleibt abzuwarten.

- **Eigentümer und Betreiber strategischer Informations- und Kommunikationsinfrastrukturen**
  Für diese gilt im Kern das oben Gesagte. Allerdings ist in vielen OECD-Ländern ersichtlich, dass sich strategisch bedeutende Informations- und Kommunikationsinfrastrukturbetreiber ihrer Bedeutung bewusst werden und – teils durch staatliche Maßnahmen, teils aus eigenem Antrieb – ihre Sicherheitsanstrengungen verbessern. Mehr dazu in Abschnitt 8 (→ Vorgaben).
  Das Vordringen der IKT in andere strategische Infrastruktursektoren hat allerdings zur Folge, dass es künftig schwieriger wird, „lupenreine" Betreiber der Informations- und Kommunikationsinfrastruktur von anderen Infrastrukturbetreibern zu unterscheiden. Das bleibt wiederum nicht ohne Folgen für die Frage, in wessen regulatorische Zuständigkeit der Umgang mit diesem Trend fällt (Abschnitt 8 → Modelle der Regulierung). Es ist daher zweifelsohne richtig, wenn mit Blick auf die Befähigung der staatlichen Behörden gefordert wird, dass die Fähigkeiten von Vollzugs- und Aufsichtsbehörden zum Umgang mit Cyberrisiken gestärkt werden müssen.[56]

- **Eigentümer und Betreiber anderer strategischer Infrastrukturen**
  Oftmals wurden (staatliche) Regelungen zur Sicherheit des Betriebs strategischer Infrastrukturen und daseinsrelevanter Dienste erlassen, bevor die jeweiligen Betriebe als strategisch bedeutende Infrastrukturen identifiziert wurden. Somit stellt sich die grundsätzliche Frage nach dem Mehrwert dieser Kategorisierung im Hinblick auf die damit verbundenen Konsequenzen für den Betreiber. Gleich verhält es sich auch mit der Frage, inwieweit die Forderung nach Cybersicherheit aus Sicht der betrieblichen Schutzmaßnahmen

56 Martin Schallbruch, IT-Beauftragter des Bundesministeriums des Innern, bei der Veranstaltung „Cyber-Security: Freiwillige Selbstverpflichtung versus staatliche Regulierung" des Bundesministeriums für Inneres und des Kuratoriums Sicheres Österreich am 27. Februar 2012 in Wien.

über das Anforderungsniveau hinausgeht, das beispielsweise ein Energienetzbetreiber gewährleisten muss, der heute schon IKT einsetzt.

Länderspezifische Unterschiede im Umgang mit dieser konzeptionellen und methodischen Herausforderung zeichnen sich ab. Spezifische Cyberrisiken für das Stromnetz sind beispielsweise in den USA Gegenstand eines Gesetzesvorschlags, der die Eignung bisheriger Standards überprüfen will, die die Zuverlässigkeit der Energienetze gewährleisten.[57] Dem Vernehmen nach sollen sich weitere Vorstöße in Vorbereitung befinden, die sogar eine Eingriffsmöglichkeit des US-Energieministeriums im Falle einer Cyberattacke gegen das US-Stromnetz vorsehen.[58] Ein anderer Gesetzesvorschlag fordert, dass eine ressortübergreifend zusammengesetzte Arbeitsgruppe Anforderungen an die Cybersicherheit verschiedener strategischer Infrastruktursektoren erarbeiten soll.[59] In gleicher Absicht werden auch in Deutschland der Umsetzungsstand der IT-Sicherheit in den strategischen Infrastruktursektoren überprüft und gegebenenfalls erforderliche Maßnahmen ergriffen.[60] Zudem werden unter Federführung des BSI und mit Beteiligung der Bundesnetzagentur Schutzprofile für Kommunikationseinheiten von Smart-Meter-Messsystemen erarbeitet.[61] In Frankreich evaluiert und zertifiziert die Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) die Sicherheit der Informationssysteme, die auch von Betreibern strategischer Infrastrukturen eingesetzt werden.[62]

- **Allgemeine Wirtschaft**

  Jenseits der Vorgaben für strategische Infrastruktursektoren gibt es auch Cybersicherheitsbestimmungen für die allgemeine Wirtschaft. Die Niederlande und Deutschland kennen beispielsweise gesetzliche Vorgaben zum unternehmerischen Risikomanagement, die mit der Einführung entsprechender Instrumente zur Erkennung und Bewertung von Risiken verbunden sind.[63] Damit sollen Unternehmen auch Cyberrisiken erfassen. Zusätzlich veröffentlichen Behörden Handbücher und Richtlinien zum Informationsschutz, wie

---

57 S. 1342 Grid Cyber Security Act of 2011 vom 11. Juli 2011, <http://thomas.loc.gov/cgi-bin/query/z?c112:S.1342:< (Zugriff: 6. März 2011).

58 Cyber Legislation (Stand: 10 November 2011), zusammengestellt vom Center for Strategic and International Studies, <http://csis.org/blog/cyber-legislation> (Zugriff: 6. März 2012).

59 H.R. 174 Homeland Security Cyber and Physical Infrastructure Protection Act vom 5. Januar 2011, <http://thomas.loc.gov/cgi-bin/bdquery/z?d112:h.r.174:> (Zugriff: 6. März 2011).

60 <http://www.bcm-news.de/2011/10/19/cyber-sicherheitsrat-beschliesst-die-ueberpruefung-der-kritis-betreiber/> (Zugriff: 6. März 2012).

61 <https://www.bsi.bund.de/DE/Themen/SmartMeter/smartmeter_node.html>; Iris Henseler-Unger, „Smarte Infrastrukturen – dereguliert und sicher?", Präsentation für das XII. Zukunftsforum Öffentliche Sicherheit, Berlin, 7. April 2011, S. 23.

