Cyber Defence - eine nationale Herausforderung (Teil 1)

Cyber Defence - eine nationale Herausforderung (Teil 1)

Walter J. Unger[1),2)]/Sigmar Stadlmeier/Andreas Troll

Der Cyberspace ist jener virtuelle[3)] Raum, der durch die Vernetzung von Computern entstanden ist. Derzeit sind bereits mehr als zwei Milliarden Menschen und zirka fünf Milliarden Geräte Teil dieses Cyberspace. Die Vernetzung nimmt nach wie vor stark zu, bis 2020 werden Schätzungen zufolge etwa fünf Milliarden Menschen und 20 Milliarden Geräte vernetzt sein.

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

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

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

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

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

Bedrohungsbild

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

Verwundbare Informationsgesellschaft

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

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

Bisherige „Industriegesellschaften“ sind auf dem Weg, „Informationsgesellschaften“ zu werden. Sie basieren (noch immer) auf der industriellen Produktion, aber mittlerweile sind der Wirtschaftsstandort und die Daseinsvorsorge erheblich vom Funktionieren der Informations- und Kommunikationsflüsse abhängig.[14)] Damit wird ein Staat aber auch gegenüber einer Störung dieser Datenflüsse anfällig. Diese zunehmende Abhängigkeit der Informationsgesellschaft von ihren Informations- und Kommunikationssystemen einerseits und die Verwundbarkeit dieser Systeme andererseits schaffen Angriffspunkte, die gezielt genutzt werden könnten, um eine Informationsgesellschaft oder Teile davon zu schwächen oder ihre Funktionalität dauerhaft und massiv zu stören. Österreich ist, wie andere postmoderne Staaten, in erheblichem Ausmaß vom Funktionieren seiner kritischen Informationsinfrastrukturen abhängig.

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

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

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

Cyber-Risikospektrum

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

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

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

Cyberwar - Analyse der Bedrohung

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

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

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

Klaus Naumann, ehemals Generalinspekteur der deutschen Bundeswehr und Vorsitzender des Militärausschusses der NATO, erwartet, dass sich *„mittelfristig über Cyber Crime und Cyber Terror die Tore zum Cyberwar öffnen könnten“*. Er meint, dass *„sehr große Staaten ab 2020 in der Lage sein dürften, kleinere Staaten teilweise oder gänzlich elektronisch auszuschalten“*.[20)]

Für Joseph S. Nye, den ehemaligen stellvertretenden US-Verteidigungsminister, ist *„…der Cyberkrieg, auch wenn er derzeit erst in den Kinderschuhen steckt, die dramatischste aller potenziellen Bedrohungen. Große Staaten mit hoch entwickelten technischen und menschlichen Ressourcen könnten im Prinzip durch Cyberangriffe auf militärische und zivile Ziele enorme Störungen und physische Zerstörungen anrichten.“* [21)]

Es ist davon auszugehen, dass etliche Staaten[22)] sich mit der systematischen Vorbereitung von Cyberattacken beschäftigen; einerseits, um im Rahmen eines Verteidigungsfalles Cybergegenangriffe starten zu können, andererseits, um in einem Konflikt zur raschen Erreichung eines politischen Zieles offensiv agieren zu können.

Diese Annahme bestätigte Ehud Barak,[23)] der ehemalige Ministerpräsident und Verteidigungsminister Israels, im Plenum des europäischen Cyber-Security-Gipfels am 11. November 2013 in Bonn, als er sagte, dass eine Armee die Landesinteressen im Web nur dann wahren könne, wenn sie die Möglichkeit habe, sich in die Computersysteme seiner Gegner zu „hacken“.

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

Szenario Cyberwar

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

- Versorgung mit elektrischer Energie,

- Telekommunikationsdienstleistungen,

- Internet,

- Banken und Geldversorgung,

- Militär, Sicherheits- und andere Behörden,

- Kraftwerk- und Staubeckensteuerungen,

- Krankenhäuser und Notfalleinrichtungen,

- Österreichischer Rundfunk (ORF), andere Medien,

- Luftverkehrskontrollzentren, Flughäfen,

- Lebensmittel- und Wasserversorgung, Abwasserentsorgung,

- Bundesbahn und andere Logistikunternehmen…

Auch wenn mit Cyberangriffen direkt keine physische Gewalt angewendet wird, ist indirekt mit Opfern in erheblichem Ausmaß zu rechnen.[24] Maßnahmen zur Beeinflussung des Willens der Bevölkerung und Regierung über neue und herkömmliche Medien (Manipulation von Internetauftritten etc.) könnten die Angriffe begleiten. Diplomatische, ökonomische feindselige Akte, verdeckte Operationen sowie eine Eskalation und der Übergang in offene militärische Maßnahmen sind zu verschiedenen Zeitpunkten des Konflikts nicht auszuschließen.[25]

Mittel und Methoden, Vorteile für den Angreifer

Zur Durchführung komplexer Cyberangriffe eignen sich Bot-Netze,[26] bösartige, schadenverursachende Software,[27] die Einbringung von schadhafter Hardware ebenso wie Methoden zur Störung bzw. Lähmung der IKT, z.B. DDoS-Attacken.[28] Die Vorteile für den Angreifer liegen darin, dass die Mittel preiswert sind, die Wahrscheinlichkeit, entdeckt zu werden, gering ist, eine juristische Strafverfolgung kaum möglich ist und die Angriffe unabhängig von Zeit und Ort sind.

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

Ableitungen

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

Da technische Vorbereitungsaktivitäten für einen Cyberangriff frühzeitig nur schwer bzw. gar nicht direkt erkennbar sind, könnten Attacken überraschend ohne Vorwarnung beginnen. Allenfalls können Indizien für die Aufklärung potenzieller Ziele erkannt werden. Jedoch laufen permanent Aktivitäten zur Ausspähung von Servern und Netzen, wobei die Zuordnung zur Vorbereitung eines kriegerischen Aktes ohne zusätzliche Erkenntnisse aus anderen Bereichen zunächst unmöglich ist.[29]

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

Dies bedeutet, dass potenzielle Angriffsziele - strategische Infrastrukturen - auch im tiefsten Frieden optimal geschützt werden müssen. Systeme und Organisationen, die nicht vorbereitet sind, könnten enorme Schäden erleiden. Daraus folgt, dass die erste „Verteidigungslinie“ zunächst einmal präventive Maßnahmen sind. Diese Sicherheitsmaßnahmen und die eingesetzte IKT müssen permanent auf aktuellem Stand gehalten, auditiert sowie an geänderte Bedrohungslagen angepasst werden (Patch-Management,[30] Verstärken physischer Sicherheitsmaßnahmen etc.). Darüber hinaus sind Vorkehrungen für eine rasche Warnung und Alarmierung zu treffen.

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

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

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

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

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

Außerdem sind unverzüglich Maßnahmen zur Härtung der IKT-Systeme umzusetzen. Das Postulat, Angriffe seien nicht wiederholbar,[31] stimmt nur dann, wenn beobachtete Angriffe/Schadware mit Reverse-Engineering-Methoden analysiert, die eigenen Systeme gepatcht und das Personal fortgebildet werden. Ein permanenter Lessons Learned-Prozess auf der Basis aktualisierter unterstützender Wissensdatenbanken ist unabdingbar.

