Universität Zürich[UZH]

Bachelorarbeit am Institut für Informatik

28.04.2014

Cyberwarfare – eine Analyse der Risiken auf der Grundlage des Vorsorgeprinzips, im Speziellen am Fallbeispiel Schweiz

Stephan Ryatt

Zürich, Schweiz

10-724-425

stephan.ryatt@uzh.ch

Betreuender Professor: Prof. Dr. Lorenz Hilty

Danksagung

Ich möchte allen herzlich danken, welche mich bei dieser Arbeit unterstützt haben. Besonders danke ich meinem Betreuer Prof. Dr. Lorenz Hilty, welcher mich durchwegs gut beraten und unterstützt hat. Für seine kritischen Beurteilungen und Verbesserungsvorschläge bin ich ihm sehr dankbar. Auch sehr hilfreich war der Austausch mit Gérald Vernez, dem Delegierten des Chefs der Armee für Cyber-Defence. Er hat mir insbesondere inhaltliche Fragen zu den Cybermassnahmen der Schweiz beantworten können und kritische Kommentare zu meinen Befunden gegeben. Zudem möchte ich meiner Familie und meinen Freunden danken, welche mir mit ihren Rückmeldungen sehr geholfen haben.

Abstract

Cyberwarfare presents a risk to a state's national security and various measures to minimize that risk have therefore been undertaken, e.g. the *United States Cyber Command (USCYBERCOM)* or the *National strategy for Switzerland's protection against cyber risks (NCS)*. Because cyberwarfare is a relatively new phenomenon, the base of knowledge is quite low. Therefore the question arises, how appropriate these measures are with respect to the existing risks. This bachelor thesis examines this question from the Precautionary Principle's (PP) perspective. The PP aims to minimize risks by taking early action to prevent irreversible damage. According to the PP, this action should even be taken in the absence of scientific consensus. Firstly, this thesis examines the question of the appropriateness of the measures with respect to the general risk situation of cyberwarfare. Secondly, with respect to the case study of Switzerland, with its *National strategy for Switzerland's protection against cyber risks (NCS)*. The general risk situation shows that lower intensity cyberattacks have become a reality. From the PP's perspective it is therefore too late to take preventative measures. Higher intensity cyberattacks have not revealed themselves as a persistent threat yet. Therefore, according to the PP, preventative measures should be taken into consideration. The case study of Switzerland shows that the persons responsible for the NCS do not pay enough attention to the risks of higher intensity cyberattacks. They regard them as too unlikely to seriously deal with and invest resources into. Based on these findings, this thesis proposes certain actions for Switzerland.

Zusammenfassung

Cyberwarfare stellt ein Risiko für die nationale Sicherheit eines Staates dar und es wurden deshalb schon verschiedene Massnahmen zur Minimierung dieses Risikos getroffen, wie z.B. der *United States Cyber Command (USCYBERCOM)* oder die *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)*. Aufgrund der Neuheit dieses Phänomens ist der Wissensstand noch relativ gering, weshalb sich die Frage stellt, wie treffend diese Massnahmen bezüglich der bestehenden Risiken sind. In dieser Arbeit wird diese Frage aus Sicht des Vorsorgeprinzips (VSP) untersucht, welches darauf abzielt Risiken zu minimieren, indem frühzeitig Massnahmen getroffen werden, um irreversible Schäden zu vermeiden, auch wenn noch kein wissenschaftlicher Konsens besteht. Zuerst wird die Frage an der generellen Risikosituation des Cyberwarfare untersucht, danach am Fallbeispiel Schweiz mit seiner *Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)*. In der generellen Risikosituation zeigt sich, dass Cyberangriffe tieferer Intensität bereits Realität sind und es somit aus Sicht des VSP zu spät ist, um Vorsorge zu leisten. Cyberangriffe höherer Intensität haben sich hingegen noch nicht als akute Bedrohung erwiesen, weshalb laut dem VSP vorsorgliche Massnahmen in Betracht gezogen werden sollten. Beim Fallbeispiel Schweiz stellt sich heraus, dass die Verantwortlichen der NCS den Risiken der Cyberangriffen höherer Intensität zu wenig Beachtung schenken, da sie diese als zu unwahrscheinlich sehen, um sich ernsthaft damit auseinanderzusetzen und Ressourcen zu investieren. Aufgrund diesen Erkenntnissen werden Handlungsvorschläge für die Schweiz präsentiert.

Inhaltsverzeichnis

1 Einleitung

Cyberwarfare ist heute ein allgegenwärtiges Thema in den Medien und die Gesellschaft ist sich der Gefahr mehrheitlich bewusst. Vor knapp einem Jahrzehnt wurde Cyberwarfare noch von verschiedenen renommierten Sicherheitsanalysten als harmlos abgestuft, da bislang nur kleine und unbedeutende Attacken stattgefunden hatten. Anfangs des 21. Jahrhunderts wurde eine Serie von Cyberspionageangriffen namens *Titan Rain* identifiziert, welche gemeinhin China angelastet werden. Diese hatten den Diebstahl von Informationen verschiedener Organisationen der US Regierung zum Ziel. 2007 wurde Estland Opfer einer Cyberattacke, welche wichtige Webseiten der Regierung, Banken und Medien lahmlegte. 2008 lancierte Russland, kurz vor seiner konventionellen Militärintervention in Georgien eine Cyber-Attacke, welche deren Kommunikationswege zum Erliegen brachte. Spätestens seit 2010, mit der *Stuxnet-Attacke*, welche in Form eines Wurms Schaden an den iranischen Urananreicherungsanlagen verursacht hat, ist man sich den Gefahren des Cyberwar bewusst geworden (Shakarian, Shakarian, & Ruef, 2013). 2013 hat die globale Überwachungs- und Spionageaffäre der *National Security Agency (NSA)* weltweit Wellen geschlagen und Fragen bezüglich der individuellen Freiheit der Internetnutzer aufgeworfen.

Da es sich beim Cyberwarfare um ein neuartiges Phänomen handelt, ist der Wissensstand noch relativ gering. Dieses fehlende Wissen und die Erkenntnis, dass Cyberwarfare eine reale Bedrohung ist, gegen welche momentan wenig Schutz besteht, führen bei den politischen Entscheidungsträgern zu Unsicherheit. Diese stellen sich insbesondere Fragen über die bestehenden Risiken und die zu treffenden Massnahmen, welche diesen Risiken entgegenwirken sollen. International wurden schon verschiedene Massnahmen getätigt. In den USA, welche eine Vorreiterrolle einnehmen, wurde 2009 beispielsweise der *U.S. Cyber Command* ins Leben gerufen. Dieser ist dem Verteidigungsministerium unterstellt und ist für die Ausführung von offensiven Cyberoperationen, wie auch die Verteidigung des US Cyberspace zuständig (U.S. Department of Defense [DoD], 2010b). Auch die Schweiz hat sich 2010 dazu entschieden eine Task Force zur Ausarbeitung einer „nationalen Strategie Cyber Defense“ zu erstellen (Vernez, Hüssy, & Sibilia, 2011). 2012 verabschiedete dann der Bundesrat eine vom *Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS)* erarbeitete *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)* (Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport [VBS], 2012).

Da diese Risikoeinschätzungen und getätigten Massnahmen noch sehr jung sind, fehlt eine kritische Analyse über deren Relevanz. Denn es stellt sich einerseits die Frage ob die Risiken richtig eingeschätzt wurden und infolgedessen, wie passend die Massnahmen bezüglich der bestehenden Risiken sind. Sollten die getätigten Massnahmen erweitert werden, da die Risiken unterschätzt wurden? Oder schiessen

diese Massnahmen sogar über das Ziel hinaus? Denn diese können auch negative Auswirkungen mit sich tragen. Dies hat beispielsweise die 2013 aufgedeckte globale Überwachungs- und Spionageaffäre der *National Security Agency (NSA)* gezeigt. Um die nationale Sicherheit zu schützen, wurde die Privatsphäre der Bürger verletzt.

Das Ziel dieser Arbeit ist, die Risiken des Cyberwarfare und die Massnahmen zur Minimierung dieser, mithilfe des Vorsorgeprinzips (VSP) am Beispiel der Schweiz zu untersuchen. Das VSP zielt darauf ab Risiken zu minimieren, in dem frühzeitig Massnahmen getroffen werden um irreversible Schäden zu vermeiden, auch wenn noch kein wissenschaftlicher Konsens besteht. Das VSP hilft deshalb bei der kritischen Einschätzung, ob die Massnahmen der Schweiz den bestehenden Risiken genügend Rechnung tragen.

In einem ersten Schritt wird das Thema Cyberwarfare (Kapitel 2) erläutert, indem der Begriff definiert wird (Kapitel 2.1), auf die verschiedenen Akteure (Kapitel 2.2), deren Strategien und Absichten (Kapitel 2.3) und mögliche Angriffsziele (Kapitel 2.4) eingegangen wird. Danach wird das Vorsorgeprinzip (Kapitel 3) erklärt, wobei zuerst eine Definition (Kapitel 3.1) gegeben wird. Danach wird gezeigt, wie das Vorsorgeprinzip einerseits in der Umweltpolitik, Umweltrecht und Umweltschutz (Kapitel 3.2) verankert ist, andererseits im Bereich der Informations- und Kommunikationstechnologie (ICT) (Kapitel 3.3).
Es wird dann am Fallbeispiel der Schweiz (Kapitel 4) gezeigt, welche Massnahmen (Kapitel 4.2) bezüglich der bestehenden Risiken (Kapitel 4.1) unternommen werden. Da die getroffenen Massnahmen selbst Risiken mit sich bringen, wird auch auf diese Risiken eingegangen (Kapitel 4.3).
Anschliessend wird eine Schlussfolgerung (Kapitel 5) gemacht. In dieser wird zuerst die generelle Risikosituation des Cyberwarfare, aus Sicht des Vorsorgeprinzips beurteilt (Kapitel 5.1). Danach folgt eine Bewertung der Massnahmen der Schweiz, hinsichtlich der bestehenden Risiken (Kapitel 5.2). Es wird wiederum das Vorsorgeprinzips hinzugezogen, um herauszufinden, ob die Massnahmen genügend Vorsorge leisten. Schlussendlich folgt ein Ausblick (Kapitel 5.3), in welchem Handlungsvorschläge für die Schweiz präsentiert werden, welche zur weiteren Entwicklung der Strategie der Schweiz (NCS) hilfreich sein könnten.

2 Cyberwarfare

Dieses Kapitel soll dem Leser einen Überblick über das Phänomen Cyberwarfare geben. Da Cyberwarfare von verschiedenen Autoren unterschiedlich aufgefasst und definiert wird, wird im ersten Unterkapitel 2.1 eine Definition gezogen, wie Cyberwarfare in dieser Arbeit zu verstehen ist. Im zweiten Unterkapitel 2.2 wird auf die verschiedenen Akteure eingegangen, welche sich am Cyberwarfare beteiligen. Dabei wird deren Charakter, Motivation und Gefahrenpotential erläutert. Im dritten Unterkapitel 2.3 wird erläutert, welche Arten von Cyberattacken existieren und worauf diese abzielen. Das vierte Unterkapitel 2.4 zeigt verschiedene Angriffsziele auf, welche von den Akteuren anvisiert werden können.

2.1 Definition

Es ist nicht einfach eine Definition für Cyberwarfare (oder auch Cyberwar) zu finden. Denn ähnlich wie bei der asymmetrischen Kriegsführung, wird es zunehmend schwierig, zwischen Kombattanten und Nicht-Kombattanten zu unterscheiden, da diese nicht zwingend Staaten angehören. Als Beispiel wären Hackergruppen wie *Anonymous* und *LulzSec* zu nennen. Folglich würde eine Definition, welche nur die Kriegsführung zwischen Staaten umschreibt, zu kurz fallen. Andererseits kann aber nicht jede Art von Cyberattacke als Kriegshandlung klassifiziert werden, wie z.B. Internetkriminelle, welche Phishing-Attacken durchführen, um andere Leute zu bestehlen.

In dieser Arbeit wird die Definition von Shakarian et al. (2013) verwendet, welche Cyberwarfare wie folgt definieren:

“Cyber war is an extension of policy by actions taken in cyber space by state or non-state actors that either constitute a serious threat to a nation’s security or are conducted in response to a perceived threat against a nation’s security” (Shakarian et al., 2013, p. 2).

Shakarian et al. nehmen die Clausewitzsche Definition des konventionellen Krieges als Grundlage: “War is merely the continuation of policy by other means“ (Clausewitz, Howard, & Paret, 1984, p. 87). Sie erweitern diese, um einerseits nichtstaatlichen Akteuren Rechnung zu tragen, andererseits werden aber nur Akteure berücksichtigt, welche eine ernsthafte Gefahr für die nationale Sicherheit eines Staates darstellen.

2.2 Akteure

In diesem Kapitel werden die verschiedenen Akteure des Cyberwarfare beschrieben. Dabei wird auf ihr Charakter, ihre Motivation und ihr Gefahrenpotential eingegangen, um zu zeigen, inwiefern diese Akteure eine Bedrohung darstellen. Das Gefahrenpotential setzt sich aus den finanziellen Mitteln und den technischen Fähigkeiten zusammen. Zudem werden jeweils aktuelle Beispiele vorgestellt.

Akteure welche zwar im Cyberwarfare-Diskurs erwähnt werden, aber nicht in die Definition dieser Arbeit passen, wie zum Beispiel Cyberkriminelle oder *Script kiddies*[1], werden hier nicht behandelt. Denn sie stellen in der Regel keine aktive Gefahr für die Sicherheit eines Staates dar.

Es ist wichtig zu erkennen, dass die hier erläuterten Kategorien von Akteuren nicht zwingend trennscharf sind, denn sie können sich gegenseitig überlappen. So können zum Beispiel *Hacktivists* und Cyberkriminelle von staatlichen Akteuren finanziert oder sogar beauftragt werden (Winterfeld & Andress, 2013).

2.2.1 Staatliche Akteure

Bei staatlichen Akteuren handelt es sich meist um militärische Einheiten, aber auch zivilen Einheiten, deren Auftrag die Ausführung von Cyberoperationen ist. Diese können defensive, wie auch offensive Strategien[2] umfassen. Welche Massnahmen durchgeführt werden, hängt stark von der Aussenpolitik eines Staates ab. Die Motivation staatlicher Akteure kann also dementsprechend variieren. Ihnen stehen meist umfassende finanzielle Mittel zur Verfügung. Dies erlaubt es ihnen einerseits technisch hochqualifiziertes Personal anzuwerben, andererseits weniger qualifiziertes Personal entsprechend auszubilden und zu trainieren. „Leider ist nicht transparent, wer wie viele Mittel wofür ausgibt. Die Militärs lassen sich nicht in die Karten sehen. Auch die Trennung von defensiven und offensiven Investitionen ist schwierig. . . . Genaue Zahlen sind nur schwer zu erhalten und stammen teilweise aus fragwürdigen Quellen“ (Gaycken, 2011, p. 190).

Eine Untersuchung des *United Nations Institute for Disarmament Research* ergab, dass im Jahre 2012, 114 von 193 Staaten ein Cybersecurityprogamm besassen, wovon 47 Staaten Cyberwarfare in ihre militärische Planung einbezogen (Lewis & Neuneck, 2013). Die beiden Nationen mit den umfassendsten Cyberwarfareprogrammen

[1] “Script kiddies or noobs (for new to hacker) are pejorative terms for the less skilled hackers. These are the folks who can only use the tools that can be found on the Internet. There are many different motivations to start hacking. Some are looking for a social experience and will try to join a hacker group (some groups will require proof of hacking ability before they grant membership), others enjoy the challenge or want to gain status across the hacker community, still others do it out of curiosity and think of it as entertainment“ (Winterfeld & Andress, 2013, p. 10).

[2] Siehe Kapitel 2.3 Strategien und Absichten

sind die Vereinigten Staaten und China, weshalb sie in diesem Kapitel auch genauer beschrieben werden. Man darf jedoch nicht vergessen, dass aufgrund der tiefen Eintrittskosten und dem geringen Risiko von Konsequenzen, auch kleinere Staaten sich am Cyberwarfare beteiligen können (Winterfeld & Andress, 2013).

- Vereinigte Staaten: Im US Militär bestehen verschiedene Cyberwarfare-Einheiten in den einzelnen Teilstreitkräften (Army, Navy und Air Force). Um diese zu koordinieren, wurde am 23. Juni 2009 der *United States Cyber Command (USCYBERCOM)* gegründet (DoD, 2010b). Der Vize-Verteidigungsminister William Lynn sagte, der USCYBERCOM sei "[the] linking of intelligence, offense, and defense under one roof" (U.S. Department of Defense [DoD], 2010a, p. 3), wobei die primäre Absichten die Sicherstellung der amerikanischen Freiheit im Cyberspace und die Verringerung der Risiken der nationalen Sicherheit sind, aufgrund Amerikas Abhängigkeit vom Cyberspace (Rosenzweig, 2013). Das offizielle Mission Statement lautet wie folgt:

  "USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries" (DoD, 2010b, p. 1).

  Seit dem Mai 2010 ist der USCYBERCOM einsatzbereit und hat sich seither hauptsächlich mit der Ausarbeitung von Strategien auseinandergesetzt. Das Resultat sind zwei verschiedene Strategien. Zum einen die *Department of Defense Strategy for Operating in Cyberspace*. Diese befasst sich mit den Gründen, weshalb Cyberspace als eigene Domäne der Kriegsführung (neben Land, Wasser und Luft) zu behandeln ist, mit der Verteidigung eigener Systeme und Netzwerke, sowie der Zusammenarbeit des Verteidigungsministeriums (Department of Defense) mit anderen staatlichen Behörden, dem privaten Sektor und internationalen Partnern. Da sich diese Strategie aber nur auf die Defensive konzentriert und die Offensive ausser Acht lässt, sah man sich veranlasst eine entsprechende zweite Strategie zu entwickeln (Rosenzweig, 2013). Im November 2011 wurde der *Department of Defense Cyberspace Policy Report* veröffentlicht. Dieser befasst sich unter anderem mit der Abschreckung von Attacken, möglichen Antworten und Gegenmassnahmen auf Attacken, und generellen offensiven Möglichkeiten gegen Bedrohungen (U.S. Department of Defense [DoD], 2011). Zu den offensiven Möglichkeiten steht im Report: "the President reserves the right to respond using all necessary means to defend our Nation, our Allies, our partners, and our interests from hostile acts in cyberspace. Hostile acts may include sig-

nificant cyber attacks directed against U.S. economy, government or military" (DoD, 2011, p. 4).

- China: Die chinesische Regierung gibt sich sehr bedeckt bezüglich ihrer Cyberwarfare-Fähigkeiten. So sind weder genaue Zahlen über Ressourcen, noch die Organisationsstruktur bekannt. Bekannt ist aber, dass sich China schon sehr früh mit dieser Thematik auseinandergesetzt und Massnahmen zum Aufbau von Cyberwarfare-Fähigkeiten ergriffen hat. Der Grund dafür liegt in der technologischen Differenz zwischen den Armeen Chinas und dem Westen, insbesondere aber der USA. Durch Cyberwarfare erhofft sich China einerseits dieser technologischen Unterlegenheit entgegenzuwirken. Andererseits ist der Westen durch seine hochtechnisierten Armeen stark abhängig von Informationstechnik, was ihn anfällig gegenüber Cyberattacken macht. Es ist daher nicht verwunderlich, dass Chinas Strategie eine offensivere Ausrichtung hat, als diejenige der USA (Gaycken, 2011). Ein Hauptziel der chinesischen Strategie ist die Schaffung günstiger Umstände, um im Falle eines Konflikts im Vorteil zu stehen. China setzt deshalb vor allem auf Cyberspionage und Aufklärungsaktionen[3], um sich einen Informationsvorteil zu verschaffen. Dies geschieht, indem die gegnerische Systemlandschaft ausspioniert wird, um im Falle eines Konflikts gezielte Angriffe durchführen zu können (Shakarian et al., 2013).

  China setzt sowohl auf militärische, als auch auf zivile Einheiten. Gemäss eines Reports der *Northrop Grumman Cooperation*, welcher im Auftrag der *US-China Economic and Security Review Commission* erstellt wurde, sind offensive Massahmen dem 4. Departement (Electronic Countermeasures) des *General Staff Department (GSD)* zugeteilt, während defensive Massnahmen dem 3. Departement (Signals Intelligence) des GSD zugewiesen sind. China scheint auch Milizeinheiten zu unterhalten, welche die Einheiten des 3. und 4. Department des GSD sowohl in offensiven, wie auch defensiven Massnahmen zu unterstützen scheinen. Um die hohen Anforderungen an Personal erfüllen zu können, greift China auch auf verschiedene zivile Sektoren zurück. Sie rekrutieren entsprechend qualifizierte Arbeitskräfte der Industrie und Forschung. Zudem wird vermutet, dass China mit hochqualifizierten Hackern und Hackergruppen zusammenarbeitet. So erwähnt der Northrop Grumman Report, dass China einerseits einzelne Hacker direkt rekrutiert, andererseits mit Sicherheitsfirmen zusammenarbeitet, welche von erfahrenen Hackern gegründet wurden (Krekel, 2009).

