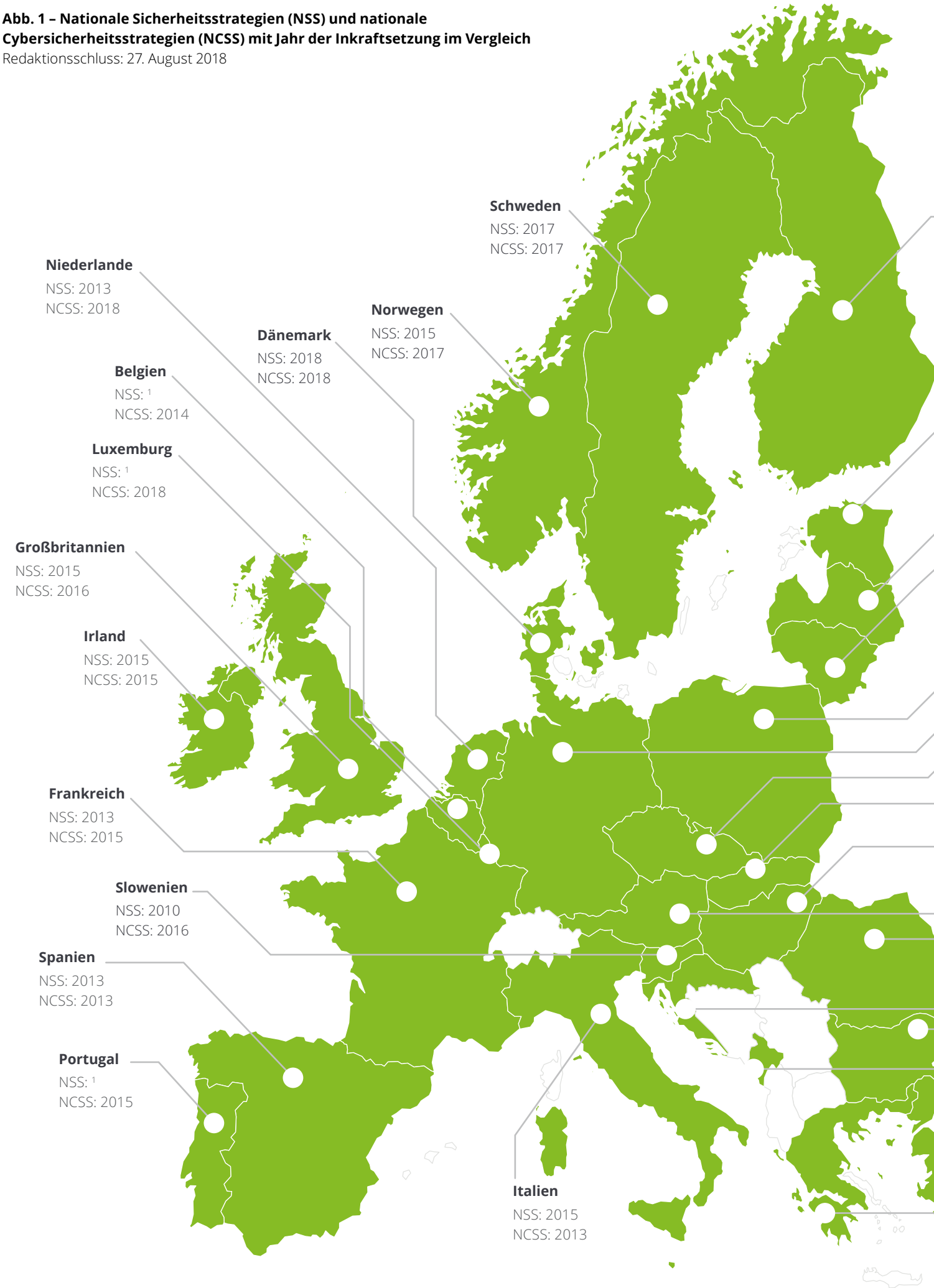
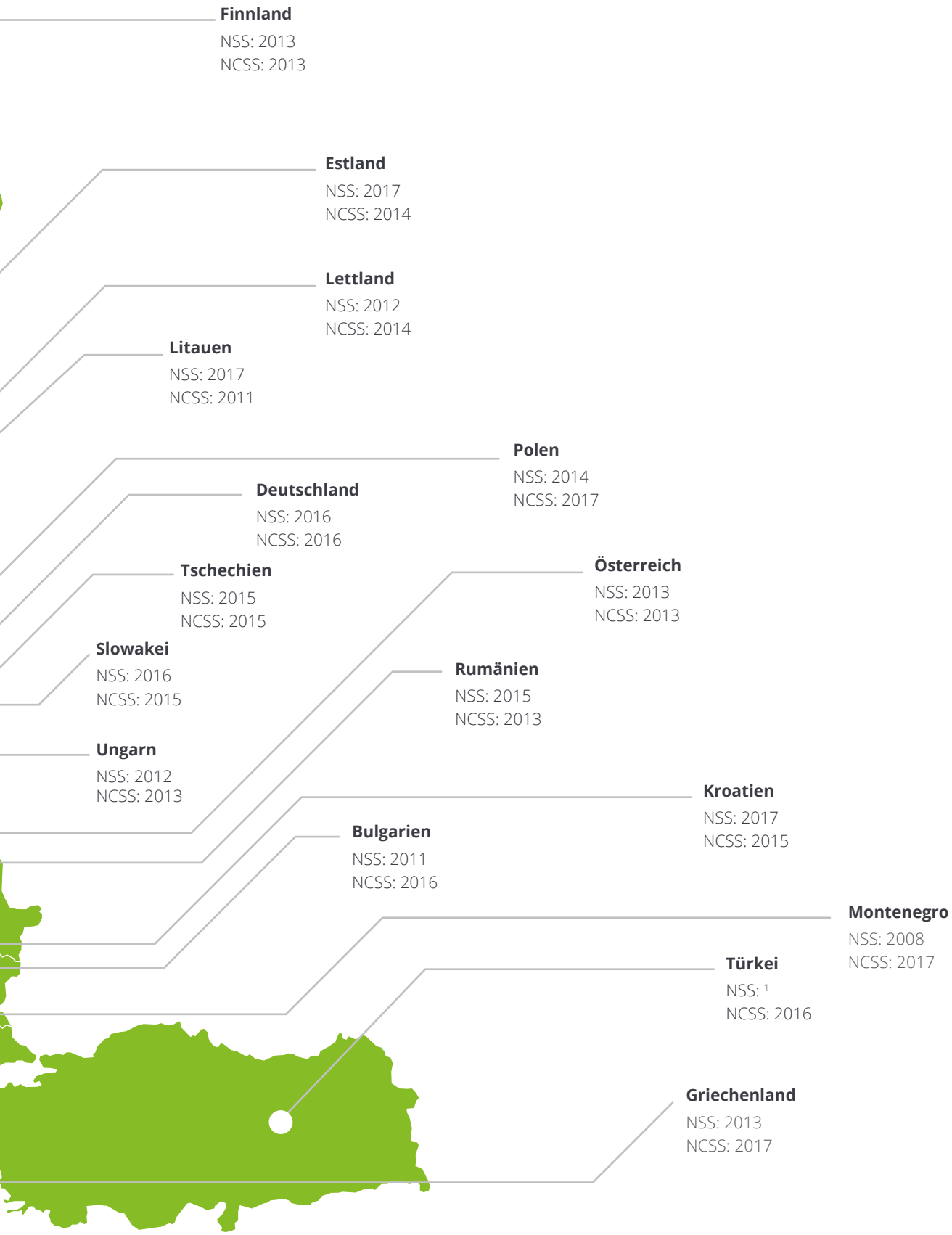
Deloitte.

European Cyber Defense

Teil 1: Strategien – Status Quo 2018

Abb. 1 – Nationale Sicherheitsstrategien (NSS) und nationale Cybersicherheitsstrategien (NCSS) mit Jahr der Inkraftsetzung im Vergleich
Redaktionsschluss: 27. August 2018





Finnland
NSS: 2013
NCSS: 2013

Estland
NSS: 2017
NCSS: 2014

Lettland
NSS: 2012
NCSS: 2014

Litauen
NSS: 2017
NCSS: 2011

Polen
NSS: 2014
NCSS: 2017

Deutschland
NSS: 2016
NCSS: 2016

Tschechien
NSS: 2015
NCSS: 2015

Slowakei
NSS: 2016
NCSS: 2015

Ungarn
NSS: 2012
NCSS: 2013

Österreich
NSS: 2013
NCSS: 2013

Rumänien
NSS: 2015
NCSS: 2013

Kroatien
NSS: 2017
NCSS: 2015

Bulgarien
NSS: 2011
NCSS: 2016

Montenegro
NSS: 2008
NCSS: 2017

Türkei
NSS: [1]
NCSS: 2016

Griechenland
NSS: 2013
NCSS: 2017

(ohne Malta und Zypern)

[1] Nicht in englischer Sprache frei verfügbar.

Vorwort

Cybersicherheit ist (auch) eine staatliche Aufgabe. Darüber sind sich die europäischen Staaten einig. Wie aber gewährt der Staat im Zusammenspiel mit Wirtschaft, Wissenschaft und Gesellschaft Cybersicherheit? Welche Bedrohungen gibt es im Cyberraum für Bürger und Unternehmen? Auf diese Fragen gibt es in Europa ganz verschiedene Antworten und Lösungsansätze.

Wir haben bei unserer Analyse staatlicher Strukturen und Maßnahmen zur Cybersicherheit festgestellt: Es gibt keinen aktuellen und kompakten Überblick über die verschiedenen nationalen Strategien, Akteure und Initiativen europäischer Staaten. Einen solchen Überblick wollen wir mit dem vorliegenden Teil 1 unseres Reports bereitstellen.

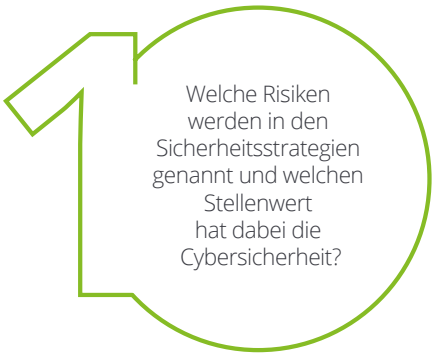
Dieser Report ist das Ergebnis eines systematischen Vergleichs der relevanten nationalen Strategiedokumente mit Aussagen zu Cyber Defense. Unter Cyber Defense verstehen wir in diesem Zusammenhang alle staatlichen Aktivitäten, mit denen Cyberrisiken begegnet werden sollen. Ein Ziel dieser Studie ist es auch, zu analysieren, was die betrachteten Staaten unter Cyber Defense verstehen.

Wir haben uns bewusst auf die Analyse öffentlich zugänglicher Dokumente beschränkt; im Wesentlichen waren dies nationale Sicherheitsstrategien (NSS) und, so vorhanden, nationale Cybersicherheitsstrategien (NCSS). Unsere Untersuchung umfasst 29 Länder, die der Europäischen Union und/oder der NATO angehören; vereinzelt haben wir auch die Cybersupermächte USA, China und Russland im Vergleich betrachtet.

Ein unterschiedliches Verständnis der Herausforderung Cybersicherheit führt zu unterschiedlichen Lösungsansätzen; dies spiegelt sich auch in der Struktur der verschiedenen Strategiedokumente wider. Angesichts des strategisch relevanten, komplexen und dynamischen Untersuchungsgegenstandes Cybersicherheit galt es, nicht der sprichwörtlichen Gefahr zu erliegen, Äpfel mit Birnen zu vergleichen. Wir haben daher versucht, Kategorien zu identifizieren, die sich in allen Strategien wiederfinden, und die entsprechenden Aussagen der jeweiligen Länder gegenübergestellt. Die Kapitel eins bis drei widmen sich jeweils der Analyse der nachfolgenden Fragestellungen:

„Die Gewährleistung von Freiheit und Sicherheit zählt zu den Kernaufgaben des Staates. Dies gilt auch für den Cyber-Raum."

(Deutschland, Cyber-Sicherheitsstrategie 2016)



Uns ist bewusst, dass es eine Diskrepanz zwischen den in Strategiedokumenten genannten Maßnahmen und dem Grad der Implementierung dieser Maßnahmen geben kann. Mit Blick auf das Ziel dieses Reports haben wir aber weder die Aussagen in den einzelnen Strategiedokumenten bewertet noch den Status quo der Strukturen und Maßnahmen untersucht.

Der Vergleich nationaler Strategien wird ergänzt durch eine Zusammenfassung der relevanten Dokumente, Aussagen zu Zielen und aktuellen Initiativen der Europäischen Union, NATO und Vereinten Nationen.

Ohne die Ergebnisse unserer Untersuchung vorwegnehmen zu wollen: Die identifizierten Cyberrisiken, strategischen Ziele und die daraus abgeleiteten Strukturen und Maßnahmen der verschiedenen europäischen Länder unterscheiden sich teilweise erheblich. Dieser Status quo hat uns angesichts der relativ jungen, gleichwohl dynamischen Herausforderung Cybersicherheit wenig überrascht.

Alle Dokumente fußen aber auf einer bestimmten Wahrnehmung des strategischen Kontexts zum jeweiligen Zeitpunkt der Erstellung. Sie gehen also von einer individuellen Einschätzung der Bedrohungslage, der Verantwortung und Reichweite des Staates sowie der Wirksamkeit von Technologie und Maßnahmen der jeweiligen Ersteller zu unterschiedlichen Zeitpunkten aus. Bei der Ausrichtung zukünftiger Strategien profitieren sicher alle Akteure von einem gemeinsamen Verständnis der möglichen Entwicklung wesentlicher Treiber, die den zukünftigen strategischen Kontext bestimmen werden.

Dieser erste Teil des Reports wird daher ergänzt durch einen zweiten Teil, in dem wir mögliche Szenarien zum Stand der Cybersicherheit in Europa im Jahr 2030 entwickelt haben.

Wir möchten mit diesen beiden Veröffentlichungen einen Beitrag zu der notwendigen Debatte zwischen Staat, Wirtschaft und Gesellschaft, aber auch zwischen einzelnen staatlichen Akteuren leisten. Bestenfalls tragen unsere Reports dazu bei, dass wir alle die richtigen Antworten auf die Herausforderung Cybersicherheit finden – oder zunächst die richtigen Fragen stellen.

Executive Summary

Technologischer Fortschritt, regulatorische Vorgaben und stetiger Wandel der Bedrohungslage sind wesentliche Einflussfaktoren im Cyberraum. Die Entwicklungen sind rasant und führen zu gravierenden Herausforderungen für Staaten, die öffentliche Sicherheit zu gewährleisten und die internationale Zusammenarbeit zu koordinieren. Diese Herausforderungen müssen bei der Erarbeitung, Inkraftsetzung und regelmäßigen Überarbeitung der nationalen (Cyber-)Sicherheitsstrategien berücksichtigt werden.

Der vorliegende erste Teil des Reports European Cyber Defense 2018 soll einen aktuellen und kompakten Überblick über die verschiedenen nationalen Strategien, Akteure und Initiativen europäischer Staaten bieten. Kern des Reports ist ein systematischer Vergleich relevanter nationaler Strategiedokumente europäischer Staaten.

Aus unserem systematischen Vergleich haben wir sechs mögliche Handlungsfelder identifiziert. Wir sind überzeugt, dass diese einen großen Raum bei der Aktualisierung nationaler Cybersicherheitsstrategien einnehmen werden.

Der erste Teil des Reports European Cyber Defense wird mit 34 Faktenblättern über nationale und internationale Cybersicherheitsstrategien abgeschlossen. Die Struktur der Faktenblätter orientiert sich an den zuvor gennanten Leitfragen. Jedes Faktenblatt zeigt prägnante Schlüsselpunkte der einzelnen Strategien. Für 32 Staaten, die Europäische Union und die NATO werden kompakt die Ziele, Cyberbedrohungen und die handelnden Akteure zusammengefasst.

Zentrale und besonders relevante Ergebnisse sind:

Knapp die Hälfte der nationalen Sicherheitsstrategien und mehr als ein Drittel der nationalen Cybersicherheitsstrategien sind vier Jahre oder älter. Globale Cybersicherheitsvorfälle in den zurückliegenden vier Jahren scheinen kaum Treiber für eine Aktualisierung zu sein. Teilweise wurden auch selbstgesteckte feste Laufzeiten der nationalen Cybersicherheitsstrategien überschritten, ohne eine Aktualisierung vorzunehmen.

Cyberbedrohungen werden als eine der größten nationalen Bedrohungen angesehen. Nach Häufigkeit der Nennung in den nationalen Sicherheitsstrategien sehen Regierungen eine überwiegende Gefahr durch Cyberbedrohungen. Sie werden in den nationalen Sicherheitsstrategien neben Terrorismus und organisierter Kriminalität genannt. Es wird außerdem festgestellt, dass immer häufiger konventionelle und unkonventionelle Methoden kombiniert eingesetzt werden (hybride Einflussnahme) oder staatliche und nicht staatliche Akteure im Verbund agieren. Die Angriffe laufen dabei oftmals unterhalb der Schwelle eines bewaffneten Konflikts ab.

Daten- und Identitätsdiebstahl sowie Spionage werden in Summe aller betrachteten Cybersicherheitsstrategien als häufigste Bedrohungen beschrieben. Beide Bedrohungen sind weltweite Phänomene der Cyberkriminalität.

In einzelnen Cybersicherheitsstrategien lässt sich schwer eine klare Abgrenzung der Verantwortung auf staatlicher Ebene erkennen. Oft wird diese über mehrere Ressorts und Hierarchieebenen hinweg verteilt. Mit der großen Bedeutung, die den hybriden Bedrohungen zugemessen wird, wird auch ein vernetzter Ansatz für eine angemessene Verteidigung gefordert. Dieser lässt sich jedoch nicht durchweg in den beschriebenen Strukturen erkennen.

Die Verwendung von einheitlichen Definitionen bestimmter Begriffe der Cybersicherheit ist nicht durchweg gegeben. Zwar führt die NATO ein Glossar mit Begriffsbestimmungen, doch mehrere Regierungen definieren einzelne Begriffe selbst oder legen sie teilweise anders aus.

1. Nationale Perspektive: Strategische Risiken und die Bedeutung von Cybersicherheit

Welche Risiken werden in der Sicherheitsstrategie genannt und welchen Stellenwert hat Cybersicherheit?

Nationale Sicherheitsstrategien sind die obersten sicherheitspolitischen Grundlagendokumente von Regierungen. Sie nehmen eine strategische Standortbestimmung vor und nennen die Interessen, Prioritäten und Ziele der nationalen Sicherheitspolitik. Die Strategien sind meist vorausschauend, um Krisen sowie Konflikten vorzubeugen und um auf Gefahren angemessen zu reagieren. Oft sind sie zugleich sicherheitspolitische Analysen und Handlungserklärungen der Regierungen gegenüber ihren nationalen Parlamenten. Als oberste sicherheitspolitische Dokumente sind sie auch die Grundlage einer nationalen Cybersicherheitsstrategie. Ausgangspunkt für den Vergleich nationaler Cybersicherheitsstrategien sollte daher zunächst der Vergleich nationaler Sicherheitsstrategien (NSS) sein.