Herausforderungen

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

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

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

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

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

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

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

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

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

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

Cyber Defence - europäische und nationale Strategien

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

1. Widerstandsfähigkeit gegenüber Cyberangriffen,

2. drastische Eindämmung der Cyberkriminalität,

3. Entwicklung einer Cyberverteidigungspolitik und von Cyberverteidigungskapazitäten im Zusammenhang mit der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP),

4. Entwicklung der industriellen und technischen Ressourcen für die Cybersicherheit,

5. Entwicklung einer einheitlichen Cyberraumstrategie der EU auf internationaler Ebene und Förderung der Grundwerte der EU.

Die Entwicklung einer Cyberverteidigungspolitik

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

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

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

- Prüfung der operativen Anforderungen an die Cyberverteidigung der EU und Förderung der Entwicklung von Cyberverteidigungskapazitäten und -technologien auf EU-Ebene, wobei alle Aspekte des Kapazitätsaufbaus zu behandeln sind (u.a. grundlegende Ziele, Leitung, Organisation, Personal, Schulung, Technologie, Infrastruktur, Logistik und Interoperabilität);

- Entwicklung eines EU-Rahmens für die Cyberverteidigungspolitik, um die Netze bei GSVP-Missionen und -Operationen zu schützen, unter Einbeziehung eines dynamischen Risikomanagements, einer besseren Bedrohungsanalyse der Bedrohungen und des Informationsaustauschs; Verbesserung der Möglichkeiten der militärischen Seite (im europäischen und multinationalen Kontext), Cyberverteidigungsschulungen und -übungen zu besuchen bzw. durchzuführen (u.a. durch Einbeziehung von Cyberverteidigungsaspekten bei bestehenden Übungen);

- Förderung des Dialogs und der Koordinierung zwischen zivilen und militärischen Beteiligten in der EU, wobei der Schwerpunkt v.a. auf dem Austausch empfehlenswerter Vorgehensweisen, dem Informationsaustausch, der frühzeitigen Warnung, der Reaktion auf Sicherheitsvorfälle, der Risikobewertung, der Sensibilisierung bzw. der Herstellung der Cybersicherheit insgesamt liegen sollte;

- Pflege des Dialogs mit den Partnern auf internationaler Ebene, u.a. mit der NATO, anderen internationalen Organisationen und multinationalen Exzellenzzentren, um effektive Verteidigungskapazitäten zu gewährleisten, Bereiche einer möglichen Zusammenarbeit zu ermitteln und Doppelarbeit zu vermeiden.

Sicheres und vertrauenswürdiges digitales Umfeld

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

- Jeder Mitgliedstaat muss eine NIS-Strategie entwickeln und eine zuständige nationale Behörde mit ausreichender Finanz- und Personalausstattung für die Prävention von NIS-Risiken und -Vorfällen sowie den Umgang damit und die Reaktion darauf benennen;

- ein Kooperationsmechanismus zwischen Mitgliedstaaten und Kommission muss geschaffen werden für den Austausch von Frühwarnungen vor Sicherheitsrisiken und -vorfällen sowie für die Koordinierung und die Durchführung regelmäßiger gegenseitiger Überprüfungen;

- Betreiber kritischer Infrastrukturen in bestimmten Bereichen (Finanzdienste, Verkehr, Energie und Gesundheitswesen), Betreiber zentraler Dienste der Informationsgesellschaft (v.a. App-Stores, eCommerce-Plattformen, Internet-Zahlungen, Cloud-Computing, Suchmaschinen, soziale Netze) und öffentliche Verwaltungen müssen Risikomanagementmethoden einführen und bedeutende Sicherheitsvorfälle in ihren wesentlichen Systemen melden.

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

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

Konsequenzen der EU-Vorgaben und ihre Umsetzung in Österreich

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

Österreichisches Programm zum Schutz Kritischer Infrastrukturen (APCIP)

Das Programm[42)] umfasst die Definition österreichischer kritischer Infrastrukturen (ACI), die relevanten Ableitungen für Österreich im Vergleich zur europäischen Ebene (so sind z.B. ein starker Fokus auf die verfassungsmäßigen Einrichtungen, die Aufrechterhaltung des Sozialsystems sowie Hilfs- und Einsatzkräfte zu nennen, unter besonderer Berücksichtigung der Prioritätensetzung auf Länder- und Regionalebene), die Kriterien für die Einstufung kritischer Infrastrukturen sowie strategische Ziele; sämtliche Maßnahmen der EU zur ACI werden behandelt, so z.B. die Intensivierung des Informationsaustauschs, das Erstellen von Sicherheits- und Notfallplänen oder eine Public-Private-Partnership (PPP).

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

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

Österreichische Sicherheitsstrategie

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

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

Österreichische Strategie für Cyber-Sicherheit (ÖSCS)

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

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

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

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

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

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

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

Im Handlungsfeld „Kooperation, Staat, Wirtschaft und Gesellschaft“ soll durch die Einrichtung einer Cybersicherheitsplattform, die Stärkung der Unterstützung für KMUs (Klein- und Mittelunternehmen) und die Ausarbeitung einer Cybersicherheits-Kommunikationsstrategie die nationale Zusammenarbeit optimiert werden.[48]

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

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

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

Im Handlungsfeld „Internationale Zusammenarbeit“ sollen die Beteiligung Österreichs an der Umsetzung der Cybersicherheitsstrategie der EU, der Europaratskonvention über Cyberkriminalität und der Gewährleistung von Menschenrechten im virtuellen Raum, besonders durch die Kooperation mit der OSZE und als Teil der NATO-Partnerschaft, die Beteiligung an der Planung und Durchführung von länderübergreifenden Cyberübungen sowie die Koordinierung entsprechender außenpolitischer Maßnahmen durch das BMeiA bearbeitet werden.[52] Damit wird diplomatischen Maßnahmen eine hohe Bedeutung zugemessen. Der ehemalige Präsident und CEO von ICANN[53] und Gründungsdirektor des U.S. National Cybersecurity Center,[54] Rod Beckstrom, vergleicht die Bedrohungen durch Atomwaffen und Cyberwaffen und fordert ein gemeinsames Verständnis als Voraussetzung, um in einen diplomatischen Dialog einzutreten.[55] Globale Definitionen, Normen und Standards für Cybersicherheit, die von Regierungen und dem privaten Sektor gemeinsam erarbeitet werden sollten, schaffen die Basis für diplomatische Initiativen, um dem Recht auch im Cyberraum zum Durchbruch zu verhelfen.

Um diesem Ziel näher zu kommen, fordert Beckstrom zunächst Vertrauensbildung im globalen Maßstab ein. Themen für erste positive Schritte für einen Vertrauensaufbau könnten der Kampf gegen den globalen Terrorismus, gegen globale Cyberbankräuber sowie gegen Menschen- und Drogenhandel sein.[56] Nach einem gelungenen Vertrauensaufbau könnten gemeinsame Standards für einen offenen Cyberraum auf der Basis der Limitierung oder sogar Ächtung von Cyberwaffen geschaffen werden.

