Phänomen Cybercrime und seine Bekämpfung

Nikolaus Gyarmati

Phänomen Cybercrime und seine Bekämpfung*

Zusammenfassung
Durch die ständig fortschreitenden technologischen Entwicklungen von Computernetzwerken und Internet hat Cybercrime (Internetkriminalität) nicht nur seinen Ursprung sondern auch seine «Daseinsberechtigung» gefunden. Cybercrime ist omnipräsent, macht vor Landesgrenzen nicht Halt und kann folglich unwahrscheinlich grosse Schäden verursachen. Zur Bekämpfung von Cybercrime muss folglich auf juristischer, auf technischer und auf menschlicher Ebene nach neuen Massnahmen und Mitteln gesucht werden.

Résumé
La cybercriminalité (criminalité sur Internet) trouve son origine et sa «raison d'être» dans l'évolution technologique constante des réseaux informatiques et d'Internet. La cybercriminalité est omniprésente, ne s'arrête pas aux frontières nationales et peut donc causer des dommages substantiels. Pour lutter contre la cybercriminalité, de nouvelles mesures et de nouveaux moyens doivent être recherchés aux niveaux juridique, technique et humain.

Summary
Cybercrime (Internet crime) has its origin and its «raison d'être» in the constantly evolving technological developments of computer networks and the Internet. Cybercrime is omnipresent, does not stop at national borders and can thus cause significant damage. In order to combat cybercrime, new measures and means must therefore be developed at the legal, technical and human levels.

I. Grundlagen von Cybercrime

1. Was wird unter Cybercrime verstanden: Grundlagen

Die heutige Welt zeichnet sich durch ihre immer weiter verbreitete Digitalisierung und Vernetzung aus. Die digitale Gesellschaft fordert schnellere Internetdienste und Netze, welche durch die Netzanbieterinnen und den Staat zur Verfügung gestellt werden sollen. Durch die ständig fortschreitenden technologischen Entwicklungen von Computernetzwerken und Internet hat Cybercrime[1] nicht nur seinen Ursprung sondern auch seine «Daseinsberechtigung» gefunden. Die möglichen Gefahren von Cybercrime sind in diesem Bereich omnipräsent, werden aber zum Teil von der Gesellschaft nicht als tatsächlich vorhanden empfunden, weil sich die Straftaten im virtuellen Raum und im Schutze der Anonymität abspielen. Die Begehung einer Straftat wird somit durch das Internet simplifiziert, beschleunigt und macht Straftaten in vielerlei Hinsicht attraktiv, weil mit einem geringen Aufwand grosse Schäden angerichtet werden können und eine Vielzahl von Opfern tangiert sind. Findet indes ein Cyberangriff den Weg in die Medien, wird die Welt in Angst und Schrecken versetzt.

1.1 Cyberspace – «global village»

Im Zuge der Technologisierung der Gesellschaft, die auf dem ersten Blick unerschöpfliche Möglichkeiten bieten sollte, sind gleichzeitig auch neue Kriminalitätsformen, die durch und über das Internet verübt werden, entstanden. Im Folgenden sollen die Grundlagen von Cybercrime erläutert werden.

Das «globale Dorf» (engl. global village) – auch Cyberspace[2] genannt – entstand mit dem Internet und ist durch all die vernetzten Geräte (mobile, standortbezogene) reich bevölkert. Dies führt dazu, dass in diesem Cyberspace jeder, der Zugang dazu hat, diesen auch für die Begehung von Straftaten nutzen kann. In Folge dessen bietet das Internet die Plattform für neue Tatgelegenheiten und Kriminalitätsformen.[3] Es liegt quasi auf der Hand, dass mit der Verbreitung des Mediums Internet und der steigenden Datenmenge auch das Interesse von Kriminellen an den dort gespeicherten Daten zunimmt.[4] Bedingt durch den Umstand, dass bisher keine wirksame nationalstaatliche Kontrolle vorhanden ist, können Daten

* Auszüge aus der Magisterarbeit; Frühlingssemester 2018; betreuende Dozentin: Dr. iur. Cathrine Konopatsch.
1 Zu Deutsch Internetkriminalität.
2 Zu Deutsch Cyberraum.
3 Wernert, Internetkriminalität, 18.
4 Büchel/Hirsch, Internetkriminalität, 3.

im Cyberspace schnell, massenhaft und weltweit verbreitet werden. Diese Tatausführungen werden im Cyberspace durch den Vorteil der Anonymität und der transnationalen Aktionsmöglichkeit erleichtert und erschweren gleichzeitig die Strafverfolgung.[5] Werden Angriffe aus dem Cyberraum getätigt, richten sich diese entweder gegen das WorldWideWeb oder nutzten das Internet für kriminelle oder terroristische Operationen.[6] Die Verwundbarkeit der Systeme im Cyberspace nehmen desto mehr zu, je mehr Geräte und Schnittstellen genutzt werden, sprich je stärker eine digitale Vernetzung vorhanden ist.[7]

Vom Cyberspace ist das Darknet zu unterscheiden, welches eine Parallelwelt zum Internet darstellt: Es handelt sich hierbei um ein Netzwerk und globaler Marktplatz für Kriminelle und dient als «underground economy» für kriminelle wirtschaftliche Aktivitäten im Untergrund.[8]

1.2 Definition von Cybercrime

Soll eine Definition von Cybercrime abgegeben werden, steht die Gesellschaft und v. a. die Jurisprudenz vor einer grossen Herausforderung. Einen von der Rechtsordnung klar definierten Begriff über Cybercrime bzw. Cyberrisiken gibt es nicht.[9] Cybercrime wird je nach Institution oder Person anders definiert. So verwendet z. B. das deutsche Bundeskriminalamt in seiner Definition der Internetkriminalität zwei Begriffe synonym: Es versteht unter Cybercrime oder Informations- und Kommunikationstechnik-Kriminalität (IuK) Straftaten, die moderne Informations- und Kommunikationstechnik ausnutzen oder gegen jene begangen werden.[10] Cyberrisiken lassen sich wie folgt beschreiben: «Cyber-Risiken sind operationelle Gefahren, die von Informationen ausgehen, die auf Datenträgern und Netzwerken gespeichert sind. Damit sind sämtliche Informationen, welche nicht physisch vorliegen, also sämtliche elektronisch verfügbaren Daten, dem Risiko von Cyber-Angriffen ausgesetzt.»[11]

1.2.1 Cybercrime im engeren Sinne

Von Cybercrime *im engeren Sinne* wird gesprochen, wenn die Tatbestandsmerkmale der jeweiligen Norm im Schweizerischen Strafgesetzbuch erfüllt sind. Hierbei handelt es sich um die Computerdelikte «unbefugte Datenbeschaffung» (Art. 143 StGB – «Datendiebstahl»), «unbefugtes Eindringen in ein Datenverarbeitungssystem» (Art. 143bis StGB – «Hacking») sowie «betrügerischer Missbrauch einer Datenverarbeitungsanlage» (Art. 147 StGB – «Computerbetrug»).[12] Ferner gehören zu den Computerdelikten die «Datenbeschädigung» Art. 144bis StGB sowie die Erschleichung einer Leistung einer Datenverarbeitungsanlage «Zeitdiebstahl» Art. 150 Abs. 4 StGB.[13] Zu den weiteren Erscheinungsformen von Cybercrime im engeren Sinne zählen Gewaltdarstellungen, Betrug, Pornographie, Ehrverletzungen, Rassendiskriminierungen und Urheberrechtsverletzungen sowie das Erschleichen einer automatisiert erbrachten Leistung.[14]

1.2.2 Cybercrime im weiteren Sinne

Zu Cybercrime *im weiteren Sinne* zählen Straftaten, zu deren Durchführung in einer ihrer Phasen ein elektronisches Datenverarbeitungssystem genutzt wird.[15] Anders gesagt, handelt es sich hierbei um Straftaten, bei denen Informations- und Kommunikationstechnik zur Planung und/oder zur Vorbereitung und/oder zur Ausführung eingesetzt werden.[16] Die Verbreitung der strafbaren Inhalte wird durch die weltweite Zunahme der Internetnutzung vereinfacht und lässt folgende Tathandlungen daraus ableiten, die unter den Begriff Cybercrime