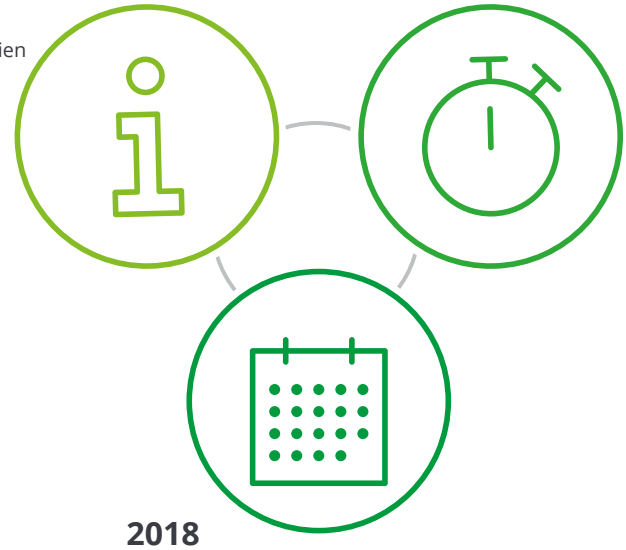
Eine langfristige, aber auch aktuelle strategische Standortbestimmung wird für europäische Regierungen zunehmend schwieriger. Die sicherheitspolitische Situation wird komplexer, Gefahren sind weniger vorhersehbar als in der Vergangenheit. Sicherheitsstrategien müssen diese Komplexität und die daraus resultierenden unsicheren Lageänderungen berücksichtigen. Dieser Abschnitt zeigt, welche Gefahren in den nationalen Sicherheitsstrategien benannt und wie sie gegenüber Cyberbedrohungen eingeordnet werden, falls Cyberbedrohungen überhaupt als nationale Gefahren erkannt worden sind. Zusätzlich erfolgt eine Analyse der Altersstruktur der Strategien.

25 nationale Sicherheitsstrategien sind öffentlich verfügbar. Knapp die Hälfte dieser Strategien ist bereits vier Jahre oder älter.

Abb. 2 – Auffallende Fakten nationaler Sicherheitsstrategien[2]

Knapp die Hälfte

der nationalen Sicherheitsstrategien ist vier Jahre oder älter.



Vor 10 Jahren

wurde bereits die älteste nationale Sicherheitsstrategie, von Montenegro, in Kraft gesetzt.

2018

wurde die jüngste nationale Sicherheitsstrategie, von Dänemark, in Kraft gesetzt.

Die nationale Sicherheitsstrategie von Dänemark wurde 2018 in Kraft gesetzt. Damit hat Dänemark die aktuellste Sicherheitsstrategie der Länder im Fokus dieser Studie. Im Gegensatz dazu haben Bulgarien, Ungarn, Lettland, Montenegro und Slowenien Strategien, deren Inkraftsetzungen im Jahr 2012 waren oder teilweise sogar bis 2008 zurückgehen. Seitdem haben zahlreiche Krisen und Konflikte die globale Sicherheitslage verändert. Zum Beispiel beeinflussten die globale Finanzkrise ab 2007, der Kaukasuskonflikt 2008, die weltweite Übertragung einer H1N1-Influenza-Pandemie 2009, der Arabische Frühling (und die damit zusammenhängenden Konflikte im Irak und in Syrien) ab 2011, die Eurokrise ab 2012, die NSA-Affäre 2013, der Ukraine-Konflikt ab 2014, die Flüchtlingskrise ab 2015 und vor allem unzählige Terroranschläge, unter anderem in Paris, Brüssel, Nizza, Berlin und Barcelona das Weltgeschehen. Diese Ereignisse werden allerdings in den einzelnen Strategien nicht explizit genannt - schlichtweg, weil teilweise das Veröffentlichungsdatum der Strategie vor den Ereignissen lag.

Gleichwohl stellt sich - insbesondere in Bezug auf das relativ neue Phänomen Cyberbedrohung - die Frage, ob zukünftige Strategien in kürzeren Zyklen aktualisiert werden, um die Erkenntnisse derartiger Angriffe berücksichtigen zu können, oder ob Strategien bewusst generisch bleiben, ohne eine explizite Referenz auf einzelne Ereignisse zu nehmen.

Die nationalen Sicherheitsstrategien von China und Russland wurden 2015 und die der USA 2017 in Kraft gesetzt. Damit sind die Strategien der Global Player jünger als das Durchschnittsalter der hier verglichenen europäischen Sicherheitsstrategien.

Die Möglichkeiten des Cyberraums bringen stets neue Herausforderungen, Bedrohungen und Risiken hervor. Die Grenzen verschwimmen und regionale, ja selbst lokale Ereignisse können globale Auswirkungen haben. Die Trennlinie zwischen äußerer und innerer Sicherheit ist im Cyberraum weitgehend aufgelöst.

[2] Ohne NSS von Belgien, Luxemburg, Portugal, Türkei.

Cyberattacken sind vergleichsweise wenig aufwendig, einfach durchzuführen und es ist schwer für die Verteidiger die Herkunft eines Angriffs zweifelsfrei zuzuordnen. Die Quellen und Intentionen eines Angriffs sind vielfältiger Natur. Sie können vom Militär, den Geheimdiensten, Extremisten, Terroristen, der organisierten Kriminalität und auch von Einzeltätern ausgehen.

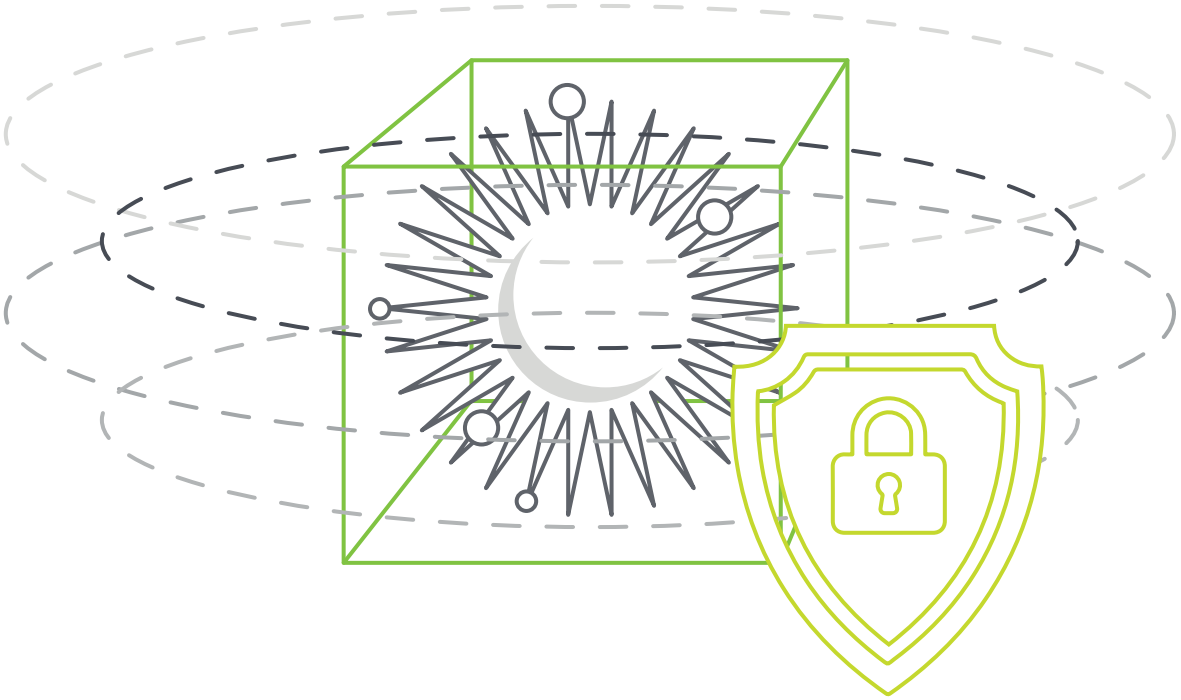
„Da der Zugang zu Software mit hohem Schadenspotenzial auch aufgrund von Proliferation vergleichsweise leicht und günstig ist, sind die für Cyberangriffe notwendigen Mittel nicht auf Staaten begrenzt. Auch terroristische Gruppierungen, kriminelle Organisationen und versierte Einzelpersonen können potenziell mit geringem Aufwand erheblichen Schaden anrichten. Damit stoßen Bemühungen um die Schaffung international verbindlicher Regelwerke oder vertrauens- und sicherheitsbildender Maßnahmen an enge Grenzen."

(Deutschland, Weißbuch 2016)

Staatliche Sicherheitsvorsorge muss die Gesamtheit aller Maßnahmen umfassen, die dem Schutz der Nationen dient und die Lebengrundlage der Gesellschaften aufrechterhält. Maßnahmen zum Schutz des Cyberraums gehören zweifelsfrei dazu.

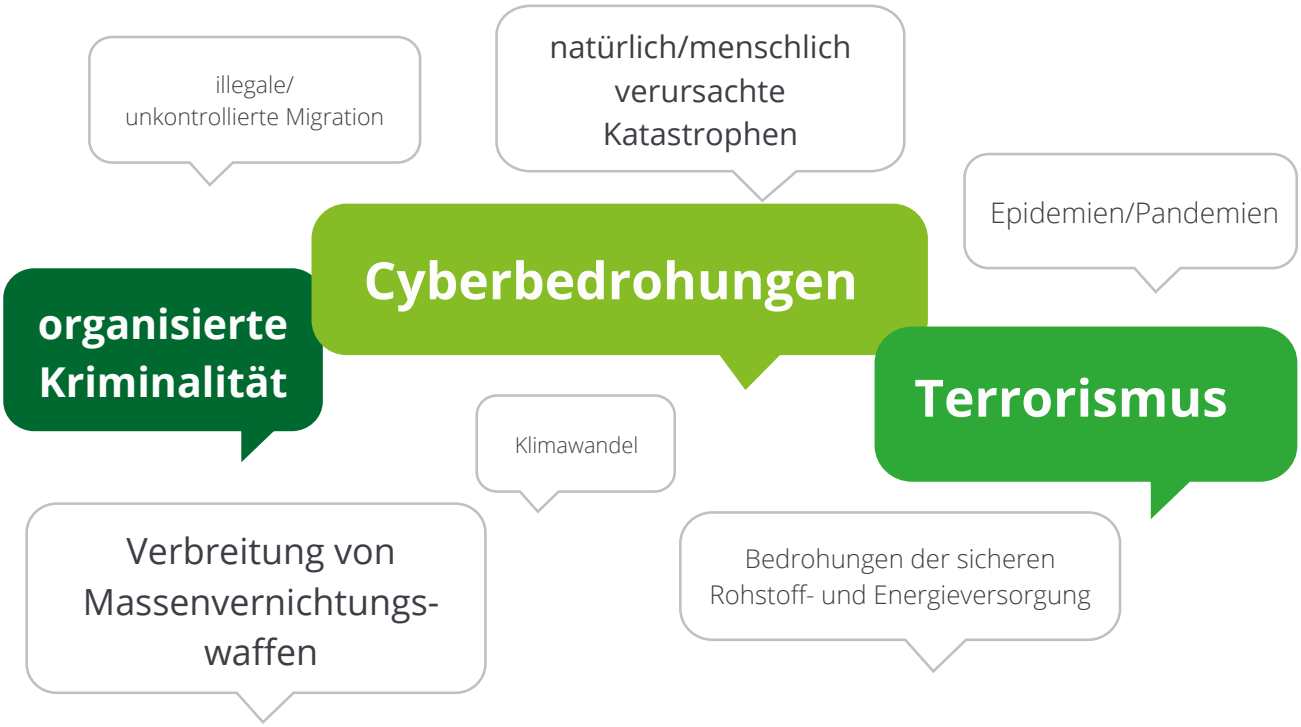
„Like terrorism, this is not simply a risk for the future. Government, the private sector and citizens are under sustained cyber attack today, from both hostile states and criminals. They are stealing our intellectual property, sensitive commercial and government information, and even our identities in order to defraud individuals, organisations and the Government."

(Großbritannien, Premierminister, National Security Strategy 2010))



Unsere Analyse zeigt: Regierungen haben die nationale Bedrohung aus und im Cyberraum erkannt. Cyberbedrohungen werden am häufigsten als nationale Bedrohung genannt, neben Terrorismus und gefolgt von organisierter Kriminalität. Alle betrachteten Sicherheitsstrategien gehen auf Cyberbedrohungen ein. Allerdings liegt den nationalen Strategien keine einheitliche Definition von Cyberbedrohungen zugrunde. Der Begriff wird unterschiedlich ausgelegt, in den einzelnen Strategien steht der Begriff gleichbedeutend für u.a. Cyberbedrohungen, Cyberattacken oder Cyberterrorismus.

Abb. 3 – Nationale Gefahren und Einordnung von Cyberbedrohungen gemäß nationaler Sicherheitsstrategien[3]



[3] Gemäß der Anzahl der Nennungen in den betrachteten Strategien.

Die französische Regierung stellt in ihrer aktuellen Sicherheitsstrategie Cyberattacken mit Terrorismus, atomarer Aufrüstung und Pandemien auf eine Stufe.[4] Gleichzeitig hebt sie hervor, dass diese Bedrohungen noch dringlicher geworden sind und dass man ihnen mit internationalen Kooperationen begegnen muss.

Großbritannien sticht mit der Einordnung seiner nationalen Gefahren heraus. So führte es 2015 zum dritten Mal nach 2010 und 2012 eine umfangreichere Risikobewertung durch. Hierbei werden nationale und internationale Risiken analysiert und ihre Eintrittswahrscheinlichkeit sowie Tragweite beurteilt. Auf dieser Grundlage werden die Risiken mit der höchsten Priorität festgelegt. Cyberbedrohungen wurden, neben fünf weiteren nationalen Bedrohungen, mit der höchsten Priorität eingestuft.[5]

Deutschland liefert mit dem Weißbuch von 2016 seine aktuelle Grundlage für die nationale Sicherheitspolitik des Landes. Die Bundesregierung schreibt, dass die Vernetzung und Verbreitung von Risiken durch die Globalisierung getrieben wird. Die Möglichkeit von Cyberangriffen wird neben Informationsoperationen, Epidemien und Terrorismus insbesondere angesprochen. Hervorzuheben ist, dass die Bundesregierung im Weißbuch vereinzelt Definitionen vornimmt.

„Die sichere und gesicherte sowie freie Nutzung des Cyber- und Informationsraums ist elementare Voraussetzung staatlichen und privaten Handelns in unserer globalisierten Welt. Die wachsende und sämtliche Lebensbereiche durchdringende Digitalisierung mit ihrer fortschreitenden Vernetzung von Individuen, Organisationen und Staaten prägt in einzigartiger Weise die Chancen unserer Gegenwart und Zukunft. Sie macht Staat, Gesellschaft und Wirtschaft jedoch zugleich besonders verwundbar für Cyberangriffe und erfordert unmittelbare Gefahrenabwehr."

(Deutschland, Weißbuch 2016)

[4] French White Paper (2013), S. 7.
[5] National Security Strategy and Strategic Defense and Security Review 2015.

Die digitale Vernetzung von Menschen, Unternehmen und Staaten in Europa nimmt mehr und mehr zu. Infrastrukturen, wie Energieversorgungsnetze, Zahlungsverkehrssysteme, Kommunikationsnetze und andere, überschreiten nationale Grenzen. Im Cyberraum verlieren nationale Grenzen auch als Sicherheitsschranken an Bedeutung. Die Unterscheidung von innerer und äußerer Sicherheit wird schwieriger und einheitliche Standards einer Gemeinschaft im Cyberraum werden zunehmend wichtiger, insbesondere bei Themen der Sicherheit. Auch im Cyberraum ist eine Gemeinschaft nur so stark wie ihr schwächstes Glied. Eine veraltete nationale Sicherheitsstrategie könnte so ein schwaches Glied sein. Sie könnte zum Beispiel geänderte Bedrohungslagen nicht abdecken oder auch den aktuellen Stand der Technik nicht berücksichtigen.

Montenegro hat mit Abstand die älteste Sicherheitsstrategie, sie wurde 2008 in Kraft gesetzt. Bedrohungen aus dem Cyberraum werden hier zwar als nationales Risiko genannt, eine Priorisierung gegenüber anderen Risiken ist hingegen nicht zu erkennen. Montenegro ist Teil einer Region, die in den vergangenen Jahren dynamischen Veränderungen ausgesetzt war. Die Regierung betrachtet die Sicherheitslage im Schwerpunkt im regionalen Kontext. In der Strategie bezieht sich Montenegro im Allgemeinen auf den strategischen Ansatz der NATO und teilt deren Einschätzung der Risiken und Bedrohungen der nationalen Sicherheit, ohne auf diese explizit einzugehen. Kurz geht die Regierung auf die zunehmende Nutzung der Informationstechnologie ein. Sie sieht dabei eine Gefährdung durch Cyberkriminalität, insbesondere in der Verkehrsinfrastruktur, Telekommunikation, Gesundheits- und Sozialsystem, Finanzsystem und in der Versorgung der Bevölkerung. Eine Priorisierung der Cyberbedrohung gegenüber anderen nationalen Bedrohungen nimmt Montenegro nicht vor.

Die Regierungen der Länder erwarten, dass Terroristen und Strukturen der organisierten Kriminalität Cyberattacken als Werkzeug einsetzen werden, um ihre Operationen zu unterstützen. Einige Nationen erwarten, dass Cyberattacken immer öfter Teil der sogenannten „hybriden Kriegsführung" oder von „Hybridattacken" werden. Diese Angriffe kombinieren konventionelle und unkonventionelle militärische Operationen mit zivilen Mitteln oder der Cyberraum wird als Werkzeug für Informationskrieg und die Verbreitung von Propaganda genutzt. Hierbei wird darauf gezielt, Ordnungskategorien (z.B. zwischen Krieg und Frieden oder zwischen Freund und Feind) zu verwischen, um den potenziellen Gegner zu verwirren und seine Reaktionsmöglichkeiten einzuschränken.[6]

[6] Gemäß Schmid, Johann: Hybride Kriegführung und das "Center of Gravity" der Entscheidung, in: Sicherheit und Frieden 2/2016, S. 114–120.

Nahezu alle Regierungen beschreiben in ihren nationalen Sicherheitsstrategien einen vernetzten Sicherheitsansatz als Antwort auf die zugrunde liegende Sicherheitslage und insbesondere als Antwort auf hybride Bedrohungen. Der vernetzte Ansatz soll die Koordination verschiedenster Akteure verbessern. Er soll mit militärischen und zivilen Mittel für nachhaltige Stabilität, Sicherheit und Frieden sorgen. In den verglichenen nationalen Sicherheitsstrategien wird verschiedensten Akteuren in Staat, Wirtschaft und Gesellschaft Verantwortung der Sicherheitsvorsorge zugeschrieben.

According to cyber-attacks: „It could therefore constitute a genuine act of war."

(Frankreich, White Paper 2013)

Militärischen Akteuren wird eine zentrale Rolle zugeschrieben, um auf Angriffe gegen die jeweilige Bevölkerung zu reagieren. Die Mehrheit der Länder erklärt, militärische Einheiten für die Verteidigung und für Operationen im Cyberraum auszubilden.

„Cyberspace has become a new operational domain of conducting combat activity."

(Slowakei, White Paper 2016)

Der Vergleich der nationalen Sicherheitsstrategien zeigt, nicht präzise definiert und von anderen Operationsräumen abgegrenzt werden kann. Wir glauben, dass einheitlichen Definitionen und Bewertungen von Bedrohungen zukünftig ein großer Stellenwert beigemessen wird. Kaum eine nationale Sicherheitsstrategie definiert diese Begriffe. Die spanische Regierung nimmt einen Versuch der Definition des Cyberraums in ihrer nationalen Sicherheitsstrategie vor.

„Cyberspace, a new area of relations which has spurred the development of new information and communication technologies, has blurred borders, making possible an unprecedented globalisation that provides new opportunities but entails serious risks and threats."