Völkerrechtliche Erwägungen

Während eines im Gang befindlichen bewaffneten Konflikts

a) Internationaler bewaffneter Konflikt

Abwehrmaßnahmen gegen Cyberangriffe im Zuge eines mit kinetischen[57)] Mitteln geführten bewaffneten Konflikts sind nach den üblichen Regeln des Rechts der bewaffneten Konflikte,[58)] unter Beachtung der etablierten Prinzipien Unterscheidung, militärische Notwendigkeit, Verhältnismäßigkeit und Menschlichkeit zu beurteilen. Ein allfälliger Dual-use-Charakter der Ziele solcher Maßnahmen wird bei Hard- und Software an der Tagesordnung sein. Die daraus zwangsläufig resultierende Schädigung Unbeteiligter schließt dabei den Charakter des Ziels als legitimes militärisches Ziel[59)] nicht aus, ist aber bei der Verhältnismäßigkeitsabwägung (Wie viel Kollateralschaden ist für den angestrebten militärischen Vorteil noch akzeptabel?) besonders zu berücksichtigen.[60)] Zu beachten ist im Cyber Warfare-Umfeld der besondere Schutz von Einrichtungen, die zur Lebensgrundlage für die Zivilbevölkerung gehören (z.B. Wasserversorgung, die ihrerseits von anderer kritischer Infrastruktur, etwa der Stromversorgung, abhängig sein wird).[61)] Das Perfidieverbot (Vortäuschen eines geschützten Status in der Absicht, den darauf vertrauenden Gegner zu schädigen)[62)] gilt wie im rein kinetischen Konflikt; „Kriegslisten“ wie Tarnung, Desinformation, Scheinoperationen (z.B. Simulation des Nachrichtenverkehrs nicht existierender Truppenteile) sind wie im kinetischen Konflikt erlaubt: Nach Angaben in der offenen Literatur[63)] führte Israel 2007 im Vorfeld des Luftangriffes auf eine syrische Nuklearanlage erfolgreich eine Cyberattacke gegen das Luftraumüberwachungssystem, die dazu führte, dass die Operatoren leere Bildschirme sahen, d.h. die von der Hardware (den Radargeräten) erfasste Luftbedrohung schlicht nicht angezeigt wurde und eine Reaktion daher unterblieb.

b) Nicht-internationaler bewaffneter Konflikt

In ähnlicher Weise sind die humanitären Regeln im nicht-internationalen Konflikt auch auf elektronische Einsatzmittel anzuwenden. Eine parallele Schutzbestimmung für lebenswichtige Infrastruktur ist auch in den Regeln zum nicht-internationalen bewaffneten Konflikt enthalten.[64)]

Bei bzw. vor Ausbruch eines bewaffneten Konflikts

Schwieriger gestaltet sich die Fragestellung nach der Zulässigkeit aktiver Abwehrmaßnahmen, solange (noch) kein bewaffneter Konflikt besteht. Dabei sind zwei Fragenkomplexe zu erörtern: zum einen eine Legitimation von Gegenmaßnahmen in verschiedenen Intensitätsstufen nach allgemeinem Völkerrecht, zum anderen völkerrechtliche Rahmenbedingungen für elektronische Anlagen in verschiedenen Sonderregimen (Seerecht, Luftfahrtrecht, Weltraumrecht, Telekommunikationsrecht), die als Bestandteile des Friedensvölkerrechts unterhalb der Schwelle des internationalen bewaffneten Konflikts anwendbar bleiben.

a) Abwehrmaßnahmen als Selbstverteidigung

Die UNO-Charta verbietet grundsätzlich die Androhung oder Anwendung von Gewalt gegen die Souveränität, territoriale Integrität oder die politische Unabhängigkeit (worunter politische Handlungsfreiheit zu verstehen ist) eines Staates.[65)] Dieses Verbot ist in zwei Fällen durchbrochen, nämlich hinsichtlich militärischer Sanktionen nach Kapitel VII der Charta und hinsichtlich der Ausübung des Selbstverteidigungsrechts (Art. 51 UNO-Charta).

Auslösetatbestand des Selbstverteidigungsrechts ist ein bewaffneter Angriff über einer signifikant hohen Relevanzschwelle. Für das kinetische Umfeld hat der Internationale Gerichtshof im Fall Nicaraguas gegen die USA (merits)[66)] jedenfalls klargestellt, dass nicht jede Anwendung von Gewalt (use of force) im Sinne des Art. 2 Z 4 UNO-Charta bereits die Schwelle des bewaffneten Angriffs (armed attack) im Sinne des Artikels 51 erreicht, und hat dies für vereinzelte Grenzscharmützel verneint. Es bedarf zumindest erheblicher Schäden an Leib und Leben von Personen bzw. physischer Zerstörungen an Gütern, um die Schwelle eines Angriffes zu erreichen, der zur Selbstverteidigung berechtigt.

Besteht der „Angriff“ in einer reinen Cyberattacke, muss zunächst geklärt werden, ob eine solche einen bewaffneten Angriff darstellen kann, und welche Intensitätsschwelle erreicht werden muss, um ein Recht auf Selbstverteidigung auszulösen. Der „bewaffnete“ Angriff in Art. 51 stellt auf das Konfliktbild des Zweiten Weltkriegs ab, das der UNO-Charta zu Grunde liegt; immerhin gibt es gute Argumente, auch im kinetischen Umfeld Behelfswaffen, nicht nur genuines Kriegsmaterial, dem Kriterium „bewaffnet“ genügen zu lassen, wenn sie vergleichbare Wirkungen zeitigen:[67)] So hat die NATO nach den Ereignissen des 11. September 2001, als ein koordinierter Angriff mit mehreren Passagierflugzeugen auf das World Trade Center in New York und das Pentagon in Washington erfolgte, zum ersten Mal in der Geschichte der Organisation den „Bündnisfall“ erklärt und damit die Auffassung zum Ausdruck gebracht, ein „bewaffneter Angriff“ im Sinne des Artikels 51, auf den Art. 5 des Washingtoner Vertrags ausdrücklich Bezug nimmt, sei eingetreten. Reicht aber das Spektrum „bewaffnet“ an sich über genuines Kriegsmaterial hinaus, dann können auch Cybermittel an dieser Intensitätsschwelle gemessen werden.

Zu Charakter und Intensität des Angriffs werden in der Literatur verschiedene Richtungen vertreten:[68)] Manche stellen auf die Absichten des Angreifers ab (hostile intent), andere auf die verwendeten Instrumente und ihr Potenzial (instrument-based approach), und schließlich zeichnet sich eine Mehrheit für den von Schmitt geprägten effect-based approach ab, der auf die Auswirkungen abstellt und eine Äquivalenz der Auswirkungen zu jener Schwelle verlangt, die der IGH im Fall Nicaraguas gegen die USA für den kinetischen Angriff gesetzt hat.

Das Hauptproblem in diesem Zusammenhang ist freilich nicht so sehr die Kinetik-Äquivalenz eines reinen Cyberangriffes, sondern seine Einstufung als

- gegen den Staat als Völkerrechtssubjekt und seine völkerrechtlich geschützten Grundpositionen gerichtet, und

- von einem Staat oder einem anderen Völkerrechtssubjekt ausgehend.