5 Sieber, Gutachten, 10; siehe auch Pfister, Hacking, 5.
6 Bei den Angriffen handelt es sich u. a. um Datensabotage sowie Blockade von Rechenzentren und Servern. Vgl. dazu Ronellenfitsch, Widerstandsbewegungen, 241.
7 Wernert, Internetkriminalität, 19.
8 Auch die Begriffe «Darkweb oder Dark Web» werden für das Darknet gleich verwendet und sind gleichbedeutend, siehe Wernert, Internetkriminalität, 19.
9 Klett/Stirnimann, Vorgehen, 72.
10 Hierzu gehören z. B. alle Straftaten, wobei Elemente der EDV in den Tatbestandsmerkmalen enthalten sind oder zur Planung, Vorbereitung oder Ausführung einer Tat eingesetzt werden. Ferner werden Straftaten im Zusammenhang mit Datennetzten (z. B. dem Internet) darunter subsumiert sowie fallen Fälle der Bedrohung von Informationstechnik darunter, siehe ausführlich Büchel/Hirsch, Internetkriminalität, 4.
11 Im weiteren Sinne gehört die Thematik der Cyber-Risiken zum Oberbegriff von «White Collar Crime», der aus 1939 stammt. Vgl. dazu ausführlich Klett/Stirnimann, Vorgehen, 72.
12 Cybercrime-Delikte werden i. d. R. in zwei Gruppen unterschieden, d. h. entweder ist das Angriffsziel (Tatobjekt) ein Computersystem/Netzwerk oder es handelt sich um Straftaten, die auch über das Internet begangen werden können. Vgl. dazu Baltisser, Datenbeschädigung, 46; Klett/Stirnimann, Vorgehen, 72.
13 Siehe hierzu ausführlich Baltisser, Datenbeschädigung, 46; Pfister, Hacking, 46.
14 Art. 135, Art. 146, Art. 197, Art. 173 ff., Art. 261bis, Art. 162 StGB. Vgl. dazu Kronig, Bekämpfung, 8 ff.; siehe auch Klett/Stirnimann, Vorgehen, 73.
15 Hierzu zählen z. B. Warenkreditbetrug, Propagandastraftaten, Verbreiten von Kinderpornographie oder Beleidigungstatbestände, siehe Büchel/Hirsch, Internetkriminalität, 4 f.
16 Somit handelt es sich um Straftaten, die durch das Tatmittel Internet ausgeführt werden, siehe Wernert, Internetkriminalität, 32.

im weiteren Sinn subsumiert werden: Zur Begehung der Tat werden die im Internet vorhandenen gespeicherten Daten genutzt (z. B. Cybermobbing), neue Daten werden generiert und veröffentlicht (z. B. Verbreitung von Pornographie jeglicher Art) oder aber Angriffe auf das Medium Internet werden selbst mittels Schadprogrammen durchgeführt (z. B. Malware, Würmer und Trojaner).[17] Zu den weiteren Phänomenen bzw. Deliktsformen von Cybercrime, die nicht ausdrücklich im Gesetz geregelt sind, zählen Facebook-Mobbing, Money-Mules, Botnets, Malware-Handel, Darknet-Drogenhandel, DDoS-Erpressungen, Ransomware[18], Fake-Sites, Cybergrooming[19], Cyberbullying[20] und das bereits mehrmals erwähnte Social-Engineering[21].

Im Folgenden sollen zum besseren Verständnis DDoS-Angriffe und Botnets noch etwas näher ausgeführt werden. Unter den *DDoS-Angriffen* («Distributed Denial of Service») können Netzwerkverbindungen und benötigte Ressourcen beeinträchtigt und Systeme zum Absturz gebracht werden. Dies bedeutet, DDoS-Angriffe führen zu einer Überlastung (Flooding) der Netzkapazität (Bandbreite), was sich schlussendlich gegen die Verarbeitungskapazität der einzelnen angegriffenen Systeme richtet.[22] Davon sind nicht nur Dienste betroffen, die für die Öffentlichkeit bestimmt sind (wie z. B. E-Commerce, Mediendienste), sondern auch standortübergreifende Netze, deren Betriebsstätten zwar mittels abgesicherten VPN- oder MPLS-Kanälen gesichert, jedoch über einen öffentlich zugänglichen Router verbunden sind.[23] Wie bereits treffend die englische Bezeichnung von DDoS beschreibt, wird die Überwachung des Datenstromes durch den verteilten DDoS-Angriff erschwert: Nicht ein einzelner Angreifer, sondern eine Vielzahl von ihnen mit völlig unterschiedlichen IP-Adressen sind beteiligt, weshalb der Angriff mit einer grossen, auf einmal eintreffenden «Wucht» von Datenmassen auf das System verglichen werden kann und eine Lahmlegung des Systems zur Folge hat. Lediglich bandbreitenstarke Anbindungen und leistungsstarke Proxyserver (vergleichbar mit einem Türsteher bei einer Diskothek) können gegen solche DDoS-Angriffe helfen.[24]

Das wohl mächtigste Werkzeug, welches dem Cybercrime zur Verfügung steht, ist das *Botnetz (auch Zombie-Netz genannt)*. Hierbei handelt es sich um Malware, die sich zunächst verbreiten und einnisten muss und sich insbesondere auf die Fernsteuerung fremder Computer (Zombies) konzentriert.[25] Dies hat zur Folge, dass den Cyberkriminellen hierdurch ermöglicht wird, die befallenen Rechner fernzusteuern, ohne dass die Anwender etwas davon merken. Da diese Botnetze sehr lukrativ einsetzbar sind, wächst deren Anzahl entsprechend sehr stark.[26]

17 Büchel/Hirsch, Internetkriminalität, 5.

18 McAffee erläuterte im Bedrohungsreport des zweiten Quartals 2012, dass Ransomware besonders problematisch sei, da der Schaden sofort eintrete. Das angegriffene System sei zudem unmittelbar unbrauchbar (z. B. Konfigurationsdateien in BIOS) und verhindert bei einem Neustart die Einrichtung des Betriebssystems sowie der gewohnten Anwenderprogramme. Da in der Regel Lösegeldforderungen seitens der Täter gestellt werden, verlieren die Opfer nicht nur ihre Daten, sondern auch noch ihr Geld, wenn sie denen nachkommen. Diese Malware wird weltweit eingesetzt und zeichnet sich im Hinblick auf die nationalen Besonderheiten durch ihren Variantenreichtum aus. Dies ist nur darum möglich, weil sie einerseits bei ihrer Installation und andererseits auch bei der Auswahl der passenden Bildschirmanzeige von einem Command & Control-Server (C&C) unterstützt wird. Vgl. dazu Kochheim, Cybercrime und Strafrecht, 87, 118; siehe auch Büchel/Hirsch, Internetkriminalität, 84.

19 «Internetstreicheln» wird von Sexualstraftätern neben den klassischen Chats und Foren, in denen sich Minderjährige befinden, genutzt, siehe Wernert, Internetkriminalität, 22.

20 Synonym für Cybermobbing. Es wird zwischen direktem und indirektem Cyberbullying unterschieden: Das sog. «Flaming» (Versenden von üblen und beleidigenden Nachrichten und Kommentaren im Netz) und das Stalking fallen unter das direkte Mobbing. Zum indirekten Mobbing zählen das Verleumden, das Annehmen einer falschen Identität (fake account) und Betrügereien im Namen des Gemobbten sowie Beschimpfungen, Beleidigungen, Verbreitung von Lügen und Gerüchten sowie Drohungen. Vgl. dazu Büchel/Hirsch, Internetkriminalität, 128 f; Wernert, Internetkriminalität, 22 f.

21 Social Engineering dient dazu, frei verfügbare Informationen (Telefonlisten, Baupläne, Presseberichte, wissenschaftliche Publikationen etc.) zu sammeln, sie zu bewerten und daraus weitreichende Schlüsse zu ziehen, um menschliche Schwächen zur Informationsbeschaffung auszunutzen sowie zur Erlangung von Zugangsrechten oder zur Überwindung von Hemmungen, die mittels Täuschung und Suggestion überwunden werden sollen. Social Engineering beutet andere zu seinem Vorteil aus, um mit oder ohne Verwendung von technischen Hilfsmitteln an Informationen zu gelangen. Angriffe mit Social Engineering können in zwei Gruppen unterteilt werden. Die erste Gruppe ist das «Human-based-social-engineering», wobei der Angriff im direkten Kontakt (Besuch in der Firma) oder via Telefon erfolgt. Die zweite Gruppe ist das «Computer-based-scoal-engineering», wobei der Angriff per E-Mail mit einem entsprechenden Betreff bzw. Anhang stattfindet. Vgl. dazu Kochheim, Cybercrime und Strafrecht, 91; m. w. H. Wernert, Internetkriminalität, 21; Büchel/Hirsch, Internetkriminalität, 19.

22 Kochheim, Cybercrime und Strafrecht, 226.

23 Systemwichtige und eigene Komponenten können auch mittels infiltrierten Clients in einem LAN abgeschlossen werden, ohne dass ein Angriff von aussen geführt wurde, siehe Kochheim, Cybercrime und Strafrecht, 31.