(Spanien,The National Security Strategy 2013)

Während die Definition der spanischen Regierung abstrakt ist, ist die deutsche Definition detaillierter und trennt die Begriffe Cyberraum und Informationsraum. Sie unterscheidet dabei „räumlich" die informationstechnischen Systeme vom Informationsraum, es erfolgt somit eine Unterscheidung der technischen von der logischen Sphäre. Allein diese beiden unterschiedlichen Auslegungen des Begriffes Cyberraum zeigen, dass den nationalen Strategien aktuell keine einheitliche Definition zugrunde liegt.

„Der Informationsraum ist der Raum, in dem Informationen generiert, verarbeitet, verbreitet, diskutiert und gespeichert werden. Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann."

(Deutschland, Weißbuch 2016)

Die litauische Regierung nimmt in ihrer nationalen Strategie eine Begriffsbestimmung von Cyberbedrohung vor und stellt den Staat, die kritischen Infrastrukturen und den Bürger als zu schützendes Gut heraus.

Wenn Regierungen Begriffe im Zusammenhang mit der Cybersicherheit definieren, dann nehmen sie diese Definitionen in den meisten Fällen im Rahmen der nationalen Cybersicherheitsstrategien vor. Einige Begriffe werden im folgenden Abschnitt vorgestellt.

Laut dem World Economic Forum zählen USA, China und Russland zu den Supermächten mit den am weitesten entwickelten Cyberfähigkeiten.[7] Eine klare Definition vom Cyberraum oder von Cyberbedrohungen liefern auch diese Staaten in ihren nationalen Sicherheitsstrategien nicht. Trotzdem lohnt sich der Blick in ihre nationalen Sicherheitsstrategien, um ihre Einordnung von Cyberbedrohungen gegenüber anderen nationalen Bedrohungen zu vergleichen.

China setzte seine nationale Sicherheitsstrategie 2015 in Kraft.[8] Eine Priorisierung von Cyberbedrohungen gegenüber anderen nationalen Bedrohungen wird nicht vorgenommen. Doch die Regierung stellt deutlich heraus, dass der strategische Wettbewerb im Cyberraum neue Dimensionen erreicht hat und dass dabei diese Art der Kriegführung beschleunigt wird. Das chinesische Ministerium für Nationale Verteidigung stellt fest, dass die weltweiten Großmächte ihre nationalen Sicherheitsstrategien an diese Beschleunigung anpassen und eine militärische Umstrukturierung dahingehend herbeiführen.

Die Russische Föderation setzte ihre nationale Sicherheitsstrategie ebenfalls 2015 in Kraft. Eine deutliche Priorisierung von nationalen Gefahren lässt die Regierung darin nicht erkennen. Doch sie hebt hervor, dass alle Aktivitäten im Zusammenhang mit der Nutzung von Informations- und Kommunikationstechnologien zur Verbreitung und Förderung von Ideologien, wie z.B. Faschismus, Extremismus, Terrorismus und Separatismus, eine Hauptbedrohung für die staatliche und öffentliche Sicherheit sind. Damit sieht die russische Regierung in der Verbreitung von Ideologien im Cyberraum eine größere Gefahr als in Faktoren, die die lebenswichtigen IT-Infrastrukturen angreifen oder zerstören können.

Im Gegensatz zur Russischen Föderation nehmen die USA die Risikoidentifizierung mit Blick auf die Sicherheit und Widerstandsfähigkeit ihrer kritischen Infrastrukturen vor und nicht in erster Linie auf die Verbreitung von Ideologien. Sie priorisieren die Risiken und ihre Schutzanstrengungen, Fähigkeiten und Abwehrmaßnahmen nach den katastrophalen oder kaskadierenden Konsequenzen von Cyberangriffen. Die nationale Sicherheitsstrategie der USA wurde 2017 in Kraft gesetzt.

„Cyber threats – actions in the cyber space aimed at disturbing the functioning of critical information infrastructures, activities of state institutions and economic sectors of importance for national security, obtaining classified or any other non-public information, committing other criminal acts and thus impairing the security of the State and its citizens."

(Litauen, National Security Strategy 2017)

[7] „The countries which are believed to have the most developed cyber warfare capabilities are the United States, China, Russia, Israel and the United Kingdom"; https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

[8] Chinese Military Strategy (2015): White Paper.

2. Ziele und Aussagen nationaler Cybersicherheitsstrategien

Welche Ziele, Aufgaben und Risiken werden in der Cybersicherheitsstrategie genannt?

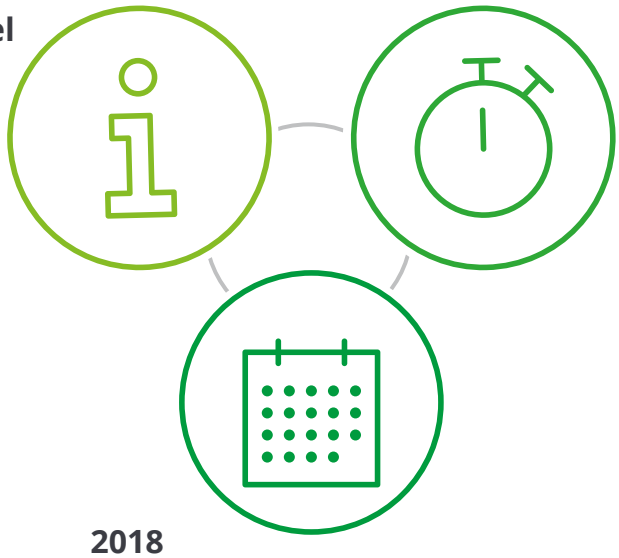
Der grenzüberschreitende Cyberraum eröffnet Chancen und birgt Risiken. Er fordert neue Ansätze und neue Handlungsfelder staatlichen Handelns. Der Staat steht in der Pflicht, den steten Veränderungen zu begegnen und Rahmenbedingungen im Interesse seiner Bürger zu schaffen. Mit einer nationalen Cybersicherheitsstrategie kann eine Regierung ein Grundlagendokument für die Cybersicherheit in Kraft setzen und wesentliche Weichenstellungen für die zukünftige Cybersicherheitspolitik einer Nation vornehmen. Sie kann strategische Leitlinien definieren, Handlungsräume abgrenzen, ressortübergreifende Verantwortung festlegen und handelnde Akteure benennen.

Dieser Abschnitt führt einen kompakten Vergleich von 29 nationalen Cybersicherheitsstrategien durch und zeigt im Kern, welche Ziele in den Strategien beschrieben und welche Cyberbedrohungen von den Regierungen benannt werden. Vorab wird verglichen, wann die nationalen Cybersicherheitsstrategien in Kraft gesetzt worden sind.

Die nationalen Cybersicherheitsstrategien sind im Schnitt jünger als die nationalen Sicherheitsstrategien. Mehr als ein Drittel der aktuellen nationalen Cybersicherheitsstrategien ist vier Jahre oder älter. Dänemark und Luxemburg besitzen die jüngsten Cybersicherheitsstrategien, sie wurden 2018 in Kraft gesetzt. Litauen besitzt die älteste Strategie, sie wurde schon 2011 in Kraft gesetzt. Seitdem sind sieben Jahre vergangen. Trotz zahlreicher Cyberangriffe in den letzten Jahren, wie zum Beispiel die Schadprogramme Stuxnet ab 2010 und Shamoon ab 2012 sowie die Ransomware Wanna Cry und die Wiper Malware Petya ab 2016, wurden ältere Strategien nicht angepasst.

Abb. 4 – Nationale Cybersicherheitsstrategien im Überblick

Mehr als ein Drittel
der nationalen Cyber-sicherheitsstrategien ist vier Jahre oder älter.



Vor 7 Jahren
wurde bereits die älteste nationale Cybersicherheits-strategie, von Litauen, in Kraft gesetzt.

2018
wurden die jüngsten Cybersicherheitsstrategien von Dänemark und Luxemburg in Kraft gesetzt.

Eine stets wiederkehrende Befassung oder Aktualisierung einer Strategie könnten die Regierungen durch feste Laufzeiten erreichen. Mit dem Erreichen des Endes der Laufzeit wird gewiss nicht die nationale Cybersicherheitsstrategie außer Kraft gesetzt, doch die Wahrscheinlichkeit einer zeitnahen Aktualisierung ist umso höher, desto näher man dem Ende der Laufzeit kommt. Eine feste Laufzeit kann verbindliche Richtschnur für eine wiederkehrende Befassung sein. In den uns vorliegenden Dokumenten haben nur elf von achtundzwanzig Regierungen einen festen Zeitrahmen zu ihren Cybersicherheitsstrategien hinzugefügt. Estland und Irland sind zwei der Staaten, die ihrer Cybersicherheitsstrategie eine feste Laufzeit hinzugefügt haben, allerdings haben sie ihren selbstgesteckten Zeitraum bereits überschritten, ohne eine Aktualisierung vorgenommen zu haben.

Die nationalen Cybersicherheitsstrategien beziehungsweise die vergleichbaren Grundlagendokumente für Cybersicherheit aus China[9] , Russland[10] und den USA[11] sind im Schnitt aktueller als die europäischen Dokumente. Russland setzte seine Cyber-Security Strategy 2014, die USA ihre Cyber Strategy 2015 und China sein Cybersicherheitsgesetzt 2016 in Kraft.

Mit einer klaren Zieldefinition können Regierungen eine zukunftsgerichtete Cybersicherheitspolitik ermöglichen und die Chancen des Cyberraums im Sinne ihrer Nationen voll ausschöpfen. Sie können dadurch auch Risiken im Cyberraum beherrschbar machen. In allen betrachteten Strategien sind Ziele definiert. In 28 von 29 Cybersicherheitsstrategien wird die Sicherung der kritischen Infrastrukturen als Ziel gesetzt. Nur die norwegische Regierung nennt dieses Ziel nicht direkt. Indirekt beschreibt sie allerdings ein Pilotprojekt, welches einen funktionsfähigen Markt für Unternehmen und Nutzer der kritischen Infrastrukturen schaffen soll.

[9] Cyber Security Law of the People's Republic of China (2016)
[10] Russian Cyber-Security Strategy (2014)
[11] The DoD Cyber Strategy (2015)

Abb. 5 – Auffallende Kernziele nationaler Cybersicherheitsstrategien[12]

97%
sehen die Sicherung kritischer Infrastrukturen als Ziel

93%
haben sich sichere und robuste Informationssysteme als Ziel gesetzt

7%
setzen auf eine schnelle Reaktion auf Cyberangriffe

76%
definieren einen sicheren Datentransfer als Ziel

Sichere und robuste Informationssysteme sind das am zweithäufigsten genannte Ziel. Beispielsweise nennt Frankreich dieses Ziel an vorderster Stelle und als politische Reaktion auf die weltweit durchgeführten Cyberangriffe. In ihrem Weißbuch beschreibt die französische Regierung, dass robuste Informationssysteme mit einer koordinierten Organisation und einer operativen Zusammenarbeit verschiedener staatlicher Stellen einhergehen müssen, um robust gegen Cyberangriffe zu sein. Montenegro und Portugal sind die einzigen beiden Staaten, die dieses Ziel nicht direkt, beziehungsweise nicht wörtlich nennen. Sie legen ihren Schwerpunkt mehr auf einen sicheren Datentransfer, welcher auch von drei Viertel der betrachteten nationalen Strategien genannt wird.

Nur 2 von 29 Regierungen, Großbritannien und Slowenien, nennen schnelle Reaktionen auf Cyberangriffe in ihren aktuellen Strategien. Großbritannien plant mit seinem nationalen Cybersicherheitszentrum (NCSC) nicht nur ein Hub von Experten aus Gesellschaft und Wirtschaft, sondern die Regierung plant damit auch eine Organisation, von der aus schnelle Reaktionen auf Hauptbedrohungen vorgenommen werden können. Slowenien definiert mit seiner Cybersicherheitsstrategie Maßnahmen, die es ihrem nationalen Cybersicherheitssystem erleichtern, schnelle Reaktionen durchzuführen. In fast allen anderen Cybersicherheitsstrategien werden Reaktionen auf Cyberangriffe erwähnt, jedoch nicht in einen zeitlichen Zusammenhang gebracht. Auch von Großbritannien und Slowenien wird der Begriff „schnell" nicht weiter definiert. Offen bleibt in beiden Strategien, ob damit proaktive oder nur reaktive schnelle Maßnahmen gemeint sind.

[12] in Prozent der Nennungen in den betrachteten Strategien

Abb. 6 – Kernziele nationaler Cybersicherheitsstrategien[13]

[13] gemäß der Anzahl der Nennungen in den betrachteten Strategien

Im Vergleich zu den nationalen Sicherheitsstrategien werden in den nationalen Cybersicherheitsstrategien im größeren Umfang hinreichende Begriffsdefinitionen vorgenommen und zum Teil Glossare beigefügt. Die österreichische Regierung hat eines der umfangreichsten Glossare. In ihrem „Cyber Sicherheit Glossar" definiert sie 29 Begriffe im Zusammenhang mit Cybersicherheit. Cybersicherheit an sich definiert sie wie folgt:

„Cyber Sicherheit beschreibt den Schutz eines zentralen Rechtsgutes mit rechtsstaatlichen Mitteln vor akteursbezogenen, technischen, organisations- und naturbedingten Gefahren, die die Sicherheit des Cyber Space (inklusive Infrastruktur- und Datensicherheit) und die Sicherheit der Nutzer im Cyber Space gefährden. Cyber Sicherheit trägt dazu bei, die Gefährdungen zu erkennen, zu bewerten und zu verfolgen sowie die Fähigkeit zu stärken, Störungen im und aus dem Cyber Space zu bewältigen, die damit verbundenen Folgen zu mindern sowie die Handlungs- und Funktionsfähigkeit der davon betroffenen Akteure, Infrastrukturen und Dienste wieder herzustellen."

(Österreich, Österreichische Strategie für Cyber Sicherheit 2013)

Die österreichische Definition von Cybersicherheit ist im Vergleich detaillierter als andere. Unter Cybersicherheit wird nicht nur die Sicherheit der Infrastruktur und der Daten verstanden, sondern auch Daten, Systeme und zusammenhängende Dienste, explizit die Sicherheit der Nutzer. Weniger umfassend nehmen Dänemark und die Türkei die Definitionen vor, da in diesen ausschließlich Daten, Systeme und den zusammenhängenden Diensten betrachtet werden.

„Cyber security provided at a national scale for any hardware and software systems associated with all services, transactions, information/data provided through the information and communication technologies that constitute national cyber space."

(Türkei, National Cyber Security Strategy 2016 to 2019)

„Cyber security encompasses protection against breaches of security resulting from attacks on data or systems via a connection to an external network or system. Cyber security thus focuses on vulnerabilities inherent to the interconnection of systems, including connections to the Internet."

(Dänemark, Danish Cyber and Information Security Strategy 2018)

„Cyber-Sicherheit ist die IT-Sicherheit der im Cyber-Raum auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme."

(Deutschland, Cyber-Sicherheitsstrategie für Deutschland 2016)

Die Bundesregierung nimmt eine der engsten Begriffsbestimmungen vor und definiert den Begriff Cybersicherheit, ähnlich wie die Türkei und Dänemark, mit Blick auf die Datenebene bzw. auf Ebene informationstechnischer Systeme.

Unabhängig von den Begriffsbestimmungen erkennen alle betrachteten Staaten Bedrohungen im Cyberraum. Sie erkennen, dass Cyberangriffe auf Staaten und auf kritische Infrastrukturen schon lange Realität sind und dass Angreifer vor entwickelten Staaten und digitalisierten Streitkräften keinen Halt machen, sondern diese vielmehr als lohnendes Ziel sehen. In mehr als der Hälfte der betrachteten nationalen Cybersicherheitsstrategien werden Daten- und Identitätsdiebstahl sowie Spionage als Cyberbedrohungen benannt. Beide Bedrohungen sind weltweite Phänomene der Cyberkriminalität. Es sind Straftaten, die unter Ausnutzung von Informations- und Kommunikationstechnik durchgeführt werden oder gegen diese gerichtet sind.[4] Die Strafverfolgung und Bekämpfung von Cyberkriminalität auf nationaler Ebene wird in den betrachteten Staaten unterschiedlich gehandhabt, in der Regel durch Organisationen mit polizeilichen Aufgaben. International kann kein Land diese Phänomene alleine lösen, die Arbeit in der Gemeinschaft wird zunehmend wichtiger. Das European Cybercrime Centre (EC3) bei Europol und Interpol bekämpfen Cyberkriminalität auf internationaler Ebene.

Abb. 7 – Am häufigsten benannte Bedrohungen gemäß nationaler Cybersicherheitsstrategien[5]

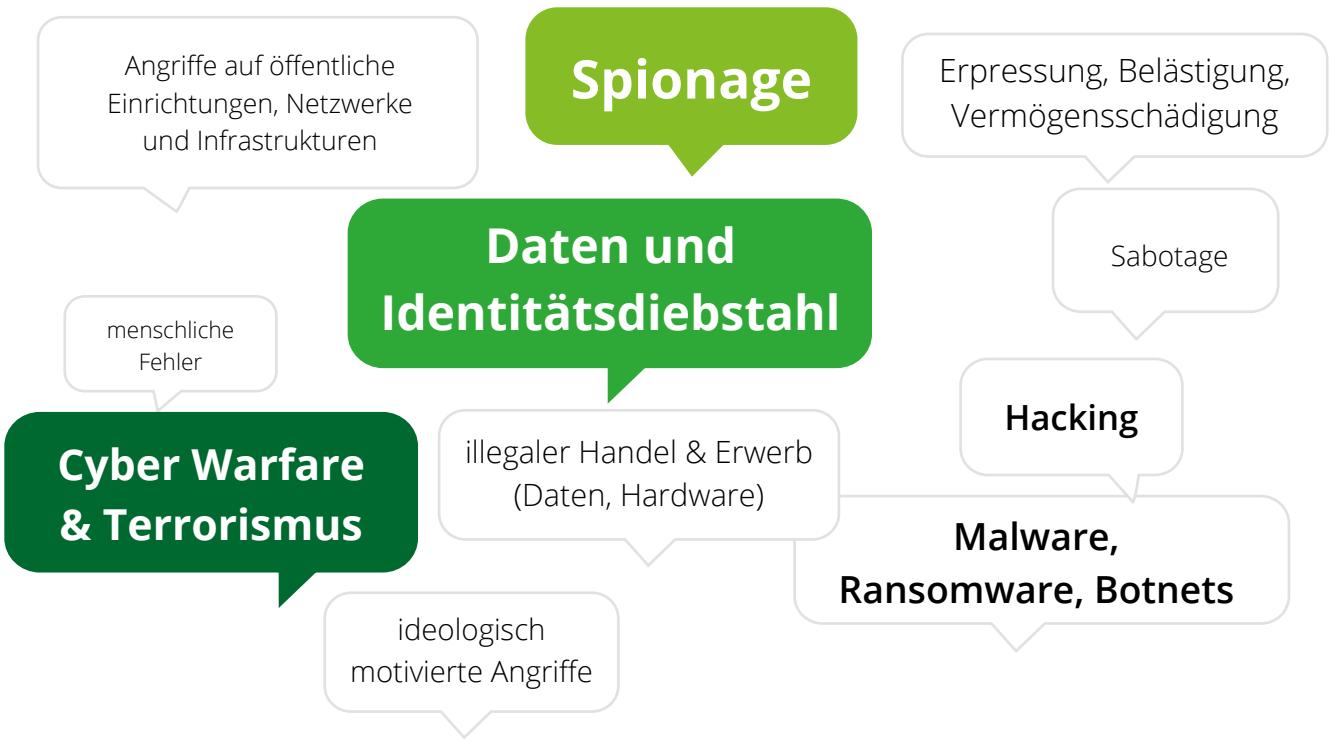
Mehr als die Hälfte
der betrachteten nationalen Cybersicherheitsstrategien benennen Daten- und Identitätsdiebstahl sowie Spionage als Bedrohungen

[4] BMI (2018), http://www.bmi.bund.de
[5] in Prozent der Nennungen in den betrachteten Strategien; USA, China und Russland benennen diese Cyberbedrohungen auch in ihren nationalen Cybersicherheitsstrategien.