62 Article R2311-6-1 Code de la défense vom 24. Juni 2010.

63 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich vom 27. April 1998, Bundesgesetzblatt Nr. 24 vom 30. April 1998, S. 786–794. In den Niederlanden börsennotierte Unternehmen müssen seit dem 1. Januar 2009 darlegen, wie sie die Bestimmungen des nationalen Corporate-Governance-Kodex umsetzen. Siehe: Dutch Corporate Governance Code (The Hague: Dutch Corporate Governance Code Monitoring Committee, 2008).

beispielsweise die Reihe „IT-Grundschutz“ des BSI in Deutschland sowie das Österreichische Informationssicherheitshandbuch des Bundeskanzleramts.[64] In Großbritannien haben das Cabinet Office, das Wirtschafts- und das Innenministerium sowie das Centre for the Protection of National Infrastructure (CPNI) in Zusammenarbeit mit Partnern der Wirtschaft und der Strafverfolgung eine Online-Plattform mit kostenlosen Ratschlägen eingerichtet, die dem gleichen Ziel dient.[65]

- **Behörden**

  Staatliche Behörden sind ebenfalls Teil der nationalen strategischen Infrastruktur. Sie können durch die Umsetzung spezifischer Bestimmungen zur Cybersicherheit eine Vorbildfunktion auch für die Wirtschaft übernehmen. Erwähnenswert ist in diesem Zusammenhang eine neue Bestimmung des deutschen Grundgesetzes, wonach Bund und Länder „die für die Kommunikation zwischen ihren informationstechnischen Systemen notwendigen Standards und Sicherheitsanforderungen festlegen“ können.[66] Eine ähnliche Stoßrichtung verfolgt in den USA ein Gesetzesvorschlag zur Definition der Anforderung an die Cybersicherheit von Informationssystemen der Regierung.[67] Vergleichbare Sicherheitsvorschriften für die Informationssysteme der öffentlichen Hand gibt es auch in Estland und in Spanien. In Spanien sieht der regulatorische Rahmen zusätzlich vor, dass von einer staatlichen Behörde Best-Practice-Beispiele für die Informationssicherheit im öffentlichen Bereich gesammelt und weitergegeben werden.[68] Darüber hinaus kann die öffentliche Hand umfassend definierte Sicherheitsaspekte auch im Rahmen ihrer IKT-Beschaffungsverfahren berücksichtigen, wie das vor dem Hintergrund der angesprochenen Ergänzung des Grundgesetzes in Deutschland verstärkt der Fall ist.

- **Bürger**

  Die Aufklärung des Bürgers über die Gefahren im Cyberspace ist Teil des staatlichen Informationsauftrags. Die mit dieser Aufgabe betrauten Behörden haben dazu in der Regel elektronische Angebote entwickelt, wie z.B. die allgemeine Gefahrenbeschreibung und die halbjährlichen Lageberichte der Melde- und Analysestelle Informationssicherung (MELANI) in der Schweiz.[69] Ein analoges Informationsangebot stellt der Verein „Deutschland

---

64 <https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html>; <https://www.sicherheitshandbuch.gv.at/> (Zugriff: 6. März 2012).

65 <http://www.getsafeonline.org/nqcontent.cfm?a_id=1> (Zugriff: 6. März 2012).

66 Artikel 91 c Grundgesetz vom 23. Mai 1949, zuletzt geändert am 27. Juli 2010, <http://www.gesetze-im-internet.de/bundesrecht/gg/gesamt.pdf> (Zugriff: 8. März 2012).

67 H.R. 174 Homeland Security Cyber and Physical Infrastructure Protection Act.

68 Estonia Country Report (Heraklion: ENISA, 201), S. 8; Spain Country Report (Heraklion: ENISA, 2011), S. 18, 29.

69 <http://www.melani.admin.ch/org/00100/index.html?lang=de> (Zugriff: 6. März 2012).

sicher im Netz e.V." zur Verfügung.[70] Spezielle Informationsangebote für das Cyberverhalten von Kindern gibt es in Deutschland mit der Initiative internauten.de und einem – inzwischen vergriffenen – Medienkoffer für Unterrichtszwecke.[71] Vergleichbare Initiativen zur Bewusstseinsbildung und -förderung unterstützt die Europäische Kommission seit 2004 mit dem Programm „Safer Internet".[72] In den USA sieht ein Gesetzesvorstoß vor, dass Musterlehrpläne zur Vermittlung von Lerninhalten rund um Cybernutzung und Cybersicherheit vom Kindergarten bis zur Stufe K-12 (16- bis 19-Jährige) erarbeitet werden.[73]

Leitfragen für die Diskussion in Österreich

- *Nach welchen Adressatenkreisen differenzieren die bestehenden Bestimmungen zur Cybersicherheit in Österreich?*
- *Welche Gründe sprechen für oder gegen die Einführung zusätzlicher Differenzierungen nach den oben genannten Beispielen?*
- *Inwieweit gibt es in Österreich eine Übersicht der spezifischen Cybersicherheitsbedürfnisse verschiedener Nutzer/Adressaten?*
- *Soweit sinnvoll und wünschenswert, wer könnte/sollte eine solche Übersicht erstellen?*

8. Regime: Wie soll reguliert werden?

Mögliche nationale bzw. internationale Regimes für die Cybersicherheit beantworten die konkrete Frage nach den inhaltlichen Vorgaben und wie diese definiert, umgesetzt sowie in ihrer Einhaltung überprüft werden. Gestützt auf die bisherigen Ausführungen sind dabei folgende Aspekte zu unterscheiden:

- **Modelle der Regulierung**

  Modelle der Regulierung beschreiben die Art und Weise, wie die unterschiedlichen Akteure, die gemeinsam für Cybersicherheit sorgen müssen, an der Erarbeitung der jeweiligen Vorgaben beteiligt werden. Idealtypisch kann zwischen der staatlichen Regulierung und der privatwirtschaftlichen Selbstverpflichtung unterschieden werden. In der Praxis haben sich die meisten Staaten für Mischansätze entschieden, wobei der Grad der Beteiligung der privatwirtschaftlichen Akteure oftmals durch die politische Kultur des jeweiligen Landes bestimmt wird.

  Ein umfassendes Beispiel einer aktiven staatlichen Rolle innerhalb eines partnerschaftlichen Rahmens findet sich in Finnland. Dort leiten sich die regulatorischen Vorgaben für

70 <https://www.sicher-im-netz.de/> (Zugriff: 6. März 2012).
71 <http://www.internauten.de/Seiten/Startseite.aspx> (Zugriff: 6. März 2012).
72 <http://www.saferinternet.org> (Zugriff: 8. März 2012).
73 SEC. 407 (c)(2) S. 2105 Cybersecurity Act of 2012.

die Sicherheit der Betreiber von Telekommunikationsinfrastrukturen aus der Strategie der nationalen Sicherheitsvorsorge ab und werden vom Regulator FICORA in detaillierten Ausführungsbestimmungen präzisiert. Ergänzt werden diese Vorgaben durch aktive Unterstützungsleistungen des Staates zur Förderung der unternehmerischen Sicherheit (Abschnitt 4 → Versorgungssicherheit) sowie durch die regelmäßige Überprüfung der Sicherheitsvorkehrungen der Unternehmen (Abschnitt 8 → Monitoring).