24 DDoS-Angriffe können nebst dem Angriffsziel auch die technische Infrastruktur der Verbindungs- und Anschlussnetzbetreiber beeinträchtigen. Vgl. dazu Kochheim, Cybercrime und Strafrecht, 185.

25 Beim Botnetz handelt es sich um einen Zusammenschluss von mit einem Schadprogramm infizierten Computern. Vgl. dazu Kochheim, Cybercrime und Strafrecht, 239 ff.

26 Einsatzbereiche von Botnetzen sind: Versand von werbenden Spam-Mail, Versand von maliziösen Spam-Mails, verteilte Angriffe (DDoS), Ausspähen der persönlichen Anwenderdaten, zum Knacken von Zugangscodes mittels gebündelter Rechenleistung sowie zur Herstellung von BitCoins (virutelles Geld). Vgl. dazu Kochheim, Cybercrime und Strafrecht, 60, 77 f.

1.2.3 Cybercrime im Sinne des Übereinkommens über die Cyberkriminalität

Das Übereinkommen über die Cyberkriminalität (CCC) des Europarates ist am 1. Juli 2009 in Kraft getreten.[27] Es subsumiert die nachfolgenden Straftaten unter den Begriff von Cybercrime:[28]

a) *Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen*
Hierunter werden folgende Straftaten aufgeführt: Ausspähen und Abfangen von Daten, Datenveränderung, Computersabotage (einschliesslich Vorbereitungshandlungen), Infizierung von Computersystemen mit Schadsoftware, Datenspionage (Hacking, Phishing), Störung des Zugriffs auf Computersysteme, Herstellen, Verschaffen und Zugänglichmachen von Passwörtern, Sicherungscode oder auf die Begehung von Straftaten abzielender Computerprogramme (hacking tools, crimeware).

b) *Computerbezogene Straftaten*
Darunter fallen betrügerische Angriffe auf das Vermögen, Betrug, Computerbetrug, bei denen im Einzelfall aber auch die missbräuchliche Verwendung der digitalen Identität eines anderen und damit der Tatbestand des Verfälschens und Gebrauchens beweiserheblicher Daten eine Rolle spielen kann. Ferner geht es auch um Cybermobbing und Cyberbullying, die Angriffe auf höchstpersönliche Rechtsgüter, wie z. B. die Ehre, darstellen.

c) *Inhaltsbezogene Straftaten*
Es handelt sich hierbei um Straftaten, bei denen über das Netz illegale Inhalte transportiert werden, sprich Informationen die vom Gesetzgeber unter Strafe gestellt sind (z. B. Kinderpornographie, Gewaltdarstellungen und Propagandadelikte).

d) *Straftaten im Zusammenhang mit Verletzung des Urheberrechts und verwandter Schutzrechte*
Diese umfassen die unerlaubte Verwertung urheberrechtlich geschützter Werke, unerlaubtes Verbreiten von Bildnissen (z. B. unerlaubtes Herunterladen und Verbreiten von Musik, Filmen, Software mittels Filesharing-Systemen oder Peer to Peer-Netzwerken wie z. B. eMule oder BitTorrent.

e) *Mittels Computersystemen begangene Handlungen rassistischer und fremdenfeindlicher Art* (gemäss Zusatzprotokoll 2006).[29]

Das schweizerische Recht orientiert sich am Cybercrime-Begriff der CCC.

1.3 Grundlegende Probleme in Bezug auf Cybercrime

Für die moderne Informationsgesellschaft stellen Straftaten im Internet oftmals ein existentielles Risiko dar. Dieses Risiko wird dadurch noch verschärft, dass ein Grossteil der Gesellschaft zu viel Vertrauen in die Integrität seiner informationstechnischen Systeme hat und darauf vertraut, von irgendwelchen Formen von Cyberangriffen verschont zu bleiben.[30] Grundsätzlich kann festgehalten werden, dass mittels Internet (als virtuelles Werkzeug) die Begehung von Straftaten stark zugenommen hat und Cybercrime auf drei Ursachen zurückgeführt werden kann: Einerseits auf die damit zusammenhängende Veränderung der tatsächlichen Kriminalitätsentwicklung, andererseits auf die Veränderungen der polizeilichen Ermittlungstätigkeit sowie auf die Anzeigebereitschaft der Bevölkerung.[31]

Nicht nur die neuen Kriminalitätsformen von Cybercrime sondern auch die zugrundliegenden Charakteristika des digitalen Ermittlungsumfelds stellen die Strafverfolgungsbehörden vor neue Probleme. Die Globalität und die Ubiquität von Computerdaten, die Anonymität des Internets, die Kontrollresistenz der Informationstechnik, die Grösse des auszuwertenden Datenvolumens sowie die Geschwindigkeit und Komplexität in diesem Bereich sind einige nennenswerte Schwierigkeiten im Zusammenhang mit Cybercrime.[32] Da es sich beim Internet um ein globales Medium handelt, können Informationen in Sekundenbruchteilen über Staatsgrenzen hinweg weltweit verteilt werden. Dies hat zur Folge, dass deliktische Handlungen von jedem Ort der Welt ausgeführt und überall auf der Welt Schäden verursachen können.[33] Unsicherheiten seitens der Strafver-

27 Abgeschlossen in Budapest am 23. November 2001; In Kraft getreten für die Schweiz am 1. Januar 2012 (CCC, SR 0.311.43).

28 Ganzer Absatz Wernert, Internetkriminalität, 27; siehe auch Büchel/Hirsch, Internetkriminalität, 6.

29 Ganzer Absatz (Bst. a–e) Wernert, Internetkriminalität, 27; siehe auch Büchel/Hirsch, Internetkriminalität, 6. Von der Schweiz wurde dieses Zusatzprotokoll am 9. Oktober 2003 unterzeichnet, hat es aber bisher noch nicht ratifiziert, BGE 141 IV 108, E. 4.3.12.

30 Sieber, Gutachten, 9.

31 Jofer, Strafverfolgung, 97.

32 Sieber, Gutachten, 35 ff.; Muggli, Netz, 187.

33 Mit Hilfe von Computersystemen agieren arbeitsteilig organisierte kriminelle Strukturen, die ebenfalls über den Erdball verstreut sind, häufig von verschiedenen Ländern aus. Vielmals können nicht einmal Cloud-Provider ohne weiteres Auskunft darüber geben, wo sich die Daten der Nutzer befinden. Vgl. dazu Sieber, Gutachten, 36.

folgungsbehörden entstehen dann, wenn unklar ist, ob der Zugriff auf bestimmte Daten das nationale Territorium betrifft oder die Souveränitätsrechte eines anderen Staates verletzen könnten.[34] Das Internet ist somit eine «terra nullius».[35]

Das Internet ermöglicht und fördert Delikte, die in der Anonymität ausgeübt werden können. Die Anonymität des Täters spielt eine zentrale Rolle, da es unzählige Möglichkeiten gibt, um die eigene Identität im Internet zu verschleiern oder die Aufdeckung derselben zu erschweren, weshalb eine Rückverfolgung von Verdächtigen oftmals mit besonders grossen Schwierigkeiten verbunden ist.[36] Zwar findet im Internet eine Kommunikation zwischen Computersystemen über sog. IP-Adressen statt, wodurch die beteiligten Rechner technisch eindeutig identifiziert werden können, allerdings werden diese IP-Adressen bedingt durch ihre Knappheit heute meist noch dynamisch vergeben.[37] Kann nun tatsächlich eine IP-Adresse eindeutig einem Computersystem zugeordnet werden, gibt es indes noch keinen Aufschluss darüber, welche Person das Computersystem tatsächlich genutzt hatte. Dieses Problem hat sich heute dahingehend etwas entschärft, als dass auch Private häufig Breitbandanschlüsse besitzen, denen teilweise eine statische IP-Adresse zugeteilt ist. Allerdings hat sich diese Problematik auch gleichzeitig verschärft, bedingt durch die Möglichkeit von Zugriffen auf E-Mailkonten mittels Smartphones, da in diesem Falle von einer Netzanbieterin dynamische IP-Adressen zugeteilt werden.[38] Aus diesem Grund sind zum jetzigen Zeitpunkt die Schweizer Mobiltelefon-Provider nicht dazu in der Lage, den Strafverfolgungsbehörden Auskunft darüber zu geben, welche IP-Adresse im Mobilfunkverkehr zu einem bestimmten Zeitpunkt von welcher Person benutzt wurde.[39]

Ein weiteres Problem, aufgrund dessen Cybercrime im Internet grosse Erfolge verzeichnet, ist die Kontrollresistenz der Informationstechnik.[40] Charakteristisch für das Internet ist die dezentrale Architektur sowie dass keine zentralen Kontroll- und Steuerungsprogramme vorhanden sind: Es bestimmt vielmehr das IP-Protokoll den schnellsten verfügbaren Weg für Datenpakete vom Sender zum Empfänger (sog. Routing).[41] Diese Technik führt dazu, dass die Kontrollierbarkeit von Datenpaketen nur schwer umsetzbar ist. Auch die Verschlüsselungsverfahren haben in Bezug auf die Kontrollresistenz des Internets eine grosse Bedeutung, womit Kommunikationen über das Internet geführt werden können, ohne dass Ermittlungsbehörden von deren Inhalt Kenntnis nehmen können.[42] Wenn von Kontrollresistenz im Internet gesprochen wird, darf ferner nicht ausser Acht gelassen werden, dass ein Datenaustausch oft in geschlossen Gruppen stattfindet, wie z. B. im Darknet.[43]

Laut Schätzung soll sich im Jahr 2018 die Anzahl der Internetnutzer weltweit auf mehr als 4 Milliarden belaufen.[44] Jeder dieser Nutzer hinterlässt Spuren im Internet, die eine Auswertung der vorhandenen Datenmassen aus personeller und technischer Hinsicht beinahe unmöglich machen.