China und die USA sehen in diesen Phänomenen der Cyberkriminalität auch Hauptbedrohungen für die nationale Cybersicherheit und benennen diese explizit in ihren nationalen Cybersicherheitsstrategien. Russland benennt diese Phänomene nicht. In der russischen Cyber-Security Strategy werden die Bedrohungen im Cyberraum von der Möglichkeit zur Verbreitung von Informationen abhängig gemacht. Russland sieht die Gefahr, dass Informations- und Kommunikationstechnologien als Waffe zur Verbreitung von Informationen eingesetzt werden. Die Bedrohung sehen sie in der Störung der öffentlichen Ordnung sowie in der Verbreitung von Hass und Terrorismus.

Cyberterrorismus, Malware, Ransomware, Botnets und Hacking sind weitere Bedrohungen, die am häufigsten in den verglichenen nationalen Cybersicherheitsstrategien genannt werden. Deutlich weniger häufig werden menschliche Fehler, illoyale Mitarbeiter oder Social Engineering in den Strategien als Cyberbedrohungen gesehen, obwohl der Risikofaktor Mensch im aktuellen Cyber Security Report vom Institut für Demoskopie Allensbach und von Deloitte als größte Gefahr für Unternehmen gesehen wird.[16]

Abb. 8 – Bedrohungen gemäß nationaler Cybersicherheitsstrategien[17]



[16] Deloitte, Cyber Security Report 2017, Teil 2, S. 14.
[17] gemäß der Anzahl der Nennungen in den betrachteten Strategien

Diese und viele weitere Bedrohungen im Cyberraum beeinflussen die Ziele der Cybersicherheit – Vertraulichkeit, Integrität und Verfügbarkeit. Cyberangriffe zielen sogar direkt und gewollt mit Mitteln der Informationstechnologie gegen ein oder mehrere IT-Systeme und die Ziele der Cybersicherheit. Um das Sicherheitsrisiko auf ein akzeptables Maß zu reduzieren, können wirksame Schutzmaßnahmen ergriffen werden. Cybersicherheit ist eine gesamtstaatliche Aufgabe und wird zunehmend durch eine Zusammenarbeit über politische Ressortgrenzen hinweg gewährleistet. Dabei muss neben der territorialen Unversehrtheit und der Souveränität die Sicherheit eines Staates auch im Cyberraum verteidigt werden. Cyber Defense, als Begriff, wird in den betrachteten nationalen Cybersicherheitsstrategien unterschiedlich ausgelegt. In Deutschland und Österreich fasst die Cyberverteidigung eher den Teil der militärischen, speziell dafür geeigneten Mittel der Verteidigung zusammen.

„Cyber-Verteidigung umfasst die in der Bundeswehr im Rahmen ihres verfassungsmäßigen Auftrages und dem völkerrechtlichen Rahmen vorhandenen defensiven und offensiven Fähigkeiten zum Wirken im Cyber-Raum, die zur Einsatz- und Operationsführung geeignet und erforderlich sind oder zur Abwehr von (militärischen) Cyber-Angriffen und damit dem Schutz eigener Informationen, IT sowie Waffen- und Wirksysteme dienen. Dazu gehört auch die Nutzung und Mitgestaltung von Strukturen, Prozessen und Meldewesen der Cyber-Abwehr unter verteidigungsrelevanten Aspekten und Situationen."

(Deutschland, Cyber-Sicherheitsstrategie für Deutschland 2016)

Im internationalen Umfeld wird der Begriff Cyber Defense eher allgemeiner und weniger militärisch ausgelegt. Oft werden alle Aufgaben darunter zusammengefasst, die IT-Systeme schützen und wiederherstellen sowie Bedrohungen erkennen und darauf reagieren.

„The application of effective protective measures to obtain an appropriate level of Cyber Security in order to guarantee Defence's operation and functionalities. This is achieved by applying appropriate protective measures to reduce the security risk to an acceptable level. Cyber Defence consists of following duties: Protect, Detect, Respond, and Recover."

(Belgien, Cyber Security Strategy for Defence 2014)

Die schwedische Regierung geht noch einen Schritt weiter und erklärt, dass auch aktive Operationen zur Cyberverteidigung gehören.

„Cyber defence capabilities are an important part of the [...] Defence. Vital systems must be protected from attack. This also requires the ability to carry out active operations in the cyber domain."

(Schweden, Sweden's Defence Policy 2016 to 2020)

Die nationalen Cybersicherheitsstrategien von Deutschland, Finnland, Frankreich, Großbritannien, den Niederlanden und Slowakei erwähnen ebenso offensive Maßnahmen und Fähigkeiten zum Schutz der eigenen Systeme und Informationen im Cyberraum. Belgien und Portugal geben in ihren Strategien einen Ausblick über die Entwicklung von zukünftigen offensiven Fähigkeiten. Die NATO definiert proaktive Maßnahmen zum Erkennen von möglichen Cyberangriffen oder zum Ermitteln des Ursprungs einer Cyberoperation mit dem Begriff Active Cyber Defense. Das können auch präventive Cyberoperation gegen die Quelle eines möglichen Cyberangriffs sein.[18]

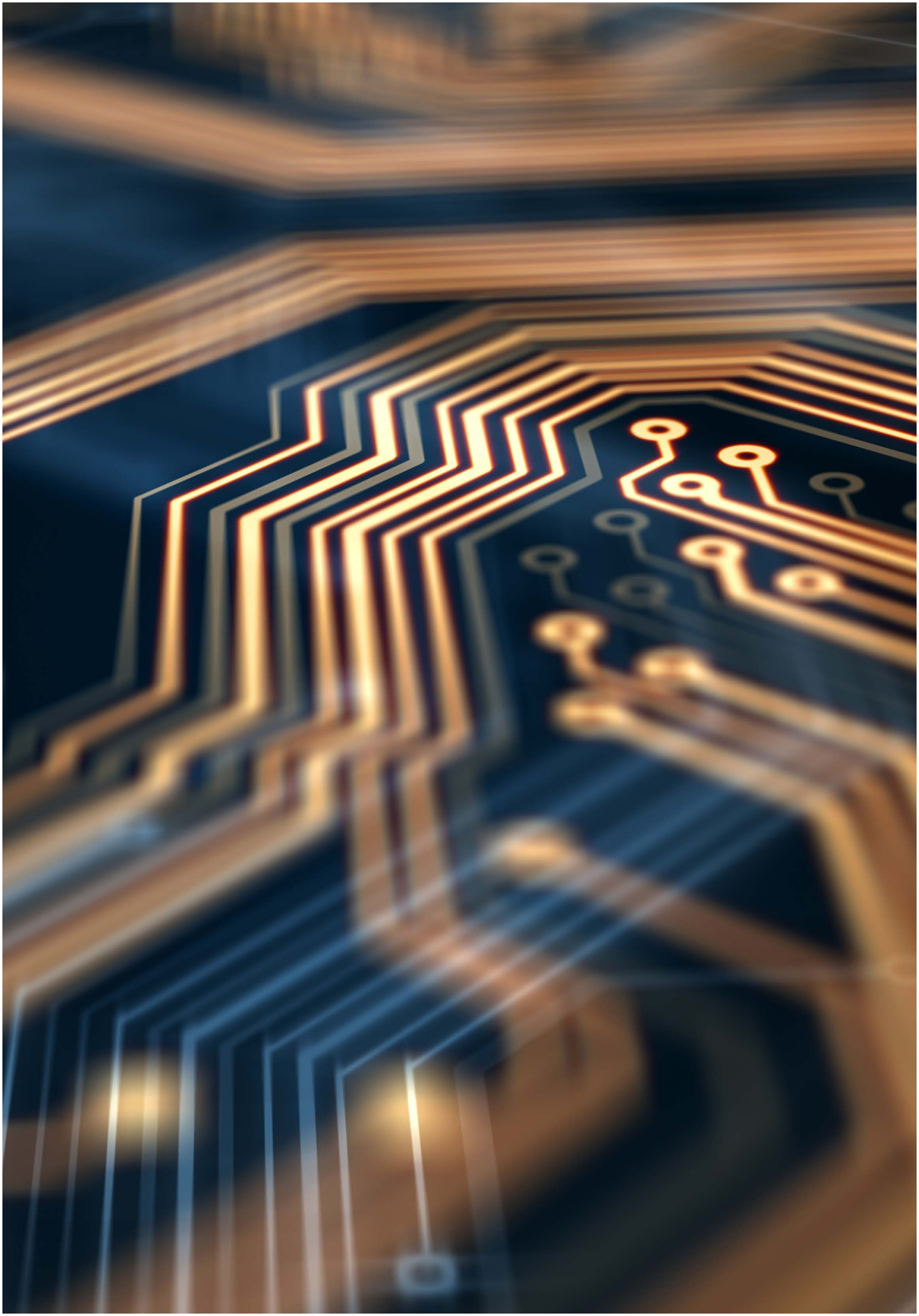
„Je kompetenter und vorsichtiger der Gegner, desto schwieriger ist die Attribution. Aber auch die besten Hacker machen Fehler, so dass es oft eine Indizienkette gibt, die auf eine bestimmte Gruppe deutet. Je qualifizierter der Gegner, desto schwieriger wird aber auch ein Gegenschlag, vor allem wenn dabei »aus der Hüfte geschossen« wird. Komplexe Cyber-Angriffe erfordern ein hohes Maß an Kenntnis des Zielsystems und seines Einsatzkontexts."

(Schulze, Matthias, Hacking back? Technische und politische Implikationen digitaler Gegenschläge, in SWP-Aktuell 59, August 2017)

Active Cyber Defense und präventive Cyberoperationen werden kontrovers diskutiert, zum Beispiel, ob auch aktiv mit konventionellen Mitteln auf einen Cyberangriff reagiert werden darf, ab welcher Wahrscheinlichkeit eines Cyberangriffs ein präventiver Gegenschlag gerechtfertigt ist und wie mit einer möglichen falschen Attribution des Gegners umzugehen ist.

Die Unterscheidung von aktiven und defensiven Maßnahmen im Cyberraum kann nicht klar abgegrenzt werden. Die aktive Verteidigung sollte maßgeschneidert auf den möglichen Angreifer sein, um wirken zu können. Dazu sollte der Verteidiger Informationen über systemspezifische Schwachstellen gewinnen. Wir sind der Meinung, dass Active Cyber Defense die Cybersicherheit verstärkt und deshalb weiterhin an Bedeutung gewinnen wird.

[18] NATO CCD COE, Definition, https://ccdcoe.org/cyber-definitions.html.



3. Akteure in der nationalen Cybersicherheitsvorsorge

Welche Institutionen auf staatlicher Ebene haben welche Verantwortung und Aufgaben für Cybersicherheit?

Die Ausgestaltung der jeweiligen Institutionen im Bereich Cyber auf nationaler Ebene unterscheidet sich von Staat zu Staat. Im Gegensatz zu der Außen- oder Verteidigungspolitik existieren in den untersuchten Staaten keine einheitlichen Strukturen, die beispielsweise in einem einzelnen Ministerium mit leitendem Verantwortungsbereich widergespiegelt sind. Der schwer einzugrenzende Cyberraum zeigt hier abermals seine Besonderheit und Komplexität, da dieser im Vergleich zu anderen Politikfeldern nicht so einfach thematisch sowie organisatorisch greifbar und damit zuzuordnen ist.

Daher ist es nicht verwunderlich, dass in der Regel die jeweiligen nationalen Cyberstrategien mehrere Akteure benennen, die mit Cybersicherheit auf staatlicher Ebene beauftragt sind. Es ist unverkennbar, dass Cyber als Thema nicht nur einem Geschäftsbereich in den Staaten zugeordnet ist. So ist das Querschnittsthema je nach Schwerpunktsetzung den einzelnen Ministerien zugeteilt, zum Beispiel Cyberkriminalität dem Innenministerium, Cyberaußenpolitik dem Außenministerium und Cyberverteidigung dem Verteidigungsministerium.

„Innere und äußere Sicherheit fallen in wenigen Bereichen so eng zusammen wie im Cyberraum. Die Bedrohungslage im Cyberraum erfordert eine ganzheitliche Betrachtung im Rahmen der Cybersicherheitspolitik. Die Wahrung der Cybersicherheit und -verteidigung ist somit eine gesamtstaatliche Aufgabe, die gemeinsam zu bewältigen ist. Dazu gehört auch der gemeinsame Schutz der kritischen Infrastrukturen. Die Konkretisierung der Aufgabenwahrnehmung erfolgt im Rahmen der Cybersicherheitsstrategie, die unter Federführung des Bundesministeriums des Innern erarbeitet wird. Verteidigungsaspekte der gesamtstaatlichen Cybersicherheit sind originäre Aufgaben des Bundesministeriums der Verteidigung und der Bundeswehr, während die Gesamtverantwortung für die internationale Cybersicherheitspolitik beim Auswärtigen Amt liegt."

(Deutschland, Weißbuch 2016)

Insgesamt unterscheiden sich die koordinierenden Institutionen bei der Cyberthematik in den jeweiligen Staaten. Zumeist ist jedoch die Federführung in einem Ministerium angesiedelt. Beispielsweise kommt im türkischen Kontext diese Rolle dem Ministerium für Transport, Marine und Kommunikation zu, welches neben dem Verfassen der nationalen Cybersicherheitsstrategie auch den Cyberaktionsplan für 2016-2019 koordiniert.

In Deutschland – trotz einer vorhandenen Aufgabenteilung – übernimmt das Bundesministerium des Innern, für Bau und Heimat die Federführung in staatlichen Cyberfragen. Auch in Irland übernimmt diese Funktion ein Ministerium, nämlich das Ministerium für Kommunikation, Energie und natürliche Ressourcen, welches mit dem dort angesiedelten National Cyber Security Centre die Cyberpolitik steuert.

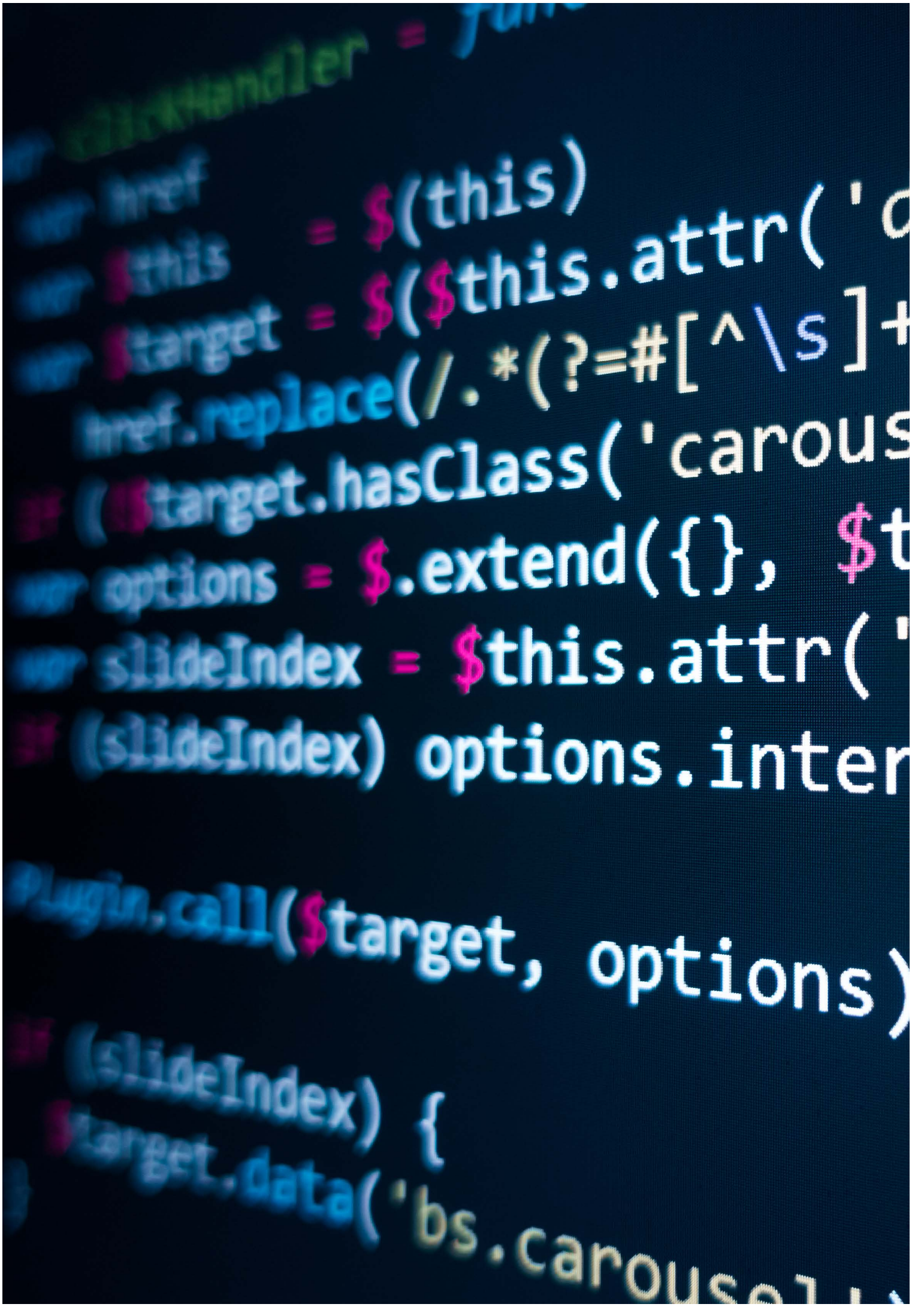
Die grundsätzliche Anzahl der Institutionen, die in den jeweiligen nationalen Cyberstrategien genannt werden, variiert teilweise stark. So werden beispielsweise in einigen Strategien drei oder weniger Akteure genannt (z.B. Litauen, Polen oder Portugal); bei anderen Staaten ist die Zahl sogar zweistellig (z.B. Lettland). Auch Deutschland gehört zu den Staaten, deren Cyberlandschaft vergleichsweise ausdifferenziert ist. So existieren neben dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Kommando Cyber- und Informationsraum (KdoCIR) weitere Institutionen wie das Nationale Cyber-Abwehrzentrum (NCAZ) oder die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS).

In einzelnen Cybersicherheitsstrategien lässt sich sogar sehr schwer eine klare Verantwortungsverteilung auf staatlicher Ebene erkennen. So wird beispielsweise in der litauischen Strategie Strategie mit dem CERT_LT gerade mal ein Akteur genannt. Daran anlehnend kann jedoch festgehalten werden, dass diese Computer Emergency Response Teams (CERT) nahezu ein fester Bestandteil der Cybersicherheit europäischer Staaten sind: CERT/CSIRT-Strukturen bzw. deren Förderung sind in knapp zwei Drittel (19 von 29) der betrachteten nationalen Cybersicherheitsstrategien benannt. So auch in Deutschland, wo bereits im Jahr 2001 das Computer Emergency Response Team Bund (CERT-Bund) gegründet wurde. Hierbei unterstützt eine Gruppe von Sicherheitsfachleuten die staatlichen Institutionen bei der Lösung von konkreten IT-Sicherheitsvorfällen. Weitere eigenständige CERT-Strukturen sind in anderen Bundesbehörden, in Länderverwaltungen, in einzelnen Unternehmen und in wissenschaftlichen Einrichtungen etabliert. Neben dem CERT-Bund existiert auch noch das Computer Emergency Response Team der Bundeswehr (CERTBw), welches die ca. 200.000 Computer der Bundeswehr vor Angriffen aus dem Internet schützt.