Die Zielrichtung gegen den Staat und seine völkerrechtlich geschützten Grundpositionen ist notwendig, weil Art. 51 UNO-Charta auf „armed attack against a member of the United Nations“ abstellt (und das können nur Staaten sein). Selbst wenn man zugesteht, dass das Selbstverteidigungsrecht ein Naturrecht (inherent right) ist, das nicht erst durch die UNO-Charta gewährt wird, sondern in der Natur seines Trägers liegt, womit auch andere Völkerrechtssubjekte in Frage kommen (etwa Aufstandsbewegungen), fehlt doch derzeit noch die völkerrechtliche Praxis, um dies zu untermauern.[69)] Hathaway u.a. bieten im Schrifttum nach einem Vergleich verschiedener Definitionen des Cyberangriffs eine Definition an, die dieser spezifischen strategischen Zielsetzung, gegen völkerrechtlich garantierte staatliche Grundpositionen gerichtet zu sein, Rechnung trägt („…any action taken to undermine the functions of a computer network for a political or national security purpose“).[70)]

Die Zurechnung (attribution) zu einem anderen Völkerrechtssubjekt ist notwendig, um völkerrechtsrelevante Angriffe auf die genannten geschützten Grundpositionen eines Staates von kriminellen bzw. terroristischen Attacken trennen zu können, auf die mit Mitteln des nationalen Rechts, insbesondere des Strafrechts und seiner Instrumente zur zwangsweisen Durchsetzung zu reagieren ist. Die Zurechnung identifiziert einen Staat (oder mehrere) als den/die Urheber des Angriffes. Das Recht der Staatenverantwortlichkeit befindet sich noch im Kodifikationsstadium, doch hat die Generalversammlung der UNO den diesbezüglichen Entwurf[71)] der International Law Commission (ein Unterorgan der Generalversammlung) angenommen und den Mitgliedstaaten zur Ratifikation empfohlen,[72)] weshalb für die Zwecke dieser Übersicht davon ausgegangen werden kann, dass der ILC-Entwurf eine konsensfähige Kodifikation des einschlägigen Völkergewohnheitsrechts darstellt.

Danach tritt die völkerrechtliche Verantwortlichkeit eines Staates nur dann ein, wenn eine ihm zurechenbare Verletzung einer völkerrechtlichen Verpflichtung vorliegt (was vom Verletzten zu beweisen ist). Dabei wird einem Staat das Handeln seiner Organe, beliehener Organe, von Personen, die unter seiner Leitung oder Aufsicht handeln, sowie faktischer Organe (die anstelle der dazu berufenen handeln) und Aufstandsbewegungen zugerechnet.

Diese Zurechnung stellt die größte faktische Herausforderung in der Cyberabwehr dar, erfordert sie doch eine Identifikation des Ausgangspunktes eines Angriffs, die bei Cyberangriffen wegen der Möglichkeit der Verschleierung von Identitäten und IP-Adressen sowie der Zwischenschaltung nichtsahnender Dritter in anderen Staaten (etwa bei Verwendung von Bot-Netzen), sehr schwierig sein kann. In der Literatur finden sich in jüngerer Zeit Vorschläge, diesem Problem mit einem strict liability approach beizukommen, der nicht auf das (nur schwer rückverfolgbare und zurechenbare) Tun der eigentlichen Täter, sondern auf das Unterlassen entsprechender Sicherheitsvorkehrungen des Staates abstellt, von dem aus der Angriff ausgegangen ist. Dies setzt aber eine positive Pflicht des Staates voraus, solche Vorkehrungen zu treffen, die in der Regel eigens völkerrechtlich begründet werden muss.[73)] Ob dies bereits nach geltendem Völkerrecht der Fall ist und auf das Schädigungsverbot gestützt werden kann, wie es sich im Umweltvölkerrecht etabliert hat,[74)] oder ob dies einer eigenen Regelung bedürfte, ist strittig.[75)] Stein und Marauhn haben vorgeschlagen, das Internet als „gemeinsame Ressource“ (vergleichbar der Hohen See) anzusehen,[76)] was eine allseitige Pflicht zum schonenden Umgang damit nach sich zöge. Eine völkerrechtliche Regelung dieser Grundsatzfrage erscheint dringend geboten.

b) Cyberabwehr als Repressalie (countermeasure)

Eine Cyberattacke, die unterhalb der Schwelle des bewaffneten Angriffs bleibt, sich aber dennoch gegen die genannten völkerrechtlich garantierten staatlichen Grundpositionen richtet, verstößt zumindest gegen das Interventionsverbot. Dieses untersagt alle Versuche, einen anderen Staat unterhalb der Schwelle bewaffneter Gewalt Zwang auszusetzen, um zu erreichen, dass er die Ausübung seiner souveränen Rechte einem fremden Willen unterordnet.[77)] Eine Völkerrechtsverletzung eines Staates kann einem anderen Staat Anlass zu Repressalien (engl. countermeasures) bieten. Darunter sind an sich rechtswidrige Handlungen eines Staates zu verstehen, die als Reaktion auf rechtswidrige Akte eines anderen Staates gegen diesen gesetzt werden und dadurch gerechtfertigt sind.[78)] Es handelt sich dabei - dogmatisch gesehen - um einen völkerrechtlichen Rechtfertigungsgrund, der das Rechtswidrige eines Handelns aufhebt; der ILC draft on State responsibility gebraucht dafür den Begriff der „circumstances precluding wrongfulness“.

Auch in diesem Fall stellt sich das Zurechnungsproblem wie vorhin diskutiert. Vor der Ergreifung von Repressalien ist der Rechtsbrecher aufzufordern, zu rechtmäßigem Verhalten zurückzukehren, und ist die Ergreifung von Repressalien anzukündigen; bei der Ergreifung von Repressalien ist auf die Verhältnismäßigkeit zwischen Rechtsbruch und Reaktion darauf zu achten und darf völkerrechtliches ius cogens (dazu gehört auch das Gewaltverbot in Art. 2 Z 4 UNO-Charta) nicht verletzt werden. Sie müssen auf die Einstellung des ursprünglichen rechtswidrigen Verhaltens gerichtet sein und sind bei Erfolg sofort einzustellen.[79)] Cyberabwehrmaßnahmen als Reaktion auf Völkerrechtsverletzungen unterhalb der Schwelle des bewaffneten Angriffes dürfen daher nicht in der Androhung oder Anwendung von Gewalt gegen die territoriale Integrität oder politische Unabhängigkeit (=Handlungsfreiheit) des Schädigers bestehen, was nur ein begrenztes Handlungsspektrum eröffnet.

c) Cyberabwehrmaßnahmen als Reaktion auf Notlage oder Staatsnotstand (distress, necessity)

Ist eine Handlung in einer Notlage die einzige vernünftige Möglichkeit, das Leben von Personen zu retten, dann entsteht daraus keine völkerrechtliche Verantwortlichkeit, es sei denn, der Staat hat zum Entstehen der Notlage beigetragen, oder das zu rechtfertigende Handeln hat eine vergleichbare oder größere Gefahr hervorgerufen.[80)] Dieser Rechtfertigungsgrund kommt ohne das Zurechnungsproblem aus, denn es ist nicht erforderlich, dass der durch die Reaktion (in Form von Cyberabwehrmaßnahmen) Geschädigte die Notlage herbeigeführt hat; der Schädiger, der die Maßnahmen ergreift, muss allerdings dartun, dass die Schädigungshandlung das einzige vernünftige Mittel ist, in dieser Notlage das Leben von Personen zu retten (z.B. einen Cyberangriff durch Gegenmaßnahmen zu stoppen, um die eigenen Netze wieder in Gang zu bringen und die Erreichbarkeit und Funktionsfähigkeit von Notdiensten sicherzustellen). Hat er jedoch (z.B. durch Vernachlässigen von Vorbereitungen zum Schutz vor Cyberangriffen) zum Eintritt der Notlage beigetragen, so muss er sich das vorwerfen lassen und kann sich nicht mehr auf die Notlage berufen, wenn er durch seine Abwehrmaßnahmen andere Staaten schädigt.