Das Internet zeichnet sich schliesslich durch seine Geschwindigkeit und Komplexität sowie seine Veränderungsfreudigkeit aus, weshalb dies einerseits Straftaten im Internet fördert, andererseits ein erschwerendes Kriterium für die Strafverfolgung darstellt.[45]

1.4 Täterstrukturen

Es stellt sich immer wieder die Frage, wer Cybercrime begeht und wie die möglichen Täter aussehen könnten? Die Antwort ist einfach: Die Täter sind geschlechtsunspezifisch (Mann oder Frau), die Tätertypen sind höchst unspezifisch, genauso ihre Motivationslage und ihr technisches Können (vom Einsteiger bis zum Profi).

34 Sieber, Gutachten, 36.
35 Dies bedeutet rechtsfreien Raum, siehe Jofer, Strafverfolgung, 225.
36 Baltisser, Datenbeschädigung, 41.
37 Dies ist in Bezug auf die Rückverfolgung von Daten im Vergleich zur Verwendung von statischen IP-Adressen schwieriger, da ausserdem festgestellt werden muss, zu welchem Zeitpunkt welche IP-Adresse mit welchem Anschluss verknüpft war, siehe ausführlich Sieber, Gutachten, 37.
38 Aufgrund einer komplizierten Technologie benutzen auch andere Personen gleichzeitig die gleiche dynamische IP-Adresse. Vgl. dazu Hansjakob, Internetverkehr, 255.
39 Hansjakob, Internetverkehr, 255.
40 Sieber, Gutachten, 37.
41 Auf unterschiedlichen Wegen und in veränderter Reihenfolge erreichen diese Datenpakete ihr Ziel, an welchem sie mit dem Internetprotokoll wieder zusammengesetzt werden. Vgl. dazu Sieber, Gutachten, 37; siehe auch Wernert, Internetkriminalität, 82.
42 Sieber, Gutachten, 38.
43 In diesem Zusammenhang erfährt das Darknet wachsende Bedeutung. Es handelt sich hierbei um einen Bereich des Internets, welcher durch Suchmaschinen nicht auffindbar ist, siehe Sieber, Gutachten, 38.
44 <https://wearesocial.com/de/blog/2018/01/global-digital-report-2018>, zuletzt besucht am 18. April 2018.
45 Daten werden in Sekundenbruchteilen um die Welt geschickt, verschlüsselt, versteckt oder gelöscht. Im Rahmen von Rechtshilfegesuchen benötigt die Sicherstellung von Daten sehr viel mehr Zeit. Vgl. dazu Sieber, Gutachten, 39.

Besonders bei den Cyberkriminellen verhält es sich so, dass sie nicht in territorialen Kategorien denken, sondern im Netz agieren.[46]

Grundsätzlich können drei Tätergruppen unterschieden werden: Script Kiddies, Hacker und Profis.[47] Bei den Script Kiddies handelt es sich um Einsteiger mit IT-Grundkenntnissen, die sich hauptsächlich mit dem Bereich des Phishings und dem Verändern von Webseiten beschäftigen, indem sie vorprogrammierte Software-Toolkits verwenden.[48] Hacker haben eine hohe Affinität zur Technik und sind bereits deutlich gefährlicher, da von ihnen strukturierte Attacken (z. B. DDoS, Drive-by-exploit etc.) ausgehen. Bei diesen Akteuren handelt es sich einerseits um Hobby- oder ideologische Hacker und andererseits um organisierte Gruppen, die über gute IT-Kenntnisse verfügten.[49] Schliesslich wird noch eine dritte Gruppe, jene der Profis vorgefunden, bei denen es sich um staatlich gelenkte Hacker, um terroristische Gruppen und Hacktivisten handelt. Die Hacktivisten definieren sich als Kämpfer gegen die Ungerechtigkeit und verstehen ihr Handeln als zivilen Ungehorsam gegen bestimmte politische Richtungen.[50] Die Hacktivisten haben zum Ziel, einen möglichst grossen Schaden anzurichten und nicht daraus einen finanziellen Profit zu ziehen.[51]

Dennoch muss an dieser Stelle erwähnt werden, dass der überwiegende Teil der Cyberkriminellen aus finanzieller Motivation heraus handelt, wobei das Spektrum vom klassischen Einzeltäter bis zur international organisierten Tätergruppierung reicht. Das Interessante hierbei ist, dass die Täter in diesem Bereich häufig weder in klassischen hierarchischen Strukturen arbeiten, noch sich oftmals persönlich kennen, sondern auch bei dieser arbeitsteiligen Kooperation die Anonymität des Internets ausnutzen.[52]

II. Prävention und Massnahmen zur Bekämpfung von Cybercrime

1. Konzepte für Präventionsmassnahmen

1.1 Vom Security Operation Center zum Cyber Fusion Center: Konzepte im Wandel

In diesem Abschnitt sollen einige präventive Massnahmen und/oder Konzepte zur Bekämpfung von Cybercrime exemplarisch umrissen werden.

Auf die rein technischen Schutzmöglichkeiten der Informationstechnik (IT) zur Abwehr von Cybercrime soll hier nur am Rande eingegangen werden, da sich diese – entsprechend der Entwicklung neuer Cybercrime-Formen – sehr dynamisch verhalten. Ausgeklammert werden die unterschiedlichen internationalen Institutionen der Zusammenarbeit im Bereich der Bekämpfung von Cybercrime.[53]

Aufgrund der Hyper-Konnektivität in unserer Gesellschaft wollen auch Unternehmungen und Institutionen ständig über das Internet erreichbar sein, womit das Risiko für einen Cyberangriff stetig steigt.[54] Dies hat zur Folge, dass «normale» Sicherheitstools (z. B. Firewalls und Viren Scanner) kaum mehr ausreichen und durch neue Konzepte ergänzt werden müssen. Insbesondere für Firmen, Staaten und Betreiber von kritischen Infrastrukturen sind die Herausforderungen im Kampf gegen Cyberattacken enorm hoch, nicht zuletzt deshalb, weil die Angreifer aus allen Richtungen kommen können: Dies bedeutet, Angreifer können sowohl Staaten, Cyberterroristen, Cyberaktivisten, organisierte Kriminelle sowie Script Kiddies sein.[55] Diese Tatsache führt dazu, dass die Sicherheit im Rahmen der IT-Aufgaben eine eigenständige Funktion ist und an höchster Stelle eingebunden werden muss.

1.1.1 Security Operation Center

Auf der einen Seite ist die Auswahl an Tools zum Schutz geschäftsrelevanter Daten und zur Entdeckung bzw. Abwehr von Cyberattacken gross und wächst täglich. Auf der anderen Seite zeigten die Erfahrungen jedoch, dass die besten Tools nicht ausreichen, solange nicht gut geschultes Personal und ein Gesamtkonzept für

46 Gerny/Flückiger, Strafen, 13.
47 Wernert, Internetkriminalität, 32 f.
48 Wernert, Internetkriminalität, 32 f.
49 Die guten IT-Erkenntnisse ermöglichen ihnen, an persönliche Daten, betriebsinterne Informationen oder vertrauliche Regierungsdokumente zu gelangen. Vgl. dazu Wernert, Internetkriminalität, 33.
50 Dies hat zur Folge, dass mittels DDoS-Attacken Internetportale lahmgelegt werden oder Datenbanken gehackt werden, um anschliessend sensible Daten zu veröffentlichen. Vgl. dazu Wernert, Internetkriminalität, 33; m. w. H. Kochheim, Cybercrime und Strafrecht, 73.
51 Wernert, Internetkriminalität, 33.
52 Kann ein Service selber nicht erbracht werden, wird dieser in der «underground economy» dazugekauft (z. B. erforderliche Schadsoftware, komplette technische Infrastrukturen), siehe Wernert, Internetkriminalität, 33.
53 Es existieren auch Institutionen wie Eurojust und Europol, die auf die internationale Zusammenarbeit spezialisiert sind.
54 Die digitale Transformation führt dazu, dass Betreiber oft einen Teil der Kontrolle abgeben müssen (z. B. mit Cloud Services, Online-Plattformen etc.), siehe von Ow, Konzepte, 85.
55 Von Ow, Konzepte, 85 f.