In den letzten Jahren zeichnet sich zudem eine Tendenz ab, dass mehr und mehr europäische Staaten den Cyberraum zunehmend als einen Ort der potenziellen Kriegsführung verstehen und dahingehend Maßnahmen ergreifen. Dies ist auch im Einklang mit der Entwicklung auf der Ebene der internationalen Organisationen, indem beispielsweise die NATO 2016 den Cyberraum als eigenständige Kriegsdimension definiert hat. Um für den „Cyberwar" im Notfall gewappnet zu sein, haben viele Staaten in den letzten Jahren militärische Cyberfähigkeiten in ihren Streitkräften etabliert. So auch die Bundesrepublik Deutschland, die innerhalb der Bundeswehr den Organisationsbereich Cyber- und Informationsraum für diesen Zweck im April 2017 offiziell aufgestellt hat. Neben Deutschland schreiben Bulgarien, Finnland, Großbritannien, Irland, Lettland, Polen und Spanien von militärischen Cyber-Defense-Kapazitäten in den nationalen Cybersicherheitsstrategien, das entspricht annähernd einem Drittel der betrachteten Strategien. Auch streben Dänemark, Deutschland, Großbritannien, Norwegen, Spanien und die USA bis Anfang 2019 an, gemeinsam Prinzipien der Cyberkriegsführung aufzustellen, die als Anleitung für ihre jeweiligen Streitkräfte beim Anwenden von Cyberoperationen dienen sollen.[19] Vor allem die großen europäischen Staaten wie Deutschland, Frankreich und Großbritannien haben in den letzten Jahren in militärische Cyberkapazitäten investiert.[20]

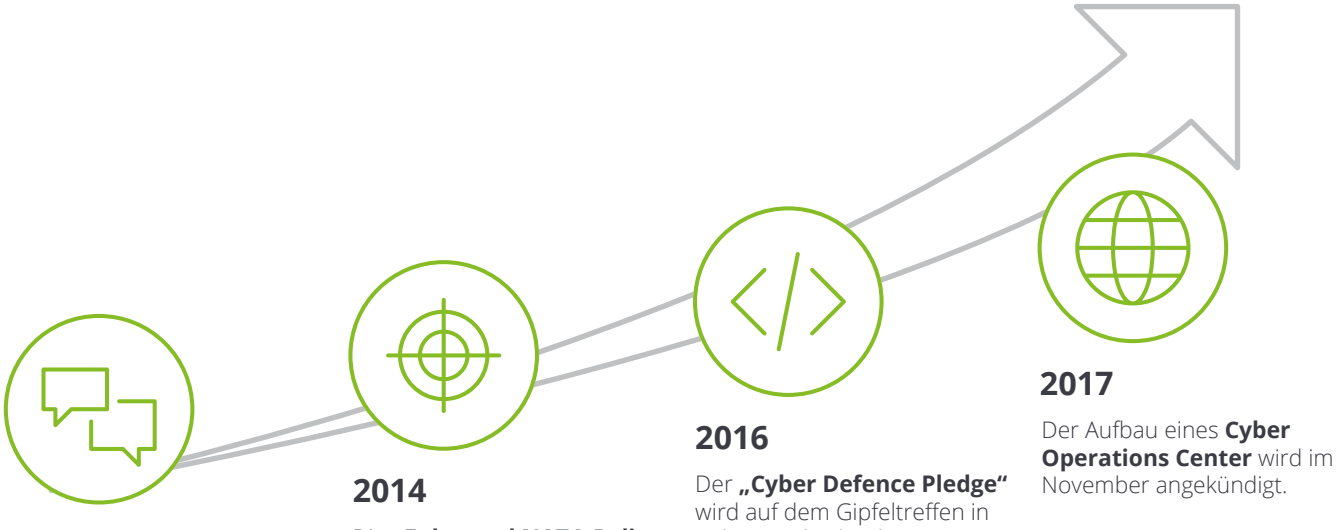
[19] https://www.reuters.com/article/us-naato-cyber/nato-mulls-offensive-defense-with-cyber-warfare-rules-idUSKBN1DU1G4?utm_source=applenews

[20] https://www.euractiv.de/section/eu-innenpolitik/news/eu-ruesten-fuer-den-cyberkrieg/


$(this)
$($this.attr('
href.replace(/.*(?=#[^\s]+
($target.hasClass('carous
options = $.extend({}, $t
slideIndex = $this.attr('
(slideIndex) options.inter
Plugin.call($target, options)
(slideIndex) {
$target.data('bs.carousel')

4. Sachstand internationaler Kooperationen zur Abwehr von Cyberbedrohungen

Abb. 9 – NATO – Internationale Kooperationen für Cyberverteidigung



2010

Cyberverteidigung findet Erwähnung im Strategischen Konzept unter den Bedrohungen für die NATO.

2014

Die **„Enhanced NATO Policy on Cyber Defence“** wird auf dem Gipfeltreffen in Wales verabschiedet.

2016

Der **„Cyber Defence Pledge“** wird auf dem Gipfeltreffen in Polen verabschiedet.

Cyber wird als eigenständige Warfare Domain benannt.

Ein Cyberangriff könnte kollektiven Verteidigungsfall auslösen.

2017

Der Aufbau eines **Cyber Operations Center** wird im November angekündigt.

NATO: Cyberverteidigung ganz oben auf der Agenda angelangt

Spätestens seit den Cyberattacken gegen Staatsbehörden und Unternehmen im NATO-Mitgliedstaat Estland im Jahr 2007, hat die Allianz sukzessive das Thema Cyberverteidigung aufgewertet und Maßnahmen diesbezüglich ergriffen. Schon im Strategischen Konzept von 2010 wird auf die zunehmende Bedrohung durch Cyberattacken hingewiesen. Ein entscheidender Wendepunkt seitens der Mitgliedstaaten war es jedoch, die sogenannte „Enhanced NATO Policy on Cyber Defence" auf dem Gipfeltreffen in Wales 2014 zu beschließen. Diese sieht vor, dass Cyberangriffe nun konkret im Kontext von ‚Kollektiver Verteidigung' gesehen werden können und dass Operationen dieser Art auf einen Mitgliedstaat auch zum Ausrufen des Bündnisfalls (Artikel 5 des NATO-Vertrags) im Ernstfall führen kann. Ferner wurde Cyberverteidigung in Verbindung mit Artikel 3 (Selbstverantwortung bei den Mitgliedstaaten bei der Sicherheit des eigenen Landes) und Artikel 4 (Möglichkeit von Konsultation im NATO-Rahmen) gesetzt.

Eine weitere Aufwertung erfolgte auf dem NATO-Gipfeltreffen in Warschau 2016, als die damals noch 28 Mitgliedstaaten den „Cyber Defence Pledge" verabschiedeten und zudem den Cyberraum als fünfte Operationsdomäne (neben Land, See, Luft und Weltraum) definierten. Er beinhaltet sieben – wenn auch nicht bindende – Ziele für die Mitglieder, die unter anderem das Behandeln von Cyberverteidigung auf höchster nationaler strategischer Ebene und die Förderung von Ausbildungsaktivitäten in den jeweiligen Staaten vorsehen. Der erste Bericht über die Implementierung dieser sieben Ziele in den jeweiligen Mitgliedstaaten wurde im Mai 2017 auf dem NATO-Treffen der Staats- und Regierungschefs vorgestellt.

„[W]hilst in many Allies the cyber defense policy framework was relatively mature, challenges existed in both resourcing, recruitment, and retention."[21]

(Robertson, Neil, NATO Policy Officer, Cyber Defense at NATO: From Wales to Warsaw, and Beyond, in: Turkish Policy Quarterly, Fall 2017)

„Cyber attacks can be as dangerous as conventional attacks. They can shut down important infrastructure. They can have a great negative impact on our operations."

(Stoltenberg, Jens zit. nach Roberston, Neil NATO Policy Officer, Cyber Defense at NATO: From Wales to Warsaw, and Beyond, in: Turkish Policy Quarterly, Fall 2017)

[21] http://turkishpolicy.com/article/887/cyber-defense-at-nato-from-wales-to-warsaw-and-beyond

Ein weiterer Schritt erfolgte im November 2017, als die NATO den Aufbau eines Cyber Operations Center ankündigte. Das Ziel des Centers soll es sein, Bedrohungen schneller vorauszusehen und die Reaktionsfähigkeit zu erhöhen. Einzelne Cybereinheiten können zudem nun auch in Operationen und Missionen der Allianz integriert werden. Die Fähigkeiten sollen vorerst auf freiwilliger Basis von den Mitgliedstaaten bereitgestellt werden. Jedoch ist noch nicht deutlich geworden, inwieweit das Center und die NATO im Einsatz auch offensive Cyberoperationen als Teil ihres Tätigkeitsfeldes ansehen.

Ferner existiert mit dem NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn eine Institution, die zur Aufgabe hat, die Kooperation zwischen der NATO und ihren Mitglieds- und Partnerstaaten im Hinblick auf Cyberverteidigung durch Ausbildung, Beratung, Forschung und Entwicklung zu erhöhen. Im Kontext der CCDCOE wurde auch das Tallinn Manual 2.0 erstellt, welches das womöglich detaillierteste Schriftstück zur Verknüpfung von internationalem Völkerrecht und Cyberraum darstellt. Das Tallinn Manual 2.0 ist eine rechtliche Analyse häufig auftretender Cybervorfälle, mit denen sich Staaten täglich konfrontiert sehen und die durch den Einsatz von Gewalt und bewaffnete Konflikte geprägt sind. Die Version 2.0 ergänzt den ursprünglichen Inhalt des Tallinn Manuals. Es beinhaltet vor allem Verstöße gegen das Gewaltverbot in internationalen Beziehungen durch schwere Cyberoperationen. Es hat jedoch keinen bindenden Charakter.

Mit der Cyber Coalition gibt es zudem eine jährliche NATO-Übung, in der die unterschiedlichen Mitgliedstaaten ihre Fähigkeiten testen und die internationale Zusammenarbeit in dem Bereich proben. Auch das CCDCOE veranstaltet die jährliche Cyberübung Locked Shields, bei den Staaten, Universitäten und große Firmen an einer Echtzeit-Simulation teilnehmen. Auf EU-Ebene wurde zudem im September 2017 unter Beteiligung der Verteidigungsminister die EU CYBRID in Tallinn durchgeführt, bei der die Entscheidungsfähigkeit angesichts von Cyber- und Hybridbedrohungen getestet worden ist.

Abb. 10 – Europäische Union – Cybersicherheit auf mehreren Ebenen

EU: Cybersicherheit auf mehreren Ebenen

Auch für die Europäische Union hat das Thema Cybersicherheit nach und nach an Wichtigkeit gewonnen. Der erste Meilenstein war hierbei die Veröffentlichung der „Cybersecurity Strategy of the European Union" im Jahr 2013. Eine der Kernaussage der Strategie ist, dass die EU sich zwar grundsätzlich konzeptionell und mit eigenen Unterorganisationen mit dem Thema beschäftigt, doch die Hauptverantwortlichen für die Prävention und Antwort auf Cyberattacken grundsätzlich die einzelnen Mitgliedstaaten auf nationaler Ebene sind. Diese Strategie wurde im September 2017 um weitere Aspekte aktualisiert, wie die Weiterentwicklung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) zu einer EU-Agentur für Cybersicherheit, der Ausbau eines europäischen Krisenmanagement-Mechanismus oder die Entwicklung von Projekten im Bereich militärischer Cyberverteidigung. Ferner hat die EU im Oktober 2017 einen diplomatischen Reaktionsrahmen verabschiedet, welcher bei etwaigen Cybervorfällen zum Tragen kommen soll. Dieser beinhaltet jedoch vorerst nur nichtmilitärische Mittel.[22]

Neben der Cybersicherheitsstrategie thematisieren auch andere Strategie- und Konzeptpapiere die Cybersicherheit, so u.a. die Digitale Agenda für Europa 2020, die Globale Strategie für die Außen- und Sicherheitspolitik der EU oder der Gemeinsame Rahmen für die Abwehr hybrider Bedrohungen.

[22] https://www.swp-berlin.org/publikation/die-eu-als-friedensmacht-in-der-internationalen-cyberdiplomatie/

Die Hauptorganisationen innerhalb der EU, die sich mit der Cybersicherheit beschäftigen, sind neben der zurzeit unterbesetzten ENISA, die Europäische Kommission, das Computer Emergency Response Team der EU (CERT-EU) und die European Public-Private Partnership for Resilience (EP3R). Weitere relevante Akteure sind das EU Intelligence and Situation Centre (EU INTCEN) und die bei INTCEN eingebettete Hybrid Fusion Cell, die sich mit der Analyse von hybriden Bedrohungen beschäftigt. Bei der Bekämpfung von Cyberkriminalität sind die grundsätzlichen Akteure das European Cybercrime Centre (EC3) und EUROPOL.

Mit dem Inkrafttreten der Network and Information Systems Directive (NIS Directive) im August 2016 wurde zudem ein Rahmen für EU-weite Regeln bei der Cybersicherheit gesetzt. Die Richtlinie sieht vor, dass die Mitgliedstaaten Maßnahmen zum Schutz vor Cyberattacken ergreifen müssen, unter anderem den Aufbau von nationalen zentralen Ansprechpartnern und Computer Security Incident Response Teams (CSIRT) als auch die Schaffung von Sicherheits- und Notifizierungsanforderungen für Betreiber von kritischen Infrastrukturen.

„Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."

(Cybersecurity Strategy of the European Union, 2013)

Tab. 1 – Europäische Union – Zuständigkeitsbereiche Cyberverteidigung und -diplomatie

Cybersicherheit in der EU[23]	Frieden,Sicherheit, Justiz	Binnenmarkt	GSVP: Cyberverteidigung	GASP: Cyberdiplomatie
Europäische Union	Europol (EC3) Eurojust EU-LISA	ENISA CSIRT-Netzwerk CERT-EU	EDA GSA	EEAS SIAC (EU INTCEN, EUMS INT) EU SITROOM EU-Hybrid Fusion Cell ERCC
National	Exekutiv- und Datenschutz-behörden	Für die NIS zuständige Behörden Nationale CSIRTs	Verteidigungs-, Militär- und Sicherheitsbehörden	Außenministerien

[23] Dr. Bendiek, A. (2018): Die EU als Friedensmacht in der internationalen Cyberdiplomatie, SWP-Aktuell 22, S. 4.

EU und NATO: Die geplante Zusammenarbeit bei der Cybersicherheit kommt langsam voran

In der „Joint Declaration" vom Juni 2016 haben beide Organisationen die Absicht erklärt, enger zu kooperieren. Auch bei der Bekämpfung von Cyberattacken will man gemeinsam agieren, indem unter anderem die EU und die NATO Konzepte mit Bezug auf Cyberverteidigung austauschen und auf die Interoperabilität bei Anforderungen und Standards in dem Bereich achten. Es sollen auch Trainingskurse für die Mitarbeiter der jeweils anderen Organisation offenstehen. Ferner sollen Forschung und technologische Innovationen zwischen beiden Akteuren als auch die gemeinsame Teilnahme an Cyberübungen gefördert werden.

Im selben Jahr haben EU und NATO ein „Technical Agreement" verabschiedet, welches den technischen Informationsaustausch zwischen dem Computer Emergency Response Team der EU (CERT-EU) und der NATO Computer Incident Response Capability (NCIRC) vorsieht.

Nichtsdestotrotz wird die Kooperation zwischen beiden Organisationen auch bei der Cyberbekämpfung von höhergelagerten Problemen gehemmt. So spielen hier das spezifische Eigenleben beider Organisationen und der ungelöste Zypern-Konflikt eine behindernde Rolle.

Cybersicherheit und die UN: Ist der Wunsch nach internationalen Cybernormen noch haltbar?

Die zunehmende digitale Vernetzung und die globalen Auswirkungen von Cyberattacken haben Staaten sich dazu bewogen, sich mit der Schaffung von internationalen Cybernormen zu beschäftigen. Der Hauptrahmen für dieses Ziel war bis zuletzt die „UN Group of Governmental Experts" (UN GGE[24]), die sich seit 2004 in fünf Verhandlungsrunden mit dieser Thematik befasst hat. Das Format besteht aus 25 Experten, die von den jeweiligen Mitgliedern nominiert werden. Ein erster Durchbruch wurde hierbei im Jahr 2013 erreicht, als die UN GGE einen Konsensbericht verabschiedete, in dem grundsätzlich die Anwendung des internationalen Völkerrechts auf den Cyberraum bestätigt wurde.

Die letzte GGE-Runde von 2016/2017 war jedoch von Ernüchterung geprägt: Die Mitglieder konnten sich nicht auf einen erneuten Konsensbericht einigen, da die entscheidende Frage, wie das internationale Völkerrecht auf den Cyberraum angewendet werden soll, sich als größter Streitpunkt zwischen den westlichen Staaten auf der einen Seite und China und Russland auf der anderen Seite herausstellte.

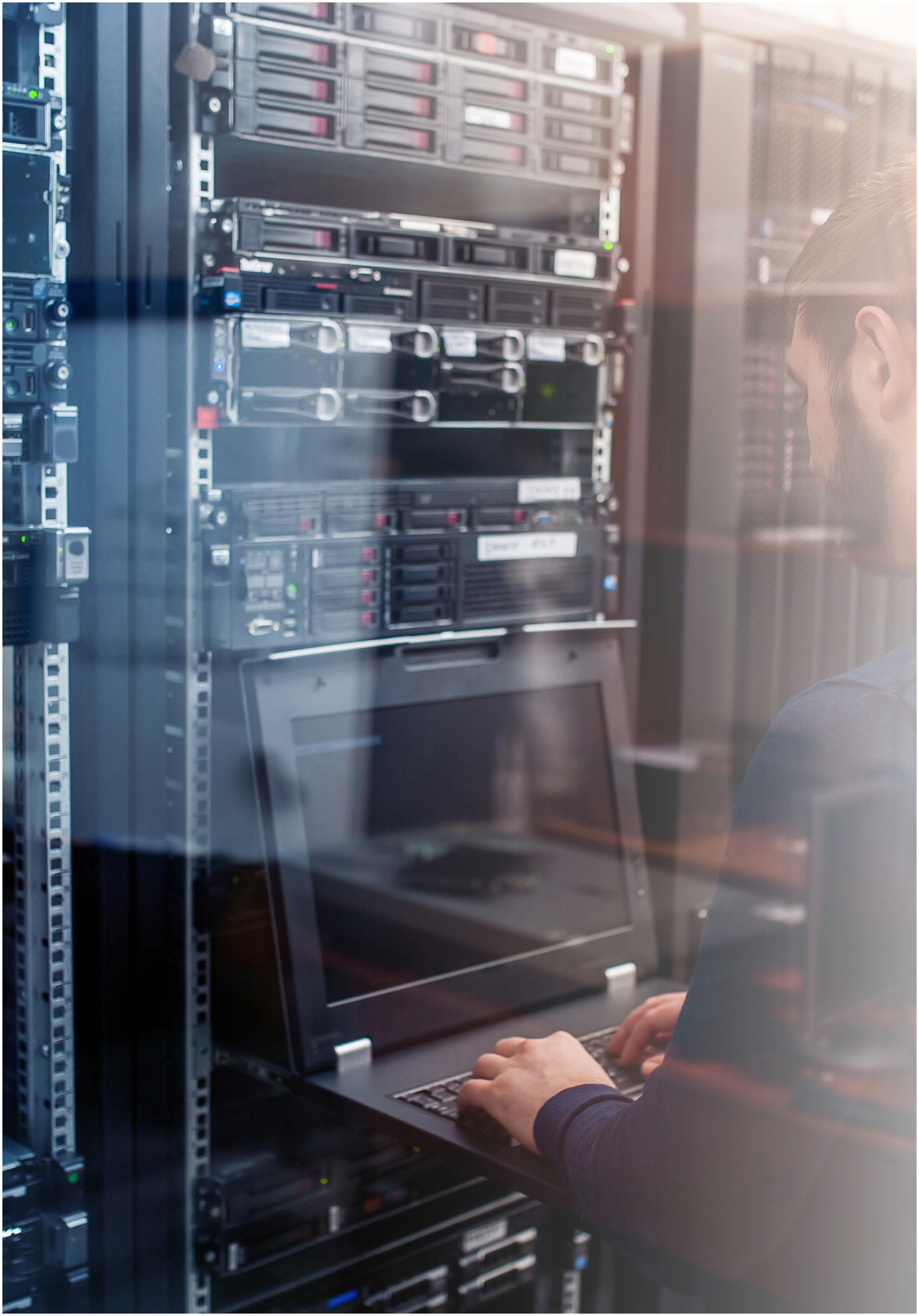
Es bleibt daher abzuwarten, ob dieses Format zur Normenbildung weiterhin bestehen bleibt oder die einzelnen Staaten sich neue Möglichkeiten zur grenzübergreifenden Verständigung im Cyberraum erschließen. So wird auch vermehrt auf bilaterale oder trilaterale Cyberkonsultationen seitens Staaten wie den USA und Deutschland gesetzt.