Im Vergleich dazu ist die staatliche Rolle in den partnerschaftlich angelegten Ansätzen Deutschlands, Großbritanniens, der Niederlande, der Schweiz und der USA weniger stark ausgeprägt. Die Ansätze dieser Länder räumen den Unternehmen – je nach Sektor – unterschiedlich große Spielräume ein, wenn es um den Schutz strategischer (Informations-)Infrastrukturen geht. In allen Ländern steht im Hintergrund aber die „staatliche Peitsche der gesetzlichen Regulierung", deren Einsatz in niederländischen und deutschen Grundlagendokumenten auch explizit angesprochen wird.[74] Auffällig ist, dass sich in den partnerschaftlichen Modellen Deutschlands, Großbritanniens, der Schweiz und der USA das Momentum zugunsten des Staates zu verlagern scheint, was an den bereits zitieren Forderungen nach anspruchsvolleren Standards für Cybersicherheit zum Ausdruck kommt.

Ein sehr wichtiger Aspekt des Regulierungsmodells betrifft die (Selbst-)Organisation der staatlichen und privatwirtschaftlichen Akteure. Im staatlichen Bereich fällt Cybersicherheit in die Zuständigkeit unterschiedlicher Ressorts. Das zieht einen entsprechenden Abstimmungsbedarf nach sich, der von der Risikoanalyse über die Strategieentwicklung und -umsetzung bis zur Mittelzuteilung reicht. Regulatorische Fragen sind davon insoweit betroffen, als staatliche Vorgaben für die strategischen Infrastruktursektoren bislang in einem vertikalen, d.h. sektorspezifischen Ansatz von den relevanten Ministerien und Behörden definiert wurden. Aber bei wem liegt beispielsweise die Zuständigkeit, wenn aus dem Mobiltelefon ein „tragbarer Geldautomat" wird oder wenn darüber die Energieversorgung des Eigenheims gesteuert wird? Cybersicherheit als Querschnittsthema erfordert eher ein horizontales bzw. vernetztes Vorgehen.

Damit ist der Dialog zwischen den staatlichen Stellen mit regulatorischer Funktion angesprochen. In den USA wird in einem aktuellen Gesetzesvorschlag beispielsweise angeregt, dass sich das Department of Homeland Security in Fragen der Cybersicherheit mit allen sektorrelevanten Ministerien abstimmen soll und diese gleichzeitig das Department darüber informieren, wenn sie für die Cybersicherheit relevante regulatorische Bestimmungen einführen wollen.[75] Ist der Telekommunikationsregulator auch für andere Infrastruktursektoren zuständig, befindet sich dieser in einer guten Ausgangslage, um in ver-

74 The National Cyber Security Strategy, S. 4; Cyber-Sicherheitsstrategie für Deutschland (Berlin: Bundesministerium des Innern, 2011), S. 12; Nationale Strategie zum Schutz Kritischer Infrastrukturen (Berlin: Bundesministerium des Innern, 2009), S. 13.

75 SEC. 106 S. 2105 Cybersecurity Act of 2012.

schiedene Märkte wirken zu können.[76] Das illustriert auch die frühe Einbindung der Bundesnetzagentur in die Erarbeitung von Sicherheitsstandards für intelligente Stromnetze in Deutschland.

Die Vorstellungen für den Informationsaustausch zwischen Behörden und Privatwirtschaft aus dem Umsetzungsplan KRITIS der deutschen Bundesregierung hat die deutsche Versicherungswirtschaft wie folgt realisiert:

- Mit der LKRZV GmbH hat die deutsche Versicherungswirtschaft zum 1. Januar 2010 ein eigenständiges Unternehmen als IT-Krisenreaktionszentrum der Branche gegründet.
- Das Unternehmen wird von den Mitgliedern des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) gemeinschaftlich finanziert.
- Das LKRZV fungiert als Informationsdrehscheibe zwischen den Mitgliedern des Verbands sowie dem Bundesamt für Sicherheit in der Informationstechnik und gibt entsprechende Informationen in anonymisierter Form weiter.
- Die Mitarbeitenden des Unternehmens wurden sicherheitsüberprüft, sodass sie auch sensitive Informationen bearbeiten können.
- Darüber hinaus betreibt der Gesamtverband ein eigenes GDV-Branchennetz, das vom BSI zertifiziert wird. Gemeinsam mit der Deutschen Versicherungsakademie und der FH Köln hat das LKRZV zudem einen Ausbildungsgang zum Chief Information Security Officer (CISO) erarbeitet.

Quellen: Ausführungen von Martin Schallbruch, IT-Beauftragter des Bundesministeriums des Innern, im Rahmen des sicherheitspolitischen Frühstücks des Bundesministeriums für Inneres, Wien, 28. Februar 2011; Jürgen Berke, „Verschlungene Wege", Wirtschaftswoche, 28. März 2011, S. 29; Fred di Giuseppe Chiachiarella, „IT-Sicherheitsstrategie der deutschen Versicherungswirtschaft", Präsentation für das Zukunftsforum Öffentliche Sicherheit, Berlin, 19. Juni 2008.

Box 2: Ansätze zur Cybersicherheit in der deutschen Versicherungswirtschaft

Gleiche Fragen der Koordination stellen sich auch im privatwirtschaftlichen Umfeld. Aufschlussreich ist in diesem Zusammenhang der Ansatz, der von der deutschen Versicherungswirtschaft gewählt wurde (Box 2). Neben sektorspezifischen Ansätzen besteht auch Bedarf an institutionellen Lösungen für die übergreifende öffentlich-private Koordination. In Deutschland, Estland und den Niederlanden wurde hierfür auf der strategischen Ebene ein Nationaler Cybersicherheitsrat eingerichtet, dem Vertreter des öffentlichen und privatwirtschaftlichen Sektors ebenso angehören wie Experten der Wissenschaft.[77] Zudem bestehen verschiedene Formen des Zusammenwirkens beim Informationsaustausch (Abschnitt 9).