die Verteidigung zur Verfügung stehen. Durch die Implementierung von sog. Security Operation Centers (SOCs) begannen Staaten, Betreiber von kritischen Infrastrukturen und grosse Firmen sich zu organisieren, um sich gegen Cyberattacken wehren zu können.[56] Die Überwachung der verschiedenen Tools und Geräte, die Analyse und Intervention bei Zwischenfällen, die Zusammenarbeit mit externen Firmen und Lieferanten und das regelmässige Reporting der Aktivitäten zählen zu den typischen Aufgaben eines SOC.[57] Durch das Security Information and Event Management System (SIEM) können enorme Mengen an Daten gesammelt, normalisiert und gefiltert werden. Das SOC übernimmt ferner die Aufgabe als zentrales Management- und Ticketing-System.[58] Wird nun durch das SIEM mittels optimierten Programmen ein Ereignis oder eine Unregelmässigkeit festgestellt, löst es eine Warnung aus und alarmiert einen hochspezialisierten Experten (z. B. CERT) bzw. Analysten, der die Meldung bearbeitet. Stellt dieser einen Angriff fest, kann er unmittelbar die notwendigen Massnahmen ergreifen oder die Bearbeitung an einen anderen Kollegen eskalieren lassen, um einen Schaden abzuwenden oder zu minimieren.[59]

1.1.2 Cyber Fusion Center

In der heutigen Zeit ist festzustellen, dass das vorgenannte SOC nicht mehr ausreicht, da die Ereignisse zunehmen, die Angriffe immer schneller geschehen und lediglich ein reaktiver Ansatz nicht mehr genügt. Dem Anspruch auf ein schnelleres und effizienteres Reagieren auf Angriffe kam man durch die Ergänzung des Cyber Fusion Center (CFC) im SOC nach. Um nicht von Ereignissen überrascht zu werden, sondern darauf vorbereitet zu sein, steht die aktive Beschaffung von Informationen und der Austausch der gewonnen Informationen im Vordergrund.[60] Die aktuelle Bedrohungslage wird aus den aggregierten und analysierten Informationen verschiedenster Quellen im CFC abgeleitet.[61]

Ein ganz entscheidender Faktor für das Funktionieren des CFC ist das Teilen der gewonnenen und vorhandenen Informationen unter den verschiedenen Organisationen, sprich unter staatlichen Stellen, Betreibern von kritischen Infrastrukturen und Firmen. Nur dadurch besteht die Möglichkeit, ein bestmögliches Bild der Bedrohungslage zu erhalten und sich auf zu erwartende Ereignisse vorbereiten zu können.[62]

Nach dem Vorgenannten bleibt allerdings hervorzuheben, dass moderne Cyber-Security noch relativ neu ist und es die meisten Organisationen aus diesem Grund bis heute nur vereinzelt geschafft haben, die drei Grundelemente entsprechend zu implementieren. Bei diesen handelt es sich um ein SOC mit 24×7 Monitoring, um eine effiziente Incident-Response-Fähigkeit und um ein Informationsbeschaffungs- bzw. Informationsaustausch-Programm über Bedrohungen.[63] Ein möglicher Grund hierfür kann darin liegen, dass ein SOC mit einem Cyber-Fusions-Konzept schlicht weg für viele kleine Betriebe oder Organisationen unrealistisch und/oder zu teuer ist. Nach von Ow sollten sich diese einen Partner suchen, der sowohl einen entsprechenden Service anbietet als auch auf einer gemeinsamen Plattform ein 24 Stunden Cyber Fusion Center für verschiedene Kunden betreibt.[64]

1.2 Vorgehen im Ernstfall: Einführung eines FraudeAidKit™

Wenn technische Entwicklungen und Massnahmen getroffen werden, bedeutete dies bei Weitem noch nicht, dass sich eine Firma unabhängig von ihrer Grösse in Sicherheit wiegen kann. Cyberkriminelle suchen sich immer die schwächste Stelle im System aus, welche oft im Faktor «Mensch» liegt. Neben der Schulung und Sensibilisierung von Mitarbeitern ist eine gute Reaktion sowie richtiges Handeln einer Unternehmung in Fällen von Non-Compliance und wirtschaftskriminellen Handlungen unabdingbar. Durch die Methode des FraudeAidKit™,

56 Hierbei ist es unerlässlich, dass die Aufgaben, Ziele, Verantwortlichkeiten und Betriebszeiten der SOC klar definiert sind, siehe von Ow, Konzepte, 86.

57 Zur Sicherstellung, dass alle Informationen und enormen Datenmengen verarbeitet werden können, wird ein Security Information and Event Management System (SIEM) eingesetzt, siehe von Ow, Konzepte, 86.

58 Von Ow, Konzepte, 87.

59 Selbst durch den hohen Automatisierungsgrad eines SOC sind es schliesslich Analysten, die ein Ergebnis abschliessend beurteilen und Massnahmen einleiten, siehe von Ow, Konzepte, 87.

60 Verschiedene Quellen können zur Beschaffung von Informationen verwendet werden, siehe ausführlich von Ow, Konzepte, 87.

61 Nur aufgrund einer Automatisierung kann die enorme Informationsflut bewältigt werden, siehe von Ow, Konzepte, 88.

62 Ein Wandel unter den sich konkurrierenden Firmen hat durch den gemeinsamen Kampf gegen Cyberangriffe dahingehend stattgefunden, dass sie im Kampf «Gut gegen Böse» zusammenarbeiten. Auch MELANI ist bei dieser Zusammenarbeit involviert, siehe von Ow, Konzepte, 88.

63 Von Ow, Konzepte, 89.

64 Von Ow, Konzepte, 89.

eine Art «Notfallkoffer», wird eine Vorbereitung auf solche Fälle dargelegt und soll ein adäquates und praxisnahes Instrument zum Vorgehen im Ernstfall sein.[65]

Damit präventiv gegen Cybercrime vorgegangen werden kann, ist ein Cyber-Risikomanagement vorausgesetzt, welches aus verschiedenen Elementen besteht. Im Bereich von Compliance geht es nicht nur darum, dass extern auferlegte Regeln eingehalten werden. Es ist auch zu erkennen und zu analysieren, wo Risiken im Unternehmen liegen. Basierend auf der erarbeiteten Risikolandschaft und der Risikotoleranz sollte ein entsprechendes Risikomanagement und eine Strategie entwickelt werden.[66] Bedingt durch die Globalisierung, der Ausweitung des Radius und der Reichweite der Geschäftstätigkeit sowie der international herrschenden Regulatorien ist eine professionelle Prüfung von Geschäftspartnern und deren Mitarbeitern vor einer vertraglichen Bindung zwingend. Weil eine Versicherung nicht alle Risiken abdecken kann, hat eine Unternehmung präventive Massnahmen innerhalb ihrer Organisation mit der Versicherungspolice abzustimmen und zu ergänzen.[67]

Um dem Risiko von Cybercrime gerecht zu werden, müssen sich Unternehmensverantwortliche vermehrt mit dieser Thematik sowie mit den notwendigen präventiven und reaktiven strategischen Führungsinstrumenten auseinandersetzen und diese implementieren. Zu den Elementen des FraudAidKit™ gehören Prävention und Krisenmanagement eines Unternehmens. Sie sollen im Ernstfall oder bei Verdacht zeigen, wie vorzugehen ist und wie die erste Phase (Eintreffen der aufgebotenen Spezialisten) überbrückt werden kann, damit die Handlungsfähigkeit eines Unternehmens aufrechterhalten bleibt.[68] Die Phasen des FraudAidKit™ sind die Folgenden: Sensibilisierung, Umsetzung, Unterhalt, Alarmierung und Abwicklung.