Neben der UN GGE beschäftigen sich auch noch weitere zahlreiche Agenturen und Institutionen mit der Cyberthematik, so zum Beispiel das UN Office on Drugs and Crime (UNODC), das UN Interregional Crime and Justice Research Institute (UNICRI) oder auch das UN Institute for Disarmament Research (UNIDIR). Dies ist allerdings nur ein Ausschnitt der Akteure im UN-Verantwortungsbereich, was sich anhand verschiedener Resolutionen der UN-Generalversammlung erkennen lässt.

Abb. 11 – Internationale Kooperationen sind überwiegend Kernziel in nationalen Cybersicherheitsstrategien

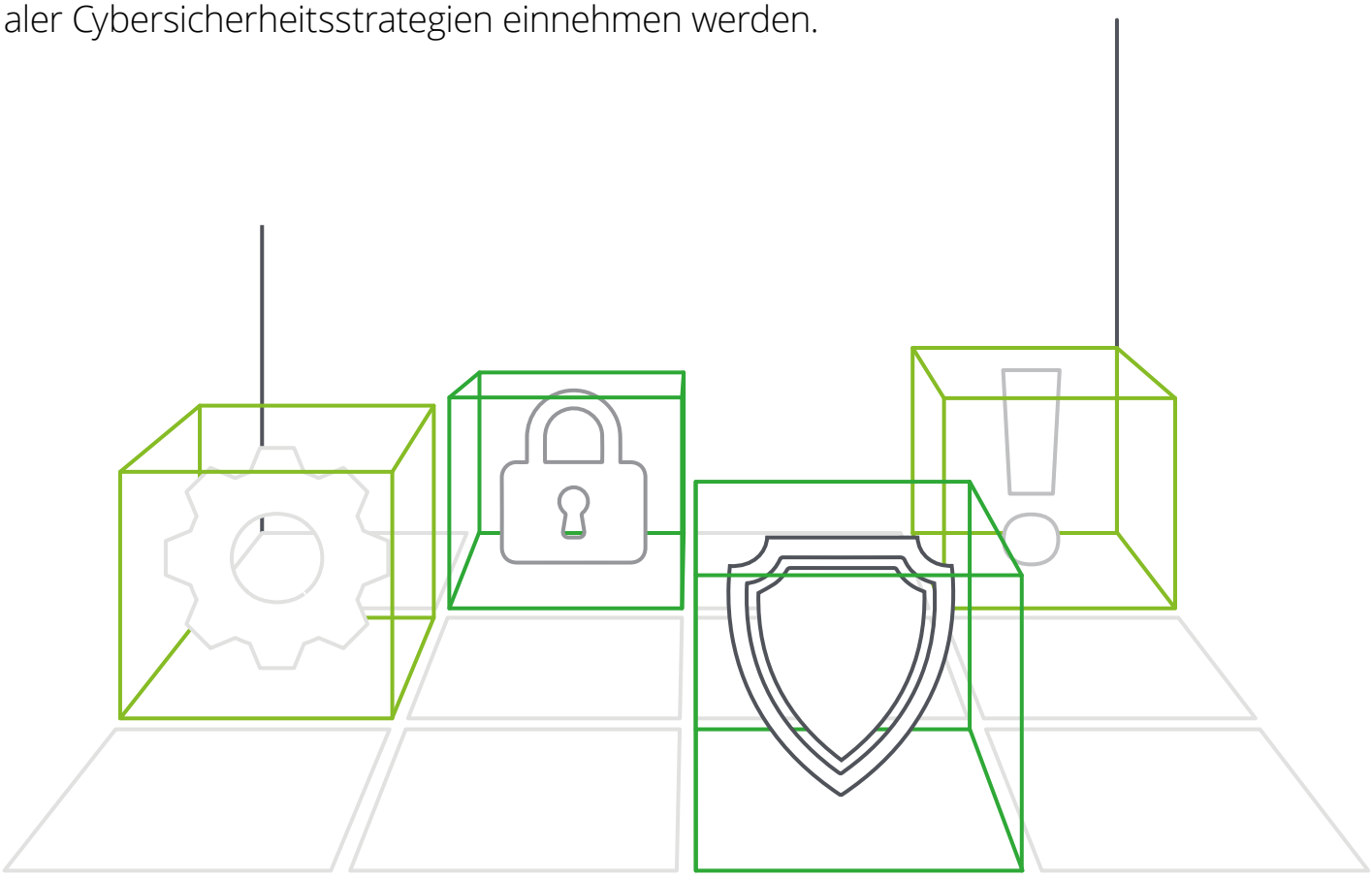
17 von 29 Strategien
setzen auf internationale Kooperationen zum Austausch von Wissen und einer schnellen Strafverfolgung; dies sollen sowohl staatliche als auch öffentlich private Partnerschaften sein.

[24] UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security



5. Handlungsfelder

Aus unserem systematischen Vergleich haben wir sechs mögliche Handlungsfelder identifiziert. Wir sind überzeugt, dass diese einen großen Raum bei der Aktualisierung nationaler Cybersicherheitsstrategien einnehmen werden.



1. Aktualisierung älterer Strategien
Staaten, kriminelle Gruppierungen oder einzelne Hacker verfeinern stets ihre „Cyberwaffen", sodass sich die Cyberbedrohungslage in rasantem Tempo ändert. Vor allem der Trend, dass Cyber zu einem neuen Operationsgebiet der Kriegsführung geworden ist, ist deutlich erkennbar. Der dazugehörige NATO-Beschluss von 2014 war hierfür das deutlichste Zeichen. Wir nehmen an, dass europäische Staaten mit älteren Strategien einen neuen Diskurs im Inland führen werden, um sich an die neue Lage anzupassen und neue Konzepte bzw. Strategien zu verfassen. Dabei werden sie die nationalen Cybersicherheitsstrategien eng mit den nationalen Sicherheitsstrategien abstimmen und zukünftig stets im gleichen Änderungsprozess anpassen. Nationale Strategien europäischer Staaten erfordern zunehmend einen gemeinsamen europäischen Strategierahmen.

2. Unterstützung und Dynamisierung der Strategiebildung mit Hilfe von Trend- und Szenarioanalysen
Um mit den vorherrschenden Unsicherheiten im Cyberraum umzugehen und diese, so gut wie es geht, zu antizipieren, erscheinen Trend- und Szenarioanalysen als ein geeignetes Hilfsmittel. Mit ihnen können zum einen langfristige Entwicklungen prognostiziert und quantifiziert werden. Zum anderen lassen sich Parameter, deren zukünftige Ausprägung unsicher ist, denen aber ein hoher Einfluss auf Cybersicherheit zugeschrieben wird, in die Strategie einbeziehen.

Die den Strategien zugrunde liegenden Perzeption von Bedrohungslage und Verantwortung könnten in geregelten Abständen oder dauerhaft überprüft werden. Wir glauben, dass damit dynamisierte Prozesse zur Anpassung von Cybersicherheitsstrategien etabliert werden. Sie könnten die Meldestellen für Cybervorfälle bis zur Inkraftsetzungsebene der Regierung einbeziehen und es den Verantwortlichen ermöglichen, schnell auf Änderungen in der Cyberbedrohungslage einzugehen und im Sinne des vorausschauenden Schutzes der Gesellschaft und Wirtschaft zu agieren. Ein Bruch in der Befassung mit einer Strategie nach der Inkraftsetzung bis zur nächsten Aktualisierung würde damit ausbleiben.

3. Einigung auf einheitliche Definitionen auf internationaler Ebene
Wir glauben, dass in Zukunft verstärkte Bemühungen erforderlich sind, einheitliche Definitionen zu etablieren, um eine effektive Zusammenarbeit auf internationaler Ebene zu ermöglichen. Dabei könnten gemeinsame und unter Umständen auch verbindliche Cybersicherheitsstandards geschaffen werden. Dies würden die Kooperation und die gemeinsame Reaktionsfähigkeit erheblich schärfen und stärken. Unter anderen könnten dabei Richtlinien für die Bekämpfung von Cyberattacken definiert werden.

4. Klare Definition der Verantwortung

Da der schwer einzugrenzende Cyberraum im Vergleich zu anderen Politikfeldern nicht so einfach räumlich, thematisch und organisatorisch greifbar ist, ist der dazugehörige Verantwortungsbereich in den einzelnen europäischen Staaten oftmals auf mehrere Ministerien und Institutionen verteilt. Wir glauben, dass es in Zukunft verstärkte Bemühungen geben wird, die Verantwortungsbereiche klar zuzuschreiben und es so zu einer partiellen Modifikation der etablierten staatlichen Sicherheitsstrukturen und der zugrunde liegenden Rechtsrahmen kommen wird.

5. Active Cyber Defense zur Stärkung der Cybersicherheit

Im Rahmen unserer Analyse der Strategien haben wir festgestellt, dass die Frage nach Wirksamkeit und Angemessenheit von offensiven Maßnahmen - präventiv oder reaktiv - im Kontext von Cyber Defense (Active Cyber Defense) aktuell intensiv und kontrovers diskutiert wird.

Ein Aspekt der Diskussion ist die Frage, ob durch präventive Maßnahmen der Aufwand und die Kosten eines potenziellen Angreifers erhöht und damit letztlich das Risiko eines Cyberangriffs gemindert werden kann. Ebenfalls diskutiert wird die Frage nach den erforderlichen Fähigkeiten um einen potenziellen Angreifer zum Abbruch seines Vorhabens zu zu zwingen, oder nach dem Einsatz von konventionellen Mitteln zur wirksamen Verteidigung bei Cyberangriffen.

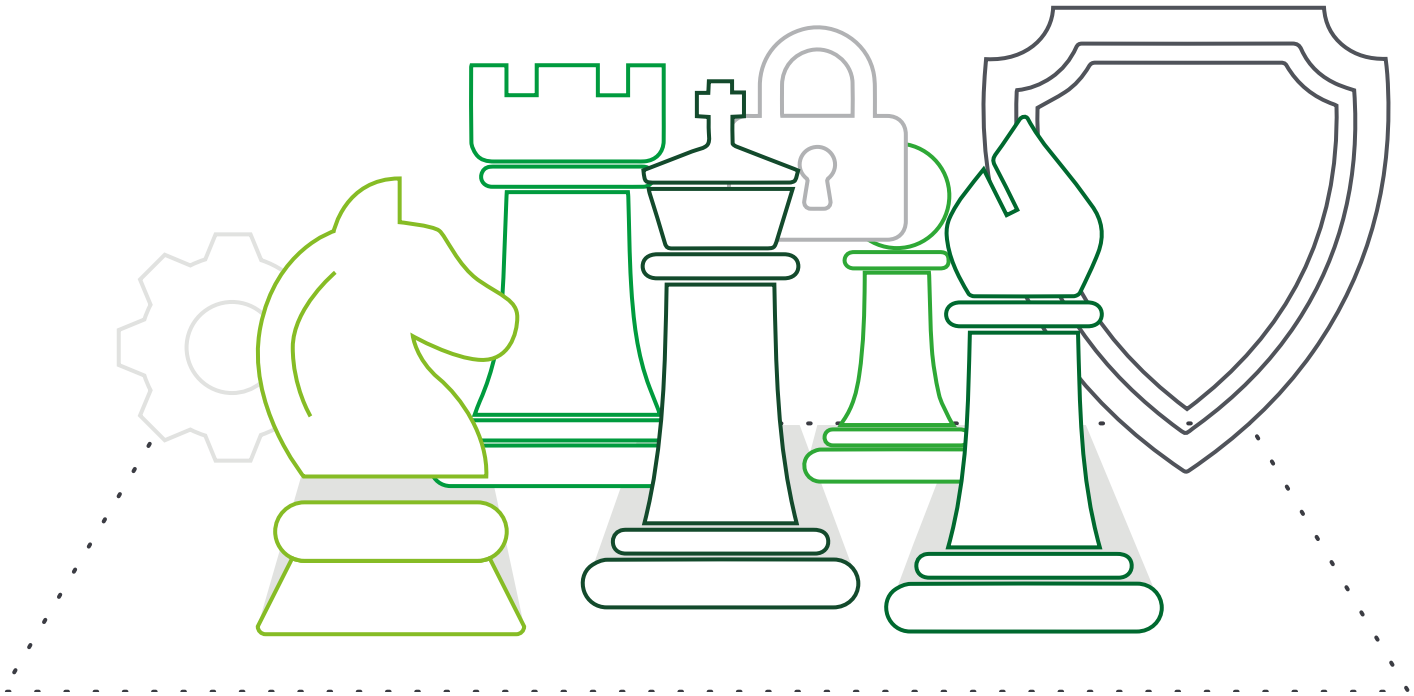
Wir sind überzeugt, dass zukünftig Aussagen zum Einsatz, zur Rechtmäßigkeit und zur Wirksamkeit von Active Cyber Defense in nationalen Strategien einen breiten Raum einnehmen werden.

6. Aufbau einer internationalen Austauschplattform und gemeinsame Übungen

Aufgrund der Unsicherheit und – im Vergleich zu anderen Phänomenen – geringerer Erfahrungswerte hinsichtlich des Cyberraums sind wir davon überzeugt, dass Staaten ihr Wissen und Know-how über gegenwärtige Trends und mögliche Cyberattacken weiter zusammentragen werden. Sie werden eine gemeinsame Wissensbasis schaffen, Best Practices teilen und Institutionen wie die NATO und EU sowie auch die bilaterale Zusammenarbeit stärken. Da der Cyberraum schwierig einzugrenzen ist und eine immense Unsicherheit hinsichtlich der Ausprägung sicherheitsrelevanter Parameter mit sich bringt, scheinen Übungen von EU- und NATO Staaten von Bedeutung zu sein, um ein gemeinsames Gefühl für eine schnelle Reaktionsfähigkeit und angemessene Antwortoptionen zu erhalten. Durch die Simulation spezifischer Szenarien und Handlungen könnten im Voraus Optionen zu bestimmten Situationen erarbeitet werden, sodass diese im Ernstfall griffbereit sind. Wir glauben, dass eine Austauschplattform und gemeinsame Übungen bestimmte Unterschiede in der Herangehensweise aufzeigen, die dann als Diskussionsgrundlage dienen und zu gemeinsamen Lösungen beitragen werden.

Innerhalb der Handlungsfelder sollten Entscheidungsträger alle beteiligten Stakeholder aus Politik, Militär, Geheimdiensten, Netzwerkbetreibern, Wirtschaft und Zivilgesellschaft in eine umfassende Cybersicherheitsstrategie miteinbeziehen. Denn eine enge Zusammenarbeit, national sowie international, aller Beteiligten auf dem Gebiet der Cybersicherheit ist eine unabdingbare Voraussetzung, professionelle Angriffe ebenso professionell abwehren zu können.

Nationale und internationale Cybersicherheitsstrategien auf einen Blick



Belgien

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

Werden als schwerwiegende Bedrohungen zur Bewahrung der nationalen Sicherheit gesehen.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2012
Herausgeber: Premierminister
Zeitrahmen: k.A.
Kernziele:

- Schaffung eines sicheren Cyberraums
- Gewährleistung von Grundrechten und Werten
- Ausbau von Sicherheitsmaßnahmen
- Schutz kritischer Infrastrukturen
- Entwicklung einer unabhängigen Cybersicherheitspolitik
- Ausbau von Partnerschaften und Kooperationen
- Investitionen in Bildung und Forschung

Dargestellte Cyberbedrohungen:

- Botnets
- Cyberspionage
- Cyber Warfare
- Cyberterrorismus

Hauptakteure:
öffentlich

- Computer Emergency Response Team (CERT.be)
- Commission for the Protection of Privacy (CPP)
- National Cyber Security Center (NCSC)
- The Belgian Federal Computer Crime Unit (FCCU)
- Federal Public Service Information and Communication Technology (Fedict)
- Security of the State: Veiligheid van de Staat (VSSE)

militärisch
k.A.

Bulgarien

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2016
Herausgeber: Regional Cybersecurity Forum, National Cybersecurity Coordinator
Zeitrahmen: 2016 - 2020
Kernziele:

- Ausbau des nationalen Cybersicherheitssystems
- verbesserte Reaktionskoordinierung gegen Cyberbedrohungen
- Ausbau kritischer Infrastrukturen
- Zusammenarbeit zwischen Regierung und Betreibern
- Bildung internationaler Koalitionen zum Informationsaustausch

Dargestellte Cyberbedrohungen:
k.A.
Hauptakteure:
öffentlich

- National Cyber Situational Center
- Computer Emergency Response Team (CERT.bg)
- Cyber Crime Center

militärisch

- Military Cyber and Information Center (Mil CiRC)

Dänemark

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

Genannt in einer Reihe mit militantem Islamismus, Terrorismus, Migrationsströmen und Klimawandel.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2018
Herausgeber: Dänische Regierung
Zeitrahmen: 2018-2021
Kernziele:

- Ausbau der Informationssicherheit kritischer Sektoren in der Wirtschaft und Öffentlichkeit
- Stärkung widerstandsfähiger digitaler Infrastrukturen und Technologien
- Weiterbildung und Aufklärung der Bevölkerung
- verbesserte Zusammenarbeit von öffentlich-privaten Partnerschaften

Dargestellte Cyberbedrohungen:

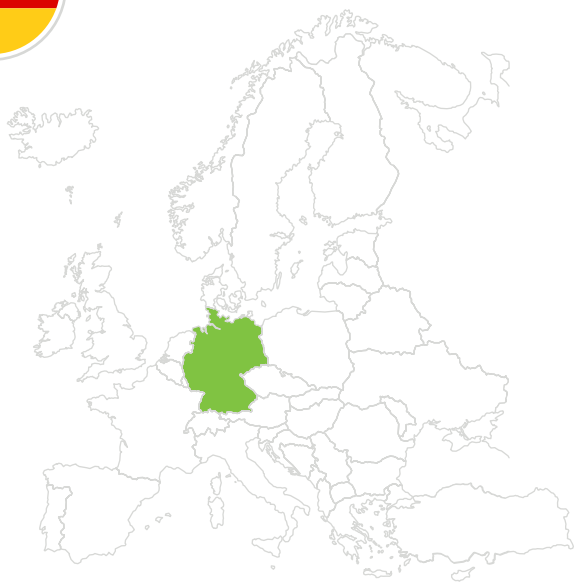
- Datendiebstahl
- Angriffe auf öffentliche Einrichtungen und kritische Infrastrukturen
- Cyberspionage, Cybersabotage, Cyberkriminalität
- Cyber Warfare, Terrorismus
- Malware, Ransomware

Hauptakteure:

öffentlich
  – Danish Centre for Cyber Security
  – Central Operational Communication Staff (DCOK)
  – National Operative Staff (NOST)
  – Government Security Committee
  – Agency for Digitization
  – Danish Security and Intelligence Services

militärisch
  k.A.