[3] Siehe Kapitel 2.3 Strategien und Absichten

2.2.2 Nicht-staatliche Akteure

Hierbei handelt es sich um Gruppierungen oder Individuen, welche nicht mit einem Staat in Zusammenhang stehen, sondern auf eigene Faust handeln und eigene Interessen verfolgen.

2.2.2.1 Hacktivists

Bei dieser Kategorie von Akteuren handelt es sich um Hacker, welche politisch, religiös oder durch Nationalstolz motiviert sind. (Winterfeld & Andress, 2013). Gewöhnlich operieren Hacktivists in lose organisierten Gruppen, können aber auch als Individuen agieren. Sie wollen mit ihren Angriffen ihre politischen Interessen durchsetzen, sich Gehör verschaffen, finanzielle Schäden verursachen oder rufschädigend wirken (VBS, 2012). Dazu versuchen sie Dienstleistungen unverfügbar zu machen, meist mittels *DDoS*[4], Daten zu stehlen oder Webseiten zu verunstalten[5]. Ihre Fähigkeiten sind sehr unterschiedlich, können aber durchaus fortgeschritten sein. Ihnen fehlen jedoch meist die finanziellen Mittel, welchen den staatlichen Akteuren zur Verfügung stehen, um schwerwiegende Schäden anzurichten.

Das wohl bekannteste Beispiel einer solchen Gruppe ist *Anonymous*. Sie kämpfen vor allem gegen die Zensur des Internets und die digitale Überwachung. Sie haben schon mehrere grosse Organisationen und Unternehmen angegriffen, welche Zensur und Überwachung unterstützen. So haben sie zum Beispiel 2010 die Server von PayPal, MasterCard und Visa lahmgelegt, da diese *WikiLeaks* die Weiterführung ihrer Dienstleistungen verweigert hatten (Addley & Halliday, 2010). Des Weiteren haben sie auch schon Webseiten der Regierungen der Vereinigten Staaten und Israel, von Urheberschutzorganisationen der Film- und Musikindustrie, sowie von extrem religiösen Gruppen angegriffen.

Ein bekanntes Beispiel für ein Individuum ist *The Jester*. Er ist ein patriotischer Hacker aus den Vereinigten Staaten, bei welchem vermutet wird, dass er früher beim Militär gedient hat. Seine Ziele sind vor allem fundamentalistisch-islamistische Terroristen, welche die nationale Sicherheit der USA gefährden und das Internet als Kommunikationsmittel nutzen. So hat er schon mehrere einschlägige Websites mittels *DDoS* lahmgelegt, aber auch Angriffe gegen Wikileaks und Anonymous durchgeführt, da diese seiner Meinung nach gegen amerikanische Interessen verstossen haben (OConnor, 2011).

[4] Siehe Kapitel 2.3.2 Denial-of-Service

[5] Siehe „Manipulation von Informationen“ in Kapitel 2.3.4 Sabotage

2.2.2.2 Cyberterroristen

Bei Cyberterroristen handelt es sich um Akteure, deren Motivation und Absichten der Definition von Denning (2000) über Cyberterrorismus entsprechen:

"Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not" (Denning, 2000, p. 1).

Bislang haben sich noch keine terroristisch motivierte Cyberattacken mit physischen Schäden ereignet, beispielsweise an kritischen Infrastrukturen. „Da terrorverursachende, dauerhafte Schäden an kritischen Infrastrukturen vielfältige Expertisen benötigen, ist es für sie ausnehmend schwierig, auf diesem Wege zu operieren. Zudem wäre es kaum lukrativ. Hunderttausende oder Millionen zu investieren, um Cyber-Söldner einen flächenintensiven Cyber-Angriff ausführen zu lassen, ist insgesamt wesentlich ineffizienter als eine um mehrere Faktoren billigere Bombe" (Gaycken, 2011, p. 194). Cyberterroristen müssten sich also bessere technische Fähigkeiten aneignen, und andererseits entsprechende finanzielle Mittel aufbringen, um eine solche Cyberattacke durchführen zu können. Das Potential ist aber definitiv vorhanden, wie der *Maroochy Water Breach* Vorfall zeigt. Aus Rache für seine Entlassung, führte ein ehemaliger Mitarbeiter der Maroochy Water Services in Queensland, Australien, Attacken auf deren Abwassersystem aus. Er übernahm mittels eines Laptops und Wirelesstechnologie die Kontrolle über 142 Abwasserpumpstationen, welche er im Rahmen seiner Anstellung mitgeholfen hatte zu installieren. Während drei Monaten liess er über eine Million Liter Abwasser in lokale Gewässer fliessen (Shakarian et al., 2013). Auch wenn hier keine terroristischen Motive mitgespielt haben, demonstriert dieser Vorfall sehr wohl die Realität und die möglichen physischen Auswirkungen eines Angriffs auf kritische Infrastrukturen.

Die Abwesenheit terroristisch motivierter Attacken bedeutet aber nicht, dass Terroristen nicht auf dem Internet aktiv sind. Sie nutzen es um Propaganda zu verbreiten, neue Mitglieder zu rekrutieren und radikalisieren, als Kommunikationsmittel innerhalb ihrer Gruppen, zur Planung von Attacken und zur Beschaffung von Geldmitteln (VBS, 2012; Lewis, 2002).

2.3 Strategien und Absichten

Im Cyberwarfare existieren verschiedene Akteure, welche unterschiedliche Ziele verfolgen. Zur Erreichung dieser Ziele können verschiedene Strategien eingesetzt werden, welche unterschiedliche Auswirkungen auf die jeweiligen Zielsysteme haben. Um diese Auswirkungen zu kategorisieren, werden die drei Prinzipien der Informationssicherheit von Winterfeld & Andress (2013) benutzt:

- Confidentiality: Damit ist die Vertraulichkeit von Daten gemeint. Daten sollen nicht in die Hände von unbefugten Personen fallen. Die Vertraulichkeit wird folglich verletzt, wenn Daten von einem System gestohlen werden.

- Integrity: Die Integrität beschreibt, dass keine Daten oder Systemfunktionen von unbefugten Personen verändert werden dürfen.

- Availability: Die Verfügbarkeit bedeutet, dass der Zugriff auf Systeme oder Daten gewährleistet ist. Sie wird verletzt, wenn zum Beispiel ein System von Hackern mittels *DDoS*[6] unverfügbar gemacht wird oder Daten gelöscht werden.

Welche Strategie eingesetzt wird und demzufolge welche Auswirkung erzielt wird, hängt stark von der Motivation der Akteure ab. Ein Cyberangriff muss sich nicht nur auf eine dieser Strategien beschränken, sondern kann auch mehrere Strategien in einen Angriff inkorporieren. Im Folgenden werden die wichtigsten Strategien erläutert.

2.3.1 Cyberreconnaissance

Hierbei handelt es sich um den Vorbereitungsprozess einer Attacke, indem eine Aufklärung des Ziels durchgeführt wird. „[Cyberreconnaissance] verweist ganz richtig auf die klassische Reconnaissance, allerdings mit dem Ziel und Mittel des Computers“ (Gaycken, 2011, p. 138). Das Ziel ist in dem Sinne analog zur klassischen Reconnaissance. Man will wesentliche Informationen über das Angriffsziel herausfinden (siehe Tabelle 1), um später gezielt und effizient eine Attacke durchführen zu können. Obwohl während der Reconnaissance-Phase noch kein voller Zugriff auf das Angriffsziel besteht, gelangen vertrauliche Informationen über dieses an den Angreifer, was eine Verletzung der *Confidentiality* bedeutet. Cyberreconnaissance wird vor fast jeder Art von Attacke (Cyberspionage, Sabotage, etc.) durchgeführt und findet meist in zwei Phasen statt.

[6] Siehe Kapitel 2.3.2 Denial-of-Service

Network Information	• IP addresses • Subnet mask • Network topology • Domain names
Host Information	• User names • Group names • Architecture type (e.g. x86 vs SPARC) • Operating system family and version • TCP and UDP services running with versions
Security Policies	• Password complexity requirements • Password change frequency • Expired/disabled account retention • Physical security (e.g. locks, ID badges, etc.) • Firewalls • Intrusion detection systems
Human Information	• Home address • Home telephone number • Frequent hangouts • Computer knowledge • Dark secrets

Tabelle 1: Wichtige Informationen der Reconnaissance-Phase (Brown, 2011).

2.3.1.1 Passive Reconnaissance

In dieser Phase der Aufklärung werden direkte Interaktionen mit dem Angriffsziel vermieden, um nicht entdeckt zu werden. Wenn man eine Analogie zu einem klassischen Einbruch in ein Haus zieht, würde man in dieser Phase den Standort des Hauses ausmachen, die Nachbarschaft auskundschaften, allgemeine Informationen über das Haus und deren Bewohner finden (z.B. Namen der Bewohner, Adresse, Telefonnummer, usw.) und vorhandene Sicherheitsvorrichtungen (z.B. einen Wachhund oder eine Alarmanlage) ausfindig machen (Brown, 2011).

Diese Phase wird auch *Footprinting* genannt, da man verschiedene Informationen zusammenträgt, um einen „Footprint“ oder Fussabdruck des Angriffsziels zu erstellen (Boyd, 2000). Man will in dieser Phase generelle Informationen über das Computernetzwerk des Angriffsziels herausfinden. Dazu gehören unter anderem IP Ad-

ressen des Zielsystems (z.B. von Routern), Vorhandensein von Sicherheitsvorrichtungen (z.B. Firewalls oder Intrusion Detection Systems) oder die Verfügbarkeit von Remote Access (Shakarian et al., 2013). Der Tabelle 1 können noch weitere Informationen entnommen werden, welche im Rahmen der Aufklärung beschafft werden können.

Diese Informationen können über verschiedene Wege beschafft werden. Informationen können *öffentlich zugänglich* sein, über *Netzwerkoperationen* ausfindig gemacht werden oder mittels *Social Engineering* in Erfahrung gebracht werden. *Öffentlich zugängliche Informationen* können über Google-Suchen gefunden werden. Zum Beispiel auf der offiziellen Website des Angriffsziels oder in Internetforen, in welchen Mitarbeiter der Zielorganisation über deren Netzwerkinfrastruktur sprechen. Zudem können Anfragen an DNS-Server gestellt werden, um an IP-Adressen und sonstige Informationen über den Host ausfindig zu machen (Shakarian et al., 2013; Winterfeld & Andress, 2013). Ein Beispiel für eine *Netzwerkoperation* ist das Kompromittieren eines vom Zielsystem benutzten Routers. So kann der Datenverkehr von und zum Zielsystem überwacht werden, ohne direkten Kontakt mit dem Ziel selbst (Winterfeld & Andress, 2013). Beim *Social Engineering* werden Menschen dazu manipuliert gewisse Aktionen durchzuführen oder Informationen preiszugeben, wodurch sie die Sicherheit ihres Systems gefährden (Winterfeld & Andress, 2013). Ein Beispiel ist, wenn der Angreifer sein Opfer per Email, mit irreführendem Absender, dazu auffordert, seine Zugriffsdaten neu einzugeben, wodurch sie in die Hände des Angreifers fallen.

2.3.1.2 Active Reconnaissance

In dieser Phase geht man einen Schritt weiter und versucht auf eine offensivere Art und Weise an Informationen zu gelangen. Es werden direkte Abfragen an das Angriffsziel gestellt, weshalb auch die Gefahr steigt, dass man entdeckt wird. Um zurück zur Analogie des klassischen Einbruchs zu kehren, würden in dieser Phase die Türen und Fenster des Hauses untersucht werden, um offene oder schwach gesicherte Eingänge ausfindig zu machen (Brown, 2011).

Die Active Reconnaissance Phase wird auch *Scanning* genannt. Man ist hier an detaillierteren Informationen über das Computernetzwerk des Angriffsziels interessiert. Benutzte Betriebssysteme, offene Ports (Kommunikationsschnittstellen eines Netzwerks) und die Konfiguration der Firewall sind einige Beispiele dafür (Shakarian et al., 2013). Aber auch die Netzwerktopologie des Angriffsziels ist wichtig. In der Tabelle 1, können weitere Informationen gefunden werden, welche ermittelt werden können.

Um an diese Informationen zu gelangen, kommen im Rahmen der Active Reconnaissance verschiedenste Techniken und Tools zum Einsatz. Zwei bekannte Techniken sind *Port Scanning* und *OS Fingerprinting*. Beim Port Scanning wird mit einem spezifischen Tool untersucht, welche Ports in Betrieb sind. Da Applikationen und Dienste spezifische Ports zugewiesen bekommen, kann man so sehen, welche Applikationen

und Dienste auf dem Netzwerk laufen. Zudem können mit dem Port Scanning ungeschützte, offene Ports identifiziert werden. Diese können möglicherweise als Sicherheitslücke ausgenutzt werden (Gaycken, 2011). OS Fingerprinting "defines any method used to determine what operating system is running on a remote computer. OS fingerprinting is a key element in network reconnaissance as most exploitable vulnerabilities are operating system specific" (Millican, 2003, p. 7). Wenn also das Betriebssystem bekannt ist, können bekannte Sicherheitslücken dieses Betriebssystems ausgenutzt werden, um Zugriff zum System zu erlangen. Dies muss aber nicht zwingen über ein Betriebssystem geschehen, sondern kann auch über Applikationen erfolgen, da auch diese Sicherheitslücken haben.

2.3.2 Denial-of-Service

Mit einer Denial-of-Service (DoS) Attacke versucht ein Angreifer ein gegnerisches System temporär lahmzulegen und zielt somit auf dessen *Availability* oder Verfügbarkeit ab. Dies wird meist dadurch erreicht, indem das anzugreifende System mit einem übermässig hohen Datenverkehr überlastet wird. Da heutzutage die meisten Systeme einen hohen Datenverkehr verarbeiten können, ist eine DoS-Attacke kaum von einem einzigen Computer ausführbar. Deshalb werden sogenannte Distributed-Denial-of-Service (DDos) Attacken durchgeführt, bei welchen mehrere Computer gleichzeitig ein System angreifen (Rogers, 2004). Angreifer machen sich dazu oft *Botnetze* zu Nutzen. Dabei handelt es sich um ein Netzwerk von befallenen Computern, deren Rechenressourcen benutzt werden um solche DDoS-Attacken durchzuführen (Shakarian et al., 2013). DDoS-Attacken werden vor allem von *Hacktivists*[7] benutzt, um Webseiten ihrer Gegner unverfügbar zu machen. Da nicht ins gegnerische System eingedrungen werden muss, sondern dieses nur von aussen mit Anfragen überlastet wird, ist diese Art der Attacke vergleichsweise einfach durchzuführen und erfordert kein grosses Fachwissen. Botnetze können sogar zu relativ erschwinglichen Preisen gemietet werden (Shakarian et al., 2013). Da die Wirkung der Attacke nur vorübergehend ist und keine bleibenden Schäden am System entstehen, bleibt DDoS, im Vergleich zu anderen Cyberattacken, ein relativ harmloses Mittel. Gaycken (2012, p. 94) beschreibt DDoS als „das digitale Pendant zu einer digitalen Sitzblockade".

DDoS hat aber schon Anwendung im militärischen Bereich gefunden. Kurz vor der Russischen Invasion 2008 in Georgien, wurden deren Kommunikationskanäle mittels DDoS lahmgelegt. Somit wurden die georgischen Medien und die Bevölkerung daran gehindert, mit der Aussenwelt zu kommunizieren (Shakarian et al., 2013).

[7] Siehe Kapitel 2.2.2.1 Hacktivists

2.3.3 Cyberspionage

Das primäre Ziel von Cyberspionage ist die Entwendung von Daten und Informationen und ist deshalb hinsichtlich der drei Prinzipien der Informationssicherheit[8] eine Verletzung der *Confidentiality*. Rosenzweig definiert Cyberspionage folgendermassen:

"Exploitation of a system for the purpose of securing data and information that is intended to be kept confidential. Espionage can come in two distinct flavors, just as in the physical world: industrial espionage for the purpose of commercial gain or governmental espionage to uncover secret or classified information. At the margins, of course, these two flavors can blend into one another" (Rosenzweig, 2013, p. 23).

Man will sich mit der Cyberspionage einen Informationsvorteil gegenüber dem Gegner verschaffen und somit eine Informationsasymmetrie kreieren. Wie in der Definition erwähnt, kann einerseits auf staatlicher Ebene spioniert werden, andererseits aber auch auf wirtschaftlicher Ebene.

Auf der staatlichen Ebene wird einerseits versucht, Zugriff auf klassifizierte Informationen von militärischen Systemen zu erlangen. Damit können einerseits gegnerische Strategien in Erfahrung gebracht werden, andererseits aber auch militärische Technologien entwendet und kopiert werden (Gaycken, 2011). Andererseits können auch die Systeme anderer Behörden ins Visier genommen werden, wie zum Beispiel von Aussenministerien. Dadurch könnten relevante Informationen zu diplomatischen Beziehungen erlangt werden.

Auf der wirtschaftlichen Ebene wird versucht, Geschäftsgeheimnisse von konkurrierenden Unternehmen zu entwenden. Dies wird auch als *Wirtschaftsspionage* oder *Industrial Espionage* bezeichnet und stellt eine mögliche Ausprägung der Cyberspionage dar (Kaperonis, 1984). Rosenzweig spricht in seiner Definition auch von der Durchmischung der staatlichen und der wirtschaftlichen Ebene. Ein Beispiel dafür sind staatliche Akteure, welche Wirtschaftsspionage betreiben. Damit kann einerseits die Wirtschaft eines gegnerischen Staates geschwächt werden. Andererseits können die eigenen Unternehmen, und somit die eigene Wirtschaft, gestärkt werden (Gaycken, 2011).

Cyberspionage ist eine der meistangewandten Strategien im Cyberwar und die Schäden belaufen sich in die Milliarden. Der Hauptgrund dafür sind die hohen Erträge, im Vergleich zu den tiefen finanziellen Aufwänden (Krekel, 2009). Zudem wird Cyberspionage meist nicht als eine kriegerische Handlung gewertet, da auf den Zielsystemen nichts verändert wird (*Integrity* und *Availability* werden nicht verletzt). Die Täter haben also keine direkten Risiken zu befürchten, abgesehen von diplomatischen Schäden (Gaycken, 2011). Insbesondere China scheint ein aktives Cyberspionageprogramm zu besitzen. Zwar ist es schwierig, handfeste Beweise für die Täterschaft solcher Datendiebstähle zu finden, doch Vorfälle wie *Titan Rain* oder

[8] Siehe Kapitel 2.3 Strategien und Absichten

Gh0stNet deuten stark auf ein chinesisches Engagement hin (Shakarian et al., 2013). Krekel begründet die staatliche Beteiligung folgendermassen: *„The operators appear to have access to financial, personnel, and analytic resources that exceed what organized cybercriminal operations or multiple hacker groups operating independently could likely access consistently over several years. Furthermore, the categories of data stolen do not have inherent monetary value like credit card numbers or bank account information that is often the focus of cybercriminal organizations. Highly technical defense engineering information, military related information, or government policy analysis documents are not easily monetized by cybercriminals unless they have a nation-state customer, making the activity "state-sponsored" by default, regardless of the affiliation of the actual operators at the keyboard"* (Krekel, 2009, p. 52).

2.3.4 Sabotage

Bei der Sabotage liegt das Ziel in der Manipulation eines gegnerischen Systems, sodass dem Gegner ein Schaden entsteht. Wenn sich der Angreifer einmal Zugriff auf ein System verschafft hat und entsprechende Rechte vorhanden sind, können viele unterschiedliche Methoden angewendet werden, um Schaden zu verursachen. *„Die durch die Funktionsvielfalt der Computer angelegten, vielen unterschiedlichen Möglichkeiten der Vernichtung, Störung und Manipulation bieten ein bislang nicht dagewesenes Spektrum an Handlungsoptionen"* (Gaycken, 2011, p. 123). Diese verschiedenen Möglichkeiten haben deshalb auch unterschiedliche Auswirkungen, weshalb bei der Sabotage die Verletzung aller drei Prinzipien der Informationssicherheit (*Confidentiality*, *Integrity* & *Availability*) möglich ist. Im Folgenden werden einige dieser Handlungsoptionen erläutert.

- Manipulation von Informationen:

  Bei dieser Taktik geht es darum, gezielt falsche Informationen in gegnerische Informationssysteme zu platzieren oder bestehende Informationen zu verändern. Deshalb ist diese Taktik, im Sinne der drei Prinzipien der Informationssicherheit, primär eine Verletzung der *Integrity*. Es ist aber möglich, dass auch die *Confidentiality* verletzt wird, da der Gegner eventuell auf vertrauliche Informationen stösst.

  Diese taktische Desinformation ist ein wichtiges Konzept des *Information Warfare*[9], wessen Ideen auch Anwendung im Cyberwarfare finden, aller-

[9] Synonym verwendet zu Information Operations: "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own" (Joint Chiefs of Staff 2012, p. 66).

dings mit digitalen Mitteln. Die Desinformation soll primär gegnerische Entscheidungsträger in ihren Entscheidungen behindern.