- **Vorgaben**

  Vorgaben für die Cybersicherheit können in Form von Gesetzen, Verordnungen, Normen, Standards oder freiwilligen Selbstverpflichtungen wie Branchenempfehlungen formuliert werden. Neben dem rechtlichen Charakter gibt es auch inhaltliche Unterschiede, je nach-

76 Trends in Telecommunication Reform 2010/11, S. 216.

77 Cyber-Sicherheitsstrategie für Deutschland, S. 9; Estonia Country Report, S. 5; The National Cyber Security Strategy, S. 5.

dem, ob die Vorgaben technischer Natur sind oder auf Aspekte des Verhaltens bzw. der Organisation ausgerichtet sind:

- **Organisationsbezogene Vorgaben:** Aufgrund der internationalen Verflechtung der Unternehmen des Telekommunikationssektors besteht das Risiko der Abhängigkeit, beispielsweise wenn operativ wichtige Einheiten wie Netzbetriebszentren physisch im Ausland liegen. Die Schweiz hat darauf mit einer rechtlichen Vorschrift reagiert und fordert die Telekommunikationsbetreiber auf, die notwendige Infrastruktur im Inland unabhängig zu betreiben.[78] Einen ähnlichen Schritt vollzieht gegenwärtig auch Estland. Dort soll die Überarbeitung der nationalen Notstandsrichtlinien offenbar vorsehen, dass IT-Systeme in strategisch relevanten Infrastruktursektoren national betrieben werden müssen.[79] Wie das Risiko der Abhängigkeit von ausländischen Betreibern mit dem Vormarsch des Cloud Computing künftig bewertet wird, bleibt abzuwarten. Es zeichnen sich allerdings bereits mögliche Konflikte ab, wenn unterschiedliche Rechtsvorschriften, beispielsweise zum Datenschutz, die auch Aspekte der physischen Lagerung der Daten beinhalten können, in der Datenwolke miteinander „kollidieren".[80]
- **Verhaltensvorgaben:** An der Schnittstelle zwischen Sicherheitsvorsorge und Krisenmanagement sowie Cybersicherheit und dem Schutz strategischer Infrastrukturen gibt es in der Schweiz und in Schweden entsprechende Verhaltensnormen. In der Schweiz haben die vier großen Telekommunikationsunternehmen mit dem Crisis Reaction Team Telecommunication (CRTT) einen Koordinationsmechanismus geschaffen, um sich in der Krise gegenseitig zu unterstützen. Das CRTT steht als Arbeitsgruppe unter dem Dach des Branchenverbands asut.[81] Die darin vertretenen Experten sind in Personalunion auch Mitglieder der Fachgruppe ICT-I Sektion Telekommunikation des Bundesamts für wirtschaftliche Landesversorgung. Das Pendant dazu in Schweden ist die National Telecommunications Coordination Group (NTSG), die vom Post- und Telekommunikationsregulator PTS geführt wird. Dieser Gruppe gehören Telekommunikationsbetreiber und verschiedene staatliche Behörden an.[82]

---

78 Artikel 90 Absatz 2 Verordnung über Fernmeldedienste.

79 Dem ging konkret die Absicht einer Bank voraus, ihre Serverinfrastruktur von Estland nach Finnland zu verlegen. In früheren Verhandlungen mit dem estnischen Innenministerium hatten Vertreter der Bank offenbar erklärt, diesen Schritt nicht ergreifen zu wollen. Siehe hierzu: „Estonian state will not allow to move state's IT infrastructure", The Baltic Course, 16. Januar 2012, < http://www.baltic-course.com/eng/Technology/?doc=51634> (Zugriff: 7. März 2012).

80 Tim Greens, „The U.S. Patriot Act has an impact on cloud security", Network World, 29. September 2009, <http://www.networkworld.com/newsletters/2009/092909cloudsec1.html> (Zugriff: 8. März 2012); Chris Connolly, The U.S. Safe Harbor – Fact or Fiction (Pymont: Galexia, 2008).

81 <http://www.asut.ch/content/content_renderer.php?id=633&link_type=1&lan=1&cms=0&bcid=263&s=1 > (Zugriff: 8. März 2012).

82 <http://www.pts.se/upload/Faktablad/En/facts-about-ntsg.pdf> (Zugriff: 8. März 2012).

- **Technische Vorgaben:** Bestehende technisch-industrielle Standards bilden oftmals die Grundlage für konkrete Sicherheitsvorschriften der Behörden. So stützt sich das Bundesamt für Kommunikation in der Schweiz mit seinen empfehlenden Richtlinien für Managementsysteme zur Informationssicherheit und für die Kontinuitätsplanung der Telekommunikationsanbieter auf gängige Industriestandards.[83] Der gleiche Ansatz liegt auch den Vorschriften zur Anwendung von Informations- und Kommunikationssystemen in strategischen Infrastruktursektoren zugrunde. Allerdings gelten für besonders kritische Anwendungen im Energiesektor (u.a. Smart Grid,[84] Vorschriften für Informationssysteme in der Nuklearindustrie) und im Finanzsektor oftmals spezifische Vorschriften.[85] Ob die bestehenden industriellen Standards den erkannten Cybersicherheitsherausforderungen genügen, wird in verschiedenen Ländern gegenwärtig untersucht. Welche Konsequenzen sich daraus ergeben und wie Regierungen und Unternehmen mit möglichen Kostenfolgen umgehen, die aus verschärften Standards resultieren könnten, bleibt abzuwarten.

- **Anreize und Sanktionen**

  Anreize und Sanktionen spielen eine wichtige Rolle, um ein bestimmtes Verhalten auszulösen. Um verschiedene Aspekte des Marktversagens (Abschnitt 4) zu bewältigen, wird die Anreizregulierung daher in verschiedenen Politikfeldern bereits seit Jahren genutzt. Als grundsätzliche Instrumente kommen beispielsweise steuerliche Vergünstigungen, haftungsrechtliche Erleichterungen sowie Anpassungen bei der Unternehmensbewertung im Falle des Ergreifens gewünschter Maßnahmen in Frage.