Ähnliches gilt für den Staatsnotstand: Ist eine Rechtsverletzung notwendig (d.h. geeignet und das einzige Mittel), um wesentliche Interessen eines Staates vor schwerer und gegenwärtiger Gefährdung zu schützen, dann entsteht daraus keine völkerrechtliche Verantwortlichkeit, es sei denn, der handelnde Staat hat zum Entstehen der Notstandssituation beigetragen. Die Rechtsverletzung darf sich nur nicht gegen gleichermaßen wesentliche Interessen der dadurch Geschädigten richten. Auch hier stellt sich kein Zurechnungsproblem, weil der durch Cyberabwehrmaßnahmen Geschädigte nicht der Verursacher des Staatsnotstands sein muss, auch hier muss sich aber der im Notstand befindliche Staat eigene Versäumnisse, die den Notstand begünstigt haben, vorwerfen lassen.[81)] Bei Cyberangriffen mit schweren Konsequenzen für das gesamte öffentliche Leben, deren Urheber nicht rasch genug identifiziert werden kann (Zurechnung!), kommt aber wohl primär der Rechtfertigungsgrund „Staatsnotstand“ für Cyberabwehrmaßnahmen in Frage.

d) Sonstige völkerrechtliche Grenzen für Cyberabwehrmaßnahmen

Kommen weder Selbstverteidigung noch andere völkerrechtliche Rechtfertigungsgründe infrage, um massive Cyberabwehrmaßnahmen zu erlauben, die in Rechtspositionen anderer Staaten eingreifen, so müssen bestehende völkerrechtliche Grenzen für „elektronisches“ Handeln[82] beachtet werden.

aa) Telekommunikationsrecht

Satzung und Gründungsvertrag der International Telecommunications Union (ITU), einer Spezialorganisation der UNO, enthalten eine Reihe von Vorschriften, die für Cyberabwehrmaßnahmen relevant sein können, wie ein Recht der Öffentlichkeit auf Nutzung der Telekommunikation, das Telekommunikationsgeheimnis, ein grundsätzliches Verbot der Störung legitimer Funkaussendungen und die Möglichkeit, private Aussendungen, die die nationale Sicherheit gefährden oder nationales Recht verletzen, zu unterbinden.[83] Die militärische Telekommunikation ist zwar grundsätzlich von den Regelungen ausgenommen, muss aber, „so weit möglich“, Vorschriften betreffend Notdienste, Frequenzzuweisung und störende Emissionen beachten. Nehmen sie am öffentlichen Telekommunikationsverkehr oder am Verkehr zwischen Regierungsdienststellen teil, so müssen sie „im Allgemeinen“ (in general) auch die für diese Dienste geltenden Vorschriften beachten.[84] Dies sollte auch in Überlegungen einfließen, das bisher körperlich vom Internet getrennte militärische IKT-Netz teilweise zum Internet hin zu öffnen. Stein und Marauhn hielten jedenfalls noch im Jahr 2000 Informationsoperationen gegen IKT-Infrastruktur außerhalb bewaffneter Konflikte generell für völkerrechtswidrig, sofern kein Rechtfertigungsgrund vorliegt.[85]

bb) Luftfahrtrecht

Das Abkommen über die Internationale Zivilluftfahrt (AIZ) von Chicago 1944[86] verlangt von seinen Vertragsstaaten, auf die Sicherheit der zivilen Luftfahrt Bedacht zu nehmen, schränkt aber in Notstandssituationen und bewaffneten Konflikten die Handlungsfreiheit seiner Vertragsstaaten nicht ein und ist auch nur auf Zivilluftfahrzeuge anwendbar. Staatsluftfahrzeuge, das sind solche, die im staatlichen Dienst (Militär, Polizei, Zoll etc.) verwendet werden,[87] fallen nicht unter seine Regelungen. Das Übereinkommen samt Zusatzprotokoll von Montreal über Straftaten gegen die Sicherheit der Zivilluftfahrt[88] verpflichtet die Vertragsstaaten, Handlungen gegen die Sicherheit der Zivilluftfahrt, gegen Zivilluftfahrzeuge im Flug, gegen Flughafen- und Flugsicherungseinrichtungen unter Strafe zu stellen.[89] Darüber hinaus zeigt die Staatenpraxis, dass auch staatliche bzw. staatlich geduldete Gefährdungen dieser Rechtsgüter nicht einfach hingenommen werden.[90] Dies setzt Cyberabwehrmaßnahmen, die sich gegen Luftraumüberwachungs- und Flugsicherungseinrichtungen richten, enge Grenzen, weil sie nur dann völkerrechtlich unbedenklich erscheinen, wenn davon keinerlei Gefährdung für die Zivilluftfahrt ausgeht.

cc) Weltraumrecht

Die Weltraumverträge sind im gegenständlichen Kontext kaum relevant. Zwar sind sie vom Gedanken der friedlichen Nutzung des Weltraums inspiriert, doch ist insbesondere keine völlige Demilitarisierung des Erdorbits (im Gegensatz zum Mond und den anderen Himmelskörpern) vorgesehen, sondern nur die Stationierung von Massenvernichtungswaffen untersagt. Die Einbeziehung von Satelliten im Erdorbit in Cyberabwehrmaßnahmen ist also nicht per se völkerrechtswidrig; wohl ist aber zu beachten, dass für Schäden (definiert als loss of life, personal injury or other impairment of health; or loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations), die Raumfahrzeuge auf der Erde oder an Luftfahrzeugen im Flug verursachen, strenge (verschuldensunabhängige) Gefährdungshaftung der launching states dieser Raumfahrzeuge gilt.[91] Der Wortlaut des Weltraumhaftungsvertrags schließt nicht aus, dass ein durch Cyberabwehrmaßnahmen geschädigter Staat, der an der Zurechnung zu einem bestimmten Verursacher scheitert, versucht, sich an den launching states der beteiligten Satelliten schadlos zu halten; dieses Szenario kann freilich im vorliegenden Rahmen nicht ausführlicher geprüft werden.