Der erste Schritt in der Prävention eines Cyberangriffs ist die Sensibilisierung und hat zum Inhalt, die «Notfallapotheke» mit den richtigen Werkzeugen und Instrumenten auszustatten.[69] In der zweiten Phase der Umsetzung geht es darum, wie die Werkzeuge für die verantwortlichen Entscheidungsträger zugänglich und verfügbar gemacht werden können, zwecks Bewahrung der Handlungsfähigkeit in den vordefinierten Ernstfällen. Unter dem Begriff Unterhalt fällt die dritte Phase des FraudAidKit™. Diese Phase stellt Werkzeuge und Instrumente zur Verfügung und soll so sicherstellen, dass die Organisation im Ernstfall richtig reagieren kann. Hierzu dienen sog. «Stress-Tests», wodurch die implementierten Vorgehensweisen und Massnahmen überprüft und allfällige vorhandene Schwachstellen aufgedeckt werden können.[70] Als letzter Schritt erfolgt die Alarmierung von vordefinierten internen oder externen Spezialisten sowie die anschliessende Nachbearbeitung durch dieses Team. Zentral ist in dieser Phase, dass die Experten eng aufeinander abgestimmt sind, damit eine effektive und effiziente Problembehebung erfolgen kann.[71]

Zusammenfassend kann betont werden, dass das Geschäftsmodell, die Marktsituation und die regulatorischen Rahmenbedingungen der Organisation bzw. Unternehmen eine wesentliche Rolle bei der Absteckung der Risikolandschaft, Ableitung der Massnahmen und der Umsetzung der FraudAidKit™-Methode spielen. Durch die Sensibilisierung der Mitarbeiter steigt das Bewusstsein möglicher Risiken und somit die Wahrscheinlichkeit, dass Unregelmässigkeiten oder gar Cyber-Angriffe frühzeitig entdeckt, rapportiert und bekämpft werden können.[72]

2. Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken

2.1 NCS 2012–2016

Die digitale Vernetzung führt dazu, dass Informations- und Kommunikationsinfrastrukturen für kriminelle, nachrichtendienstliche, machtpolitische oder terroristischen Zwecke missbraucht oder in ihrer Funktion beeinträchtigt werden können.

Da im nationalen Interesse die Informations- und Kommunikationsinfrastrukturen vor Cyberrisiken geschützt werden müssen, hat der Bundesrat am 27. Juni 2012 die erste Nationale Strategie zum Schutz der Schweiz vor

65 Klett/Stirnimann, Vorgehen, 71.
66 Klett/Stirnimann, Vorgehen. 75.
67 Siehe hierzu ausführlich Klett/Stirnimann, Vorgehen, 75.
68 Klett/Stirnimann, Vorgehen, 76 f.
69 Unternehmensintern sind die Risikolandschaft und deren Beurteilung zu evaluieren, siehe Klett/Stirnimann, Vorgehen, 77.
70 Das Ziel besteht darin, dass die betroffenen Personen sich und ihrem Team im Ernstfall vertrauen können und wissen, wie sie zu reagieren haben. Vgl. dazu Klett/Stirnimann, Vorgehen, 77.
71 Von Vorteil ist es, wenn es sich um ein bereits eingespieltes Team handelt, wodurch Kommunikationsprobleme gemindert werden können und dem Unternehmensverantwortlichen den Rücken für andere Aufgaben freigehalten werden kann. Vgl. dazu Klett/Stirnimann, Vorgehen, 77.
72 Klett/Stirnimann, Vorgehen, 78.

Cyberrisiken (NCS) beschlossen und in Auftrag gegeben. Diese endete 2017.[73]

Basierend auf den geleisteten Arbeiten und Analysen der aktuellen Bedrohungslagen, beauftragte der Bundesrat das Informatiksteuerungsorgan des Bundes (ISB) in Zusammenarbeit mit den betroffenen Stellen eine Nachfolgestrategie für die Jahre 2018–2022 auszuarbeiten und diese bis Ende 2017 dem Bundesrat vorzulegen.[74]

Wesentliche Rahmenbedingungen und Voraussetzungen, um Cyberrisiken reduzieren zu können, basieren auf dem Prinzip der Eigenverantwortung (dezentraler Ansatz) und der nationalen Zusammenarbeit zwischen der Wirtschaft und den Behörden sowie der Kooperation mit dem Ausland.[75] Das Ziel besteht somit darin, dass der Staat nur eingreifen soll, wenn öffentliche Interessen auf dem Spiel stehen oder er im Sinne der Subsidiarität handelt.[76]

Die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken erklärt Folgendes:

«(…) Der nationalen Strategie liegt die Überlegung zugrunde, dass jede Organisationseinheit aus Politik, Wirtschaft und Gesellschaft die Verantwortung trägt, diese Cyber-Ausprägung zu erkennen, die damit einhergehenden Risiken in ihren jeweiligen Prozess zu adressieren und soweit machbar zu reduzieren. Die dezentralen Strukturen in Verwaltung und Wirtschaft sollen für diese Aufgaben gestärkt werden und bereits bestehende Ressourcen und Prozesse konsequent genutzt werden. (…)»[77]

2.1.1 Massnahmen der NCS 2012–2016

Die drei strategischen Hauptziele, die durch die NCS verfolgt werden, sind die Frühwarnung/Erkennung von Bedrohungen und Gefahren im Cyberbereich, die Stärkung der Widerstandsfähigkeit der kritischen Infrastrukturen und die wirksame Reduktion von Cyberrisiken, insbesondere Cyber-Kriminalität, Cyber-Spionage und Cyber-Sabotage.[78] Bei der NCS handelt es sich um eine integrale Strategie. Sie beinhaltet 16 Massnahmen, wodurch die Schweiz gegenüber Cyber-Bedrohungen geschützt werden soll.[79]

2.1.2 Wirksamkeitsüberprüfung der NCS 2012–2016

Zwecks Überprüfung, ob die 16 Massnahmen tatsächlich wirksam umgesetzt werden konnten, hatte der Bundesrat im Beschluss zum Umsetzungsplan der NCS dem Informatiksteuerungsorgan Bund (ISB) den Auftrag erteilt, im April 2017 eine Wirksamkeitsüberprüfung der NCS vorzulegen.

Damit die strategischen Ziele der NCS, d. h. die Früherkennung von Bedrohungen und Gefahren, die Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen und die Reduktion von Cyber-Risiken erreicht werden können, wird vorausgesetzt, dass im Umsetzungsplan die 16 Massnahmen genau vorgeben, was welche Organisationseinheiten bis Ende 2017 leisten müssen.[80]

Zusammengefasst kann festgehalten werden, dass durch die NCS 2012–2016 ein Fundament gelegt wurde und dass sie, sowohl auf der Ebene der Massnahmen als auch bei den Schnittstellen und den massnahmenübergreifenden Fragen, als Erfolg gewertet werden kann. Jedoch handelt es sich nur um ein Etappenziel: In der Schweiz muss der Schutz vor Cyberrisiken weiter ausgebaut werden, insbesondere darum, weil sich Cyber-

73 <https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs.html>, zuletzt besucht am 15. Mai 2018.

74 In diesem Zusammenhang hatte der Bundesrat entschieden, dass die Finanzierung der bisherigen 30 Stellen der NCS zur Weiterführung und zum Ausbau des Schutzes vor Cyber-Risiken in den verschiedenen Departementen unbefristet verlängert werden sollen. <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-66487.html>, zuletzt besucht am 15. Mai 2018.

75 Im Rahmen bestehender Strukturen und Zuständigkeiten reduziert die NCS Strategie grundsätzlich Cyberrisiken und geht davon aus, dass die Verantwortung bei den Betreibern kritischer Infrastrukturen, der Wirtschaft und der Verwaltung liegen muss. Transparenz und Vertrauen soll mit permanenten gegenseitigen Informationsaustausch geschaffen werden. Vgl. dazu Strategie, 3; Factsheet NCS, 2; Wirksamkeitsüberprüfung, 8, 12.

76 Strategie, 3.

77 Strategie, 3.

78 Mittels der vorliegenden Strategie wird mehreren parlamentarischen Vorstössen Rechnung getragen, in denen verstärkte Massnahmen gegen Cyber-Risiken gefordert wurden. Vgl. dazu Strategie, 3; Factsheet NCS, 1.

79 Zu diesen 16 Massnahmen zählen: Risiko- und Verwundbarkeitsanalyse, Verwundbarkeitsanalyse IKT-Infrastrukturen der Bundesverwaltung mittels Prüfkonzept, Erstellung Lagebild und Lageentwicklung, Vorfall-Analyse und Nachbearbeitung von Vorfällen, Konzept Übersicht Straffälle und Koordination interkantonaler Fallkomplexe, aktive Massnahmen und Identifikation der Täterschaft, Kontinuitätsmanagement zur Verbesserung der Resilienz der kritischen Teilsektoren, Koordination der Aktivitäten mit den direkt betroffenen Akteuren und Unterstützung mit fachlicher Expertise, Konzept Führungsabläufe und -prozesse mit Cyber-Ausprägung, Identifikation von Cyber-Risiken durch Forschung, Übersicht Kompetenzbildungsangebote, vermehrte Nutzung der Kompetenzbildungsangebote und Schliessung von Angebotslücken, Internet Governance, internationale Kooperation Cyber-Sicherheit, internationale Initiativen und Standardisierungsprozesse im Bereich Sicherheit sowie Handlungsbedarf rechtliche Grundlagen. Siehe ausführlich Jahresbericht.