  Anreizregulierung im Hinblick auf sicherheitspolitische Ziele wird in Europa erst ansatzweise in Betracht gezogen. In den USA wurden seit 2001 gesetzliche Vorschriften anreizorientiert modifiziert, um beispielsweise die Forschung und Entwicklung von Unternehmen für sicherheitsrelevante Medikamente anzustoßen.[86] Die Idee der Anreizregulierung wird neuerdings auch auf die Cybersicherheit übertragen. Beim Hearing eines US-Kongressausschusses im Februar 2012 wurden steuerliche Vergünstigungen, Beihilfen und Darle-

---

83 Richtlinien zur Sicherheit und Verfügbarkeit von Fernmeldeinfrastrukturen und -diensten.

84 Siehe hierzu beispielsweise die technischen Richtlinien des BSI <https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html> sowie in den USA die Standards des National Institute of Standards and Technology <http://www.nist.gov/smartgrid/> (Zugriff: 8. März 2012).

85 So beispielsweise die Mindestanforderungen an das Risikomanagement der deutschen Bundesanstalt für Finanzdienstleistungsaufsicht, die konkrete Vorgaben für den Umgang mit IT-Risiken enthält. Siehe hierzu: <http://www.bafin.de/nn_722570/DE/Unternehmen/BankenFinanzdienstleister/ArbeitskreisBA/FgMaRisk/fgmarisk__node.html?__nnn=true> (Zugriff: 7. März 2012).

86 Heiko Borchert, „Engaging the Science and Technology Community in the Fight against Terrorism“, in: Andrew James (ed.), Science and Technology for the Anti-Terrorism Era (Amsterdam: IOS Press, 2006), S. 111–124); Philip E. Auerswald et. al. (eds.), Seeds of Disaster, Roots of Response. How Private Action Can Reduce Public Vulnerability (Cambridge: Cambridge University Press, 2006), S. 279–290; 379–394.

hen für Unternehmen angeregt, die nachweislich in ihre Cybersicherheit investieren.[87] Einen haftungsrechtlichen Anreiz unterbreitete Senator Lieberman mit dem Vorschlag, Unternehmen unter bestimmten Voraussetzungen von Haftungsansprüchen aus Cyberzwischenfällen zu befreien. Dafür müssten diese die in seiner Gesetzesinitiative vorgeschlagenen Sicherheitsmaßnahmen ergreifen, zertifiziert oder von einem unabhängigen Dritten geprüft werden und zum Zeitpunkt des Zwischenfalls nachweislich alle erforderlichen Cybersicherheitsanforderungen erfüllen.[88]

Positive Anreize können durch Sanktionen (negative Anreize) ergänzt werden. In Deutschland fallen mögliche Sanktionen im Telekommunikationsbereich in die Zuständigkeit der Bundesnetzagentur. Das Maßnahmenspektrum umfasst Bußen in unterschiedlicher Höhe (z.B. bis zu 100.000 € für die Durchsetzung der Verpflichtung zu Schutzmaßnahmen), die vorübergehende Einschränkung sowie die teilweise oder vollständige Untersagung des Betriebs.[89] Einen Schritt näher in Richtung Bekämpfung von Cyberrisiken reichen die Kompetenzen der Telekommunikationsregulatoren in Australien und in den Niederlanden. Die Australian Communications and Media Authority kann vor Gericht eine Anordnung gegen Personen erwirken, die unerwünschte elektronische Werbung (Spam) in Umlauf bringen. Der niederländische Regulator OPTA kann im Kampf gegen Spam und Spionagesoftware Bußen aussprechen. 2007 hat die Behörde von dieser Kompetenz Gebrauch gemacht und eine Buße in Höhe von 1 Million € gegen drei niederländische Unternehmen verhängt, die Spionagesoftware vertrieben hatten.[90]

- **Monitoring**

  Monitoring bezieht sich auf die Frage, wie überprüft wird, ob die Vorgaben zur Cybersicherheit eingehalten werden. Diese Überprüfung kann durch staatliche Stellen, durch Unternehmen selbst oder durch unabhängige Dritte erfolgen. In einigen Ländern sind strategische Infrastrukturbetreiber verpflichtet, der Regulierungsbehörde umfassende Sicherheitskonzepte vorzulegen, die auch IT-Aspekte berücksichtigen. Das ist beispielsweise in Deutschland und in Frankreich der Fall.[91] Die Umsetzung der Sicherheitskonzepte und anderer relevanter Vorgaben kann in beiden Ländern von staatlichen Behörden überprüft

---

87 Es handelt sich dabei um eine Anhörung vor dem Subcommittee on Communications and Technology des House Energy & Commerce Committee vom 8. Februar 2012. Die Aussagen der Experten sind online verfügbar: <http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=9250> (Zugriff: 7. März 2012).

88 SEC. 105 (d) S. 2105 Cyber Security Act of 2012. Allerdings stellt sich die Frage, ob es gesellschafts- und wirtschaftspolitisch akzeptabel ist, die „freiwerdende" Haftungsrolle unbesetzt zu lassen oder ob der Staat die Rolle als „ultimative Haftungsinstanz" übernehmen würde.

89 § 115 Telekommunikationsgesetz vom 22. Juni 2004, zuletzt geändert am 22. Dezember 2011, <http://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf> (Zugriff: 8. März 2012).

90 Trends in Telecommunications Reform 2010/11, S. 221.

91 § 109 Telekommunikationsgesetz; Instruction générale interministérielle relative à la sécurité des activités d'importance vitale, no. 6600/SGCN/PSE/PPS vom 26. September 2008, S. 26–31, <http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir_1338.pdf> (Zugriff: 7. März 2012).

werden.[92] Entsprechende Möglichkeiten zu staatlich durchgeführten Inspektionen bzw. Audits kennen auch Finnland und Estland.[93] Eine interessante Mischform schlägt der US-Cyber Security Act vor. Dieser kombiniert den Einsatz unabhängiger und zertifizierter Dritter zur Überprüfung von Cybersicherheitsmaßnahmen mit der Möglichkeit, dass auch das Department of Homeland Security Cybersicherheitsbewertungen vornehmen kann.[94]