So könnte zum Beispiel eine Nation X, falsche oder widersprüchliche GPS-Daten der Truppen von Nation Y, in deren C4ISR-System[10] einspeisen. Deren Kommandant könnte dann zögern, seinen Truppen weitere Befehle zu erteilen, aus der Angst, dass er sie in einen Hinterhalt schicken würde. Dies kann der Nation X einen taktischen Vorteil verschaffen (Gaycken, 2011). Eine weitere Möglichkeit besteht darin, beim Gegner falsche oder fehlerhafte Baupläne wichtiger Infrastrukturen, militärischen Einrichtungen oder Waffen zu platzieren. So hat es die CIA während dem Kalten Krieg geschafft, bei der Sowjetunion sabotierte Baupläne einer Ölpipeline in Sibirien zu hinterlegen, damit diese bei hoher Belastung explodiert. Diese wurde dann nach diesen fehlerhaften Plänen gebaut und explodierte mit der Explosionskraft einer 3-Kilotonnen-Atombombe (Reed, 2004).

Es existieren aber auch harmlosere, dafür durchaus öfter vorkommende Ausprägungen dieser Taktik, wie zum Beispiel *Website Defacement*. Dabei werden Webseiten gehackt und deren Inhalt verändert. Diese Art der Attacke ist relativ einfach auszuführen, da Webseiten in der Regel kein sehr hohes Schutzniveau aufweisen. Deshalb wird Website Defacement oft von *Hacktivists* benutzt, um die Reputation ihrer Gegnern zu schädigen oder ihre eigene Propaganda auf deren Website zu verbreiten (Shakarian et al., 2013).

- Störung und Zerstörung von Systemen, Prozessen oder Infrastrukturen:

  Unabhängig davon, welche Art von System angegriffen wird, besteht die Möglichkeit dieses zu stören oder zu zerstören. Will man ein System stören, so wird dieses insofern verändert, dass es nicht mehr wie von den Betreibern vorgesehen funktioniert. Demzufolge ist dies eine Verletzung der *Integrity* jenes Systems. Je nach Angriff kann das System aber auch temporär unverfügbar gemacht werden, in welchem Fall auch die *Availability* verletzt würde. Da eine Vielzahl verschiedener Systeme, mit unterschiedlichem Zweck, Funktionen und Aufbau existieren, sind die Möglichkeiten für Sabotage nahezu unbegrenzt. Es sind Sabotageakte an militärischen, wie auch an zivilen Einrichtungen möglich. Ein denkbares militärisches Szenario wäre die Störung von gegnerischen Radarwarn- oder Luftabwehrsystemen, im Vorfeld eines Luftangriffs, um der eigenen Luftwaffe eine sichere Flugroute zu ermöglichen (Gaycken, 2011). Ein ziviles Szenario könnte die Störung des

[10] "C4ISR steht für "Command, Control, Computer, Communication, Intelligence, Surveillance, Reconnaissance". Sie ist ein neues technostrategisches Paradigma intensiver organisatorischer und informationstechnischer Vernetzung aller Streitkräfte miteinander. Die gesamte Lage soll sekundengenau über die gesamten Streifkräfte hinweg erfasst, Kommandofähigkeiten entsprechend erhöht werden" (Gaycken, 2011, p. 40).

Stromnetzes eines Gegners sein, um einen Stromausfall zu erzeugen. Die Motivation dahinter wäre höchst wahrscheinlich der ökonomische Schaden, der beim Gegner entstehen würde. Ein Report von ICF Consulting (2003) schätzt, dass die Kosten des Stromausfalls im Nordosten der USA im Jahre 2003 zwischen $6.8 Mrd. und $10.3 Mrd. betragen. Zudem wird erwähnt, dass eine koordinierte, gezielte Attacke zu weitaus höheren Kosten führen könnte.

Bei der Zerstörung eines Systems wird ähnlich vorgegangen, wie bei der Störung eines Systems. Der Unterschied liegt darin, dass bei der Zerstörung permanente Schäden erzielt werden. Diese können direkt an Systemen oder auch an Infrastrukturen erfolgen, welche von einem System gesteuert werden. Wenn der Schaden direkt an einem System verursacht wird, dann können entweder Daten gelöscht werden, in dem zum Beispiel die Festplatte formatiert wird. Oder es kann auch die Hardware zerstört werden, beispielsweise indem sie gezielt überhitzt wird (Gaycken, 2011). Wenn die Kontrollsysteme (sogenannte ICS) von kritischen Infrastrukturen[11] angegriffen werden, wie zum Beispiel Dämme, Kraftwerke oder Ampelsysteme des Verkehrs, dann kann dies physische Schäden zur Konsequenz haben.

Solche Angriffe müssen nicht unmittelbar durchgeführt werden, sondern können zeitlich verzögert werden. Ein Angreifer hat verschiedene Möglichkeiten den Angriff verzögert durchzuführen. Er kann einen Timer einbauen, welcher nach dem Ablauf einer fix eingestellten Zeit, die Sabotage startet. Möglich ist auch, dass ein logischer Mechanismus installiert wird, welcher oft auch als *Logic Bomb* bezeichnet wird. Dabei kann eine frei wählbare Kondition festgelegt werden, welche erfüllt sein muss, damit die Sabotage eingeleitet wird. Beispielsweise könnte man festlegen, dass ein Angriff nur dann durchgeführt wird, wenn der Gegner im Ernstfall zu einem Angriff mobilisiert. So wären im Prinzip auch präventive Sabotagen möglich.

Diese zeitliche Verzögerung eines Angriffs bietet vor allem zwei Vorteile. Zum einen können vor der eigentlichen Durchführung der Sabotage, die eigenen Spuren verwischt werden. Andererseits bietet es sich an, mittels eines Timers, mehrere Sabotageakte zeitlich zu koordinieren und gleichzeitig ablaufen zu lassen. Damit kann die Wirkungskraft erhöht werden, was vor allem bei grösseren militärischen Kampagnen interessant sein kann (Gaycken, 2011).

2.4 Angriffsziele

Im letzten Kapitel (2.3) wurden verschiedene Strategien im Cyberwarfare erläutert. In diesem Kapitel werden mögliche Angriffsziele dieser Strategien näher betrachtet.

[11] Siehe Kapitel 2.4.1 Kritische Infrastrukturen

Dabei wird auf deren Charakter, Auswirkungen durch einen Angriff und der einhergehenden Motivation für den Angriff eingegangen.

2.4.1 Kritische Infrastrukturen

Kritische Infrastrukturen sind Einrichtungen, welche das Funktionieren von Staat, Gesellschaft und Wirtschaft, durch die Bereitstellung von zentralen Gütern und Dienstleistungen ermöglichen. Ihr Ausfall hätte schwerwiegende Folgen für diese drei Entitäten (VBS, 2012; Lewis, 2002). Dazu gehört unter anderem die Wasserversorgung, Energieversorgung, Kommunikationsinfrastruktur, Verkehrsinfrastruktur und Finanzinfrastruktur. Diese kritischen Infrastrukturen werden meist von sogenannten *Industrial Control Systems (ICS)* betrieben, welche auch als *Supervisory Control and Data Acquisition (SCADA)* Systeme bezeichnet werden. Ihre Aufgabe ist hauptsächlich die Überwachung und Kontrolle von verschiedensten Prozessen. Oft sind diese ICS veraltet und besitzen deshalb eine ungenügende Systemsicherheit. Zudem sind einige von ihnen nicht von der Aussenwelt abgeschnitten, was sie über das Internet angreifbar macht (Vernez, personal communication, 2014a).

Interessant ist die Tatsache, dass ein Ausfall eines ICS Systems, und somit einer kritischen Infrastruktur, Kettenreaktionen verursachen kann. Denn kritische Infrastrukturen sind eng mit unserer Wirtschaft und Gesellschaft verbunden, welche ein soziotechnisches System darstellen. Fällt die kritische Infrastruktur aus, dann erleidet auch dieses System einen teilweisen oder vollständigen Kollaps. Dies führt zu ökonomischen Schäden. Es wird zwischen intrainfrastrukturellen und interinfrastrukturellen Folgen unterschieden (Gaycken, 2011). Wenn ein partieller Ausfall innerhalb einer Infrastruktur zum Ausfall eines rein infrastrukturinternen Funktionsgefüge führt, spricht man von intrainfrastrukturellen Folgen. Wenn hingegen ein partieller oder vollständiger Ausfall einer Infrastruktur zum Ausfall weiterer, angegliederten Infrastrukturen führt, handelt es sich um interinfrastrukturelle Folgen (Beer, 2005). Ein Beispiel für eine interinfrastrukturelle Folge wäre ein Ausfall des Stromnetzes. Da alle Infrastrukturen Strom benötigen, um zu funktionieren, wären auch die Wasserversorgung, Kommunikationsinfrastruktur und Finanzinfrastruktur betroffen. Die genauen Folgen sind aber schwer abzuschätzen. Denn einerseits sind die einzelnen Infrastrukturen und deren ICS relativ komplex. Andererseits sind die Abhängigkeiten zwischen den einzelnen Infrastrukturen noch wenig erforscht (Gaycken, 2011).

Zudem können diese Attacken auch physische Schäden zur Folge haben (Winterfeld & Andress, 2013). Das beste, bislang bekannte Beispiel hierfür ist der *Stuxnet-Wurm*. Dieser hat sich Zugriff auf die ICS der iranischen Urananreicherungsanlage in Natanz verschafft. Dadurch konnte die Rotationsgeschwindigkeit der Zentrifugen verändert werden, was zur Zerstörung von über 10% der vorhandenen Zentrifugen geführt hat. Interessanterweise konnten die Angreifer das System überlisten, so dass es keinen Fehlbetrieb meldete und der Schaden erst zu spät bemerkt wurde (Albright, Brannan, & Walrond, 2010).

2.4.2 Wirtschaft

Die Wirtschaft kann mit zwei unterschiedlichen Absichten angegriffen werden. Einerseits kann ein Angreifer das Ziel verfolgen, seinem Gegner einen ökonomischen Schaden zuzufügen. Er wird dann mittels Sabotage[12] versuchen die gegnerische Volkswirtschaft zu schwächen. Andererseits kann er aber auch, mittels Diebstahl von Geschäftsgeheimnissen im Rahmen der Wirtschaftsspionage[13], die eigene Volkswirtschaft stärken. Es ist zu beachten, dass zwischen diesen beiden Absichten keine scharfe Trennlinie verläuft. So kann zum Beispiel ein ausspioniertes Unternehmen durchaus systemrelevant sein.

Wenn ein Angreifer dem Gegner ökonomischen Schaden zufügen will, dann wird er sich primär auf die Sabotage systemrelevanter Unternehmen konzentrieren. Denn systemrelevante Unternehmen erbringen für eine Volkswirtschaft zentrale Leistungen, auf welche nicht verzichtet werden kann. Zudem können diese Leistungen nicht durch andere Marktteilnehmer in einer Frist ersetzt werden, welche für die Volkswirtschaft tragbar ist. Weitere Merkmale systemrelevanter Unternehmen sind deren Grösse, Marktkonzentration, und hohe Vernetzung mit anderen Unternehmen (Expertenkommission zur Limitierung von volkswirtschaftlichen Risiken durch Grossunternehmen, 2010). Deshalb sind, nebst den direkten Folgen eines Ausfalls oder Beeinträchtigung eines systemrelevanten Unternehmens, auch Kettenreaktionen zu erwarten, wodurch weitere, potentiell systemrelevante Unternehmen beeinträchtigt werden können. Laut der Theorie der *Self-organized Criticality,* können in hochkomplexen Systemen, wie beispielsweise einer Volkswirtschaft, bereits kleine Ereignisse, massive und unvorhersehbare Auswirkungen haben (Schneider, 2011). Daraus kann gefolgert werden, dass bereits temporäre Ausfälle solcher systemrelevanten Unternehmen zu massiven, wirtschaftlichen Schäden führen können. Welche Unternehmen systemrelevant sind, hängt vom jeweiligen Staat ab, da in unterschiedlichen Ländern andere Sektoren der Volkswirtschaft relevant sind. Grosse Finanzinstitute (z.B. Banken) werden jedoch in vielen Ländern als systemrelevant bezeichnet, da sie zentrale Dienstleistungen, wie zum Beispiel den Zahlungsverkehr und die Kreditvergabe, für die gesamte Volkswirtschaft bereitstellen. Andere Unternehmen hängen stark von diesen Finanzdienstleistungen ab und können ohne sie nicht funktionieren.

Wenn ein Angreifer mittels Diebstahl von Geschäftsgeheimnissen im Rahmen der Wirtschaftsspionage die eigene Volkswirtschaft stärken will, kann er ein breites Spektrum von Unternehmen verschiedener Branchen anvisieren. Denn praktisch alle Unternehmen besitzen Geschäftsgeheimnisse, aus welchen möglicherweise Kapital geschlagen werden kann. Besonders interessant scheinen aber technologische Unternehmen zu sein, welche viel Kapital in Forschung und Technologie investieren (Thorleuchter & Van den Poel, Dirk, 2013). Diese neu erforschten Technologien sind für ein Unternehmen natürlich sehr wertvoll. Denn häufig sind diese Technologien

[12] Siehe Kapitel 2.3.4 Sabotage
[13] Siehe Kapitel 2.3.3 Cyberspionage

nicht unternehmensspezifisch und können deshalb auf verschiedene Unternehmen angewandt werden (Kaperonis, 1984). Andererseits kann eine neue Technologie einem Unternehmen einen erheblichen Wettbewerbsvorteil gegenüber der Konkurrenz beschaffen. Zudem sind eigene Forschungs- und Entwicklungsprojekte sehr teuer und aufwändig (Gaycken, 2011).

2.4.3 Militär

Militärische Einrichtungen werden zunehmend von IT-Systemen betrieben, da somit neue strategische Möglichkeiten eröffnet werden und deren Betreibung ökonomischer wird. Die heutigen Militärs, vor allem diejenigen des Westens, stützen sich mittlerweile so stark auf die Technik, dass praktisch keine Einrichtungen mehr ohne IT-Systeme funktionieren können (Gaycken, 2011). Als Beispiele sind einerseits einzelne Waffensysteme zu nennen, wie zum Beispiel Kampfflugzeuge, Drohnen oder Luftabwehrsysteme, andererseits aber auch koordinierende Systeme, wie Kommunikations-, Überwachungs- und Navigationssysteme.

In den letzten Jahren hat sich zusätzlich ein neuer Trend abgezeichnet, nämlich die zunehmende Vernetzung von militärischen IT-Systemen. Dieser Trend wird als *C4ISR-Kriegsführung* bezeichnet, wobei C4ISR für „Command, Control, Computer, Communication, Intelligence, Surveillance, Reconnaissance“ steht. Dabei werden sämtliche militärische IT-Systeme zusammengeschlossen, um einen Informationsaustausch zu ermöglichen. Das Ziel dabei ist es, Informationen über die gesamten Streitkräfte zusammenzutragen, zu verarbeiten und an die richtigen Entscheidungsträger zu verteilen. Somit sollen Entscheidungen und Befehle auf verschiedensten Stufen erleichtert und effizienter gemacht werden (Gaycken, 2011).

Militärische Einrichtungen waren schon vor der Einführung der Technik interessante Angriffsziele. Durch ihre technologische Abhängigkeit sind sie nun auch im Rahmen des Cyberwarfare zu interessanten Angriffsvektoren geworden. Ein Angriff ist dadurch viel einfacher, da dieser vergleichsweise kostengünstig aus der Distanz und ohne grosse Risiken ausgeführt werden kann (Gaycken, 2011). Dabei können verschiedene Strategien[14] verfolgt werden.

Zum einen enthalten militärische IT-Systeme wertvolle Informationen, welche mittels Cyberspionage[15] gestohlen werden können. Ein bekannter Vorfall ereignete sich 2009, als die USA feststellen mussten, dass Daten ihres teuersten Waffenprogramms, dem Joint Strike Fighter-Programm, von den Systemen einiger ihrer Contractors entwendet wurden. Dieses $300 Mrd. teure Programm befasst sich mit der Entwicklung und Beschaffung eines neuen Kampfflugzeugs, dem F-35 Lightning II. Es wurden Daten über das Design und die elektronischen Systeme des Flugzeugs

[14] Siehe Kapitel 2.3 Strategien und Absichten
[15] Siehe Kapitel 2.3.3 Cyberspionage

gestohlen. Das genaue Ausmass des Schadens, bezüglich der Sicherheit des Waffenprogramms und der Finanzen, ist bislang nicht bekannt. Die USA vermuten, dass China hinter dem Diebstahl steckt (Gorman, Cole, & Dreazen, 2009).

Zum anderen kann es taktisch sinnvoll sein, ein militärisches System zu sabotieren. Es ist insbesondere denkbar, dass diese Sabotage zur Unterstützung von konventionellen Militäroperationen geschieht. Dabei können einerseits gegnerischen Entscheidungsträger falsche Informationen zugespielt werden, wodurch diese in ihrer Entscheidungsfähigkeit behindert werden. Andererseits kann die Kontrolle von militärischen Einrichtungen, wie zum Beispiel von Waffensystemen, übernommen werden, um diese zu stören oder zerstören. Spezifische Vorfälle solcher Sabotage sind bisher jedoch nicht bekannt. Nicht zuletzt, da es sowohl im Interesse des Angreifers wie auch des Angegriffenen liegt, solche Vorfälle nicht publik zu machen. Der Angreifer will Schwachstellen des Gegners exklusiv nutzen können und der Angegriffene will diese Schwachstellen nicht weiteren Parteien mitteilen (Gaycken, 2011). Solche Szenarien sind aber durchaus denkbar, da jedes IT-System Sicherheitslücken besitzt und somit angreifbar ist.

Die Möglichkeiten an Szenarien sind sehr zahlreich, da sehr viele unterschiedliche militärische Systeme existieren. Einige dieser Szenarien wurden schon im Kapitel 2.3.4, über Sabotage, angesprochen.

3 Vorsorgeprinzip

In diesem Kapitel wird das Vorsorgeprinzip (VSP) erklärt, um es später zur Beurteilung der Massnahmen der Schweiz, hinsichtlich der Risikosituation des Cyberwarfare, zu benutzen. Im Unterkapitel 3.1 wird das VSP definiert und verschiedene Ausprägungen dessen erläutert. Danach wird in den Unterkapitel 3.2 und 3.3 gezeigt, wie das VSP in zwei verschiedenen Gebieten angewendet wird, um das Verständnis für das VSP und dessen Anwendung im Kontext des Cyberwarfare zu erhöhen.

3.1 Definition

Das Vorsorgeprinzip (VSP) wird in der Wissenschaft sehr unterschiedlich aufgefasst. In dieser Arbeit wird die Definition von Hilty et al. benutzt, welche das VSP folgendermassen definieren:

„Das Vorsorgeprinzip (VSP) dient dem Umgang mit Risiken in Situationen, in denen keine akute Gefährdung gegeben ist. Es hat den Zweck, auch solche Risiken zu minimieren, die sich möglicherweise erst langfristig manifestieren, und Freiräume für zukünftige Entwicklungen zu erhalten“ (Hilty et al., 2003, p. 29).

Im Gegensatz zum *Prinzip der Gefahrenabwehr*, welches nur die Abwehr akuter Gefahren vorsieht, muss beim VSP keine imminente Gefahr bestehen und auch keine wissenschaftlichen Beweise vorliegen um Regulierungsmassnahmen zu ergreifen (Hilty et al., 2003). Beim VSP wird also proaktiv gehandelt, wenn ein potentielles Risiko erkannt wird und nicht erst, wenn eine akute Gefahr besteht (Kloepfer, 2004).

Das VSP hat zwei unterschiedliche Begründungen, welche als eigene Theorien in der juristischen Literatur vorzufinden sind. Zum einen die *Ignoranz-Theorie*, welche das Treffen von Massnahmen durch den eingeschränkten Wissensstand, und die daraus resultierende Ungewissheit rechtfertigt. Somit sollen auch ungeklärte Risiken in Betracht gezogen werden. Zum anderen die *Freiraum-Theorie*, welche aussagt, dass das VSP für den Erhalt von Handlungsfreiräumen zukünftiger Generationen eingesetzt werden soll. Dies kann dadurch erfolgen, dass zum Beispiel bei umweltbelastenden Vorgängen, das gesetzlich erlaubte Belastungslimit nicht vollkommen ausgeschöpft wird (Beyer, 1992; Koechlin, 1989).

Es lassen sich zwei extreme Ausprägungen des VSP feststellen, das *schwache* und das *starke* VSP. Das schwache VSP sagt aus, dass Regulierungsmassnahmen nur ergriffen werden sollen, wenn man mit grossen, irreversiblen Risiken konfrontiert ist, das wissenschaftliche Nachweisniveau hoch ist und die Kosten dieser Massnahmen relativ gering sind. Das starke VSP besagt, dass Regulierungsmassnahmen auch zu

treffen sind, wenn bereits kleinere, reversible Risiken vorliegen, nur spekulative Hinweise existieren und wenn die Kosten der Massnahmen hoch sind (Sandin, 1999; Van den Daele, Wolfgang, 2001; Wiener, 2001).