dd) Seerecht

Im UNO-Seerechtsübereinkommen finden sich einige wenige Bestimmungen von Relevanz für Cyberabwehrmaßnahmen. Im Küstenmeer (= während einer friedlichen Durchfahrt) verbietet es (einmal mehr) die Androhung oder Anwendung von Gewalt gegen die geschützten Grundpositionen des Staates, das Sammeln von Nachrichten, die die Sicherheit und Verteidigung des Küstenstaats betreffen, Propagandaakte gegen Sicherheit und Verteidigung des Küstenstaates und Beeinträchtigung von Kommunikations- und ähnlichen Einrichtungen.[92] Auf hoher See werden die Vertragsstaaten aufgefordert, bei der Verhinderung unzulässiger Aussendungen zusammenzuarbeiten und die vorsätzliche (wilful)[93] Beschädigung von Unterseekabeln unter Strafe zu stellen.[94] Beides kann für Cyberabwehrmaßnahmen relevant sein.

ee) Sonstiges

Die Cybercrime Convention des Europarats[95] verpflichtet ihre Signatarstaaten zwar, diverse Computerdelikte rund um illegalen Zugang, illegales Abfangen gesendeter Daten, Verfälschung von Daten, Störung von Computersystemen etc.[96] unter Strafe zu stellen, stellt dabei aber immer auf die fehlende Autorisierung des Täters ab („without right“ als Tatbestandsmerkmal). Die Erläuterungen zur Cybercrime Convention stellen klar, dass entsprechend autorisiertes Handeln von Staatsorganen im Dienste der Landesverteidigung oder der öffentlichen Sicherheit davon nicht erfasst sein soll.[97] Darauf wird im Rahmen der nationalen Befugnislage einzugehen sein. *(Wird fortgesetzt)*

ANMERKUNGEN:

1) Der Autor dankt Frau Ella-Maria Moritz für ihre wertvolle Unterstützung.
2) Der Artikel folgt im ersten Teil weitgehend folgendem Aufsatz: Walter J. Unger: Cyber Defence - eine nationale Herausforderung. In: Michael Brzoska et al. (Hrsg.): S+F Sicherheit und Frieden. Security and Peace. 32/1 (2014), S.8-16.
3) Der „virtuelle“ Raum beginnt und endet im physischen Raum und umfasst Endgeräte, Netzwerkgeräte, Leitungen etc.
4) Laut Studie BitKom vom 2.12.2011, „WIRTSCHAFT DIGITALISIERT, Wie viel Internet steckt in den Geschäftsmodellen deutscher Unternehmen?“, sind 50% der deutschen Unternehmen vom Internet abhängig und nur 18% kommen ohne Internet aus.
5) Nationale IKT-Sicherheitsstrategie, Bundeskanzleramt, Wien, 2012 unter http://www.kiras.at/uploads/media/IKT_Sicherheitsstrategie.pdf.