Leitfragen für die Diskussion in Österreich

- *Wer koordiniert in Österreich die cyberrelevanten regulatorischen Vorgaben der staatlichen Behörden?*
- *Wie wird dabei ein kohärentes Vorgehen im Hinblick (1) auf die verfolgten Schutzziele und (2) die Vorgaben für die einzelnen Adressaten (Abschnitt 7) sichergestellt?*
- *Gibt es eine Übersicht, welche Adressaten gegenwärtig welche Vorgaben zur Cybersicherheit erfüllen müssen?*
- *Gibt es ein Verständnis darüber, inwieweit sich die bestehenden Vorgaben für Cybersicherheit überschneiden und wo möglicherweise Lücken bestehen?*
- *In welchen strategischen Infrastruktursektoren bemühen sich die Akteure um die Erarbeitung eigener Vorgaben für die Cybersicherheit?*
- *Wie werden dabei sektorübergreifende Abhängigkeiten berücksichtigt?*
- *Mit welchen Anreizen kann der Staat diese Arbeiten fördern?*

9. Rahmenordnung: Welche Begleitmaßnahmen soll es geben?

Begleitmaßnahmen, die Verbindungen zu anderen Politikfeldern ermöglichen, können die Wirkung regulatorischer Vorgaben zusätzlich verstärken. Aus dem internationalen Ländervergleich erweisen sich drei Ansatzpunkte als besonders fruchtbar: Informationsaustausch, Übungen sowie Forschung und Entwicklung.

- **Informationsaustausch**

  Der Informationsaustausch unterstützt regulatorische Vorgaben zur Cybersicherheit, ist in vieler Hinsicht aber auch unerlässliche Voraussetzung dafür. Ohne Informationsaustausch gibt es kaum Anhaltspunkte darüber, in welcher Form bestehende Vorgaben bereits umgesetzt werden. Entsprechend schwierig ist die Beurteilung, ob die Vorgaben noch der aktuellen Risikobewertung entsprechen. Der Informationsaustausch bezieht sich

92 § 115 Telekommunikationsgesetz; Instruction générale interministérielle relative à la sécurité des activités d'importance vitale, S. 35–36.

93 Section 124 Communications Market Act, 393/2003, <http://www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf> (Zugriff: 7. März 2012); Estonia Country Report, S. 15.

94 SEC. 106 (d) Cyber Security Act of 2012.

dabei nicht nur auf die Weitergabe von Erkenntnissen zwischen Behörden und der Privatwirtschaft, sondern muss gleichermaßen auch auf der behördlichen Seite und zwischen den einzelnen Unternehmen organisiert werden. Verschiedene Aspekte sind dabei zu berücksichtigen:

- **Rechtsschutz:** Informationen zur Früherkennung und Abwehr von Cyberrisiken sind sensibel. Dementsprechend wichtig sind Regelungen des Zugangs zu und Umgangs mit diesen Informationen. Viele Länder haben hierzu einen pragmatischen Ansatz auf Basis des sogenannten Ampel-Prinzips gewählt. In Großbritannien, den Niederlanden, der Schweiz und in Ungarn bestimmt derjenige, der eine Information weitergeben will, in welcher Form, wie und von wem diese verwendet werden darf. Dafür werden verschiedene Farbcodes verwendet. Deutschland hat für den Umgang mit klassifizierten Informationen ein spezielles Verfahren (Geheimschutzbetreuung der Wirtschaft) entwickelt.[95] Im US-Kongress wurde im November 2011 eine Gesetzesinitiative eingebracht, die eine Rechtsgrundlage schaffen würde, damit cyberrelevante Informationen der US-Nachrichtendienste an andere Behörden und an die Privatwirtschaft weitergegeben werden könnten.[96]

- **Informationspflicht:** Auf die Frage, ob für den cyberrelevanten Informationsaustausch eine Informationspflicht eingeführt werden soll, gibt es in der Praxis keine eindeutige Antwort. Eine solche Pflicht besteht beispielsweise in Spanien und in Finnland. In Spanien bezieht sich diese allerdings eher auf Ereignisse, die zur Störung oder zum Ausfall der Telekommunikationsinfrastrukturen führen. Sie regelt detailliert, wann den Behörden welche Information zu übermitteln ist.[97] In Finnland bezieht sich die Informationspflicht auf Verstöße gegen die Informationssicherheit, beispielsweise als Folge einer DDoS-Attacke, der Verbreitung von Schadsoftware oder versuchter Informationsabschöpfung durch Social Engineering.[98] In Deutschland wird eine solche Verpflichtung gegenwärtig als nicht umsetzbar betrachtet, doch soll es demnächst die Möglichkeit geben, entsprechende Zwischenfälle anonym online melden zu können. In der Schweiz wiederum besteht für alle Telekommunikationsbetreiber die Pflicht, das Bun-

95 <https://bmwi-sicherheitsforum.de/start/> (Zugriff: 8. März 2012).

96 H.R. 3523 Cyber Intelligence Sharing and Protection Act of 2011 vom 30. November 2011, <http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.3523:> (Zugriff: 7. März 2012).

97 Spain Country Report (Heraklion: ENISA, 2011), S. 36–37.

98 Explanatory Notes to Regulation 9 on the Obligation to Notify of Violations of Information Security in Public Telecommunications (Helsinki: FICORA, 2009), <http://www.ficora.fi/attachments/englantiav/5mCqGm7Cb/MPS09en.pdf> (Zugriff: 7. März 2012).

desamt für Kommunikation über Netzstörungen zu informieren,[99] während Meldungen zur Cybersicherheit im Rahmen von MELANI freiwillig erfolgen.

- **Struktur:** Bei der Strukturierung der Informationsaustauschbeziehungen zur Cybersicherheit ist große Sorgfalt geboten, denn oftmals gibt es in den verschiedenen strategischen Infrastruktursektoren bereits etablierte Informationsflüsse zwischen den Behörden und den Infrastrukturbetreibern. Ob und in welcher Form im Rahmen dieser bestehenden Austauschprozesse cyberrelevante Informationen weitergegeben werden, ist einzelfallabhängig.

  In vielen Ländern hat sich zum Zweck des Cyberinformationsaustauschs ein Modell etabliert, bei dem auf der staatlichen Seite ein Ansprechpartner bestimmt wurde, der die Informationen sammelt, auswertet, erforderlichenfalls anonymisiert und weiterleitet. Dieses Modell wird in Deutschland, Großbritannien, den Niederlanden, der Schweiz und in Ungarn angewendet. Nur weil allerdings eine zentrale Anlaufstelle auf der staatlichen Seite geschaffen wurde, bedeutet dies, wie Großbritannien zeigt, noch nicht, dass die etablierten sektorspezifischen Informationsstränge aufgegeben werden.