Die praktische Anwendung des Vorsorgeprinzips, findet meist zwischen diesen beiden extremen Ausprägungen statt. Insbesondere das starke VSP ist realitätsfremd und deshalb kaum durchsetzbar. Denn dessen Durchsetzung hätte zur Folge, dass wissenschaftliche Beweise für jegliche Vorgänge geliefert werden müssten, bevor diese gesetzlich erlaubt würden (Marti, 2011).

3.2 Anwendung in der Umweltpolitik, Umweltrecht und Umweltschutz

Das Vorsorgeprinzip ist aus der Diskussion über den Umweltschutz entstanden und findet auch heute vor allem in diesem Bereich Anwendung.

In den 1960er Jahren ist sich die Öffentlichkeit erstmals bewusst geworden, dass unsere Umwelt nicht unbegrenzt verschmutzt werden kann, ohne langfristige Schäden an der Umwelt und der Gesundheit des Menschen in Kauf zu nehmen. Folglich wurde im Rahmen der Umweltpolitik diskutiert, wie mit den natürlichen Ressourcen umzugehen ist. Parallel dazu entstand das Umweltrecht, welches sich aber anfänglich nur mit Problemen befasste, welche bereits eingetreten waren, also mit der Gefahrenabwehr (Marti, 2011). Dabei wurden zum Beispiel gesetzliche Grenzwerte für umweltschädigende Aktivitäten erlassen. Jedoch nur für diejenigen, für welche wissenschaftlich nachweisliche Risiken bestanden.

Die ersten Ansätze des Vorsorgeprinzips lassen sich im Umweltbericht der deutschen Bundesregierung, 1976 finden: „Umweltpolitik erschöpft sich nicht in der Abwehr drohender Gefahren und der Beseitigung eingetretener Schäden. Vorsorgende Umweltpolitik verlangt darüber hinaus, dass die Naturgrundlagen geschützt und schonend in Anspruch genommen werden“ (Deutscher Bundestag, 1976, p. 8).

Seither hat das Vorsorgeprinzip auch in anderen internationalen Gesetzgebungen Einzug gefunden. In der Schweiz zum Beispiel ist das VSP seit 1983 im Umweltschutzgesetz (USG) verankert:

- Artikel 1, Abs. 2: „Im Sinne der Vorsorge sind Einwirkungen, die schädlich oder lästig werden könnten, frühzeitig zu begrenzen“ (Bundesgesetz über den Umweltschutz (Umweltschutzgesetz, USG), 1983).

- Artikel 11, Abs. 2: „Unabhängig von der bestehenden Umweltbelastung sind Emissionen im Rahmen der Vorsorge so weit zu begrenzen, als dies technisch und betrieblich möglich und wirtschaftlich tragbar ist“ (Bundesgesetz über den Umweltschutz (Umweltschutzgesetz, USG), 1983).

Trotz dieser gesetzlichen Verankerung des Vorsorgeprinzips ist es immer wieder passiert, dass frühe Warnungen ignoriert wurden und nachhaltige Schäden an der Umwelt und dem Menschen entstanden sind. Der "Late lessons from early warnings"-Report der European Environment Agency (EEA) hat einige dieser Fälle untersucht, unter anderem die Beschädigung der Ozonschicht durch Halogenkohlenwasserstoff, die Überfischung der Ozeane und Verstrahlung durch Röntgen. Die EEA zieht zwölf Lehren aus diesen Ereignissen, welche unter anderem die Chancen erhöhen sollen, kostenträchtige Auswirkungen frühzeitig zu antizipieren (European Environment Agency [EEA], 2001).

Aktuelle Beispiele, welche momentan diskutiert werden sind die Gen- und Nanotechnologie. Beide Technologien versprechen gesellschaftliche, wirtschaftliche, wie auch medizinische und ökologische Fortschritte. Durch ihre Komplexität sind aber die genauen Auswirkungen auf den Menschen und die Umwelt unbekannt.

3.3 Anwendung in der ICT

Das Vorsorgeprinzip ist zwar aus dem Bereich des Umweltschutzes entstanden, doch handelt es sich dabei um ein sehr generelles Prinzip. Deshalb kann es auch auf andere Bereiche angewendet werden, beispielsweise auf die Informations- und Kommunikationstechnologie (ICT). Denn neue Technologien bieten für die Gesellschaft zwar viele Chancen, jedoch tragen sie auch gewisse Risiken mit sich. Neben den aus dem Umweltschutz bekannten Risiken für die Umwelt und Gesundheit, können Technologien auch soziale Risiken mit sich tragen. So kann eine neue Technologie Veränderungen in unseren sozialen Regeln und Strukturen hervorrufen (Som, Hilty, & Köhler, 2009). Som et al. (2009) haben elf soziale Problemfelder identifiziert (siehe Tabelle 2), welche durch die ICT entstanden sind.

Privacy	Where does individual freedom to collect data end, in conflict with the right to information self-determination (which stems from the principle of autonomy)?
Security	What level of security for an information system needs to be guaranteed for it to be responsible to use the system? Who is responsible for security flaws? Is it a criminal act or a service to society to identify and publicize security flaws?
Unmastered complexity	In the case of complex, and particularly distributed, information systems, it is generally not possible to give a formal guarantee of certain properties of such systems. Does the increasing dependence on such systems result in a loss of decision-making responsibility?
Free speech	What are the limits of the right to free speech with respect to the use of electronic media, when it comes into conflict with

	other fundamental rights? May or should there be censorship of Internet content?
Intellectual property	Where is the boundary between information as public property, which must be available to everyone for reasons of social justice, and intellectual property, over which the owner has autonomous control?
Digital divide	The jeopardisation of social justice through the division of society into those who have access to the information society and those who are excluded, e.g. low-income households, the elderly, those with disabilities (also known as the 'global digital divide': the ICT gap between developed and developing countries)
Education	Changes to the education process through the use of ICT and the implications for social justice
Gender issues	How does the use of ICT in the workplace and in private life change social justice between genders?
Cultural diversity	What effect does ICT have on social justice between different cultures (e.g. dominance of the English language)? Will cultural diversity be preserved for future generations?
Cultural heritage	Will future generations still be able to share in our knowledge if today's digital storage media are no longer readable in the future?
Autonomy, dependability and trust	Does the increasing dependence on ICT infrastructures threaten the autonomy of the individual? Will we be forced, because of the complexity of structures, to trust without having sufficient verification facilities?

Tabelle 2: Elf soziale Problemfelder, die durch ICT hervorgerufen wurden (in Anlehnung an Table I aus Som et al., 2009, p. 496–496).

Ein aktuelles Beispiel im Bereich der ICT, welches potentielle Risiken mit sich trägt, ist *Pervasive Computing,* auch *Ubiquitous Computing* genannt. Pervasive Computing „involves the miniaturization and embedding of microelectronics in non-ICT objects and wireless networking, making computers ubiquitous in the world around us" (Som et al., 2009, p. 496). Computer werden also in alltägliche Gegenstände eingebettet und sind so zunehmend omnipräsent in unserem Alltag. Diese Miniaturcomputer können mit Sensoren ausgestattet sein, untereinander kommunizieren und uns somit in verschiedenen Bereichen des Lebens unterstützen (Hilty et al., 2003).

Pervasive Computing wirft einige Fragen bezüglich dessen Risiken auf, welche in der Gesellschaft diskutiert werden müssen. Diese lassen sich zu einem grossen Teil den elf Problemfeldern der Tabelle 2 zuordnen. Ein Beispiel ist die unbeherrschte Komplexität. Da Pervasive Computing zunehmend komplexere Computersysteme untereinander vernetzt, ist das Verhalten solcher Systeme schwierig vorherzusagen (Hilty

et al., 2003). Ein weiteres Beispiel ist die Privatsphäre, welche durch Pervasive Computing bedroht ist. Denn Computer sind zusehends im Alltag vertreten und in alltäglichen Gegenständen versteckt. Dieser Umstand kann dazu führe, dass diese Computer zu Überwachungszwecken missbraucht werden (Hilty et al., 2003).

4 Fallbeispiel Schweiz

Der Bundesrat hat am 10. Dezember 2010 das *Eidgenössische Departement für Verteidigung, Bevölkerungsschutz & Sport (VBS)* damit beauftragt, eine Strategie zu erarbeiten, welche die Schweiz vor Cyberrisiken schützen soll. Am 27. Juni 2012 verabschiedete der Bundesrat die *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)*. Diese befasst sich einerseits mit der Analyse der aktuellen Lage, in welcher die durch Cyberrisiken bedrohten Strukturen (z.B. kritische Infrastrukturen) und die daraus resultierenden Cyberrisiken erhoben werden. Andererseits befasst sich die NCS mit der Planung eines Dispositivs zum Schutz vor Cyberrisiken. Innerhalb dieses Dispositivs sind 16 Massnahmen ausgearbeitet worden, welche in 4 Bereiche unterteilt werden können (VBS, 2012). Die NCS wurde 2013 durch den *Umsetzungsplan NCS* erweitert. Dieser spezifiziert einerseits grob, wie und wann diese Massnahmen umgesetzt werden sollen. Die genauen Aufgaben und Pflichten zur Umsetzung der Massnahmen sind aber den jeweils zuständigen Departementen und Ämtern freigestellt. Andererseits wird im Umsetzungsplan NCS festgehalten, wie die Zusammenarbeit zwischen den involvierten Departementen und Ämtern ablaufen soll (Informatiksteuerungsorgan des Bundes [ISB], 2013).

Es muss an dieser Stelle erwähnt werden, dass sich die NCS mit einem breiteren Spektrum von Cyberrisiken befasst als nur Cyberwarfare. Diese gefährden aber nicht alle die nationale Sicherheit eines Staates, wie zum Beispiel Cyberkriminalität. Diese Risiken entsprechen somit nicht der Definition von Cyberwarfare in dieser Arbeit[16]. Dementsprechend werden die Massnahmen der NCS Strategie hinsichtlich der Definition in Kapitel 2.1 bewertet.

Im Kapitel 4.1 werden die Risiken des Cyberwarfare für die Schweiz erläutert. Da diese bereits in der NCS erarbeitet wurden, werden diese mehrheitlich daraus entnommen, jedoch durch eigene Analysen und Einschätzungen erweitert. Diese Risiken aus der NCS werden aber auch durch eigenhändig identifizierte Risiken erweitert. Danach werden im Kapitel 4.2 die geplanten Massnahmen der NCS, hinsichtlich ihrer Ziele, Planung und Umsetzung erläutert. Diese getroffenen Massnahmen können aber selbst Risiken mit sich tragen. Zum Beispiel können Überwachungsmassnahmen die Privatsphäre der Bürger einschränken, wie die globale Überwachungs- und Spionageaffäre der *National Security Agency (NSA)* gezeigt hat. Diese Risiken der Massnahmen werden im Kapitel 4.3 identifiziert und besprochen.

[16] Siehe Kapitel 2.1 Definition

4.1 Risiken des Cyberwarfare

Die Risiken des Cyberwarfare für die Schweiz ergeben sich im Prinzip aus den im Kapitel 2.4 genannten Angriffszielen des Cyberwarfare: kritische Infrastrukturen, die Wirtschaft und das Militär.

Es ist zu erwähnen, dass die Abgrenzung zwischen kritischen Infrastrukturen und der Wirtschaft nicht ganz trennscharf ist. Denn gewisse Betreiber kritischer Infrastrukturen werden nicht vom Staat, sondern von privaten Unternehmen bereitgestellt, wie zum Beispiel die Finanzinfrastruktur durch die *SIX AG* oder ein Teil der Stromversorgung durch die *Alpiq Holding AG*. Die NCS erfasst wichtige Unternehmen (wie z.B. Banken) als Teil der kritischen Infrastrukturen. Deshalb wird in diesem Kapitel bewusst nicht zwischen kritischen Infrastrukturen und der Wirtschaft unterschieden.

Die Armee ist in der vom Bundesamt für Bevölkerungsschutz (2012b) erarbeiteten *Nationalen Strategie zum Schutz kritischer Infrastrukturen* als Teil dieser kritischen Infrastrukturen aufgeführt (siehe Tabelle 3). Im Kontext des Cyberwarfare kommt ihr aber eine spezielle Bedeutung zu, weshalb sie in einem separaten Unterkapitel behandelt wird.

In diesem Kapitel werden die Ausprägungen dieser Angriffsziele in der Schweiz erläutert. Zuerst werden die Risiken für kritische Infrastrukturen, inklusive der wichtigen privaten Unternehmen besprochen, danach diejenigen für die Schweizer Armee.

4.1.1 Kritische Infrastrukturen

Die Schweiz hat parallel zur NCS eine *Nationale Strategie zum Schutz kritischer Infrastrukturen* erarbeitet. Darin wurde der Bestand der kritischen Infrastrukturen, welche in Sektoren und Teilsektoren unterteilt sind, und deren Kritikalität erhoben (siehe Tabelle 3). Im Folgenden werden einige dieser Sektoren und Teilsektoren besprochen. Dabei wird einerseits erläutert, welche Art von Angriffe[17] auf diese Sektoren möglich sind. Andererseits werden strategisch wichtige Akteure und Unternehmen genannt, welche konkrete Ziele eines Angriffs sein könnten. Die Auswahl dieser Akteure und Unternehmen basiert auf deren Systemrelevanz[18], ihrer strategischen Bedeutung bezüglich der Sicherheitspolitik, ihrem geistigen Eigentum (z.B. Technologien) und ihrer Unternehmensgrösse, welche auf deren Umsatz und Anzahl Mitarbeiter beruht (Handelszeitung & Bisnode, 2013).

[17] Siehe Kapitel 2.3 Strategien und Absichten
[18] Siehe Kapitel 2.4.2 Wirtschaft

Sektoren	Teilsektoren
Behörden	Diplomatische Vertretungen und Sitze internationaler Organisationen
	Forschung und Lehre
	Kulturgüter
	Parlament, Regierung, Justiz, Verwaltung
Energie	Erdgasversorgung
	Erdölversorgung
	Stromversorgung
Entsorgung	Abfälle
	Abwasser
Finanzen	**Banken**
	Versicherungen
Gesundheit	Ärztliche Betreuung und Spitäler
	Labors
Industrie	Chemie- und Heilmittelindustrie
	Maschinen-, Elektro- und Metallindustrie
Information und Kommunikation	**Informationstechnologien**
	Medien
	Postverkehr
	Telekommunikation
Nahrung	Lebensmittelversorgung
	Wasserversorgung
Öffentliche Sicherheit	Armee
	Blaulichtorganisationen (Polizei, Feuerwehr, Sanität)
	Zivilschutz
Verkehr	Luftverkehr
	Schienenverkehr
	Schiffsverkehr
	Strassenverkehr
	Sehr grosse Kritikalität*
	Grosse Kritikalität*
	Reguläre Kritikalität*

* – Die Kritikalität steht für die relative Bedeutung des Teilsektors bezüglich Bevölkerung, Wirtschaft und Dependenzen (≠ absolute Bedeutung). Zur Ableitung eines allfälligen Handlungsbedarfs sind zusätzlich jeweils die konkrete Bedrohungslage und die Verletzlichkeit der kritischen Infrastrukturen zu berücksichtigen.
– Die Gewichtung macht keine Aussagen über die Kritikalität von Einzelobjekten.
– Die Gewichtung orientiert sich an einer normalen Gefährdungslage.

Tabelle 3: Kritischen Infrastrukturen der Schweiz und jeweiliger Kritikalität (BABS, 2012b, p. 5)

4.1.1.1 Telekommunikation

Die Telekommunikationsinfrastruktur ist für die Übertragung von Informationen zuständig und umfasst unter anderem Vermittlungseinrichtungen, Satellitennetze, Netze für Hör- und Fernsehfunk, sowie Kabelfernsehnetze.

„Die Telekommunikation ist ein grundlegender Bestandteil moderner Gesellschaften und dient der Wirtschaft, dem Staat und der Bevölkerung als Mittel zum Austausch von Informationen. Beispiele für Telekommunikationsmittel sind das Telefon, der Telefax, das Mobiltelefon, der Internet-PC, etc. . . . Die Telekommunikation durchdringt immer stärker unser Berufs- und Privatleben. Aus wirtschaftlicher Perspektive treten vor allem die enormen Effizienzsteigerungen hervor, sei es in der Wirtschaft (verbesserte Produktions- und Arbeitsabläufe etc.), sei es in der Verwaltung (z.B. vereinfachte administrative Prozesse)“ (Bundesamt für Bevölkerungsschutz [BABS], 2010b, p. 1). Deshalb hätte ein Ausfall der Telekommunikationsinfrastruktur gravierende Folgen für das öffentliche Leben, vor allem aber für die Wirtschaft. Zudem wären auch andere Teilsektoren der kritischen Infrastrukturen betroffen (z.B. Banken, Blaulichtorganisationen und Verkehr).

In der Schweiz ist die *Swisscom AG* der grösste Anbieter. Sie ist vom Bund dazu beauftragt, die Grundversorgung der Telekommunikationsinfrastruktur bereitzustellen. “Diese besteht darin, ein Basisangebot von grundlegenden Telekommunikationsdiensten allen Bevölkerungskreisen in allen Landesteilen zur Verfügung zu stellen. . . . Die Grundversorgung umfasst Telefonie, Fax, Datenübertragung, Breitband-Internetverbindung, Zugang zu Notrufdiensten, öffentliche Sprechstellen und besondere Dienste für Behinderte“ (BABS, 2010b, p. 1). Die Swisscom vermietet einen Teil ihrer Infrastruktur, nämlich die Kabelleitung zwischen dem Teilnehmeranschluss und der Ortszentrale (auch bekannt als „letzte Meile“), an andere Anbieter, wie z.B. die *Orange Communications SA* oder die *Sunrise Communications AG*, da diese keine Infrastruktur für die letzte Meile besitzen.

Da die Telekommunikationsinfrastruktur mittels Informationstechnologie betrieben wird, wäre die Sabotage der Telekommunikationsinfrastruktur (z.B. der Swisscom), oder ein Teil dieser, eine interessante Strategie für einen Angreifer. Denn einerseits wären aufgrund der starken Abhängigkeit der Wirtschat, Staat und Bevölkerung viele Akteure betroffen. Andererseits wären aufgrund der Wertschöpfungskette in der Wirtschaft Kettenreaktionen zu erwarten. Der erzielte Schaden wäre also massiv, gleichzeitig aber auch unkontrollierbar.

Die Absicht hinter einem solchen Angriff könnte ein wirtschaftlicher Schaden sein, aber auch die gezielte Lähmung des Staates, um eine konventionelle Kriegskampagne zu unterstützen.

4.1.1.2 Stromversorgung

„Die Stromversorgung umfasst alle Einrichtungen und Tätigkeiten, die für die Belieferung der Verbraucher mit elektrischer Energie (Elektrizität) erforderlich sind. Die Stromversorgung beinhaltet die Produktion, den Transport, die Verteilung und den Handel von Elektrizität. Sie ist somit ein zentraler Teilsektor der kritischen Infrastrukturen, der sich im Fall von Ausfällen oder Störungen schwerwiegend und unmittelbar auf die anderen Sektoren und somit auf Staat, Wirtschaft und Bevölkerung auswirkt. Diesen drei Akteuren ermöglicht die Elektrizitätsversorgung das Ausführen wichtiger Prozesse und die Erfüllung der Grundbedürfnisse des täglichen Lebens. Für die Wirtschaft ist Strom unentbehrlich für Abwicklung von zentralen Geschäftsprozessen (Informatik, Beleuchtung, Kommunikationstechnologien etc.), für die Industrie ist Elektrizität zusätzlich ein bedeutender Energieträger und für die Bevölkerung stellt Strom u.a. das Funktionieren der Haushaltsgeräte, der Beleuchtung, der Kommunikationstechnologien sicher“ (Bundesamt für Bevölkerungsschutz [BABS], 2012c, p. 1).

Die Stromversorgung der Schweiz setzt sich aus verschiedenen Erzeugungsquellen zusammen. Im Jahr 2011 stammten 53.7% des Stroms von Wasserkraftwerken, 40.7% von Kernkraftwerken und 5% aus fossilen und anderen thermischen Quellen (z.B. Erdöl, Holz und Abfälle). Die Schweiz betreibt auch Import und Export von Strom mit dem Ausland, um Defizite oder Überschüsse auszugleichen (Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation [UVEK], 2014).

Ein zentraler Player in der Stromversorgung ist die *Swissgrid*. Sie betreibt das nationale Übertragungsnetz, welches aus 6.700 km Hochspannungsleitungen besteht, und ist somit für die Stromverteilung zuständig. Dieses Übertragungsnetz besitzt Knotenpunkte, wie jedes andere Netzwerk auch. Diese Knotenpunkte könnten theoretisch angegriffen werden, um einen möglichst flächendeckenden Stromausfall zu bewirken. Die Swissgrid wird deshalb auch in der “Too big to fail“-Analyse, der vom Bundesrat beauftragten Expertenkommission zur Limitierung von volkswirtschaftlichen Risiken durch Grossunternehmen (2010), als systemrelevant[19] bezeichnet. Da die Swissgrid aber ein integraler Teil des Stromhandels in Europa ist, hätte deren Ausfall nicht nur für die Schweiz, sondern auch europaweite Konsequenzen.