80 In diesem Zusammenhang war sich der Bundesrat bewusst, dass die Thematik von Cyber-Risiken komplex ist und sich sehr rasch entwickelt. Vgl. dazu Wirksamkeitsüberprüfung, 70.

risiken rasant weiterentwickeln und somit ein Stillstand einen Rückschritt darstellen würde.[81] Eine Weiterführung der bereits geleisteten Arbeiten ist unabdingbar, denn nur durch eine kontinuierliche Anstrengung und Weiterentwicklung wird es möglich sein, die Schweiz bestmöglich vor Cyberrisiken schützen zu können.[82]

2.2 NCS 2018–2022

Am 18. April 2018 hat der Bundesrat die neu erarbeitete Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) für die Jahre 2018–2022 verabschiedet.

Die Vision der NCS 2018–2022 wird dazu wie folgt definiert:

«Bei der Nutzung der Chancen der Digitalisierung ist die Schweiz angemessen vor Cyber-Risiken geschützt und ist diesen gegenüber resilient. Die Handlungsfähigkeit und Integrität ihrer Bevölkerung, Wirtschaft und des Staates gegenüber Cyber-Bedrohungen ist gewährleistet.»[83]

2.2.1 Hintergründe und Weiterentwicklung der NCS 2018–2022

Die Schweiz befindet sich inmitten eines Digitalisierungsprozesses. Er eröffnet auf der einen Seite grosse Chancen, welche die Schweiz zwecks langfristiger Sicherung und Ausbau der Wohlfahrt zu nutzen bestrebt ist. Auf der anderen Seite ist deutlich hervorzuheben, dass die Digitalisierung auch Risiken mit sich bringt. Durch die zunehmende Abhängigkeit von Informations- und Kommunikationstechnologien (IKT) wird die Schweiz verwundbarer gegenüber Ausfällen, Störungen und Missbräuchen dieser Technologien.[84]

Um die Schweiz vor Cyberrisiken schützen zu können, sind Meinungen aus sicherheits-, aus wirtschafts- und gesellschaftspolitischer Sicht zu berücksichtigen.[85] Die Erfahrungen mit Cyberrisiken zeigen, dass ein vollständiger Schutz vor diesen mit verhältnismässigen Massnahmen allerdings nicht erreicht werden kann. Aus diesem Grund muss die Schweiz ihre Resilienz gegenüber Cyber-Vorfällen zwingend erhöhen.[86]

Die Notwendigkeit der Weiterentwicklung bzw. Weiterführung der NCS begründet sich ferner darin, dass die vorhanden Kapazitäten und Fähigkeiten weiter ausgebaut, die geschaffenen Prozesse, Strukturen und Grundlagen für die Umsetzung von Massnahmen weiter genutzt und sie verstärkt als nationale Strategie über die Bundesverwaltung und die kritischen Infrastrukturen hinaus wirksam sein soll. Durch die NCS soll ein Netzwerk zum Schutz der Schweiz vor Cyberrisiken entwickelt werden.[87]

Die zweite NCS hat folgende Aufgaben zu erfüllen: Die Fortführung und die Ausweitung der Arbeiten der ersten NCS und die Ergänzung mit neuen Massnahmen sowie die Gewährleistung der Kontinuität der Arbeiten. Weitere Aufgaben sind die Sicherstellung der Ziele, Grundsätze, Handlungsfelder und Massnahmen seit 2012 sowie das Antizipieren künftiger Trends. Bezüglich der relevanten Bereiche bei den Cyberrisiken bildet sie zur Stärkung der Prävention, Früherkennung, Reaktion und Resilienz somit den strategischen Rahmen.[88]

Des Weiteren soll die dezentrale Organisationsstruktur der NCS mit einer stärkeren strategischen Führung ergänzt werden. Auf diese Weise kann angesichts der hohen Dynamik der Cyberrisiken jederzeit auf neue Entwicklungen reagiert werden und die NCS wird dadurch in der Öffentlichkeit und der Politik klarer wahrgenommen.[89]

81 Jahresbericht, 19; Wirksamkeitsüberprüfung, 71.

82 Die Etablierung und Aufbau von Spezialwissen, funktionierenden Prozessen sowie Strukturen ist in allen Bereichen gelungen, womit die Schweiz besser als noch im Jahr 2012 auf Cyberrisiken vorbereitet ist, siehe Wirksamkeitsüberprüfung, 71.

83 Voraussetzung zur Realisierung der Vision ist, dass sieben strategische Ziele durch die Schweiz erreicht werden müssen, siehe ausführlich Entwurf NCS, 7, NCS 2018–2022, 8.

84 Die rasante Entwicklung der Bedrohungen im Cyberspace zeigen sich wie folgt: Die omnipräsente Cyber-Kriminalität, die Spionagetätigkeiten mit Hilfe von Cyber-Angriffen, die Cyber-Sabotage auf kritische Infrastrukturen (Spitäler oder Energieversorger), die Verbreitung von gestohlener oder manipulierter Information zu Desinformations- und Propagandazwecken und die Zunahme von hybriden Konfliktformen zwecks Destabilisierung von Staaten und Gesellschaften. Vgl. dazu Entwurf NCS, 1; NCS 2018–2022, 2.

85 Aus sicherheitspolitischer Sicht müssen Massnahmen getroffen werden, zwecks Wahrung der Unabhängigkeit und Sicherheit des Landes vor den neu entstehenden oder sich akzentuierenden Bedrohungen und Gefahren im Cyberspace. Damit die Schweiz die Chancen der Digitalisierung konsequent nutzen und den Standortvorteil als sicheres Land erhalten kann, muss sie sich ferner aus wirtschafts- und gesellschaftspolitischer Sicht vor Cyber-Risiken schützen. Vgl. dazu Entwurf NCS, 1; NCS 2018–2022, 2.

86 Unter Resilienz wird die Widerstandsfähigkeit verstanden, Entwurf NCS, 1; NCS 2018–2022, 2.

87 Weil Cyber-Bedrohungen die ganze Wirtschaft, Gesellschaft und Politik betreffen, müssen die Zielgruppen der NCS entsprechend erweitert und die bisherige Zusammenarbeit gestärkt und verknüpft werden, siehe Entwurf NCS, 6 f.; NCS 2018–2022, 7 f.

88 Die NCS stellt eine Art Handlungsanleitung und Orientierungshilfe dar und der zur Strategie gehörende Umsetzungsplan definiert die Zuständigkeiten und Umsetzungsverantwortung für die in der Strategie bestimmten Massnahmen, Vgl. dazu Entwurf NCS, 1; NCS 2018–2022, 2.

89 Entwurf NCS, 6; NCS 2018–2022, 7.

2.2.2 Handlungsfelder und Massnahmen der NCS 2018–2022

Die Massnahmen der neuen NCS 2018–2022 sollen in erster Linie durch Organisationseinheiten der Bundesverwaltung in Zusammenarbeit mit Behörden, Verbänden und Unternehmen umgesetzt werden. Die Auswirkungen dieser Massnahmen betrifft hingegen die ganze Schweiz. Zu den Zielgruppen der NCS gehören die kritischen Infrastrukturen (wie z. B. Atomkraftwerke), Behörden (Dienstleistungen der Verwaltung und Behörden von Bund, Kanton und Gemeinden), Bevölkerung (Schutz) und Wirtschaft (sichereres und vertrauenswürdiges Umfeld als Grundlage für eine gute Wirtschaft).[90] Es sind Massnahmen in unterschiedlichen Bereichen nötig, weil Cyberrisiken verschiedene Bereiche der Wirtschaft, Politik und Gesellschaft gleichzeitig tangieren: Zum Schutz vor Cyberrisiken übernehmen sowohl Wirtschaft, Gesellschaft als auch der Staat eine gemeinsame Verantwortung.[91] Ferner sollen Bund, Kantone, Wirtschaft und Gesellschaft die Massnahmen der NCS in enger Kooperation implementieren und gleichzeitig die jeweiligen Kompetenzen optimal einbringen.[92] Die neuen Massnahmen müssen in sehr unterschiedlichen Bereichen umgesetzt werden, damit die strategischen Ziele der NCS erreicht werden können.