  Auch bei der Organisation dieser staatlichen Informationsdrehscheibe gibt es beachtliche Unterschiede. Das CPNI ist Teil des britischen Innenministeriums und kann daher auch auf Informationen des Inlandsnachrichtendienstes zugreifen. In Ungarn liegt diese Funktion beim CERT, das von einer eigenen Stiftung betrieben und vom Büro des Premierministers überwacht wird.[100] In der Schweiz ist MELANI organisatorisch dem Eidgenössischen Finanzdepartement zugeordnet, greift aber auch auf nachrichtendienstliche Organisationselemente im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport zu.

  Die Organisationsoptionen für Informationsdrehscheiben in der Privatwirtschaft sind ebenfalls vielfältig. In Deutschland hat die Versicherungswirtschaft hierfür ein eigenständiges Unternehmen gegründet (Box 2). Im Schweizer Bankensektor verfügt die Bankiervereinigung mit der Kommission für Sicherheit über einen zentralen Ansprechpartner, dessen inhaltliche Zuständigkeit von der Informationssicherheit über die Wirtschaftskriminalität bis zur physischen Sicherheit reicht.[101]

  Diese nationalen Initiativen werden auf internationaler Ebene ergänzt. So wurde beispielsweise 2005 auf Initiative des CPNI der European SCADA and Control Systems Information Exchange (EuroSCSIE) gegründet. Staatliche Behörden, wissenschaftliche Einrichtungen und Betreiber aus verschiedenen europäischen Ländern tauschen dar-

99 Artikel 96 Verordnung über Fernmeldedienste.

100 <http://www.cert-hungary.hu/en/node/6> (Zugriff: 7. März 2012).

101 Jahresbericht 2010/2011 (Basel: Schweizerische Bankiervereinigung, 2011), S. 23 <http://www.swissbanking.org/swissbanking_jb_d_10_11.pdf> (Zugriff: 7. März 2012).

über Erkenntnisse zur Informationssicherheit von Steuerungsanlagen aus.[102] Mit Mitgliedern aus 138 Ländern noch umfassender ist die International Multilateral Partnership Against Cyber Threats (IMPACT). IMPACT hat den Hauptsitz in Malaysia und wird von der International Telecommuncation Unit (ITU) unterstützt. Eine der Kernaufgaben ist der Betrieb des Global Response Center, das der weltweiten Frühwarnung zu Cybergefahren in Beinahe-Echtzeit dient.[103]

- **Inhalte:** Dort, wo es Vorgaben zu den Inhalten des Informationsaustauschs gibt, beziehen sich diese meist auf prozedurale Aspekte. Das trifft für die meisten Vorschläge zum cyberbezogenen Informationsaustausch zu, die in den letzten Monaten im US-Kongress eingebracht wurden. Inhaltlich etwas präziser ist der deutsche Umsetzungsplan KRITIS, der für den Informationsaustausch zu Cyberrisiken drei Aufgabenfelder benennt: anlassbezogene Kommunikation zur Krisenfrüherkennung, Kommunikation und Alarmierung sowie Krisenbewältigung und Informationsaustausch zur Krisenvermeidung.[104] In Ergänzung dieser eher ereignisorientierten Ansätze erscheinen zwei inhaltliche Zusatzaspekte bedenkenswert:

  - **Wertschöpfungskette:** Entlang der cyberrelevanten Wertschöpfungskette agiert eine unüberschaubare Zahl von Akteuren. Um deren technische Fähigkeiten bewerten und ihre möglichen strategischen Absichten beurteilen zu können, ist der Austausch zwischen Behörden und Unternehmen unerlässlich.
  - **Investitionstransparenz:** Finanzielle Anreizregulierung setzt voraus, dass Transparenz bezüglich bestehender Sicherheitsinvestitionen und -kosten besteht. Es ist zu überlegen, ob die Bestimmung zur Informationspflicht[105] des neuen Telekommunikationsgesetzes in Österreich hierfür genutzt werden könnte. Zusammen mit dem ebenfalls vorzulegenden Sicherheitskonzept könnten daraus spezifische sicherheitsrelevante Leistungskennzahlen entwickelt werden.

- **Übungen**

  Übungen sind ein geeignetes Mittel, um zu überprüfen, ob vorhandene Konzepte, Verfahren, Instrumente und Fähigkeiten geeignet sind, Ereignisse zu bewältigen. Das gilt auch für regulatorische Vorgaben, insoweit sie beispielsweise Bestimmungen zu spezifischen

---

102 Igor Nai Fovino, „The European SCADA and Control System Information Exchange“, GCSEC Newsletter, 2:2 (February 2012), S. 2–3, <http://newsletter.gcsec.org/documenti/1/List%20Documents/gcsec-newsletter-02-2012.pdf > (Zugriff: 7. März 2012).

103 <http://www.impact-alliance.org> (Zugriff: 7. März 2012).

104 Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen (Berlin: Bundesministerium des Innern, 2007), S. 30–32. Wichtige Inhalte dieses Dokuments wurden inzwischen von der Deutschen Cybersicherheitsstrategie übernommen und aktualisiert.

105 §16 a Abs. 3 Telekommunikationsgesetz.