6) Beschluss der Bundesregierung vom 18.3.2013; Bundeskanzleramt, Wien März 2013 unter http://www.bundeskanzleramt.at/DocView.axd?CobId=50748.
7) Entschließung des Nationalrates vom 3. Juli 2013, Österreichische Sicherheitsstrategie, Sicherheit in einer neuen Dekade - Sicherheit gestalten; Wien, Juli 2013.
8) Vgl. Gemeinsamer Bericht des Bundeskanzlers und des Bundesministers für Inneres betreffend das österreichische Programm zum Schutz kritischer Infrastrukturen; Masterplan APCIP (= Austrian Program for Critical Infrastructure Protection); Beschluss des Ministerrates vom 2. April 2008.
9) Ministerratsbeschluss 180/8 vom 20.3.2013; Gemeinsamer Bericht des Bundeskanzlers, der Bundesministerin für Inneres, des Bundesministers für europäische und internationale Angelegenheiten und des Bundesministers für Landesverteidigung und Sport betr. Österreichische Strategie für Cyber Sicherheit (ÖSCS).
10) ÖSCS, Wien, März 2013, S.21.
11) Auszug aus Walter Unger: Cyber Defence - eine militärische Herausforderung, ÖMZ 6/2012, S.698ff.
12) Vgl. „Armeechef sieht Cyberwar als gefährlichste Bedrohung“, NZZ online (www.nzz/ch/aktuell/startseite/armeechef-sieht-cyberwar -als-gefährlichste-bedrohung) vom 6. September 2010.
13) Im EPCIP (European Program for Critical Infrastructure Protection) werden elf Sektoren kritischer Infrastrukturen angeführt: Energie, Nuklearindustrie, IKT, Wasser, Lebensmittel, Gesundheit, Finanzen, Transport, Chemische Industrie, Raumfahrt und Forschungseinrichtungen. Auf der Basis des Europäischen Programms für den Schutz kritischer Infrastrukturen wurde der Masterplan zur Erstellung des österreichischen Programms zum Schutz kritischer Infrastrukturen (APCIP) auf nationaler Ebene festgelegt. Der Masterplan beschreibt die Grundsätze des Programms, beinhaltet die Auflistung der vorrangig zu untersuchenden Sektoren, definiert Kriterien für die Einstufung kritischer Infrastrukturen, benennt die Risikofaktoren und die Akteure, listet die Maßnahmen zum Schutz kritischer Infrastrukturen auf und entwickelt einen Aktionsplan mit detaillierten Teilzielen. Die Schwerpunkte bei der nationalen österreichischen kritischen Infrastruktur sollen hingegen auch die verfassungsmäßigen Einrichtungen, die Aufrechterhaltung des Sozialsystems und der Verteilungssysteme sowie die Hilfs- und Einsatzkräfte umfassen.
14) Vgl. Deutscher Bundestag, Bericht des Ausschusses für Bildung, Forschung und Technologiefolgenabschätzung zum TA-Projekt: „Gefährdung und Verletzbarkeit moderner Gesellschaften - am Beispiel eines großräumigen und lang andauernden Ausfalls der Stromversorgung“, Drucksache 17/5672 vom 27. April 2011, S.44, grafische Darstellung der massiven Abhängigkeiten anderer Infrastrukturen von der Stromversorgung, Telekommunikation und den Informationssystemen und -netzen gem. einer Studie des Schweizer Bundesamtes für Bevölkerungsschutz.
15) Hacktivismus (Kofferwort aus Hack und Aktivismus, engl. Hacktivism), ist die Verwendung von Computern und Computernetzwerken als Protestmittel, um politische Ziele zu erreichen. Die erste Verwendung erfuhr der Begriff im Juli 2004 von Mitgliedern eines Hacker-Kollektivs namens Omega unter http://de.wikipedia.org/wiki/Hacktivismus.
16) In diesem Spektrum ist Vandalismus ebenso enthalten wie die Veröffentlichung vertraulicher Daten zur Bloßstellung von Personen oder Organisationen ohne Bereicherungsmotiv oder politischer Aktivismus.
17) Alle darunter liegenden Bedrohungen sind durch die Strafverfolgungsbehörden zu bekämpfen.
18) Vgl. Carl von Clausewitz: „Vom Kriege“, 1832, Ullstein-Verlag 1980, S.27-29.
19) Vgl. Cyberwar: Konzept, Stand und Grenzen; Center for Security Studies (CSS), ETH Zürich, CSS Analysen zur Sicherheitspolitik, Nr. 71, April 2010, S.2 und auch ÖSCS, S.22.
20) Klaus Naumann: Was heißt Verteidigung im 21. Jahrhundert? In: ÖMZ 2/2014, S.142.
21) Vgl. „Cyberkrieg: Die Bedrohung, die aus dem Netz kommt“, Joseph S. Nye, ehem. stellvertretender US-Verteidigungsminister in der Tageszeitung „Die Presse“ vom 16. April 2012, S.26-27.
22) Sean Watts: Combatant Status and Computer Network Attacks, Virginia Journal of International Law 50 (2010), 391, unter: http://ssrn.com/abstract=1460680 (4.10.2011).
23) Ehud Barak, ehemaliger Ministerpräsident und Verteidigungsminister Israels im Plenum des europäischen Cyber-Security-Gipfels in Bonn, Vgl. „Die Schweiz wappnet sich“; unter: http://www.sonntagszeitung.ch/ vom 17.11.2013 (4.12.2013).
24) Vgl. Deutscher Bundestag, Bericht des Ausschusses für Bildung, Forschung und Technologiefolgenabschätzung zum TA-Projekt: „Gefährdung und Verletzbarkeit moderner Gesellschaften - am Beispiel eines großräumigen und lang andauernden Ausfalls der Stromversorgung“, Drucksache 17/5672 vom 27. April 2011.
25) Wie großangelegte Angriffe ablaufen könnten, ist in Ansätzen an den Beispielen Estland 2007 und Georgien 2008 zu studieren. Hierzu ist umfangreiche Literatur verfügbar, z.B. Robert Knake: Cyber War: The Next Threat to National Security and What to Do About It. Ecco, April 2010.
26) Bot, Botnet: Unter einem Bot (vom Begriff robotic abgeleitet) versteht man ein Computerprogramm, das weitgehend autonom ständig gleichen, sich wiederholenden Aufgaben nachgeht. Es handelt sich dabei meist um ein eher simples, aber effektives Programm. Gebräuchlich ist die Bezeichnung auch für quasi-selbstständige Programme im Bereich der künstlichen Intelligenz. Kommunizieren Bots untereinander in einem fernsteuerbaren Netzwerk, so spricht man von einem Botnet (robotic network). Vgl. http://de.wikipedia.org/wiki/Bot und http://de.wikipedia.org/wiki/Botnet. Dabei infiziert in der Regel ein Angreifer zahlreiche Rechner mit einem Bot, der sich dann zu einem IRC-Server verbindet, einen bestimmten Channel betritt und dort auf Befehle des Botnet-Besitzers, des so genannten Botmasters, wartet, wie beispielsweise das Starten eines DDoS-Angriffs oder das Versenden von Spam. Unter http://forum.computerbetrug.de/threads/vorsicht-mails-mit-rechnung-zip-enthalten-trojaner.25594/page-2, zuletzt am 25.1.2014.
27) Im Jahr 2012 sind ca. 37 Millionen neuer Schadprogramme im Internet beobachtet worden (ca. 100.000 pro Tag), vgl. Dr. Hartmut Isselhorst: Bundesamt für Sicherheit in der Informationstechnik, Vortragsunterlage der Cybersecurity 2013, Berlin 10.6.2013.
28) DoS, DDoS: Als Denial of Service bezeichnet man einen Angriff auf einen Host (Server) oder sonstigen Rechner in einem Datennetz mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen. In der Regel geschieht dies durch Überlastung. Erfolgt der Angriff koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von verteilter Dienstblockade bzw. DDoS (Distributed Denial of Service). Zuletzt am 25.1.2014 unter http://www.chanology-wiki.info/anonymous/hintergrund/ddos.
29) Ein potenzieller Aggressor sollte jedoch nicht übersehen, dass auch einfache Maßnahmen der Aufklärung (Computer Network Exploitation) tendenziell zur Eskalation eines schwelenden Konflikts beitragen können. Da die verbleibende Reaktionszeit extrem kurz sein könnte, könnten beobachtete Aufklärungsversuche einen „Erstschlag“ im Sinne eines präemptiven Vorgehens provozieren.
30) Ein Patch ist eine Korrekturauslieferung für Software oder Daten aus Endanwendersicht, um Sicherheitslücken zu schließen, Fehler zu beheben oder bislang nicht vorhandene Funktionen nachzurüsten. Unter http://de.wikipedia.org/wiki/Patch_%28Software%29; zuletzt am 25.1.2014.
31) Beispielsweise verbreitete und verursachte das Schadprogramm „Conficker“ erhebliche Schäden, z.B. wurde die Landesverwaltung von Kärnten im Januar 2009 zur Gänze lahmgelegt, obwohl schon Monate zuvor ein Sicherheitspatch mit entsprechenden Warnhinweisen zur Verfügung gestellt wurde.
32) Es stellt sich daher die Frage, wie z.B. ein DDoS-Angriff auf der Basis eines großen Bot-Netzes mit Zombie-Rechnern in 150 Staaten oder eines eingeschleusten Schadprogramms (Beispielsweise STUXNET) einem konkreten Angreifer zugeordnet werden könnte.
33) Eine weiterführende Analyse findet sich im Abschnitt „Völkerrechtliche Erwägungen“ sowie bei: Sigmar Stadlmeier und Walter Unger: Cyber War und Cyber Terrorismus aus völkerrechtlicher Sicht. In: Kirsten Schmalenbach (Hrsg.): Aktuelle Herausforderungen des Völkerrechts, Beiträge zum 36. Österreichischen Völkerrechtstag (2011), Wien 2012, S.63ff.
34) Vgl. Cybersecurity Strategy of the European Union, unter: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security bzw. http://eeas.europa.eu/policies/eu-cyber-security/index_de.htm (8.12.2013).
35) Cybersecurity Strategy of the European Union, unter: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security; S.13.
36) Unter http://www.eu-info.tradepress.eu/2013/07/31/neuen-richtlinie-zur-netz-und-informationssicherheit-meldung-machen-in-brussel/; (25.1.2014).
37) www.enisa.europa.eu (8.12.2013).
38) http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm (4.12.2013).
39) http://www.e-government.gv.at/DocView.axd?CobId=47986 (4.12.2013).