Es gibt insgesamt zehn Handlungsfelder der NCS, worin 29 Massnahmen umschrieben sind. Zu diesen zehn Handlungsfeldern gehören: Kompetenz und Wissensaufbau als zentrale Voraussetzung zur Minderung von Cyberrisiken[93], die Bedrohungslage, das Resilienz-Management (Widerstands- und Regenerationsfähigkeit), wobei die Massnahmen nicht nur auf eine Stärkung der Abwehr, sondern auch zur Eindämmung von Schäden und zur Verringerung der Ausfallszeit bei Vorfällen abzielen.[94] Bei der Standardisierung/Regulierung soll u. a. eine Meldepflicht für Cyber-Vorfälle geprüft werden.[95] Sowohl die Vorfallbewältigung, das Krisenmanagement, die Strafverfolgung, die Cyber-Defence als auch die aktive Positionierung der Schweiz in der internationalen Cyber-Sicherheitspolitik zählen zu den Handlungsfeldern. Als letztes Handlungsfeld wird die Aussenwirkung und Sensibilisierung aufgeführt, die das Ziel verfolgt, dass durch eine aktive Information des Bundes an die Bevölkerung bzgl. Cyberrisiken gleichzeitig mehrere Synergien generiert werden sollen.[96]

90 Entwurf NCS, 8 f.; NCS 2018–2022, 9 f.

91 In diesem Zusammenhang ist es zentral, dass eine gemeinsame Vision verfolgt und übergeordnete strategische Ziele formuliert werden, damit die Strategie in ihrer Diversität kohärent bleibt, siehe Entwurf NCS, 7; NCS 2018–2022, 8.

92 In diesem Zusammenhang unterstützt und koordiniert die NCS diese individuellen Schutzbemühungen, siehe Entwurf NCS 1; NCS 2018–2022, 2.

93 Mittels Zusammenarbeit zwischen Wirtschaft, Forschung und Staat soll ein Umfeld («Ökosystem») geschaffen werden, das die Entstehung, die Produktion und den Vertrieb von innovativen Lösungen im Bereich IT-Sicherheit fördert. Hierunter fallen die folgenden Massnahmen: Früherkennung von Trends und Technologien und Wissensaufbau, Ausbau und Förderung von Forschungs- und Bildungskompetenz und Schaffung von günstigen Rahmenbedingungen für eine innovative Sicherheitswirtschaft in der Schweiz. Vgl. dazu Entwurf NCS, 10, 11 f.; NCS 2018–2022, 11, 12 f.

94 Folgende Massnahmen fallen unter diesen Bereich: Verbesserung der IKT-Resilienz der kritischen Infrastrukturen, Verbesserung der IKT-Resilienz in der Bundesverwaltung sowie Erfahrungsaustausch und Schaffung von Grundlagen zur Stärkung der IKT-Resilienz in den Kantonen. Vgl. dazu Entwurf NCS, 10, 14 f.; NCS 2018–2022, 11, 15 f.

95 Zu den Massnahmen zählen: Evaluierung und Einführung von Minimalstandards, Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung, Globale Internet-Gouvernanz und Aufbau von Expertisen zu Fragen der Standardisierung in Bezug auf Cyber-Sicherheit. Bei den Massnahmen wird der internationale Kontext berücksichtigt und beeinflusst diese wesentlich, weshalb die Entwicklungen weiterhin verfolgt werden müssen. Vgl. dazu Entwurf NCS, 10, 17; NCS 2018–2022, 11, 17 f.

96 Synergien sind das Wissen über mögliche Schutzmassnahmen, die zur Prävention und zur Verbesserung der Widerstandsfähigkeit beiträgt und gleichzeitig hilft, Verunsicherungen zu mindern. Hierzu zählen folgende Massnahmen: Erstellung und Umsetzung eines Kommunikationskonzepts zur NCS und die Sensibilisierung der Öffentlichkeit für Cyberrisiken (Awareness). Vgl. dazu Entwurf NCS, 10, 26; NCS 2018–2022, 11, 27.

Literaturverzeichnis

Baltisser Annina, Datenbeschädigung und Malware im Schweizer Strafrecht (Diss. Zürich 2012 = Zürcher Studien zum Strafrecht Bd. 69), Zürich 2013 (zit. Datenbeschädigung).

Büchel Michael/Hirsch Peter, Internetkriminalität, Phänomene-Ermittlungshilfen-Prävention, Die Schriftenreihe der «Kriminalistik», Heidelberg/München/Landsberg, Frechen, Hamburg, 2014 (zit. Internetkriminalität).

Gerny Daniel/Flückiger Jan, «Wir brauchen höhere Strafen» – Bundesanwalt Lauber über den Kampf gegen die Mafia, den Terrorismus – und Probleme im eigenen Haus, in: Recht im Spiegel der NZZ, NZZ Nr. 276, vom 25. November 2016, 13 (zit. Strafen).

Hansjakob Thomas, Die Erhebung von Daten des Internetverkehrs – Bemerkungen zu BGE 6B_656/2015 vom 16. Dezember 2016, forumpoenale 4/2017, 252–257 (zit. Internetverkehr).

Jofer Robert, Strafverfolgung im Internet, Phänomenologie und Bekämpfung kriminellen Verhaltens in internationalen Computernetzen (Diss. Frankfurt am Main 1999 = Europäische Hochschulschriften, Reihe II Rechtswissenschaft, Bd. 2555), Frankfurt am Main 1999 (zit. Strafverfolgung).

Klett Barbara/Stirnimann Sonja, Cyber-Crime: Verantwortung und Vorgehen im Ernstfall, in: Sicherheit & Recht, 2/2017, 71–78 (zit. Vorgehen).

KOCHHEIM DIETER, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, München 2015 (zit. Cybercrime und Strafrecht).

KRONIG PHILIPP, Bekämpfung der Internet-Kriminalität in der Schweiz, Anwaltsrevue 8/2002, 8 ff. (zit. Bekämpfung).

MUGGLI SANDRA, Im Netz ins Netz – Pädokriminalität im Internet und der Einsatz verdeckten Ermittlern und verdeckten Fahndern zu deren Bekämpfung (Diss. Zürich 2014 = Schulthess Juristische Medien AG Zürcher Bd. 78), Zürich 2014 (zit. Netz).

PFISTER CHRISTA, Hacking. Die Schweizer Hacking-Strafnorm (Art. 143bis StGB) im Vergleich mit den Bestimmungen der Cybercrime Convention, des Rechts der Europäischen Union, des deutschen und des österreichischen Strafrechts (Diss. Zürich 2007 = Schriftenreihe Sanktionenrecht in Europa Bd. 6), Berlin 2008 (zit. Hacking).

RONELLENFITSCH MICHAEL, Der Umgang mit der fluiden Widerstandsbewegungen unter besonderer Berücksichtigung des Datenschutzes, in: Joachim Hruschka/Jan C. Joerden (Hrsg.) Jahrbuch für Recht und Ethik, Band 23, Berlin 2015 (zit. Widerstandsbewegungen).

SIEBER ULRICH, Straftaten und Strafverfolgung im Internet, Gutachten C zum 69. Deutschen Juristentag, in: Verhandlungen des 69. Deutschen Juristentages, in: Ständigen Deputation des Deutschen Juristentages (Hrsg.) Band I, Gutachten Teil C, München 2012 (zit. Gutachten).

WERNERT MANFRED, Internetkriminalität, Grundlagenwissen, erste Massnahmen und polizeiliche Ermittlungen 3. aktualisierte Aufl., Stuttgart 2017 (zit. Internetkriminalität).

VON OW ANDREAS, Konzepte gegen Cyberspace-Angriffe, in: digma – Zeitschrift für Datenrecht und Informationssicherheit, 2015, 86 -89 (zit. Konzepte).

Materialien

Bericht Wirksamkeitsüberprüfung NCS, Informatiksteuerungsorgan Bund ISB, 30. November 2016, Projekt-Nr. 12.415.14.01 (zit. Wirksamkeitsüberprüfung) <https://www.efd.admin.ch/efd/de/home/dokumentation/nsb-news_list.msg-id-66487.html> (zuletzt besucht am 10. Mai 2018).

Entwurf zur Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022, (zit. Entwurf NCS) <http://www.rr.be.ch/etc/designs/gr/media.cdwsbinary.RRDOKUMENTE.acq/99dc69939323426ca1299fb179e5af1d-332/3/PDF/2017.STA.1490-Beilage-DF-161775.pdf> (zuletzt besucht am 10. Mai 2018).

Factsheet NCS 2014, Die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) (zit. Factsheet NCS) <https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs.html> (zuletzt besucht am 10. Mai 2018).

Jahresbericht 2016, Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) (zit. Jahresbericht) <https://www.efd.admin.ch/efd/de/home/dokumentation/nsb-news_list.msg-id-66487.html> (zuletzt besucht am 10. Mai 2018).

Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken, 19. Juni 2012 (rev.) (zit. Strategie) <https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/strategien.html> (zuletzt besucht am 10. Mai 2018).

Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022 (zit. NCS 2018–2022) <https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html> (zuletzt besucht am 10. Mai 2018).

Nikolaus Gyarmati
lic. iur.