Weitere wichtige Unternehmen sind die Betreiber der Kernkraftwerke. Mit 38% der Stromproduktion, welche nur mittels fünf verschiedenen Anlagen realisiert wird, besteht ein erhebliches Risiko. Denn ein Ausfall eines solchen Kernkraftwerks würde ein beträchtliches Loch in der Stromversorgung verursachen. Ein noch grösseres Risiko besteht aber in den Kernreaktoren, welche radioaktives Material enthalten. Es besteht die entfernte Gefahr, dass die *SCADA-Systeme*[20], welche die Kernreaktoren steuern, sabotiert werden und somit radioaktives Material freigesetzt würde. Beson-

[19] Siehe Kapitel 2.4.2 Wirtschaft
[20] Siehe Kapitel 2.4.1 Kritische Infrastrukturen

ders zu erwähnen ist die *Axpo AG*, welche die Besitzerin von zwei der fünf schweizerischen Kernkraftwerke ist und diese auch selbst betreibt, und somit ein besonders gefährdeter Akteur in der Stromversorgung ist.

Ein weiteres Risiko sind Wasserkraftwerke. Sie machen zwar 57% der Stromproduktion aus, diese ist aber auf mehrere hundert Kraftwerke verteilt, was einen wirksamen Angriff erschwert. Das eigentliche Risiko sind Speicherkraftwerke, welche mittels einer Staumauer Wasser aufstauen und speichern. Da auch diese Kraftwerke, bzw. der Abfluss der Staumauer, von SCADA-Systemen gesteuert werden, stellen auch sie ein potentielles Risiko für die Bevölkerung dar. Ein gezieltes Ablassen von grossen Wassermengen könnte verheerende Schäden an Menschen, Objekten und der Umwelt verursachen. Eine der Hauptbetreiberinnen von Speicherkraftwerken ist die *Alpiq Holding AG*, welche rund 20 solche Kraftwerke besitzt.

4.1.1.3 Schienenverkehr

„Der Sektor Schienenverkehr umfasst den Personen- und Güterverkehr auf dem schweizerischen Schienennetz. Ein funktionsfähiges, zuverlässiges und leistungsfähiges Transport- und Verkehrssystem ist heutzutage eine Grundvoraussetzung für eine moderne Wirtschaft, die auf die Mobilität von Gütern und Personen angewiesen ist. Mit zunehmender Globalisierung von Produktion und Absatz sowie der rasanten Entwicklung im internationalen Personenverkehr hat sich der Schienenverkehr zu einem zentralen Faktor für die Versorgung von Wirtschaft und Bevölkerung mit Gütern und Dienstleistungen entwickelt. . . . Konkret beliefert der Schienenverkehr die Industrie z.B. mit Gütern und erlaubt die Mobilität von Arbeitskräften. Für die Bevölkerung ermöglicht er die Mobilität sowohl für die Arbeit als auch für die Freizeit, sowie die Versorgung von Geschäften mit Gütern (Lebensmittel, Rohstoffe, Dienstleistungen, Postsendungen etc.). Störungen im schweizerischen Schienenverkehr wirken sich auf nahezu alle Lebensbereiche direkt aus; insbesondere die Wirtschaft (Verzögerungen bei Produktion und Warenauslieferung, Verfügbarkeit von Personal), aber auch Bevölkerung (fehlende Mobilität im Arbeits- und Freizeitbereich etc.) werden durch länger anhaltende Störungen nachhaltig beeinträchtigt. Gleichzeitig ist der Schienenverkehr auf die Funktionsfähigkeit anderer Sektoren zwingend angewiesen, wie z.B. die Stromversorgung oder die Informations- & Kommunikationstechnologien“ (Bundesamt für Bevölkerungsschutz [BABS], 2010a, p. 1).

Der grösste Player im Schienenverkehr sind die *Schweizerischen Bundesbahnen (SBB)*. Von den insgesamt 5‘148 km des Streckennetzes ist die SBB in Besitz von 3‘011 km. Dazu gehören alle Hauptverkehrsachsen innerhalb und zwischen den grossen Agglomerationen. Für den Fernverkehr befindet sich die SBB in einer Monopolstellung. Sie übernimmt auch einen Teil des Regionalverkehrs, welchen sie sich mit verschiedenen Privatbahnen teilt (Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation [UVEK]).

Die Schienenverkehrsinfrastruktur ist stark von IT-Systemen abhängig. Als Beispiel ist das *European Train Control System (ETCS)* zu nennen, welches die Zugsicherheit

gewährleistet, indem es dem Lokführer die Fahrerlaubnis, Geschwindigkeitsangaben und Streckendaten anzeigt. Ein Angriff auf solche Systeme kann aus verschiedenen Gründen erfolgen. Einerseits kann er sie unverfügbar machen, wodurch der Schienenverkehr gestört würde. Dies hätte natürlich direkte Folgen für die Wirtschaft und Bevölkerung. Andererseits könnte ein Zugsicherheitssystem, wie das ETCS, sabotiert werden, so dass inkorrekte Informationen (z.B. ungültige Fahrerlaubnis, zu hohe Höchstgeschwindigkeit, etc.) angezeigt würden, wodurch Entgleisungen und Zusammenstösse der Züge provoziert würden. Die Beweggründe könnten in diesem Fall einerseits die Verbreitung von Angst und Schrecken[21], andererseits die Erpressung des Infrastrukturbetreibers und somit finanzielle Motive sein.

4.1.1.4 Strassenverkehr

Da der Strassenverkehr auch für den Personen- und Gütertransport zuständig ist, herrscht hier eine ähnliche Situation wie beim Schienenverkehr[22]. Er ist von zentraler Bedeutung für die Wirtschaft und Bevölkerung und ein längerer Ausfall hätte verheerende ökonomische Folgen. Der Unterschied liegt darin, dass der Strassenverkehr weniger abhängig von Informations- und Kommunikationstechnologie (ICT) ist, als der Schienenverkehr. Deshalb sind die Möglichkeiten für Cybersabotagen limitierter. Es ist aber denkbar, dass aufgrund der immer grösser werdenden Präsenz von Computern im Alltag[23], der Strassenverkehr in Zukunft eine grössere Abhängigkeit gegenüber ICT aufweist.

Ein wichtiger Teil der Strassenverkehrsinfrastruktur, der von Informationstechnologie gesteuert wird, sind die Lichtsignalanlagen (LSA). Diese werden zentral gesteuert und sind somit anfällig für einen Sabotageangriff. Über die Systeme, welche die LSA steuern, könnten die LSA ausser Betrieb genommen werden. Dies würde zu einem Verkehrschaos führen, insbesondere zu den Stosszeiten. Auch denkbar wäre, dass die LSA in ihrer Logik sabotiert werden, so dass es zu mutwilligen Verkehrsunfällen kommt, um Angst und Schrecken zu verbreiten[21] oder den Betreiber der LSA zu erpressen.

4.1.1.5 Banken

„Der Teilsektor Banken umfasst die Banken, andere Finanzdienstleister, die Börsen sowie die Provider der verschiedenen Finanzmarktinfrastrukturen. Er ist die Basis für das Funktionieren der Wirtschaftskreisläufe, die Bargeldversorgung, den zunehmenden bargeldlosen Zahlungsverkehr sowie die Vergabe von Krediten an Personen und Unternehmen. Mit einer Wertschöpfung von 12% am Bruttoinlandprodukt und gegen 200‘000 Beschäftigten kommt dem Teilsektor zudem eine zentrale wirtschaftliche Bedeutung zu.

[21] Siehe Kapitel 2.2.2.2 Cyberterroristen
[22] Siehe Kapitel 4.1.1.3 Schienenverkehr
[23] Siehe *„Pervasive Computing“* in Kapitel 3.3 Anwendung in der ICT

Gleichzeitig ergeben sich, wie die Finanzmarktkrise vor Augen geführt hat, aufgrund der Grösse und Vernetzung innerhalb und ausserhalb des Teilsektors systemische Risiken, die sich auf die gesamte schweizerische Volkswirtschaft auswirken können. Es ist bei Störungen und Ausfällen im Bankensektor zum Beispiel mit Auswirkungen auf Staat, Wirtschaft und Bevölkerung zu rechnen. Insbesondere Störungen im Zahlungsverkehr können Geschäftsprozesse in der Wirtschaft behindern, die Bevölkerung in den bargeldlosen Einkäufen blockieren, oder in der Bargeldabhebung hindern. Wie die verschiedenen Finanzkrisen bereits aufgezeigt haben, können Unsicherheiten und Spekulationen bzgl. Der Stabilität und Kreditwürdigkeit eines Finanzdienstleisters zudem auch Auswirkungen auf die finanzielle Stabilität eines Landes und dessen Wirtschaft haben (Nervosität an den Börsen, Austrocknung des Kreditmarktes etc.). Zwar ist der Teilsektor mit seiner Vielzahl von Banken, Kreditinstituten und anderen Finanzdienstleistern sehr dezentral strukturiert und daher in seiner Gesamtheit weniger von Totalausfällen betroffen, einzelne zentrale Akteure sind jedoch von grosser Bedeutung für die Aufrechterhaltung der Finanzkreisläufe“ (Bundesamt für Bevölkerungsschutz [BABS], 2012a, p. 1).

Ein solch zentraler Akteur im schweizerischen Finanzmarkt ist die *Six Group*. Sie ist die Betreiberin der Schweizer Börse *SIX Swiss Exchange* und bietet Dienstleistungen im Bereich der Securities, Finanzinformationen und Zahlungsabwicklung an. Mit dem Betrieb der Börse ist die SIX Group ein Knotenpunkt der Schweizer Finanzplatzinfrastruktur und stellt somit ein systemisches Risiko dar. Denn von dieser systemrelevanten[24] Funktion hängen unzählige weitere Beteiligte der Wirtschaft ab, insbesondere aber Kreditinstitute. Ein erfolgreicher Sabotageangriff auf die Börse, welcher zum Beispiel dessen Transaktionssysteme ausser Betrieb setzt, würde die Lähmung des Schweizer Finanzplatzes und somit einen gravierenden Schaden für die Wirtschaft zur Folge haben. Nicht nur die Banken wären betroffen, sondern auch andere Unternehmen, sowohl in der Schweiz, als auch im Ausland. Auch die Bevölkerung wäre betroffen, da sie keine Wertpapiere mehr handeln könnte und in der bargeldlosen Bezahlung eingeschränkt wäre.

Auch die beiden Grossbanken, *UBS AG* und *Credit Suisse AG* sind sehr wichtige Akteure auf dem Schweizer Finanzplatz. Die “Too big to fail“-Analyse der vom Bundesrat beauftragten Expertenkommission zur Limitierung von volkswirtschaftlichen Risiken durch Grossunternehmen (2010) stuft beide aufgrund folgender Gründe als systemrelevant[24] ein:

- Grösse: Die Bilanzsumme der UBS und Credit Suisse ist zusammen etwa fünfmal so gross wie das Schweizer BIP. Zudem beträgt ihr gemeinsamer Marktanteil an inländischen Krediten und Einlagen über einen Drittel. Der Schweizer Banksektor stellt somit aufgrund der Grösse und der Konzentration der beiden Grossbanken einen Ausnahmefall dar.

[24] Siehe Kapitel 2.4.2 Wirtschaft

- **Vernetzung:** Die beiden Grossbanken sind stark vernetzt und nehmen eine zentrale Rolle in der Kredit und Liquiditätsversorgung ein. Einerseits sind sie eng mit der Volkswirtschaft verbunden und agieren als Kreditgeber für andere Unternehmen und private Personen. Andererseits sind sie auch stark mit anderen Banken vernetzt und sorgen für deren Liquiditätsversorgung und für den Liquiditätsausgleich.

- **Substituierbarkeit:** Die Dienstleistungen der beiden Grossbanken können schlecht substituiert werden, insbesondere nicht in einer nützlichen Frist. Zum einen kann dies zu einer Kreditklemme führen, da alternative Kreditgeber nicht rechtzeitig gefunden werden können. Andererseits sind bei einem Ausfall die Vermögen von Privatpersonen und Unternehmen gefährdet. Diese können während dem Ausfall auch nicht auf ihre Depositen zugreifen, was zu einer Einschränkung des Konsums und der Investitionen führt.

Die Auswirkungen eines Sabotageakts an den IT-Systemen der beiden Grossbanken wären also fatal. Auch wenn deren IT-Systeme ein sehr hohes Sicherheitsniveau aufweisen, ein Restrisiko ist immer vorhanden. Das Motiv eines solchen Angriffs wäre die Schwächung der Schweizer Volkswirtschaft.

Die beiden Grossbanken sind zwar die interessantesten Ziele für einen Angreifer, da bei ihnen der grösste Schaden erzielt werden kann. Es können aber durchaus auch andere Banken oder Finanzinstitute angegriffen werden. Denn ein erfolgreicher Angriff würde ein Reputationsschaden für den gesamten Schweizer Bankensektor bedeuten.

4.1.1.6 Industrie

Neben dem Dienstleistungssektor ist die Industrie, mit 26% der Bruttowertschöpfung, ein sehr wichtiger Teil der Wirtschaft (Bundesamt für Statistik [BFS], 2012). So beträgt die Industrieproduktion der Schweiz pro Kopf $12‘400. Dies ist doppelt so viel wie in der USA und achtmal so viel wie in China (Schwarz & Schär, 2012). Die wichtigsten Branchen sind die Uhrenindustrie, Maschinen-, Elektro- und Metallindustrie, Chemie- und Pharmaindustrie, Nahrungsmittelherstellung und Medizintechnik.

Der Wettbewerbsvorteil der Unternehmen im Industriesektor liegt oft in Technologien, Designs und Innovationen, also geistigem Eigentum. Dies macht diese Firmen besonders anfällig für Cyberspionage, bzw. Wirtschaftsspionage[25]. Die nationale Sicherheit ist durch einzelne Spionageangriffe meist nicht direkt gefährdet. Diese können aber Teil eines grösseren Unterfangens sein, welches die Beeinträchtigung eines

[25] Siehe Kapitel 2.3.3 Cyberspionage

Staates (z.B. der Schweiz) zum Ziel hat. Denn diese Angriffe können trotzdem einen beträchtlichen wirtschaftlichen Schaden verursachen.

Innerhalb der Chemie- & Pharmaindustrie sind die *Novartis AG*, die *Roche Holding AG* und die *INEOS Holdings AG* die drei grössten Unternehmen mit einem Umsatz von 53‘114 Mio., 45‘499 Mio. und 38‘500 Mio. Novartis und Roche sind zugleich unter den fünf grössten Pharmakonzernen der Welt. Diese Unternehmen sind stark von Innovationen abhängig, vor allem in Form von neuen Rezepturen für Medikamente und Chemikalien. Im Ranking der 20 Unternehmen mit den weltweit grössten Ausgaben in Forschung und Entwicklung (R&D), sind Novartis und Roche unter den Top 10 (Jaruzelski, Loehr, & Holman, 2013). Diese hohen Investitionen in R&D machen sie zu einem attraktiven Ziel für Cyberspionage.

Auch in der stark technologieabhängigen Maschinen-, Elektro- und Metallindustrie ist die Innovation zentral für ein Unternehmen, um sich im Wettbewerb behaupten zu können. In der Schweiz ist die *ABB Ltd*, mit 37'369 Mio. Umsatz der weitaus grösste Vertreter dieser Branche. Sie beschäftigt sich vor allem mit der Energie- und Automatisationstechnik. Ein weiterer wichtiger Vertreter ist die *RUAG Holding AG*. Sie ist unter anderem in der Luft- & Raumfahrttechnik und der Rüstungsindustrie tätig und beliefert verschiedene zivile, aber auch staatliche/militärische Kunden. Darunter befindet sich auch das Schweizer Militär, weshalb der RUAG eine strategische Bedeutung für die Schweiz zukommt.

4.1.2 Armee

Der Auftrag der Schweizer Armee (n.d.) ist die Wahrung der Sicherheit in der Schweiz und umfasst folgende Aufgaben:

- Verteidigung des Landes: Diese Aufgabe umfasst die Abwehr von bewaffneten Angriffen und stellt die Kernaufgabe der Armee dar.

- Unterstützung der zivilen Behörden: Wenn die Mittel der zivilen Behörden nicht ausreichen, kann die Armee subsidiäre Leistungen erbringen. Diese umfassen Katastrophenhilfe, Schutz von Personen, Objekten (u.a. auch kritische Infrastrukturen) oder Veranstaltungen (z.B. das WEF) oder die Unterstützung des Grenzwachkorps. Zudem erbringt die Armee luftpolizeiliche Dienste zur Wahrung der Lufthoheit. Diese Aufgabe macht den Hauptanteil der heutigen Einsätze aus.

- Friedensförderung im internationalen Rahmen: „Die Armee setzt sich im Ausland für Sicherheit und Frieden ein. Sie hilft im Auftrag internationaler Organisationen in anderen Ländern mit, nach Kriegen und Krisen wieder eine stabile Ordnung aufzubauen. Eine friedlichere Welt kommt auch der Schweiz zugute“ (Schweizer Armee, n.d.). Aktuell stellt die Schweiz der

UNO unbewaffnete Militärbeobachter zur Verfügung. Zudem beteiligt sich die Schweiz an zwei bewaffneten Einsätzen zur Friedensförderung im Ausland: der *KFOR*-Mission in Kosovo und der *EUFOR*-Mission in Bosnien.

Um diese Aufgaben erfüllen zu können, betreibt die Armee eigene Infrastrukturen. Diese umfassen zum Beispiel die Logistik, die Führungsunterstützung und die Luftwaffe. Sie sind alle stark von Informationstechnologie abhängig und deshalb auch anfällig für Cyberangriffe. Insbesondere die Luftwaffe wäre durch eine Sabotage ihrer IT-Systeme stark eingeschränkt. Da das Ausmass eines Schadens schwer einzuschätzen ist, wäre der Flugbetrieb stark beeinträchtigt.

Die Armee und ihre Infrastrukturen sind aber massgeblich von anderen kritischen Infrastrukturen abhängig, insbesondere von der Stromversorgung, der Telekommunikationsinfrastruktur und dem Luft- und Schienenverkehr. Die Stromversorgung und die Telekommunikationsinfrastruktur sind wichtig für den Betrieb der IT-Systeme und ermöglichen deren Daten- und Informationsaustausch. Die Transportmöglichkeiten durch den Luft- und Schienenverkehr sind vor allem für die Logistik massgebend. Es liegt deshalb im Interesse der Armee, diese kritischen Infrastrukturen zu schützen.

Die Armee kann also auf zwei unterschiedliche Weisen in ihrem Auftrag gestört werden. Einerseits direkt, indem die IT-Systeme der Armee angegriffen werden. Andererseits auf indirekte Weise, indem die Infrastrukturelemente sabotiert werden, von welchen die Armee abhängig ist.

4.2 Massnahmen der Schweiz

In der Schweiz sind verschiedene Bestrebungen vorhanden, um sich vor Cyberrisiken zu schützen. Diese decken unterschiedliche Bereiche der Cyberproblematik ab, welche in Abbildung 1 ersichtlich sind und im Folgenden kurz beschrieben werden:

- Einerseits gibt es die *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)*, welche für diese Arbeit sehr zentral ist. Sie deckt vor allem den Bereich *Cyber-Resilienz* ab, welcher den Schutz der kritischen Infrastrukturen vorsieht. Die NCS befasst sich am Rande aber auch mit dem Nachrichtendienst, da dieser für die Informationsbeschaffung zuständig ist und vor allem bei der Analyse der Bedrohungslage und der Identifikation der Täterschaft zum Zuge kommt.
  Ursprünglich sollte die NCS auch den Teil Cyber-Defence beinhalten. Doch nach einem internen Richtungswechsel wurde entschieden, dass die NCS nur auf die Friedenszeit ausgerichtet sein soll und den Konflikt- oder Kriegsfall ausklammert und der Armee zuweist (ISB, 2013).

- Das *Cyber-Defence* Konzept der Schweizer Armee (CYD) deckt genau diesen Konflikt- und Kriegsfall ab, welchen die NCS ausklammert. Zudem sieht es den Schutz der militärischen Infrastrukturen vor Cyberangriffen vor. Das CYD ist als vertraulich eingestuft und deshalb für die Öffentlichkeit nicht zugänglich, weshalb es in dieser Arbeit gezwungenermassen nicht näher behandelt werden kann.

- Das *Eidgenössisches Justiz- und Polizeidepartement (EJPD)* hat bereits einen funktionierenden Apparat zur Bekämpfung der Cyberkriminalität, im Rahmen der *Cyberjustiz,* aufgebaut. Es sind verschiedene Organe innerhalb des EJPD daran beteiligt, wovon vor allem folgende zwei massgebend sind: Die *Bundeskriminalpolizei (BKP)*, welche als die Ermittlungsbehörde des Bundes für die Erkennung, Bekämpfung und Verfolgung begangener Straftaten zuständig ist, und die *Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)*, welche dafür zuständig ist, „Straftaten im Internet rechtzeitig zu erkennen, Doppelspurigkeiten bei der Strafverfolgung zu vermeiden und die Internetkriminalität zu analysieren“ (VBS, 2012).
  Da Cyberkriminalität aber nicht in der Definition dieser Arbeit[26] liegt, wird dieser Bereich hier auch nicht behandelt.