40) http://www.bka.gv.at/DocView.axd?CobId=50748 (4.12.2013).
41) http://www.bka.gv.at/DocView.axd?CobId=50748 (4.12.2013).
42) http://www.kiras.at/uploads/media/MRV_APCIP_Beilage_Masterplan_FINAL.pdf (4.12.2013).
43) Österreichische Sicherheitsstrategie unter: http://www.bka.gv.at/DocView.axd?CobId=52099 (4.2.2013).
44) Sämtliche Inhalte dieses Subkapitels sind der Österreichischen Strategie für Cyber-Sicherheit (ÖSCS) entnommen: http://www.bka.gv.at/DocView.axd?CobId=50748 (24.1.2014).
45) Vgl. Österreichische Strategie für Cyber-Sicherheit (2013), S.10.
46) Vgl. ebd., S.11.
47) Vgl. ebd., S.12.
48) Vgl. Österreichische Strategie für Cyber-Sicherheit (2013), S.12f.
49) Vgl. ebd., S.14.
50) Vgl. ebd., S.14f.
51) Vgl. ebd., S.15f.
52) Vgl. ebd., S.16.
53) Die Internet Corporation for Assigned Names and Numbers (ICANN) koordiniert die Vergabe von einmaligen Namen und Adressen im Internet. Dazu gehört die Koordination des Domain Name Systems und die Zuteilung von IP-Adressen. Die ICANN hat ihren Hauptsitz in Los Angeles und ist in Kalifornien als Non-Profit-Organisation registriert. Zuletzt am 29.5.2014 unter http://de.wikipedia.org/wiki/Internet_Corporation_for_Assigned_Names_and_Numbers.
54) The National Cybersecurity Center (NCSC) is an office within the United States Department of Homeland Security (DHS) created in March 2008, and is based on the requirements of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), reporting directly to the DHS Secretary. The NCSC is tasked with protecting the U.S. Government's communications networks. The Center will monitor, collect and share information on systems belonging to NSA, FBI, DoD, and DHS. Zuletzt am 29.5.2014 unter http://en.wikipedia.org/wiki/National_Cybersecurity_Center.
55) Beckstrom, Rod, It's a MAD, MAD, MAD Cyber World. Posted in Cyber Security, 21-Feb-14. Zuletzt am 17.5.2014 unter http://www.worldsecuritynetwork.com/Cyber-Security/rod-beckstrom-1/Its-a-MAD-MAD-MAD-Cyber-World.
56) Beckstrom.
57) „Kinetisch" bedeutet hier „mittels physischer Einwirkung" und wird als Begriffsgegensatz zu „cyber" bzw. „elektronisch" verwendet.
58) Vgl. die Übersicht bei Stadlmeier in Reinisch (Hrsg.), Österreichisches Handbuch des Völkerrechts, Band I, 5. Auflage 2013, 663ff.
59) Art. 52 (2) ZP I 1977 zu den GK 1949.
60) Art. 57 ZP I.
61) Art. 54 ZP I.
62) Art. 37 ZP I.
63) Hathaway u.a. The Law of Cyber Attack, 100 Cal. L. Rev. 817.
64) Art. 14 ZP II.
65) Art. 2 Z 4 UN-Charta.
66) ICJ, Military and Paramilitary Activities in and around Nicaragua (Nicaragua vs United States of America), Merits, 1986 ICJ Reports 14.
67) So schon Stein und Marauhn, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 2000, 1.
68) Vgl. die Nachweise in Stadlmeier/Unger: Cyber War und Cyber Terrorismus aus völkerrechtlicher Sicht. In: Schmalenbach (Hrsg.), Aktuelle Herausforderungen des Völkerrechts. Beiträge zum 36. Österreichischen Völkerrechtstag 2011, 63, und Hathaway u.a. The Law of Cyber Attack, 100 Cal. L. Rev. 817.
69) Dies wäre schon deswegen nicht ausgeschlossen und durchaus mit Art. 51 in Einklang zu bringen, weil Art. 31 WVK die nachfolgende Praxis der Parteien eines völkerrechtlichen Vertrages zu den primären Auslegungsmitteln zählt.
70) Hathaway u.a. The Law of Cyber Attack, 100 Cal. L. Rev. 817. - Die Definition von Brown im Harvard Draft Proposal for an International Convention to regulate the Use of Information Systems in Armed Conflict, 47 Harv. Int'l L.J. 179, kann damit nicht verglichen werden, weil sie sich auf die taktische bzw. operative Ebene im bereits laufenden Konflikt bezieht.
71) UN Doc A/56/49(Vol. I)/Corr.4.
72) General Assembly resolution 56/83 of 12 December 2001.
73) Vgl. den Fall des diplomatischen und konsularischen Personals der USA in Teheran vor dem IGH: Statt dem Iran die Botschaftsbesetzung vorzuwerfen, was eine Zurechnung der „Studentendemonstration" erfordert hätte, warfen die USA dem Iran vor, die Verpflichtung zum Schutz der Botschaft missachtet zu haben, was leichter beweisbar und zurechenbar war. Dies war aber nur deswegen erfolgreich, weil eine ausdrückliche Pflicht zum Schutz der Botschaft und ihres Personals in der WDK enthalten ist.
74) Die von Stein und Marauhn, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 2000, 1, vorgeschlagene Heranziehung des Schädigungsverbots kann als Ansatz dienen, verlangt es doch vom Staat auch, schädigendes Verhalten Dritter hintanzuhalten, setzt aber voraus, dass der Staat (über Genehmigungsverfahren u. dgl.) dazu auch in der Lage ist. Vgl. dazu in jüngerer Zeit den Fall Pulp Mills on the River Uruguay (Uruguay vs Argentina) vor dem IGH.
75) Die Feststellung von Castel in 10 Can. J. L. & Tech. 89, Dritte „would have to be substantially involved", um als Ziel für Selbstverteidigungsakte in Frage zu kommen, erscheint hier etwas oberflächlich.
76) Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 2000, 1.
77) Vgl. die Friendly Relations-Deklaration der UN-Generalversammlung, GA Res 2625 (XXV), und im gegenständlichen Kontext Stein und Marauhn, Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 2000, 1.
78) Vgl. die Kapitelüberschrift vor Art. 20 im ILC draft on State responsibility.
79) Vgl. Art. 49-53 ILC draft on State responsibility.
80) Art. 24 ILC draft; vgl. Hafner und Wittich in Reinisch (Hrsg.), Österreichisches Handbuch des Völkerrechts, Band I, 5. Auflage 2013, 642ff.
81) Art. 25 ILC draft.
82) Vgl. zum Folgenden die Übersicht bei Hathaway u.a., The Law of Cyber Attack, 100 Cal. L. Rev. 817.
83) Art. 33 ff ITU Constitution.
84) Art. 48 ITU Constitution.
85) Vgl. nochmals Stein und Marauhn: Völkerrechtliche Aspekte von Informationsoperationen, ZaöRV 2000, 1.
86) ICAO Doc 7300/9.
87) Vgl. für Österreich die missglückte Definition in § 11 Abs. 2 LFG, die nur hinsichtlich der Militärluftfahrzeuge AIZ-konform ist.
88) Kundmachungen in BGBl 248/1974 und 63/1990.
89) Vgl. § 186 StGB.
90) Vgl. die Auseinandersetzungen zwischen den USA und Großbritannien einerseits, Libyen andererseits wegen des Anschlags von Lockerbie 1988 auf ein US-amerikanisches Passagierflugzeug.
91) Art. I (a) iVm II Weltraumhaftungsvertrag.
92) Art. 19 SRÜ 1982.
93) Wilful wird meist als Gegensatz zu negligent gebraucht und daher hier mit „vorsätzlich" übersetzt. Man vermische dies nicht mit der dogmatischen Differenzierung zwischen „vorsätzlich" und „absichtlich" im österreichischen (!) Strafrecht.
94) Art. 109 und 113 SRÜ 1982.
95) European Treaty Series No 185, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.
96) Art. 2-5 Cybercrime Convention; für Österreich vgl §§ 118a, 119a, 126a-c StGB.
97) Explanatory Report, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.