Deutschland



Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

Werden in einer Reihe mit transnationalem Terrorismus, zwischenstaatlichen Konflikten, Massenvernichtungswaffen, Klimawandel, irregulärer Migration, Epidemien und Pandemien, fragilen Staaten und Regierungsführungen sowie der Versorgungssicherung von Transport- und Handelswegen eingestuft.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2016
Herausgeber: Bundesministerium des Innern, für Bau und Heimat
Zeitrahmen: k.A.
Kernziele:

- sicheres und selbstbestimmtes Handeln aller Bürger und Industrien
- leistungsfähige und nachhaltige nationale Cybersicherheitsarchitektur
- Förderung der Zusammenarbeit von Regierung und Industrien
- Bildung internationaler Kooperationen und Diskussionsplattformen
- Förderung und Erwerb von Technologien

Dargestellte Cyberbedrohungen:

- Daten- und Identitätsdiebstahl
- Angriffe auf öffentliche Einrichtungen und kritische Infrastrukturen
- Fake News, Cyberspionage, Cybersabotage, Cyberkriminalität
- Malware, Ransomware, Spam, Botnets, Side-Channel-Attacks, Drive-By-Exploits, Exploit-Kits

Hauptakteure:

öffentlich
  – Bundesamt für Sicherheit in der Informationstechnik (BSI)
  – Computer Emergency Response Team (CERT)
  – Cyber Situation Center
  – Nationales Cyber-Abwehrzentrum (NCAZ)
  – Zentralstelle für Informationstechnologie im Sicherheitsbereich (ZITiS)

militärisch
  – Kommando Cyber- und Informationsraum (Kdo CIR)

Estland

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

Genannt in einer Reihe mit volkswirtschaftlicher Instabilität, Radikalisierung, Terrorismus, organisierter Kriminalität, Korruption, Migrationsströmen und einer Vielzahl anderer Notfälle.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2014
Herausgeber: Bundesministerium für Wirtschaft und Nachrichtenwesen
Zeitrahmen: 2014-2017
Kernziele:

- Erhöhung des Nationalbewusstseins gegen Cyberbedrohungen
- Schutz von Informationssystemen
- verbesserte Bekämpfung von Cyberkriminalität
- Entwicklung einer nationalen Cyberverteidigung
- Förderung branchenübergreifender Zusammenarbeit

Dargestellte Cyberbedrohungen:

- Cyberkriminalität
- Abhängigkeit von IKT-Infrastrukturen und elektronischen Diensten

Hauptakteure:
öffentlich

- Estnische Behörde für Informationssysteme (RIA)
- Abteilung zum Schutz kritischer Infrastrukturen (CIIP)
- Cybereinheit der estnischen Verteidigungsliga (EDL CU)

militärisch
k.A.

Finnland

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2013
Herausgeber: Sekretariat des Sicherheits- und Verteidigungsausschusses
Zeitrahmen: k.A.
Kernziele:

- Kooperationsmodell zwischen Behörden und Institutionen
- Gewährleistung der öffentlichen Cybersicherheit
- Stärkung von existenzrelevanten Infrastrukturen
- Ausbau der Fähigkeiten von Polizei und Militär
- Beteiligung an internationalen Organisationen
- Ausbau eines Rechtsrahmens zur Strafverfolgung

Dargestellte Cyberbedrohungen:
k.A.
Hauptakteure:
öffentlich

- Government Information Security Management Board (VAHTI)
- National Cyber Security Centre
- Finnish Communications Regulatory Authority (FICORA)
- Strategic Cyber Security Centre of Excellence (TIVIT

militärisch

- Military Cyber Defence Forces

Frankreich

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

Im „White Paper“ von 2008 und 2013 werden Cyberangriffe mit Terroranschlägen, Massenvernichtungswaffen, Natur- und Gesundheitskrisen, industriellen Unfällen, Angriffen auf den Staat und deren Bürger gleichgestellt.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2015
Herausgeber: Premierminister
Zeitrahmen: k.A.
Kernziele:

- Verteidigungsfähigkeit und Sicherheit staatlicher Informationssysteme und kritischer Infrastrukturen
- Wahrung von Privatsphäre, Datenschutz und Cyberraumstabilität
- Aufklärung, Sensibilisierung und Weiterbildung der Bevölkerung
- Schaffung von Vertrauen in der Bevölkerung
- Ausbau digitaler Geschäftstechnologien

Dargestellte Cyberbedrohungen:

- Cyberspionage, Malware
- Daten- und Identitätsdiebstahl
- Erpressung, Sabotage
- Handel mit illegalen Produkten

Hauptakteure:

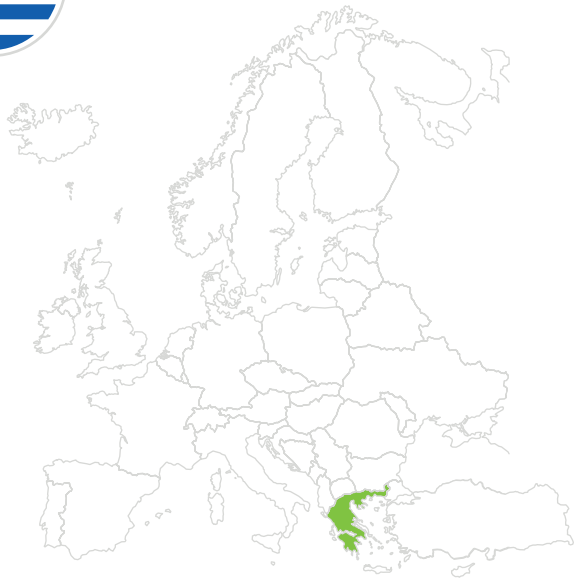
öffentlich

- National Cybersecurity Agency (ANSSI)
- Defence Procurement Agency (DGA)

militärisch

- Commandement de cyberdéfense (COMCYBER/COCYBER)
- La réserve de cyberdéfense

Griechenland



Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2017
Herausgeber: k.A.
Zeitrahmen: k.A.
Kernziele:

- Verbesserung der allgemeinen nationalen Onlinesicherheit
- Wahrung zuverlässiger- und ausfallsicherer kritischer Infrastrukturen
- Sicherung von vertraulichem digitalen Datentransfer
- Aufbau und Integration sicherer und widerstandsfähiger Cyberräume
- Optimierung der Cyberschutzfähigkeit
- institutionelle Abschirmung nationaler Cybersicherheitsrahmen
- Förderung der öffentlichen Cyberkultur zum Schutz der Bürger

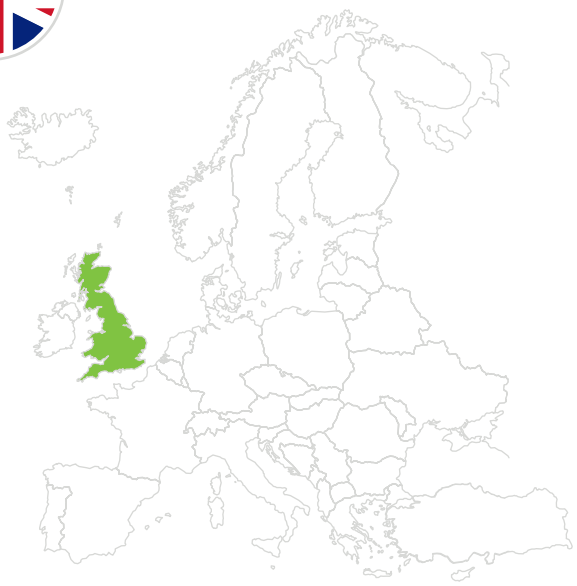
Dargestellte Cyberbedrohungen:

k.A.

Hauptakteure:

Es werden im Allgemeinen öffentliche und private Akteure erwähnt.

Großbritannien



Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

Benannt neben Terrorismus, Militärkonflikten, Volksgesundheit, Überseeinstabilität und großen natürlichen Naturgefahren.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2016
Herausgeber: Die Regierung Ihrer Majestät
Zeitrahmen: 2016-2021
Kernziele:

- schnelle Reaktionen zur Abwendung von Cyberangriffen
- Sicherung von Netzwerken, Daten und Systemen
- Verfolgung von Straftätern
- Förderung von Forschung und Technologieentwicklung
- Ausbau internationaler Partnerschaften

Dargestellte Cyberbedrohungen:

- Cyberkriminalität
- Script-Kiddies
- Cyberterrorismus

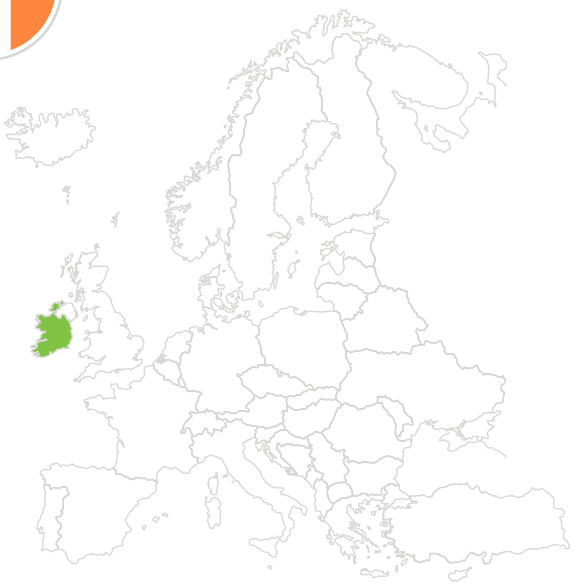
Hauptakteure:
öffentlich

- National Cyber Security Centre (NCSC)
- Government Communications Headquarters (GCHQ)
- National Crime Agency (NCA), National Cyber Crime Unit (NCCU)
- Government Digital Service (GDS)
- National Technical Authority for Information Assurance (CESG)
- National Computer Emergency Response Team (CERT-UK)

militärisch

- Cyber Security Operations Centre (CSOC)
- Ministry of Defence (MoD)

Irland



Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2015
Herausgeber: Ministerium für Kommunikation, Energie und natürliche Ressourcen
Zeitrahmen: 2015-2017
Kernziele:

- Ausbau widerstandsfähiger kritischer Infrastrukturen im öffentlichen Sektor und in entscheidenden Wirtschaftszweigen
- umfassender regulatorischer Rechtsrahmen
- Aufbau öffentlicher Verwaltungskapazitäten
- Aufklärung und Sensibilisierung der Bevölkerung im Umgang mit Daten
- Förderung internationaler Kooperationen

Dargestellte Cyberbedrohungen:

- Hacking, Cyberkriminalität, Cyberspionage, Datendiebstahl
- menschliches Fehlverhalten verursacht Software- und Geräteausfälle

Hauptakteure:
öffentlich

- National Cyber Security Center (NCSC)
- Computer Security Incident Response Team (CSIRT-IE)

militärisch

- Cyber Defence Force (DF)

Italien

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2013
Herausgeber: Ministerpräsident des Ministerrats
Zeitrahmen: k.A.
Kernziele:

- Entwicklung technischer Innovationen
- verstärkte Kooperation nationaler Institutionen
- technische Verbesserung operationaler und analytischer Fähigkeiten aller Cyberinstitutionen
- Verstärkung kritischer Infrastrukturen
- Erhöhung von Sicherheitsstandards
- Zusammenarbeit öffentlich-privater Partnerschaften zum Schutz nationalen geistigen Eigentums
- Bildungsprogramme zum Ausbau der Sicherheitskultur

Dargestellte Cyberbedrohungen:

- Cyberkriminalität: Daten- und Identitätsdiebstahl, (Internet-)/Betrug
- Cyberspionage: illegaler Erwerb vertraulicher Daten
- Cyberterrorismus: ideologisch motivierte Absichten
- Cyber Warfare

Hauptakteure:

öffentlich

- Agency for digital Italy
- Computer Emergency Response Team (CERT-SPC/PA)
- Department for Intelligence and Security (DIS)
- Committee for the Security of the Republic (CISR)
- National Anti-crime Computer Centre for the Protection of Critical Infrastructure (CNAIPIC)

militärisch

k.A.

Kroatien

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2015
Herausgeber: k.A.
Zeitrahmen: k.A.
Kernziele:

- Gewährleistung eines sicheren Datentransfers
- Schaffung eines zuverlässigen und belastbaren Cyberraums
- Ausbau des nationalen Rechtssystems zur Strafverfolgung
- Maßnahmen zur Sensibilisierung von Cyberraumnutzern, juristischen- und Einzelpersonen und der Öffentlichkeit
- öffentliche Aufklärung durch Bildungsprogramme
- Entwicklung und Forschung von neuen Technologien
- international koordinierter Wissens- und Informationsaustausch

Dargestellte Cyberbedrohungen:

k.A.

Hauptakteure:

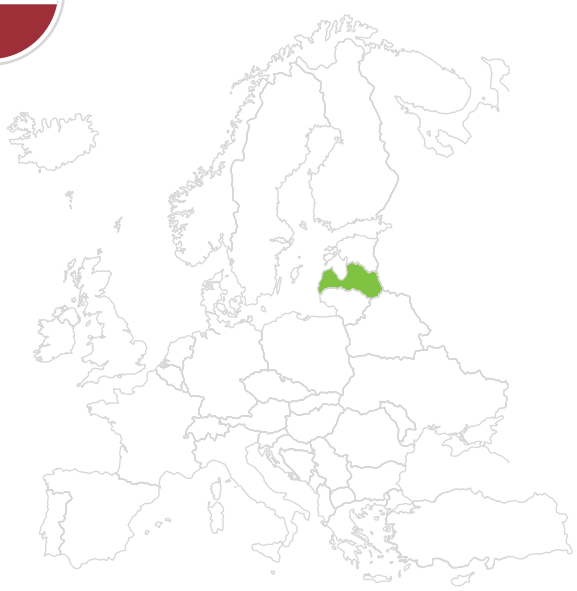
öffentlich

- National Cyber Security Council
- Operational and Technical Cyber Security Coordination Group
- Computer Emergency Response Team (CERT)

militärisch

k.A.

Lettland



Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2014
Herausgeber: k.A.
Zeitrahmen: 2014-2018
Kernziele:

- Förderung von nationalen und internationalen Kooperationen
- Aufklärung der Öffentlichkeit, staatlicher Institutionen und Privatunternehmen über Auswirkungen eigener Aktivitäten und Cyberbedrohungen
- vereinfachter Zugang zu Informations- und Kommunikations-technologien für alle Bürger
- Wahrung der Rechte und Grundfreiheiten einzelner Privatpersonen

Dargestellte Cyberbedrohungen:
k.A.
Hauptakteure:
öffentlich

- Nationaler Sicherheitsrat für Information und Technologie
- Ministry of Foreign Affairs (MFA)
- Financial and Capital Market Commission (FCMC)
- Ministry of the Interior (MoI)
- IT Computer Emergency Response Team (IT CERT.LV)
- Ministry of Education and Science (MoES)
- Safer Internet Centre of Latvia (Net.Safe)
- Constitution Protection Bureau (CPB)
- Ministry of Justice (MoJ) and Data State Inspectorate (DSI)

militärisch

- Streitkräfte (NAF) und Cyber Abwehreinheit (CDU)
- Ministry of Defence (MOD)

Litauen

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2011
Herausgeber: Regierung der Republik Litauen
Zeitrahmen: 2011-2019
Kernziele:

- Sicherheit staatlicher Informationsressourcen
- verbesserte Überwachung elektronischer Informationssysteme
- Ausbau des Rechtssystems
- Sicherung kritischer Infrastrukturen
- Förderung internationaler Zusammenarbeit
- Aufklärung und Sensibilisierung der Bevölkerung im Umgang mit Daten

Dargestellte Cyberbedrohungen:
k.A.
Hauptakteure:
öffentlich

- Computer Emergency Response Team (CERT.LT)

militärisch
k.A.

Luxemburg

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2018
Herausgeber: Government Council
Zeitrahmen: 2018-2020
Kernziele:

- Stärkung des öffentlichen Vertrauens in der digitalen Umwelt
- Sicherung digitaler Infrastruktur
- Förderung der Wirtschaft

Dargestellte Cyberbedrohungen:

- Ransomwares, DDOS, Brickerbot, BlackMail
- Spionage, Sabotage, Cyberkriminalität, Datendiebstahl
- Bedrohung von Geschäftsprozessen in Unternehmen

Hauptakteure:
öffentlich

- Cybersecurity Board (CSB)
- High Commissioner for National Protection (HCPN)
- State's Information Technology Centre (CTIE)
- Governmental Computer Emergency Response Centre (GOVCERT)
- National Agency for the Security of Information Systems (ANSSI)
- Ministry of Defence
- Ministry of State, Media and Communication Unit
- State Intelligence Services
- Ministry of Economy
- National Centre for Cybersecurity Skills (C3)
- Coordination and Post-Incident Action Unit (CIRCL)
- Ministry of Foreign and European Affairs (MAEE)

militärisch

- Luxembourg Army

Montenegro

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2017
Herausgeber: Ministry of Public Administration
Zeitrahmen: 2018-2021
Kernziele:

- Ausbau der Cyberverteidigungsfähigkeit
- Zentralisierung von Cyber-Know-how und Ressourcen
- Sicherung kritischer Infrastrukturen
- Stärkung von interinstitutioneller Zusammenarbeit auf regionaler und nationaler Ebene
- Ausbau öffentlich-privater Partnerschaften
- Aufklärung und Sensibilisierung der Bevölkerung

Dargestellte Cyberbedrohungen:

- Cyberangriffe, Cyberwarfare
- Hacking, Spionage, Sabotage
- Angriffe fremder Regierungen, extremistischer und radikaler Gruppen
- Cyberterrorismus, Cyberkriminalität
- menschliches Fehlverhalten und Naturkatastrophen

Hauptakteure:
öffentlich

- Ministry of Public Administration within which the national CIRT operates
- National Security Agency
- Ministry of Defence / Army of Montenegro
- Ministry of Interior / Police Administration
- Ministry of Justice
- Ministry of Education
- Directorate for Protection of Confidential Data

militärisch

k.A.

Niederlande

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2018
Herausgeber: National Cyber Security Agenda, A cyber secure Netherlands
Zeitrahmen: k.A.
Kernziele:

- Aufbau einer belastbaren und zuverlässigen digitalen Domäne
- Förderung einer starken öffentlich-privaten Partnerschaft
- Schutz vitaler Interessen
- Widerstandsfähigkeit gegen Cyberangriffe
- Bekämpfung von Cyberkriminalität
- Entwicklung sicherer IKT-Produkte
- Förderung von Cyberkenntnissen und -fähigkeiten
- Bildung von nationalen und internationalen Koalitionen

Dargestellte Cyberbedrohungen:

- Daten- und Identitätsdiebstahl
- Cyberspionage
- Botnets, Ransomware
- Cybercrime-as-a-Service

Hauptakteure:
öffentlich

- Joint Sigint Cyber Unit (JSCU)
- National Cyber Security Centre (NCSC)
- Security Operations Centre (SOC)
- Digital Trust Centre (DTC)
- Computer Emergency Response team (CERT)

militärisch

- k.A.