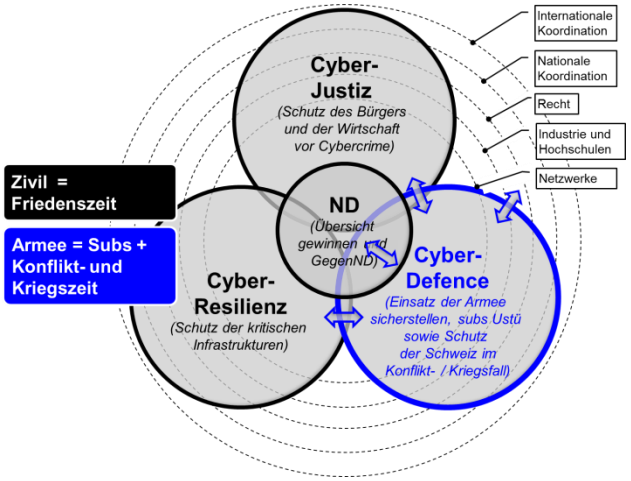

Abbildung 1: Die unterschiedlichen Bereiche in der Bekämpfung der Cyberproblematik (Vernez, 2013 p. 47; Vernez, personal communication, 2014b)

Zuerst werden im Kapitel 4.2.1 die zivilen Massnahmen des Cyber-Resilienz Bereichs behandelt. Anschliessend wird im Kapitel 4.2.2 auf das öffentlich zugängliche Material der militärischen Massnahmen des *Cyber-Defence* Bereichs eingegangen.

[26] Siehe Kapitel 2.1 Definition

4.2.1 Massnahmen der Cyber-Resilienz

In diesem Kapitel wird die *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)* erläutert. Dabei wird im ersten Unterkapitel 4.2.1.1 auf deren Ziele und Organisation eingegangen, um die Ausganglage und den Fokus der Strategie aufzuzeigen. Im zweiten Unterkapitel 4.2.1.2 werden dann die konkreten Massnahmen und deren Umsetzung ausgeführt.

4.2.1.1 Ziele und Organisation

Die Schweiz verfolgt mit der *Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)* folgende drei strategische Ziele:

- die frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich
- die Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen
- die wirksame Reduktion von Cyber-Risiken, insbesondere Cyber-Kriminalität, Cyber-Spionage und Cyber-Sabotage (VBS, 2012)

Zur Umsetzung dieser Ziele wurde ein dezentraler Ansatz gewählt. Dieser soll der ebenfalls dezentral organisierten Schweizer Wirtschafts- und Staatsstruktur Rechnung tragen, indem auf die bestehenden Strukturen aufgebaut wird. Aus diesem Grund wurde auf eine zentrale Führungsstelle verzichtet. Anstelle dieser wurden ein Steuerungsausschuss und eine Koordinationsstelle (KS NCS) eingerichtet, zur strategischen, operationellen und fachlichen Koordination (siehe Abbildung 2).

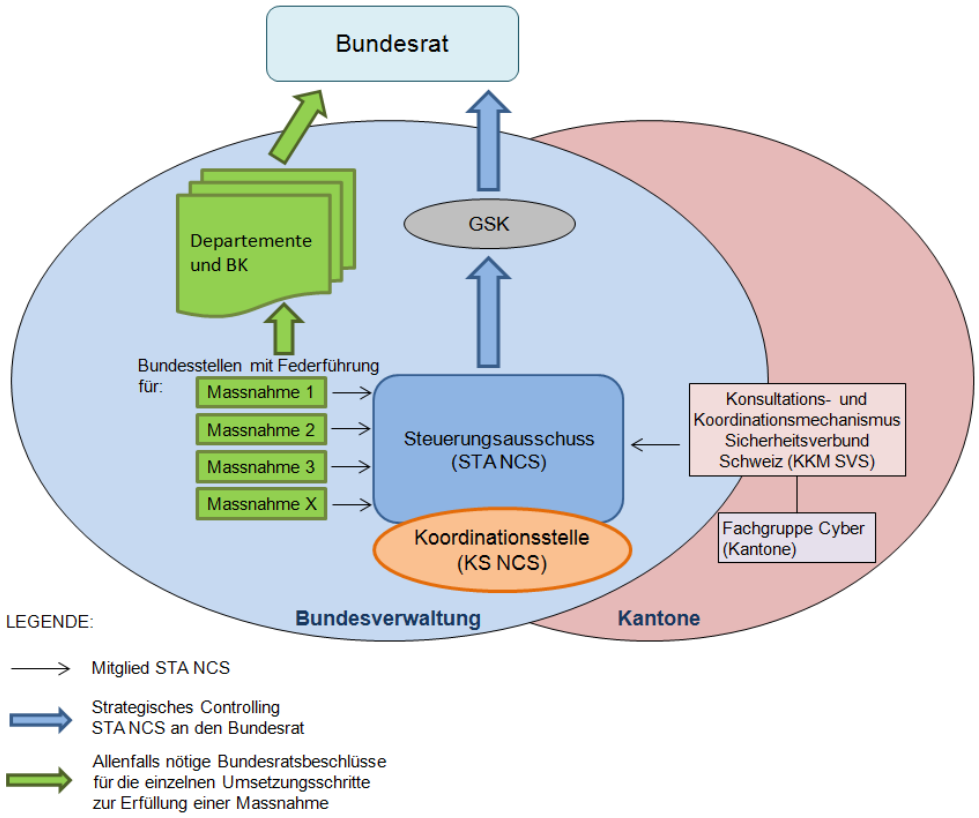

Abbildung 2: Umsetzungsorganisation NCS (ISB, 2013, p. 9)

Es sind viele verschiedene Akteure von Cyberrisiken betroffen: Betreiber kritischer Infrastrukturen (KI), Unternehmen der Wirtschaft, Leistungserbringer der Informations- und Kommunikationstechnologien (ICT oder IKT), Systemlieferanten, Behörden auf Kantons- und Bundesebene, und die Armee. Diese besitzen jeweils unterschiedliche Aufgaben, Verantwortungen und Prozesse, welche alle eine Cyber-Ausprägung haben. Die Strategie setzt auf die Eigenverantwortung dieser involvierten Akteure, indem sie ihnen die Aufgabe überträgt „diese Cyber-Ausprägung zu erkennen, die damit einhergehenden Risiken in ihren jeweiligen Prozess aufzunehmen und damit zu reduzieren“ (VBS, 2012, p. 30). „Zu diesem Zweck sollen die dezentral bestehenden Strukturen befähigt, allenfalls gestärkt werden, um die cyber-spezifische Ausprägung [der] Aufgaben und Verantwortlichkeiten [der verschiedenen Akteure] umfassend abzudecken“ (VBS, 2012, pp. 30–31).

Der Staat unterstützt aber die involvierten Akteure mit der NCS, indem er die Kommunikation und die Zusammenarbeit unter ihnen erleichtert und subsidiär Leistungen erbringt. Eine dieser Leistungen erfolgt durch die *Melde- und Analysestelle Informationssicherung (MELANI)*, welche Informationen über Vorfälle und Bedrohungen sammelt, Analysen erstellt und diese unter den KI-Betreibern verteilt. Eine weitere Leistung wird durch den *Nachrichtendienst des Bundes (NDB)* erbracht. Er be-

schafft mit nachrichtendienstlichen Mitteln Informationen im In- und Ausland, analysiert und verbreitet diese. Im Inland umfassen diese Informationen folgende Themen: „Terrorismus, gewalttätiger Extremismus, Proliferation, Angriffe auf die kritischen Infrastrukturen und verbotenen [sic] Nachrichtendienst“ (VBS, 2012, p. 18). Im Ausland umfassen diese Sicherheitspolitische Fragen, unter anderem: „Proliferation, Terrorismus, Streitkräfteentwicklung sowie Rüstungstechnologie und Rüstungshandel sowie . . . strategische Analysen“ (VBS, 2012, p. 18).

Ein direkter Eingriff des Staates wird also vermieden. Dieser erfolgt nur, wenn öffentliche Interessen auf dem Spiel stehen oder er im Sinne der Subsidiarität handelt.

4.2.1.2 Massnahmen und Umsetzung

Konkret umfasst die NCS 16 Massnahmen, welche in der Tabelle 4 mit einer kurzen Beschreibung aufgelistet sind. Im Anhang dieser Arbeit werden diese Massnahmen noch ausführlicher umschrieben. Diese können in vier Bereiche aufgeteilt werden (siehe Abbildung 3):

- Massnahmen der Prävention
- Massnahmen der Reaktion
- Massnahmen des Kontinuitäts- und Krisenmanagement
- Massnahmen der Unterstützung

Die Umsetzung dieser Massnahmen hat im Juni 2013 begonnen und soll bis Ende 2016 erfolgen (Vernez, personal communication, 2014a). Sie ist im Umsetzungsplan der NCS festgelegt, welcher die Grundlage für alle involvierten Akteure darstellt. Der Umsetzungsplan macht aber keine genauen Angaben zu deren Aufgaben und Pflichten, denn diese Akteure sollen die Massnahmen selbst konkretisieren und implementieren können. Man erhofft sich dadurch eine effizientere und direktere Umsetzung aufgrund der Erfahrungen der Akteure in ihrem jeweiligen Geschäftsfeld (ISB, 2013).

Zur Umsetzung wurde vom Bund eine Bedarfsschätzung bezüglich der notwendigen Ressourcen gemacht. Man ist zum Schluss gekommen, dass insgesamt 30 neue Stellen notwendig sind, welche sich über verschiedene Departemente verteilen.

Handlungsfeld 1	Massnahmen	
Forschung und Entwicklung	1	Neue Risiken im Zusammenhang mit der Cyber-Problematik sollen erforscht werden
Handlungsfeld 2	**Massnahmen**	
Risiko- und Verwundbarkeitsanalyse	2	Selbständige Überprüfung der Systeme Risikoanalysen zur Risikominimierung in Zusammenarbeit mit Behörden, den IKT-Leistungserbringern und Systemlieferanten
	3	IKT-Infrastruktur auf systemische, organisatorische, und technische Verwundbarkeiten untersuchen
Handlungsfeld 3	**Massnahmen**	
Analyse der Bedrohungslage	4	Erstellung Lagebild und Lageentwicklung
	5	Nachbearbeitung von Vorfällen für die Weiterentwicklung von Massnahmen
	6	Fallübersicht und Koordination interkantonaler Fallkomplexe
Handlungsfeld 4	**Massnahmen**	
Kompetenzbildung	7	Schaffung einer Übersicht über Kompetenzbildungsangebote und Identifikation von Lücken.
	8	Schliessung der Lücken bei Kompetenzbildungsangeboten und vermehrte Nutzung qualitativ hochstehender Angebote
Handlungsfeld 5	**Massnahmen**	
Internationale Beziehungen und Initiativen	9	Aktive Teilnahme der Schweiz im Bereich der Internet-Governance.
	10	Kooperation auf der Ebene der internationalen Sicherheitspolitik
	11	Koordination der Akteure bei der Beteiligung an Initiativen und Best-Practices im Bereich Sicherheits- und Sicherungsprozesse
Handlungsfeld 6	**Massnahmen**	
Kontinuitäts- und Krisenmanagement	12	Stärkung und Verbesserung der Widerstandsfähigkeit (Resilienz) gegenüber Störungen und Ereignissen
	13	Koordination der Aktivitäten in erster Linie mit den direkt betroffenen Akteuren und Unterstützung der Entscheidfindungsprozesse mit fachlicher Expertise
	14	Aktive Massnahmen zur Identifikation der Täterschaft und allfälligen Beeinträchtigung deren Infrastruktur bei einer spezifischen Bedrohung
	15	Erarbeitung eines Konzeptes für Führungsabläufe und -prozesse zur zeitgerechten Problemlösung
Handlungsfeld 7	**Massnahmen**	
Rechtsgrundlagen	16	Überprüfung bestehender Rechtsgrundlagen aufgrund der Massnahmen und Umsetzungskonzepte und Priorisierung von unverzüglichen Anpassungen

Tabelle 4: Massnahmen und Handlungsfelder der NCS (VBS, 2012, p. 4)

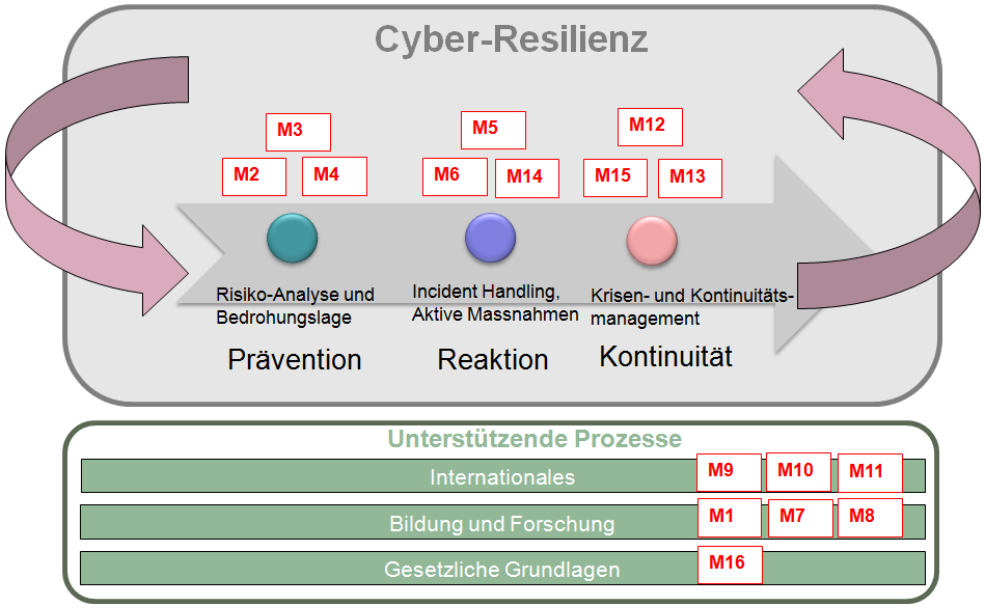

Abbildung 3: Massnahmen der NCS in vier Bereiche aufgeteilt (ISB, 2013, p. 12)

4.2.2 Massnahmen der Cyber-Defence

Nachdem entschieden wurde, dass die NCS eine rein zivile Strategie wird und den Konflikt- und Kriegsfall ausschliesst, hat die Schweizer Armee ein eigenes Konzept entworfen und bereits mit dessen Umsetzung begonnen. Dieses Cyber-Defence Konzept (CYD) ist als vertraulich eingestuft, weshalb der genaue Inhalt der Öffentlichkeit verwehrt ist. Es ist aber geplant, eine zensierte Version zu veröffentlichen (Vernez, personal communication, 2014a). Im Folgenden werden einige Grundkonzepte der CYD erläutert.

Um ihren verfassungsmässigen Auftrag[27] ausführen zu können, beschäftigt sich die Armee laut Vernez (2013, p. 50) mit folgenden drei Schlüsselfragen:

- „Wie soll sich die Armee vor Cyber-Bedrohungen schützen und diese abwehren?
- Wie kann die Armee die Zusammenarbeit mit Leistungserbringern gestalten, von denen sie zur Erfüllung ihres eigenen Auftrags abhängig ist?
- Was muss die Armee generell für Leistungen zum Schutz der kritischen Infrastrukturen und des Landes u.a. subsidiär erbringen?“

[27] Siehe Kapitel 4.1.2 Armee

Konkret will die Armee folgende vier Kernprozesse einführen. Einerseits um ihre Einsatzfähigkeit und Handlungsfähigkeit zu bewahren, andererseits um jederzeit Cyber-Bedrohungen erkennen, sich davor schützen und diese abwehren zu können:

- „Führung, um jeder Zeit und dauernd in der Lage zu sein, der [sic] Bereich Cyber-Defence in allen Einsatz- und Entwicklungstätigkeiten der Armee sicherzustellen und die dazu benötigten Partner und Leistungserbringer bestmöglich einzusetzen.

- Antizipation, um jeder Zeit über das nötige Wissen zur Sicherstellung der Entscheidfindungsprozesse zu verfügen, sei es im Rahmen von lang- und mittelfristigen Planungs- und Weiterentwicklungstätigkeiten, oder von kurzfristigen Ereignissen im Rahmen einer Operation oder im Krisenmanagement.

- Prävention, welche es erlauben soll, in allen möglichen Segmenten (technisch, organisatorisch, menschlich, usw.) die durch Cyber-Bedrohungen bedingten Risiken zu verringern und die Einsatzfähigkeit der Armee jeder Zeit aufrechtzuerhalten und im Angriffsfall wieder herzustellen; dies soll auch in einem stark gestörten oder sogar nicht mehr funktionierenden Cyber-Raum erfolgen.

- Reaktion, die es der Armee erlauben soll, im Falle eines Cyber-Ereignisses dieses genau und rechtzeitig zu detektieren, zu verstehen und danach richtig zu handeln, sowohl im technischen, wie auch im nicht-technischen Bereich, z.B. durch rechtliche Schritte oder diplomatische Zusammenarbeit“ (Vernez, 2013, p. 50).

Neben der Notwendigkeit ihre eigenen Infrastrukturen zu schützen und somit ihre Einsatzfähig zu erhalten, wurde der Armee, mit dem *Umsetzungsplan NCS* vom 15.05.2013 der Auftrag erteilt, auch subsidiäre Cyber-Leistungen zugunsten der zivilen Akteure zu erbringen. Der genaue Umfang dieser Leistungen wird im Rahmen der Umsetzung der NCS und des nächsten sicherheitspolitischen Berichts ermittelt. Laut dem Delegierten des Chefs der Armee für Cyber-Defence, Gérald Vernez, könnten diese aber folgende Aufgaben umfassen:

- „Sicherstellung krisenresistenter Kommunikation zu Gunsten der Landesregierung, der Behörden und ausgewählter kritischer Infrastrukturen;

- Unterstützung ausgewählter kritischer Infrastrukturen und Partnern der öffentlichen Sicherheit zur Erhöhung von deren Resilienz;

- Erbringung verschiedenster Leistungen zur Wiedererlangung der Funktionalität kritischer Infrastrukturen;

- Schutz (logisch, physisch, semantisch und elektromagnetisch) besonders sensibler Objekte;

- Beitrag zur Analyse und Abwehr der Bedrohungen im Cyber-Bereich“ (Vernez, 2013, p. 51).

4.3 Risiken der Massnahmen

Die in Kapitel 4.2 geschilderten Massnahmen können selbst Risiken mit sich tragen. Diese werden im Folgenden erläutert.

Durch neue Schutzmassnahmen für kritische Infrastrukturen ergibt sich das Risiko, dass deren Wirtschaftlichkeit beeinträchtigt wird. Diese werden nämlich zu einem grossen Teil von Unternehmen betrieben, welche dem Wettbewerb unterliegen. Diese Schutzmassnahmen kommen oft in Form von neuen Regelungen, welche beim betroffenen Unternehmen höhere Kosten verursachen und es anderen Unternehmen oder ausländischen Unternehmen gegenüber weniger konkurrenzfähig macht. Kosten können durch Neuanschaffungen entstehen, wenn zum Beispiel die bestehenden IT-Systeme angepasst oder ersetzt werden müssen. Es können auch Kosten entstehen, indem neues Personal eingestellt werden muss, insbesondere Fachkräfte. Zudem kann es sein, dass Prozesse innerhalb des Unternehmens überarbeitet werden müssen, um neuen Sicherheitsstandards zu genügen. Dadurch entstehen einerseits Kosten durch die Umstrukturierung der Prozesse. Andererseits könnten die überarbeiteten Prozesse ineffizienter sein als die Alten.

Ein weiteres Risiko besteht in einem potentiellen Interessenskonflikt zwischen den Projektleitern und den Betreibern der kritischen Infrastrukturen. Die Projektleiter sind primär daran interessiert, dass die kritischen Infrastrukturen der Schweiz bestmöglich geschützt sind, während die Betreiber vor allem an einem optimalen Betriebsergebnis, bzw. Gewinn interessiert sind. Da die Schutzmassnahmen aber gewisse Kosten mit sich bringen und die Betreiber an der Umsetzung der Massnahmen mitinvolviert sind, könnten sie diese behindern.

Die Massnahme 14 der NCS[28] könnte zu diplomatischen Auseinandersetzungen mit anderen Staaten führen. Denn diese sieht „Aktive Massnahmen zur Identifikation der Täterschaft und allfälligen Beeinträchtigung deren Infrastruktur bei einer spezifischen Bedrohung“ (VBS, 2012, p. 4) vor. Die Identifikation der Täterschaft kann nämlich nicht erfolgen, ohne dass in gegnerische Systeme eingedrungen wird, um Beweise zu sammeln. Und diese Systeme können sich in anderen Staaten befinden

[28] Siehe Tabelle 4, S. 41 & Anhang – Massnahmen der NCS

oder sogar anderen Staaten gehören. Zudem kann ein Gegenschlag, zur Beeinträchtigung der gegnerischen Infrastruktur, relativ problematisch sein, da die rechtliche Lage unklar ist. Es ist nicht klar, wann ein Angriff als eine kriegerische Handlung gilt und einen Gegenschlag rechtfertigt. Zudem ist unklar, was für Gegenmassnahmen (konventionelle oder mit Cybermitteln) in welchem Fall gerechtfertigt wären.