Koordinationsmechanismen, Verfahrensabläufen oder Reaktionszeiten enthalten. Auch im Cyberumfeld gewinnen Übungen an Bedeutung. Im November 2011 musste beispielsweise der britische Bankensektor in einer Übung darlegen, wie eine Cyberattacke auf die Bargeldautomaten des Landes bewältigt würde.[106] Ebenfalls im letzten Jahr wurde in Deutschland die LÜKEX 2011 durchgeführt. Mehr als 2.500 Teilnehmer übten dabei den Angriff auf IT-Strukturen der Verwaltung und der Wirtschaft durch einen Trojaner, der alle Eigenschaften der in jüngster Zeit durchgeführten Cyberangriffe aufwies.[107] Nationale Übungen werden ergänzt durch internationale Initiativen. 2010 führte die ENISA die erste europäische Cyberübung durch, an der sich Vertreter aus 22 Mitgliedstaaten der Union beteiligten. Ein Jahr später folgte mit Cyber Atlantic 2011 die erste EU-US-Cyberübung, bei der u.a. auch Angriffe gegen die SCADA-Systeme der Energieinfrastrukturbetreiber geprobt wurden.[108]

- **Forschung und Entwicklung**

  Die Förderung von Forschung und Entwicklung (F&E) zur Bewältigung von Cyberrisiken unterstützt die Innovations-, Wirtschafts- und Sicherheitspolitik. Nicht ohne Grund engagiert sich die deutsche Bundesregierung unter dem Stichwort „technologische Souveränität“ beispielsweise an der Entwicklung eines Sicherheitsbetriebssystems und eines europäischen Internet-Routers.[109] Auch auf der europäischen Ebene wurde die Bedeutung von F&E für Cybersicherheit erkannt. Bereits der ESRIF-Schlussbericht aus dem Jahre 2009 stellte in verschiedenen Feldern der damals vorgeschlagenen künftigen Forschungs- und Innovationsagenda Bezüge zu diesem Thema her. Das künftige Rahmenprogramm für Forschung und Innovation (Horizont 2020) formuliert gestützt darauf im Handlungsfeld „Integrative, innovative und sichere Gesellschaften“ die Stärkung der Computer- und Netzsicherheit als eigenständigen Schwerpunkt und spricht dessen Bedeutung auch in den anderen fünf Handlungsfeldern an.[110]

---

106 Huw Jones, „UK banks tested with cyber attack, travel exercise“, Reuters, 22. November 2011, <http://www.reuters.com/article/2011/11/22/banks-idUSL5E7ML2NH20111122> (Zugriff: 7. März 2012).

107 <https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Luekex-2011_30112011.html>; < http://www.spiegel.de/netzwelt/netzpolitik/0,1518,801114,00.html > (Zugriff: 7. März 2012).

108 Cyber Europe 2010: Evaluation Report (Heraklion: ENISA, 2011); <http://www.enisa.europa.eu/activities/res/ce2010/cyber-europe-2010/cyber-europe-2010-report/>; Cyber Atlantic 2011: Evaluation Report (Heraklion: ENISA, 2012), <http://www.enisa.europa.eu/activities/res/ca2011/ca2011-report/at_download/fullReport > (Zugriff: 7. März 2012).

109 Jürgen Berke, „Bedingt vertrauenswürdig“, Wirtschaftswoche, 1. August 2011, S. 64–69, hier S. 66.

110 ESRIF Final Report (Brussels: European Security Research and Innovation Forum, 2009); Vorschlag für Beschluss des Rates über das spezifische Programm zur Durchführung des Rahmenprogramms für Forschung und Innovation „Horizont 2020“ (2014–2020), KOM(2011) 811, Brüssel, 30. November 2011, insbesondere S. 95.

Leitfragen für die Diskussion in Österreich

- *Auf welcher rechtlichen Grundlage können Behörden und Unternehmen in Österreich cyberrelevante Informationen austauschen?*
- *Inwieweit werden im Rahmen bestehender Informationsaustauschprozesse in Österreich bereits Aspekte der Cybersicherheit berücksichtigt?*
- *Welche Akteure müssen wen über welche Aspekte der Cybersicherheit informieren?*
- *Durch welche staatlichen Stellen werden Informationen zur Cybersicherheit an nichtstaatliche Akteure weitergegeben?*
- *Wie organisieren sich die Betreiber strategischer Infrastrukturen, um untereinander und mit dem Staat Informationen zur Cybersicherheit auszutauschen?*
- *Welche Akteure können zur Beurteilung der Cybersicherheitslage in Österreich überhaupt welche Informationen beisteuern?*
- *Gibt es Vorbehalte zur Beteiligung bestimmter Akteure am Informationsaustausch zu Fragen der Cybersicherheit?*
- *Gibt es bei den beteiligten Akteure Vorbehalte gegenüber der Weitergabe bestimmter Informationen?*
- *Welche Möglichkeiten bestehen zur Durchführung bi- und multilateraler Cyberübungen mit Österreichs Nachbarn?*
- *Mittels welcher F&E-Schwerpunkte im Bereich der Cybersicherheit können österreichische Unternehmen und Institute gleichzeitig einen Beitrag zur nationalen Sicherheitsvorsorge, zur Stärkung der Wettbewerbsfähigkeit und zur Erschließung internationaler Märkte leisten?*

10. Autorenhinweis

Heiko Borchert ist Inhaber und Geschäftsführer der Sandfire AG und seit 1997 in der sicherheitsstrategischen Beratung für Kunden im öffentlichen und privatwirtschaftlichen Sektor tätig. Zu seinen Themenschwerpunkten zählen der Schutz kritischer Infrastrukturen, die öffentlich-private Sicherheitszusammenarbeit, maritime Sicherheit, Energie- und Rohstoffversorgungssicherheit, Energieinfrastruktursicherheit, die Transformation der Streitkräfte, die Theorie und Praxis der Vernetzten Sicherheit sowie die sicherheitspolitische Vorausschau (Security Foresight). Heiko Borchert publiziert regelmäßig zu seinen Themenschwerpunkten, ist Mit-Herausgeber der Schriftenreihe Vernetzte Sicherheit (Nomos Verlag) und Mitglied des Redaktionsbeirats der Zeitschrift für Außen- und Sicherheitspolitik. Er doziert regelmäßig an sicherheitspolitischen Aus- und Weiterbildungseinrichtungen wie dem Strategischen Führungslehrgang der Landesverteidigungsakademie (Wien), der Bundesakademie für Sicherheitspolitik (BAKS) und dem George C. Marshall European Center for Security Studies (Garmisch-Partenkirchen). Von 2005 bis 2012 war Heiko Borchert Beirat von IPA Network International Public Affairs (Berlin). Seit 2007 ist er zudem Subject Matter Expert des The Hague Center for Strategic Studies (Den Haag). Heiko Borchert hat an der Universität St. Gallen Internationale Beziehungen, Betriebswirtschaftslehre, Volkswirtschaft sowie Rechtswissenschaft studiert und mit einer Arbeit über Europas Sicherheitsarchitektur promoviert. Er ist u.a. Mitglied des International Institute for Strategic Studies (IISS) und der International Studies Association (ISA).