5 Schlussfolgerungen und Ausblick

In diesem Kapitel wird zuerst die generelle Risikosituation des Cyberwarfare (Kapitel 5.1) zusammengefasst und aus Sicht des Vorsorgeprinzips bewertet. Dadurch wird aufgezeigt, bei welchen Risiken die Notwendigkeit besteht vorsorgliche Massnahmen zu treffen. Anschliessend wird eine Schlussfolgerung zum Fallbeispiel Schweiz gemacht, mit seiner *Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)* (Kapitel 5.2), um zu bewerten, inwiefern die Massnahmen der NCS die bestehenden Risiken minimieren und Vorsorge[29] leisten.

5.1 Risikosituation des Cyberwarfare aus Sicht des Vorsorgeprinzips

In der Einleitung wurde die Frage eröffnet, ob die getätigten Massnahmen den bestehenden Risiken Rechnung tragen. Diese Frage wird im Folgenden mithilfe des Vorsorgeprinzips beantwortet, welches im Kapitel 3 erläutert wurde.

Im Kapitel 2.2 wurde festgestellt, dass sich unterschiedliche Akteure mit unterschiedlichen technischen Fähigkeiten und finanziellen Mitteln am Cyberwarfare beteiligen. Aus diesen beiden Faktoren ergeben sich auch die strategischen Möglichkeiten (Kapitel 2.2) und möglichen Angriffsziele (Kapitel 2.3) dieser Akteure. Der spezifische Angriff, welcher sich aus der Strategie und dem Angriffsziel zusammensetzt, kann in seiner Intensität bzw. Auswirkung variieren. Angriffe tieferer Intensität, wie zum Beispiel Cyberspionage, sind heute Realität, wie verschiedene Beispiele im Kapitel 2.3.3 gezeigt haben. Angriffe höherer Intensitäten, wie zum Beispiel die Sabotage von Systemen kritischer Infrastrukturen, sind bisher selten beobachtet und haben eine tiefere Eintrittswahrscheinlichkeit. Die Möglichkeit dazu ist aber vorhanden, da einerseits jedes System Schwachstellen aufweist und somit verwundbar ist. Andererseits haben Vorfälle wie *Stuxnet*[30] und der *Maroochy Water Breach*[31] demonstriert, wie SCADA-Systeme von kritischen Infrastrukturen kompromittiert und in ihrer Funktion gestört wurden, und Schaden angerichtet wurde.

Aus Sicht des Vorsorgeprinzips sind die Angriffe tieferer Intensität eigentlich kein Thema mehr, da sich diese Risiken bereits zu Gefahren, bzw. Bedrohungen[32] manifestiert haben. Es ist also zu spät um Vorsorge zu leisten, denn wir befinden uns hier

[29] Siehe Kapitel 3 Vorsorgeprinzip
[30] Siehe Kapitel 2.4.1 Kritische Infrastrukturen
[31] Siehe Kapitel 2.2.2.2 Cyberterroristen
[32] „*Bedrohung* setzt einen Willen voraus, die Schweiz oder ihre Interessen zu schädigen oder zumindest eine solche Schädigung in Kauf zu nehmen. *Gefahr* setzt keinen Willen zur Schädigung voraus (z.B. Naturgefahren und technische Gefahren)“ (Schweizer Bundesrat, 2010, p. 10).

bereits im Bereich der *Gefahrenabwehr*[33]. Das heisst aber nicht, dass diese Bedrohungen nicht mehr abgewehrt oder minimiert werden können. Denn es können zum Beispiel weiterhin Massnahmen zur Erhöhung der Systemsicherheit implementiert werden, um der Bedrohung der Cyberspionage entgegenzuwirken. Da sich immer mehr Akteure am Cyberwarfare beteiligen und sich diese Bedrohung somit zunehmend erhöht, kann gesagt werden, dass es durchaus sinnvoll ist in eine Erweiterung der bestehenden Massnahmen zu investieren.

Die Risiken der Angriffe höherer Intensität haben sich hingegen noch nicht als akute Bedrohung erwiesen. Über das Ausmass der Risiken wird heute hitzig diskutiert und es gibt Stimmen, wie zum Beispiel Dunn Cavelty (2013), welche diese ablehnen und als Angstmache und Täuschung der Sicherheitsindustrie darstellen, die dadurch den Verkauf ihrer Produkte und Dienstleistungen erhöhen wolle. Fakt ist, dass Vorfälle wie *Stuxnet*, die Cyberangriffe in Estland und Georgien, und der *Maroochy Water Breach* demonstriert haben, dass ein Risiko vorhanden ist, auch wenn über dessen Ausmass debattiert werden kann. Aus Sicht des Vorsorgeprinzips sollte dieses Risiko, auch wenn dessen Eintrittswahrscheinlichkeit klein ist, in Betracht gezogen werden und über Massnahmen zur Vorbeugung und Minimierung dieses Risikos diskutiert werden.

Die Erweiterung der Massnahmen gegen die Risiken von Angriffen tieferer und höherer Intensität, kann in zwei unterschiedlichen Bereichen erfolgen. Es kann in defensive und offensive Massnahmen investiert werden. Defensive Massnahmen können zum Beispiel die Sicherheit der *Infrastructure Control Systems (ICS)* von kritischen Infrastrukturen erhöhen, damit diese besser gegen Sabotageangriffe geschützt sind. Offensive Massnahmen minimieren die Risiken des Cyberwarfare insofern, als dass sie das Abschreckungspotential erhöhen. Sie können beispielsweise die Rekrutierung von Spezialisten umfassen, um die eigene Cyberspionagefähigkeiten eines Staates zu erweitern.

5.2 Fallbeispiel Schweiz

Im Kapitel 6.1 wurde aufgezeigt, dass weitere Massnahmen notwendig sind, um der Risikosituation des Cyberwarfare gerecht zu werden. In diesem Kapitel wird dies am Fallbeispiel Schweiz untersucht, mit seiner *Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)*. Dabei wird zuerst auf die Ausgestaltung der Massnahmen der NCS eingegangen (Kapitel 5.2.1), um zu bewerten, inwiefern die getroffenen Massnahmen in die richtige Richtung führen. Anschliessend wird die Umsetzung dieser Massnahmen beurteilt (Kapitel 5.2.2). In einem letzten Schritt wird wieder eine Bewertung der Massnahmen aus Sicht des Vorsorgeprinzips[33] gemacht (Kapitel 5.2.3), um zu beurteilen, inwiefern die NCS den Risiken des Cyberwarfare Vorsorge leistet oder ob eher Gefahrenabwehr betrieben wird.

[33] Siehe Kapitel 3 Vorsorgeprinzip

5.2.1 Ausgestaltung der Massnahmen

Um sich gegen Cyberrisiken und deshalb auch gegen Risiken des Cyberwarfare zu schützen, hat die Schweiz einen Ansatz gewählt, welcher sich über drei Bereiche[34] erstreckt: Der Schutz der kritischen Infrastrukturen, wozu auch die Wirtschaft gehört, die Verteidigung des Landes durch die Armee und die Bekämpfung der Cyberkriminalität durch die Bundeskriminalpolizei. Die *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)* war ursprünglich umfassender geplant. Sie sollte nämlich die ersten beiden Bereiche abdecken. Man hat sich dann aber dazu entschieden, dass der Konflikt- und Kriegsfall nicht behandelt werden soll, weshalb der zweite Bereich aus der Strategie ausgeschlossen wurde. Das Defizit wurde jedoch erkannt und die Armee hat eine entsprechende Strategie erarbeitet.

Die Schweiz setzt mit den Massnahmen 6, 9, 10 und 11 der NCS[35] zudem auf internationale Kooperation. Dabei werden Informationen zu Vorfällen ausgetauscht und an der Entwicklung der Internet-Governance, der internationalen Sicherheitspolitik und an Best-Practices für Sicherheits- und Sicherungsprozesse gearbeitet. Insgesamt kann also gesagt werden, dass die Schweiz einen sehr weitgreifenden Ansatz gewählt hat, der auf den Einbezug vieler verschiedener Akteure setzt. Dies hat den Vorteil, dass die Risiken weitreichender abgedeckt werden können.

Die Massnahmen der NCS sind eher defensiver Natur. Es wird vor allem darauf fokussiert, wie mit den Folgen eines Cyberangriffs umzugehen ist. Die Prävention findet nur im Rahmen von Risikoanalysen, durch die Überprüfung der betroffenen Systeme und der Erstellung eines Lagebilds durch den Nachrichtendienst des Bundes (NDB) und der *Melde- und Analysestelle Informationssicherung (MELANI)* statt. Ein wichtiger Teil der Prävention liegt aber auch in der Abschreckung von Angriffen. Diese wird dadurch erreicht, dass auf einen Angriff die Identifikation des Angreifers und aktive Gegenmassnahmen erfolgen können, und der potentielle Angreifer sich diesen Konsequenzen bewusst ist. Solche Gegenmassnahmen sind zwar in der Massnahme 14[35] der NCS geplant, wie diese Gegenmassnahmen aber genau aussehen, ist unklar. Es wird lediglich gesagt, dass die Infrastruktur der Gegenseite beeinträchtigt werden kann.

Hier stellt sich auch die Frage, wie die rechtlichen und völkerrechtlichen Aspekte von Cyberangriffen bzw. vom Cyberwarfare aussehen. Ab wann ist ein Cyberangriff als ein „bewaffneter Angriff" zu werten? Reicht dabei ein Schaden an IT-Systemen oder muss ein physischer Schaden erfolgen? Was für Gegenmassnahmen sind legitim? Diese und viele weitere Fragen sind zu klären, da sie den Handlungsspielraum der Schweiz definieren. Die Massnahme 16[36]. der NCS macht einen Schritt in diese Richtung, indem die rechtlichen Grundsätze im Hinblick auf die Massnahmen überprüft und allfällige Anpassungen vorgenommen werden. Leider ist auch diese Massnahme

[34] Siehe Abbildung 1
[35] Siehe Tabelle 4, S. 41 & Anhang – Massnahmen der NCS
[36] Siehe Tabelle 4, S. 41 & Anhang – Massnahmen der NCS

relativ ungenau ausgestaltet. Es ist unklar, welche rechtlichen Aspekte gemeint sind und wie umfassend die Anpassungen geplant sind. Zudem fehlt hier die Zusammenarbeit mit anderen Staaten, da die völkerrechtlichen Aspekte ein internationales Anliegen sind.

5.2.2 Umsetzung der Massnahmen

Für die Umsetzung der Massnahmen der NCS wurde ein dezentraler Ansatz gewählt. Dies hat den Vorteil, dass damit die ebenfalls dezentral organisierte Wirtschafts- und Staatsstruktur der Schweiz wiedergespiegelt wird. Somit kann auf den bestehenden Strukturen aufgebaut werden, indem deren Cyberausprägungen ermittelt und die erkannten Risiken minimiert werden können.

Zur Umsetzung dieses dezentralen Ansatzes wurde auf eine zentrale Führungsstelle verzichtet. Stattdessen wurden ein Steuerungsausschuss und eine Koordinationsstelle errichtet, welche die unterschiedlichen Bestrebungen in den verschiedenen Organisationseinheiten abstimmen sollen. Der Vorteil liegt darin, dass die vielen unterschiedlichen Akteure so in den Prozess mitinvolviert werden können, indem sie ihre Interessen und ihr Fachwissen einbringen. Dies hat aber den entscheidenden Nachteil, dass keine klare Führung besteht, welche effiziente Entscheidungen fällen und die Umsetzung vorantreiben kann. Die Resultate sind ineffiziente interne Debatten und ein langsamer Fortschritt in der Umsetzung der NCS.

Die Massnahmen der NCS sind generell sehr offen gehalten. Dies hat einerseits den Vorteil, dass die für die jeweiligen Massnahmen zuständigen Organisationseinheiten viel Freiheit in der Umsetzung haben. Sie können somit ihre Erfahrungen, ihr Fachwissen ihres jeweiligen Bereiches und ihre eigenen Bedürfnisse einfliessen lassen. Der Nachteil besteht aber darin, dass den zuständigen Organisationseinheiten Richtlinien zur Umsetzung fehlen und sie zu wenig Unterstützung erhalten. Laut Gérald Vernez, dem Delegierten des Chefs der Armee für Cyber-Defence, sind gewisse Unternehmen und Behörden der Kantone sehr verärgert, da sie konkrete Handlungsvorschläge aus der NCS erwartet haben und nicht nur eine generelle Methodik (Vernez, personal communication, 2014a).

Da diese Massnahmen sehr offen sind, wurden auch keine präzisen Meilensteine definiert, an welchen der Fortschritt der Umsetzung gemessen werden kann. In der *Roadmap NCS*[37] sind wohl Meilensteine vorhanden, doch diese enthalten keine konkreten Lieferprodukte, welche jeweils pro Meilenstein erwartet werden. Zudem sollten diese Lieferprodukte die jeweils benötigten Ressourcen aufzeigen. Da der Fortschritt der NCS dadurch nicht transparent ist, kann keine effiziente Projektführung stattfinden. Folglich dauert die Umsetzung länger und sie wird teurer.

[37] http://www.isb.admin.ch/themen/01709/01841/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCEeoN5gGym162epYbg2c_JjKbNoKSn6A--&t=.pdf

Es besteht auch die Möglichkeit, dass sich im Rahmen der Umsetzung der Massnahmen ein Interessenskonflikt bei den zuständigen Organisationseinheiten ergibt. Da beispielsweise die Betreiber der kritischen Infrastrukturen (KI) meist private Unternehmen sind, ist deren primäres Ziel die Profitabilität. Neue Sicherheits- und Schutzmassnahmen verursachen aber Mehrkosten und liegen somit nicht unbedingt im Interesse der KI-Betreiber. Diese könnten die Umsetzung der Massnahmen behindern und somit deren Fortschritt bremsen, insbesondere aufgrund ihrer starken Beteiligung an der Umsetzung. Dieser Interessenskonflikt ist aber inhärent gegeben und nicht durch die NCS, da die KI-Betreiber dem Wettbewerb ausgesetzt sind.

Ein weiteres Problem ist der Mangel an qualifiziertem Fachpersonal, denn dieses ist ein integraler Teil in der Umsetzung der NCS. So sind nicht nur Techniker gefragt, sondern auch Krisenmanager, Nachrichtendienstanalysten, Forscher, Ausbildner, etc. Es besteht weltweit ein grosser Wettbewerb um solche Spezialisten. Dieser wird sich zudem in den kommenden Jahren weiter verschärfen. Einerseits aufgrund der wachsenden Bedeutung der Cyberwarfare-Thematik, andererseits wegen der generell zunehmenden Abhängigkeit von der Informationstechnologie. Diese Problematik besteht aber nicht nur in der Schweiz, sondern auch international. Auch die USA und China haben Mühe solche Spezialisten anzuwerben, auch wenn offizielle Berichte zu ihren Massnahmen Anderes glauben lassen.

5.2.3 NCS aus Sicht des Vorsorgeprinzips

Als die *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)* 2012 vom Bundesrat verabschiedet wurde, waren Cyberangriffe tieferer Intensität, wie zum Beispiel Cyberspionage, schon weit etabliert und ein allgegenwärtiges Risiko. Die ersten Vorfälle der Cyberspionage ereigneten sich bereits Anfangs des 21. Jahrhunderts. Es gab also frühe Warnzeichen für dieses Risiko, welche aber lange ignoriert wurden. Hinsichtlich des Vorsorgeprinzips lässt sich also sagen, dass für diese Angriffe tieferer Intensität zu spät gehandelt wurde und man nun eigentlich *Gefahrenabwehr* betreibt, anstatt *Vorsorge* zu leisten.

Angriffe hoher Intensität, wie zum Beispiel ein Sabotageakt an kritischen Infrastrukturen, sind auch in der Schweiz noch nicht vorgekommen. Wie im Kapitel 4.1, über die Risiken des Cyberwarfare aber gezeigt wurde, besteht auch für die Schweiz das Risiko, dass sie in Zukunft solchen Angriffen ausgesetzt sein könnte. So hat der Bundesrat 2013 eine *strategische Führungsübung (SFU 13)* durchgeführt, welche ein Szenario mit verschiedenen Cyberangriffen auf die Schweiz vorsah. Unter anderem auf Finanzinstitute (*Postfinance, UBS AG* und verschiedene Kantonalbanken*)*, Schienenverkehr (*SBB)* und eine Chemiefabrik. Die SFU 13 hat gezeigt, dass die Schweiz bezüglich der bestehenden Bedrohungslage zu wenige Ressourcen investiert. Das liegt primär daran, dass die Verantwortlichen der NCS diesen Risiken zu wenig Beachtung schenken. Denn viele sehen diese als zu unwahrscheinlich, um sich ernsthaft damit auseinanderzusetzen und Ressourcen zu investieren. Aus Sicht des Vor-

sorgeprinzips ist dies aber ein fataler Fehler. Denn Risiken sollten auch dann behandelt werden, wenn ihre Eintrittswahrscheinlichkeit noch schwer eingeschätzt werden kann und wissenschaftliche Aussagen über das Ausmass des möglichen Schadens noch mit hoher Unsicherheit verbunden sind. Zudem ist die massive Auswirkung eines Sabotageangriffs auf kritische Infrastrukturen, wie zum Beispiel auf die Stromversorgung, in Betracht zu ziehen und gegen die Wahrscheinlichkeit abzuwägen. Die Zeit zum Handeln ist also jetzt, bevor sich dieses Risiko als akute Bedrohung manifestiert und es zu spät ist um Vorsorge zu leisten.

5.3 Ausblick

Aufgrund der in Kapitel 5.2 gewonnen Erkenntnissen, werden in diesem Kapitel einige Handlungsvorschläge für die Schweiz und ihre *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)* vorgestellt.

Die höchste Priorität der Schweiz sollte die schnellstmögliche Umsetzung der geplanten 16 Massnahmen[38] der NCS sein. Denn ohne diese ist die Schweiz verwundbar, da sie keine grössere Cyberangriffe abwehren kann, geschweige denn mit den resultierenden Folgen umgehen kann. Laut Gérald Vernez haben insbesondere die Massnahmen 2, 3, 4, 13, 14 und 15[38] Priorität, da sich diese vor allem mit der Prävention, aber auch der Reaktion und dem Kontinuitäts- und Krisenmanagement befassen[39] und somit das Grundgerüst für eine effektive Verteidigung darstellen (Vernez, personal communication, 2014a).

Dazu sollten einerseits die Massnahmen konkretisiert werden, um den beteiligten Akteuren mehr als nur eine Methodik bzw. Guideline zu bieten. So kann auch dem Interessenskonflikt, zwischen der Erhöhung der Sicherheit und der Profitabilität der Unternehmen, vorgebeugt werden, indem den Betreibern der kritischen Infrastrukturen genauere Handlungsvorschläge gegeben und eventuell sogar Sicherheitsvorschriften erlassen werden.

Parallel sollten die definierten Meilensteine konkretisiert werden, indem genaue Lieferobjekte, mit den jeweils benötigten Ressourcen, definiert werden. Damit wird für die Projektverantwortlichen der Fortschritt der Umsetzung transparenter und das Projekt kann besser und zielgerichteter gesteuert werden.

Man sollte auch in Erwägung ziehen, eine Führungsstelle mit einer grösseren Entscheidungskompetenz auszustatten. Damit könnten Entscheide effizienter gefällt und somit der Fortschritt massgebend schneller vorangetrieben werden. Es ist aber wichtig zu erkennen, dass ein Trade-off zwischen schnellem Vorankommen und dem optimalen Einbezug aller beteiligten Akteure besteht.

[38] Siehe Tabelle 4, S. 41 & Anhang – Massnahmen der NCS
[39] Siehe Abbildung 3

Ein weiterer Ansatzpunkt ist die Rekrutierung von Fachpersonal. Ohne diese fehlt es an spezialisiertem Wissen, welches bei der Umsetzung von grosser Bedeutung ist. Es sollten also weitere Massnahmen getroffen werden, um dieses Defizit kurz-, sowie langfristig zu verringern. Kurzfristig kann eine Rekrutierungsplattform erstellt werden, über welche der Kontakt zu Fachkräften hergestellt werden kann. Zudem könnte aktiv Werbung gemacht werden, beispielsweise für baldige Studienabgänger an Universitäten. Eine weitere Möglichkeit besteht in dem Aufbau eines Kompetenznetzwerks durch den Staat, in Zusammenarbeit mit Unternehmen der Privatwirtschaft. So kann das vorhandene Wissen unter den verschiedenen Akteuren ausgetauscht und verbreitet werden. Langfristig gesehen, kann in die Bildung investiert werden, um spezialisiertes Wissen zu fördern. Dies kann durch das Anbieten oder Sponsoring von Kursen und Studiengängen an Universitäten erfolgen.

Neben der schnellen Umsetzung der 16 Massnahmen der NCS ist es sehr wichtig, dass die Strategie insofern erweitert wird, dass die Schweiz auch gegen Cyberangriffe höherer Intensitäten gewappnet ist. Dies hat insbesondere eine Bedeutung, wenn die Risiken aus Sicht des Vorsorgeprinzips betrachtet werden. Will man also vorsorglich handeln, sollte schon jetzt mit einem höheren Bedrohungslevel gerechnet und entsprechende Massnahmen eingeleitet werden. Dazu muss aber die aktuelle Denkweise revidiert werden, welche die Risiken der Angriffe hoher Intensität aufgrund der geringen Eintrittswahrscheinlichkeit ignoriert.

Literaturverzeichnis

Addley, E., & Halliday, J. (2010, September 12). WikiLeaks supporters disrupt Visa and MasterCard sites in 'Operation Payback': MasterCard and Visa attacked after restricting dealings with WikiLeaks – and hackers say Twitter is next. *The Guardian*. Retrieved from http://www.theguardian.com/world/2010/dec/08/wikileaks-visa-mastercard-operation-payback

Albright, D., Brannan, P., & Walrond, C. (2010). *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* Retrieved from http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

Beer, T. (2005). *Cyberwar: Bedrohung für die Informationsgesellschaft*. Marburg: Tectum.

Beyer, H.-M. (1992). *Das Vorsorgeprinzip in der Umweltpolitik*. *Schriftenreihe Wirtschafts- und Sozialwissenschaften: Bd. 10*. Ludwigsburg: Verlag Wissenschaft & Praxis.

Boyd, I. M. (2000). *The Fundamentals Of Computer HACKING*. Retrieved from http://www.sans.org/reading-room/whitepapers/hackers/fundamentals-computer-hacking-956

Brown, C. (2011). *SI110 Introduction to Cyber Security Technical Foundations*. Retrieved from http://www.usna.edu/CS/si110/lec/l32/lec.html

Bundesamt für Bevölkerungsschutz. (2010a). *Schienenverkehr: Beschreibung der Teilsektoren Kritischer Infrastrukturen in der Schweiz*. Retrieved from http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/kritische_infrastrukturen.parsys.0001210.downloadList.55826.DownloadFile.tmp/schienenverkehrd.pdf

Bundesamt für Bevölkerungsschutz. (2010b). *Telekommunikation: Beschreibung der Teilsektoren Kritischer Infrastrukturen in der Schweiz*. Retrieved from http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/kritische_infrastrukturen.parsys.0001140.downloadList.1068.DownloadFile.tmp/telekommunikationd.pdf

Bundesamt für Bevölkerungsschutz. (2012a). *Banken: Beschreibung der Teilsektoren Kritischer Infrastrukturen in der Schweiz*. Retrieved from http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/kritische_infrastrukturen.parsys.000171.downloadList.9030.DownloadFile.tmp/bankend.pdf

Bundesamt für Bevölkerungsschutz. (2012b). *Nationale Strategie zum Schutz kritischer Infrastrukturen*. Retrieved from http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/nationaleskistrategie.parsysrelated1.54058.downloadList.15281.DownloadFile.tmp/natstratski2012d.pdf

Bundesamt für Bevölkerungsschutz. (2012c). *Stromversorgung: Beschreibung der kritischen Infrastruktur-Teilsektoren in der Schweiz*. Retrieved from

http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/kritische_infrastrukturen.parsys.000130.downloadList.56418.DownloadFile.tmp/stromversorgungd.pdf

Bundesamt für Statistik. (2012). *Bruttowertschöpfung nach Sektor*. Retrieved from http://www.bfs.admin.ch/bfs/portal/de/index/themen/07/03/blank/ind24.indicator.240102.2401.html

Clausewitz, C. v., Howard, M. E., & Paret, P. (1984). *On War*. Princeton, N.J: Princeton University Press.

Denning, D. E. (2000). *CYBERTERRORISM: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*. Retrieved from http://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm

Deutscher Bundestag. (1976). *Umweltbericht '76: Fortschreibung des Umweltprogramms der Bundesregierung vom 14. Juli 1976*. Stuttgart: W. Kohlhammer.

Dunn Cavelty, M. (2013). Gefahrendarstellungen im Cyber(un)Sicherheitsdiskurs. In C. Daase, S. Engert, & J. Junk (Eds.), *Verunsicherte Gesellschaft - überforderter Staat. Zum Wandel der Sicherheitskultur.* Frankfurt am Main: Campus Verlag.

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation. *Zukunft der nationalen Infrastrukturnetze in der Schweiz: Schiene*. Retrieved from http://www.uvek.admin.ch/infrastrukturstrategie/02570/02597/02599/?lang=de

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation. (2014). *Zuverlässige Energieversorgung dank breiter Abstützung: Viele Glieder in der Stromversorgungskette*. Retrieved from http://www.uvek.admin.ch/themen/service_public/00605/?lang=de

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport. (2012). *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken*. Retrieved from http://www.isb.admin.ch/themen/01709/01710/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCEeX9,fGym162epYbg2c_JjKbNoKSn6A--&t=.pdf

European Environment Agency. (2001). *Late lessons from early warnings: The precautionary principle 1896-2000*. *Environmental issue report: Vol. 22*. Copenhagen, Luxembourg: Office for official publications of the European communities.

Expertenkommission zur Limitierung von volkswirtschaftlichen Risiken durch Grossunternehmen. (2010). *Schlussbericht der Expertenkommission zur Limitierung von volkswirtschaftlichen Risiken durch Grossunternehmen*. Retrieved from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCgQFjAA&url=http%3A%2F%2Fwww.sif.admin.ch%2Fdokumentation%2F00514%2F00519%2F00592%2Findex.html%3Fdownload%3DNHzLpZeg7t%2Clnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdIN2hGym162epYbg2c_JjKbNoKSn6A--

%26lang%3Dde&ei=KMnuUoHSLuK64AT8-ID4Bw&usg=AFQjCNHmdcsxRE-HIsxhUus_S_bxIaBX1-g&sig2=219r99cwshkBzciic-QbZLA&bvm=bv.60444564,d.bGE

Gaycken, S. (2011). *Cyberwar: Das Internet als Kriegsschauplatz* (1. Aufl). *Changes*. München: Open Source Press.

Gaycken, S. (2012). Die vielen Plagen des Cyberwar. In R. Schmidt-Radefeldt & C. Meissler (Eds.), *Forum Innere Führung: Bd. 35. Automatisierung und Digitalisierung des Krieges. Drohnenkrieg und Cyberwar als Herausforderungen für Ethik, Völkerrecht und Sicherheitspolitik* (pp. 89–116). Baden-Baden: Nomos.

Gorman, S., Cole, A., & Dreazen, Y. (2009, April 21). Computer Spies Breach Fighter-Jet Project. *The Wallstreet Journal*. Retrieved from http://online.wsj.com/news/articles/SB124027491029837401?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB124027491029837401.html#mod=todays:us_page_one

Handelszeitung & Bisnode. (2013). *Top 500: Die grössten Unternehmen der Schweiz*. Retrieved from http://www.segmentas.ch/top500

Hilty, L. M., Behrendt, S., Binswanger, M., Bruinink, A., Erdmann, L., Fröhlich, J., … (2003). *Das Vorsorgeprinzip in der Informationsgesellschaft: Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt*. *Technology assessment: Vol. 46*. Bern: Zentrum für Technologiefolgen-Abschätzung.

ICF Consulting. (2003). *The Economic Cost of the Blackout:: An issue paper on the Northeastern Blackout, August 14, 2003*. Fairfax, VA. Retrieved from http://www.solarstorms.org/ICFBlackout2003.pdf

Informatiksteuerungsorgan des Bundes. (2013). *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken: Umsetzungsplan NCS*. Retrieved from http://www.news.admin.ch/NSBSubscriber/message/attachments/30607.pdf

Jaruzelski, B., Loehr, J., & Holman, R. (2013). The Global Innovation 1000: Navigating the Digital Future. *Strategy+Business*, (73), 33–45. Retrieved from http://www.booz.com/media/file/BoozCo_2013-Global-Innovation-1000-Study-Navigating-the-Digital-Future.pdf

Kaperonis, I. (1984). Industrial Espionage. *Computers & Security*, *3*(2), 117–121. doi:10.1016/0167-4048(84)90053-1

Kloepfer, M. (2004). *Umweltrecht* (3. Aufl). München: C.H.Beck.

Koechlin, D. (1989). *Das Vorsorgeprinzip im Umweltschutzgesetz: Unter besonderer Berücksichtigung der Emissions- und Immissionsgrenzwerte*. *Neue Literatur zum Recht Nouvelle littérature juridique Nuova letteratura nel campo del diritto*. Basel: Helbing & Lichtenhahn.

Krekel, B. (2009). *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. McLean, VA. Retrieved from http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-030.pdf

Lewis, J. A. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Retrieved from http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

Lewis, J. A. & Neuneck, G. (2013). *The Cyber Index: International Security Trends and Realities*. Geneva, Switzerland. Retrieved from http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Marti, U. (2011). *Das Vorsorgeprinzip im Umweltrecht: Am Beispiel der internationalen, europäischen und schweizerischen Rechtsordnung*. *Collection genevoise*. Zürich: Schulthess.

Millican, A. (2003). *Network Reconnaissance - Detection and Prevention*. Retrieved from http://www.giac.org/paper/gsec/2473/network-reconnaissance-detection-prevention/104296

OConnor, T. J. (2011). *The Jester Dynamic:: A Lesson in Asymmetric Unmanaged Cyber Warfare*. Retrieved from http://www.sans.org/reading-room/whitepapers/attacking/jester-dynamic-lesson-asymmetric-unmanaged-cyber-warfare-33889?show=jester-dynamic-lesson-asymmetric-unmanaged-cyber-warfare-33889&cat=attacking

Reed, T. C. (2004). *At the Abyss:: An Insider's History of the Cold War* (1st ed). New York: Presidio Press/Ballantine Books.

Rogers, L. (2004). *What is a Distributed Denial of Service (DDoS) Attack and What Can I Do About It?* Retrieved from http://www.sei.cmu.edu/library/abstracts/news-at-sei/securitymatters20041.cfm

Rosenzweig, P. (2013). *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*. *Changing face of war*. Santa Barbara, Calif: Praeger.

Sandin, P. (1999). Dimensions of the Precautionary Principle. *Human and Ecological Risk Assessment: An International Journal*, *5*(5), 889–907. doi:10.1080/10807039991289185

Schneider, S. (2011). *Globale Neubewertung der Risiken: Teil II*. Retrieved from http://www.dbresearch.de/PROD/DBR_INTERNET_DE-PROD/PROD0000000000272628.PDF

Schwarz, G. & Schär, M. (2012). *Schweiz: Das am stärksten industrialisierte Land der Welt*. Retrieved from http://www.avenir-suisse.ch/21027/schweiz-das-am-starksten-industrialisierte-land-der-welt/

Schweizer Armee. (n.d.). *Die Aufgaben der Armee*. Retrieved from http://www.vtg.admin.ch/internet/vtg/de/home/themen/auftraege.html

Bundesgesetz über den Umweltschutz (Umweltschutzgesetz, USG), Schweizer Bundesrat 07.10.1983.

Schweizer Bundesrat. (2010). *Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz*. Retrieved from http://www.vbs.admin.ch/internet/vbs/de/home/documentation/bases/sicherheit.parsys.9457.downloadList.86387.DownloadFile.tmp/sipolbd.pdf

Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to Cyber-Warfare: A multidisciplinary approach*. Waltham MA: Syngress.

Som, C., Hilty, L. M., & Köhler, A. R. (2009). The Precautionary Principle as a Framework for a Sustainable Information Society. *Journal of Business Ethics*, *85*(S3), 493–505. doi:10.1007/s10551-009-0214-x

Thorleuchter, D., & Van den Poel, Dirk. (2013). Protecting research and technology from espionage. *Expert Systems with Applications*, *40*(9), 3432–3440. doi:10.1016/j.eswa.2012.12.051

U.S. Department of Defense. (2010a). *Statement of General Keith B. Alexander Commander United States Cyber Command before the House Committee on Armed Services*. Retrieved from http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf

U.S. Department of Defense. (2010b). *U.S. Cyber Command Fact Sheet*. Retrieved from http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf

U.S. Department of Defense. (2011). *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*. Retrieved from http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf

Van den Daele, Wolfgang. (2001). Zur Reichweite des Vorsorgeprinzips: Rechtliche und politische Perspektiven. *Gentechnik im nichtmenschlichen Bereich--was kann und was sollte das Recht regeln*, 101–125.

Vernez, G. (2013). Cyber-Defence: Quo vadis?: Teil 2: Entwicklung der Bedrohung, Nationale Strategie, Rolle der Armee, Sicherheitspolitische Aspekte. *Military Power Revue*, (2), 46–52. Retrieved from http://mercury.ethz.ch/serviceengine/Files/ISN/173666/ipublicationdocument_singledocument/d5a8de22-1f6b-4983-8144-210ced9fcda5/en/Gesamtausgabe+def+18-11-2013+-+MPR+2+-+2013.pdf

Vernez, G. (2014a, März 25). Besprechung über Cybermassnahmen der Schweiz (Interview).

Vernez, G. (2014b, April 17). Besprechung über Cybermassnahmen der Schweiz (Email).

Vernez, G., Hüssy, R., & Sibilia, R. (2011). Cyber Defense der Schweiz: Teil 1: die Bedrohung und die strategische Stossrichtung. *Military Power Revue*, (1). Retrieved from http://www.vtg.admin.ch/internet/vtg/de/home/dokumentation/publik_zeitrschr/military_power_revue.parsys.79525.downloadList.6488.DownloadFile.tmp/mpr1111052011.pdf

Wiener, J. B. (2001). Precaution in a Multi-Risk World. *Human and Ecological Risk Assessment: Theory and Practice*, 1509–1531. doi:10.2139/ssrn.293859

Winterfeld, S., & Andress, J. (2013). *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Waltham MA: Syngress.

Anhang – Massnahmen der NCS

Im Folgenden werden die 16 Massnahmen der NCS (2012, pp. 34–44) genauer beschrieben:

Massnahme 1

„Die verantwortlichen Bundesstellen tauschen sich untereinander und mit Akteuren ausserhalb der Bundesverwaltung zu aktuellen und zu erforschenden Entwicklungen im Zusammenhang mit Cyber-Risiken aus und treiben bei Bedarf intra-muros Forschung oder erteilen Forschungsaufträge."

Massnahme 2

„Risiko- und Verwundbarkeitsanalysen sollen auf allen Stufen (Bund, Kantone und KI-Betreiber) unter Einbezug der IKT-Leistungserbringern und Systemlieferanten erstellt werden. Dies umfasst die selbstständige und regelmässige Überprüfung der Systeme durch die Betreiber. Die Erarbeitung von (sektoriellen) Risikoanalysen erfordert eine enge Zusammenarbeit mit den Behörden."

Massnahme 3

„Die Behörden, KI-Betreiber und Forschungseinrichtungen untersuchen, unter Einbezug der IKT-Leistungserbringer und Systemlieferanten, ihre IKT-Infrastrukturen auf Verwundbarkeiten. Dazu gehören systemische, organisatorische, und technische Schwächen. Die Erkenntnisse werden konsolidiert und bewertet und bei öffentlichem Interesse in entsprechenden Berichten publiziert."

Massnahme 4

„Aus nicht öffentlichen und öffentlichen Quellen werden nachrichtendienstliche, polizeiliche, forensische und technische Informationen zur Bedrohungs- und Risikolage im Cyber-Bereich beschafft, bewertet und analysiert. Diese Erkenntnisse sollen im Rahmen des Public-Private-Partnership-Modell von MELANI gesammelt, gesamthaft bewertet, analysiert und in einer Lagedarstellung und Lagefortschreibung fusioniert, sowie mit Lageentwicklungsmöglichkeiten versehen werden. Diese Ergebnisse werden zugunsten der relevanten und verantwortlichen Akteure zur Verfügung gestellt."

Massnahme 5

„Der Bund, die Kantone und die KI-Betreiber sollen relevante Vorfälle nachbereiten und Möglichkeiten zur Weiterentwicklung der eigenen Massnahmen im Umgang mit Vorfällen im Zusammenhang mit Cyber-Risiken überprüfen. Dies erfolgt grundsätzlich im Rahmen des eigenen Auftrags individuell. Diese Erkenntnisse sollen im Rahmen der Public-Private-Partnership von MELANI gesammelt, gesamthaft bewertet, analysiert und die Ergebnisse den relevanten Akteuren, insbesondere jenen die für

Risiko- und Verwundbarkeitsanalysen zuständig sind, zur Verfügung gestellt werden."

Massnahme 6

„Es sollen auf nationaler Ebene eine möglichst vollständige Fallübersicht (Straffälle) geführt und interkantonale Fallkomplexe koordiniert werden. Die gewonnen Informationen aus der Fallübersicht und die Erkenntnisse zu Fallkomplexen insbesondere aus der technisch-operativen Analyse der Strafverfolgung in Strafverfahren sollen in die gesamtheitliche Lagedarstellung einfliessen."

Massnahme 7

„Es soll eine Übersicht über bestehende Kompetenzbildungsangebote geschaffen werden. Diese dient als Grundlage, um einerseits Angebotslücken zu erkennen und andererseits die Akteure aus Wirtschaft, Verwaltung und Zivilgesellschaft bedürfnisgerecht über Angebote zum Umgang mit Cyber-Risiken zu informieren."

Massnahme 8

„Es sollen erkannte Lücken des Kompetenzbildungsangebots zum Umgang mit Cyber-Risiken angegangen, wie auch die vermehrte Nutzung der bestehenden qualitativ hochstehenden Angebote vorangetrieben werden."

Massnahme 9

„Die Schweiz (Wirtschaft, Gesellschaft, Behörden) setzt sich aktiv und soweit möglich koordiniert für eine Internet-Governance ein, welche mit den Schweizer Vorstellungen von Freiheit und (Selbst-)Verantwortung, Grundversorgung, Chancengleichheit, Menschenrechten und Rechtsstaatlichkeit vereinbar ist. Die Schweiz setzt sich zudem für eine vernünftige Internationalisierung und Demokratisierung der Internetverwaltung ein. Durch ihre Erfahrung im demokratischen Entscheidfindungsprozess erbringt sie einen Mehrwert bei der Konsensfindung."

Massnahme 10

„Die Schweiz kooperiert auf der Ebene der internationalen Sicherheitspolitik, um der Bedrohung im Cyber-Raum in Zusammenarbeit mit anderen Staaten und internationalen Organisationen zu begegnen. Sie verfolgt die entsprechenden Entwicklungen auf diplomatischer Ebene und fördert den politischen Austausch im Rahmen von internationalen Konferenzen und anderen diplomatischen Initiativen."

Massnahme 11

„Im Rahmen privater und staatlicher Initiativen, Konferenzen und Standardisierungsprozessen im Bereich Sicherheit und Sicherung koordinieren sich die Betreiber, Verbände und Behörden, um sich in diese Gremien einzubringen."

Massnahme 12

„Die Akteure aus Wirtschaft, Gesellschaft und Behörden sollen mit einem Kontinuitätsmanagement die Widerstandsfähigkeit (Resilienz) gegenüber Störungen und Ereignissen in enger Zusammenarbeit stärken und verbessern."

Massnahme 13

„In einer Krise sollen die Aktivitäten in erster Linie mit den direkt betroffenen Akteuren durch MELANI koordiniert und die Entscheidfindungsprozesse innerhalb der bestehenden Strukturen für das Krisen- Kontinuitätsmanagement mit fachlicher Expertise unterstützt werden, um ein kohärentes Handeln zur Bewältigung der Krise zu gewährleisten. Dabei sind auch die Gesetzmässigkeiten der Strafverfolgung zu berücksichtigen. Der nationale und internationale Informationsaustausch spielt für die Krisenbewältigung eine wesentliche Rolle und muss deshalb sichergestellt werden und koordiniert erfolgen."

Massnahme 14

„Im Falle einer spezifischen Bedrohung werden aktive Massnahmen zur Identifikation der Täterschaft und ihrer Absichten, zur Ermittlung der Fähigkeiten der Täterschaft und zur Beeinträchtigung ihrer Infrastruktur vorgesehen."

Massnahme 15

„Es soll dafür gesorgt werden, dass Führungsabläufe und -prozesse innerhalb der bestehenden Strukturen, welche einem erhöhten Führungsrhythmus zur zeitgerechten Problemlösung im Falle einer Krise dienen, der Cyber-Ausprägung Rechnung tragen. Dies erfolgt in Abstimmung mit der Nationalen Strategie zum Schutz Kritischer Infrastrukturen und den Departementen."

Massnahme 16

„Bestehende rechtliche Grundlagen sind im Hinblick auf die Massnahmen auf ihre Kohärenz und Lückenlosigkeit hin zu überprüfen. Dabei ist eine Priorisierung vorzunehmen um jene Grundlagen unverzüglich anzupassen, die nicht erst im Rahmen einer periodischen Revision einer Überarbeitung bedürfen."