Norwegen

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2017
Herausgeber: The Ministry of Government Administration, Reform and Church Affairs
Zeitrahmen: k.A.
Kernziele:

- Abwehr von Bedrohungen durch ein verbessertes Situationsverständnis
- schnelle Reaktionsfähigkeit in Ernstfällen
- Entwicklung robuster IKT-Infrastrukturen
- Förderung von Kompetenzen und Fähigkeiten
- Gewährleistung der Schutzfähigkeit von Informationssystemen
- Ausbau von Bildungs- und Forschungsprogrammen zur Aufklärung

Dargestellte Cyberbedrohungen:

- Cyberspionage, Cybersabotage, Cyberterrorismus
- Daten- und Identitätsdiebstahl
- illoyale Mitarbeiter

Hauptakteure:
öffentlich

- Die Norwegische Nationale Sicherheitsbehörde (NSM)
- Computer Emergency Response Team (NorCERT)
- Die norwegische Post- und Telekommunikationsbehörde (PT)
- Das norwegische Zentrum für Informationssicherheit (NorSIS)
- Norwegische Direktion für Bevölkerungsschutz (DSB)
- Norwegischer Nachrichtendienst (NIS)
- Norwegischer Polizei-Sicherheitsdienst (PST)
- Die norwegische Datenschutzbehörde (DT)

militärisch

- k.A.

Österreich

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

In einer Reihe mit internationalem Terrorismus, Massenvernichtungswaffen, nationalen und internationalen Konflikten, Ressourcenknappheit, organisierter Kriminalität, Migration und Wirtschaftskrisen eingestuft.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2013
Herausgeber: Bundeskanzleramt
Zeitrahmen: k.A.
Kernziele:

- Schaffung eines sicheren Cyberraums für den Austausch von Daten
- Ausbau einer widerstandsfähigen Infrastruktur gegen Cyberbedrohungen
- Sensibilisierungsmaßnahmen und Förderung neuer Initiativen im nationalen Cyber-Sicherheits-Dialog
- Ausbau notwendiger IKT-Infrastrukturen
- Ausbau eines stärkeren Rechtsrahmens zur Vereinfachung internationaler Strafverfolgungen
- Schutz von Interessen auf nationaler und kommunaler Ebene
- Förderung von öffentlich-privaten Kooperationen
- Schutz der Identität und Privatsphäre von Bürgern

Dargestellte Cyberbedrohungen:

- Identitätsbetrug
- Missbrauch des Internets für extremistische Zwecke

Hauptakteure:
öffentlich

- Government Computer Emergency Response Team (GovCERT.at)
- Lenkungsgruppe Cybersicherheit
- Cyber Crime Competence Center (C4)

militärisch

- Military Cyber Emergency Readiness Team (MilCERT)
- Bundesministerium für Landesverteidigung (BMLV)

Polen

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

Werden neben Umweltkatastrophen, Angriffen auf kritische Infrastrukturen und Terrorismus genannt.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2017
Herausgeber: Ministry of Administration and Digitization, Internal Security Agency
Zeitrahmen: 2017-2020
Kernziele:

- Schutz des Informationsaustausches zwischen Nutzern des polnischen Internets
- Schaffung eines rechtlich und organisatorischen Rechtsrahmens
- Entwicklung, Verwaltung, Koordinierung und Sicherung des Cyberraums
- Schutz kritischer Infrastrukturen

Dargestellte Cyberbedrohungen:
k.A.
Hauptakteure:
öffentlich

- Governmental Computer Security Incident Response Team (CERT.GOV.PL)

militärisch

- Armed Forces and Departmental Centre for Security Management of ICT Networks and Services

Portugal

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2015
Herausgeber: Premierminister
Zeitrahmen: k.A.
Kernziele:

- Wahrung der Grundrechte und der Meinungsfreiheit
- Schutz der Bürger, deren Privatsphäre und persönlicher Daten
- Ausbau des Cyberraums und kritischer Infrastrukturen
- Sensibilisierung der Gesellschaft
- freie, sichere und effiziente Nutzung des Cyberraums für alle Schichten der Gesellschaft

Dargestellte Cyberbedrohungen:

- organisierte Kriminalität
- Daten- und Identitätsdiebstahl
- ideologisch motivierte Angriffe
- Cyberspionage, Cybersabotage
- Bankenbetrug

Hauptakteure:
öffentlich

- National Centre for Cybersecurity (CNCS)
- Cyber Defence Centre (CCD)
- Computer Security Incident Response Team (CSIRT)
- Cyberspace Crisis Management Office

militärisch

k.A.

Rumänien

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2013
Herausgeber: Premierminister
Zeitrahmen: k.A.
Kernziele:

- Anpassung von regulatorischen und institutionellen Rechtsrahmen
- Gewährleistung eines sicheren und zuverlässigen Cyberraums und einer entsprechenden Infrastruktur
- Förderung von nationalen und internationalen Kooperationen
- Sensibilisierung der Bevölkerung, durch Entwicklung einer Sicherheitskultur

Dargestellte Cyberbedrohungen:

- Bedrohung kritischer Infrastrukturen aus dem Cyberraum
- Cyberterrorismus, Cyberkrieg, Cyberkriminalität, Cyberspionage
- Angriffe staatlicher und nicht staatlicher Akteure
- Zugriffe und Angriffe auf Cyberinfrastrukturen
- Diebstahl, Löschungen, Beschädigungen von Daten
- Belästigung, Erpressung, Vermögensschädigungen

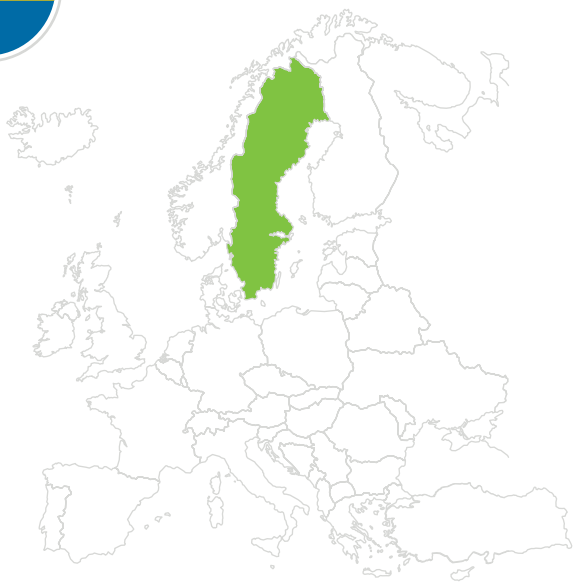
Hauptakteure:
öffentlich

- Supreme Council of National Defense
- National Cyber Security System (NSCC)
- Cyber Security Operative Council (COSC)
- Computer Emergency Response team (CERT-RO)

militärisch

k.A.

Schweden



Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2017
Herausgeber: Justizministerium
Zeitrahmen: k.A.
Kernziele:

- Cybersicherheitsstrategie zur Abwehr gegen Cyberangriffe
- Stärkung von IKT-Infrastrukturen
- Verbesserung und Verwaltung von Netzwerken, Produkten und der Systemsicherheit
- Verbesserung von Fähigkeiten, Technologien und Fachwissen
- internationale Kooperationen zur Abwehr von Cyberkriminalität

Dargestellte Cyberbedrohungen:
k.A.
Hauptakteure:
öffentlich
k.A.
militärisch
k.A.

Slowakei

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

Werden neben internationalem Terrorismus und Massenvernichtungswaffen genannt.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2015
Herausgeber: Premierminister
Zeitrahmen: 2015-2020
Kernziele:

- national geschützter und offener Cyberraum
- Förderung von Vertrauen in der Bevölkerung
- Absicherung und Entwicklung kritischer Infrastrukturen
- innerstaatliche Programme fördern den Austausch zwischen dem privaten und dem akademischen Sektor
- Ausbau internationaler Kooperationen zum Schutz grundlegender Menschenrechte und Grundfreiheiten

Dargestellte Cyberbedrohungen:
k.A.
Hauptakteure:
öffentlich

- National Computer Emergency Response Team (CERT XY)
- Government Computer Emergency Response Team (government CERT)
- Ministry of the Interior
- Committee for Cyber Security
- Central State Authorities

militärisch
k.A.

Slowenien

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2016
Herausgeber: k.A.
Zeitrahmen: 2016-2020
Kernziele:

- Aufbau eines umfassenden Systems zur Cyberabwehr
- Ausbau einer ausnahmslos zuverlässigen Infrastruktur, für staatliche und private Einrichtungen
- Festlegung von Regulierungen
- Sicherheit der Bürger und der Wirtschaft
- Betriebsgewährleistung kritischer Infrastrukturen
- Bekämpfung von sowie Verteidigung gegen Cyberkriminalität
- Förderung von internationalen Kooperationen

Dargestellte Cyberbedrohungen:

- menschliche Fehler
- digitale Piraterie, Missbrauch, Erpressung, Betrug
- Verbreitung von Kinderpornographie
- Cyberspionage

Hauptakteure:

öffentlich

- Slovenia National Computer Emergency Response Team (SI-CERT)
- Public Administration Computer Emergency Response Team (SIGOV-CERT)
- Slowenische Nachrichten- und Sicherheitsagentur (SOVA)
- Agentur für elektronische Kommunikationsnetze und -dienste der Republik Slowenien (AKOS)
- IT Directorate at the Ministry of Public Administration
- Centre for Computer Investigations with the capacities to combat cybercrime

militärisch

- Ministry of Defence

Spanien

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2013
Herausgeber: Premierminister
Zeitrahmen: k.A.
Kernziele:

- sichere Nutzung von Informations- und Telekommunikationssystemen
- Förderung der Widerstandsfähigkeit von Informationstechnologien
- Präventionsverbesserungen und Koordinationsfähigkeit
- Sensibilisierung der Gesellschaft
- Ausbau von Fähigkeiten, Technologien
- Stärkung internationaler Kooperationen

Dargestellte Cyberbedrohungen:

- Hacking, Sabotage, Spionage
- terroristische Organisationen
- technisch verursacht Naturphänomene
- Cyberkriminalität

Hauptakteure:

öffentlich

- Government Computer Emergency Response Team (Government CERT)
- Computer Emergency Response Team for Security and Industry (CERT)
- National Cryptology Centre (CCN-CERT)
- Spanish Public Administration System (SARA network)
- Nationaler Sicherheitsrat

militärisch

k.A.

Tschechien

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

In einer Reihe mit menschlichem Versagen und Umweltkatastrophen angeführt.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2015
Herausgeber: Nationales Cybersicherheitszentrum der nationalen Sicherheitsbehörden
Zeitrahmen: 2015-2020
Kernziele:

- Ausbau von relevanten Infrastrukturen
- Zusammenarbeit nationaler und internationaler Behörden
- Schutzgewährleistung von national relevanten Informationsnetzwerken und Infrastrukturen
- Förderung von Kooperationen im öffentlich-privaten Sektor
- Stärkung des Verbrauchervertrauens Innerhalb der Bevölkerung
- Aufklärung und Sensibilisierung durch öffentliche Bildung
- Stärkung von Forschung und Entwicklung
- Verbesserung der nationalen Strafverfolgung

Dargestellte Cyberbedrohungen:

- Cyberspionage
- organisierte Kriminalität
- Verbreitung falscher Informationen gegen staatliche Institutionen
- Cyberterrorismus
- Malware, Datendiebstahl

Hauptakteure:
öffentlich

- National Cyber Security Centre (NCSC)
- Computer Emergency Response Team (CERT.cz)
- National Security Authority (NSA)

militärisch

k.A.

Türkei

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2015
Herausgeber: Ministry of Transport Maritime Affairs and Communications
Zeitrahmen: 2016-2019
Kernziele:

- Gewährleistung eines sicheren Datentransfers im Cyberraum
- Sicherheitsmaßnahmen zur Begrenzung von Cyberangriffen
- Notfallpläne zur Wiederherstellung von Systemen
- Aufrechterhaltung des Datenschutzes und schnelle Strafverfolgung
- Entwicklung kritischer Technologien auf lokaler Ebene

Dargestellte Cyberbedrohungen:

- Cyberkriminalität, Identitäts- und Datendiebstahl, Terrorismus
- Phishing, Warfare, Malware, Botnets, Netzwerkangriffe
- Störung der öffentlichen Ordnung, anti-staatliche Propaganda

Hauptakteure:
öffentlich

- Ministerium für Verkehr, Maritime Angelegenheiten und Kommunikation (MoTMC)
- Ministerium für auswärtige Angelegenheiten (MoFA)
- Innenministerium
- Untersekretariat für öffentliche Ordnung und Sicherheit (UoPOS)
- Nationale Nachrichtenorganisation (NIO)
- Behörde für Informations- und Kommunikationstechnologien (ICTA)
- Wissenschaftlicher und Technologischer Forschungsrat (STRCoT)
- Ratsvorsitz für Telekommunikation und Kommunikation (PoTC)

militärisch

- Generalstab der türkischen Streitkräfte
- Ministerium für Nationale Verteidigung (MoND)

Ungarn

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2013
Herausgeber: Premierminister
Zeitrahmen: k.A.
Kernziele:

- Schaffung eines öffentlichen Cyberbewusstseins
- Förderung öffentlicher Institutionen
- Ausbau eines sicheren Cyberraums
- Wahrung der nationalen Sicherheit
- Ausbau effizienter Cyberfähigkeiten
- Schutzgewährleistung des Cyberraums und nationaler Datenbestände
- Qualitätssicherung von IT- und Kommunikationsprodukten und -diensten
- Qualitätssicherung von Bildung, Forschung und Entwicklung
- Qualitätssicherung des Cyberraums für Kinder und zukünftige Generationen

Dargestellte Cyberbedrohungen:
k.A.
Hauptakteure:
öffentlich

- National Cyber Security Coordination Council
- Computer Emergency Response Team (EU CERT Mitglied)
- Sectoral Incident Response Centre

militärisch
k.A.

China

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2016
Herausgeber: 12. Nationaler Volkskongress
Zeitrahmen: k.A.
Kernziele:

- Wahrung der Verfassung und ihrer grundlegenden Rechte
- Aufrechterhaltung von nationalen Interessen, wie der öffentlichen Sicherheit und des Sozialwesens
- Währung der Cybersouveränität

Dargestellte Cyberbedrohungen:

- Identitätsdiebstahl und Verlust persönlicher Daten
- Computerviren, Netzwerkangriffe, Malware
- Datenmanipulation und -fremdverwendung
- illegaler Datenhandel und Übermittlung rechtlich geschützter Daten
- illegaler Handel mit Hardware für Cyberkriminalität

Hauptakteure:
k.A.

Russland

Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

k.A.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2014
Herausgeber: Russische Regierung
Zeitrahmen: 2014-2020
Kernziele:

- Entwicklung von zuverlässigen und nachhaltigen kritischen Infrastrukturen, sowohl in Friedens- wie in Kriegszeiten
- Förderung der nationalen und internationalen Politik in Bezug auf Cybersicherheit und Verteidigung

Dargestellte Cyberbedrohungen:

- Informations- und Kommunikationstechnologien (Informationswaffen)
- Nutzung von Informationstechnologien für terroristische Zwecke
- Cyberkriminalität
- Störung der öffentlichen Ordnung durch Informationstechnologien
- anti-staatliche Propaganda

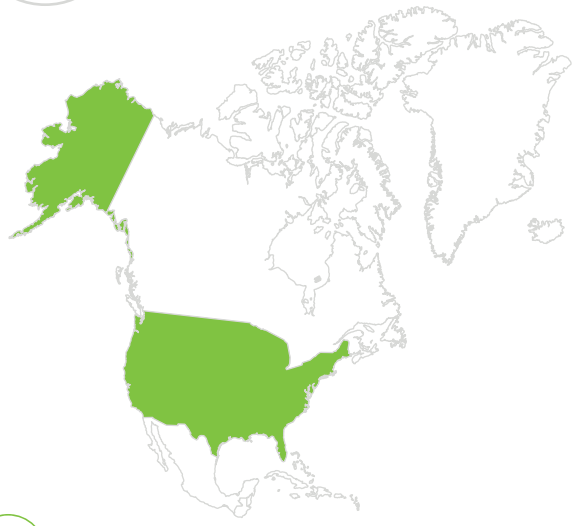
Hauptakteure:
öffentlich

- Russischer Sicherheitsrat
- Ministerium für Auswärtige Angelegenheiten
- Ministerium für Kommunikation
- Justizministerium

militärisch

- Verteidigungsministerium

Vereinigte Staaten von Amerika (USA)



Einordnung von Cyberbedrohungen gegenüber anderen nationalen Gefahren (NSS)

Genannt neben Angriffen auf das Heimatland oder kritischen Infrastrukturen, Bedrohung von Staatsbürgern im Ausland und von Verbündeten, globalen Wirtschaftskrisen und Infektionskrankheiten, Klimawandel und Massenvernichtungswaffen.

Nationale Cybersicherheitsstrategie (NCSS)

Veröffentlichung: 2015
Herausgeber: Verteidigungsministerium
Zeitrahmen: 2015-2021
Kernziele:

- Gewährleistung der Verteidigungsfähigkeit gegen Cyberangriffe
- Schaffung und Aufbau von Cyberstreitkräften
- Durchführung reaktionsschneller Cyberraum Operationen
- Sicherung der Verteidigungsinformationsnetze zum Schutz lebenswichtiger Interessen der USA
- Förderung internationaler Allianzen und Partnerschaften
- internationale Stabilität und Sicherheit

Dargestellte Cyberbedrohungen:

- Cyberangriffe auf die Netzwerke des Verteidigungsministeriums
- Datendiebstahl und -zerstörung
- ideologisch motivierte Propaganda
- Cyberkriminalität insbesondere gegenüber Finanzinstitutionen

Hauptakteure:
öffentlich

- Office of Cybersecurity and Communications (CS&C)
- National Cybersecurity and Communications Integration Center (NCCIC)

militärisch

- United States Cyber Command (USCYBERCOM)
- Cyber Mission Force (CMF) of the Department of Defense (DoD)
- Military Departments Computer Emergency Response Teams (CERT)

Europäische Union (EU)

Einordnung von Cyberbedrohungen gegenüber anderen Gefahren

Macht keine direkten Vergleiche. In einer Untersuchung der ENISA werden Cyberbedrohungen gegen die EU mit natürlichen Umweltkatastrophen, zwischenstaatlichen Konflikten, Wirtschaftskrisen, ABC-Angriffen verglichen.

Cybersicherheitsstrategie

Veröffentlichung: 2013
Herausgeber: Europäische Kommission
Zeitrahmen: k.A.
Kernziele:

- Ausbau der Cyberverteidigungsfähigkeiten aller Mitgliedsstaaten
- gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP)
- Entwicklung von technischen Ressourcen
- Reduzierung von Cyberkriminalität durch internationale Zusammenarbeit

Dargestellte Cyberbedrohungen:

- Malware, Ransomware, Denial-of-Service, Exploit-Kits
- Phishing, Spam, Botnets, Cyberspionage, Informationslecks
- physische Manipulationen, Insider Bedrohungen
- Datenschutzverletzungen, Identitätsdiebstahl

Hauptakteure:

- Europäische Agentur für Netz- und Informationssicherheit (ENISA)
- European Cybercrime Centre (EC3)
- Computer Emergency Response Team (CERT-EU)
- Netzwerk von zuständigen Behörden
- Europäische Verteidigungsagentur (EDA)
- Europäisches Sicherheits- und Verteidigungskolleg (ESVK)
- Europäische Gruppe zur Bekämpfung der Cyberkriminalität (ECTEG)

Organisation des Nordatlantikvertrags (NATO)

Einordnung von Cyberbedrohungen gegenüber anderen Gefahren

k.A.

Cybersicherheitsstrategie

Veröffentlichung: 2016
Herausgeber: NATO
Zeitrahmen: k.A.
Kernziele:

- kollektive Verteidigung durch verbesserten Informationsaustausch und gegenseitige Unterstützung der Bündnispartner
- Wahrung gleicher Interessen und international geltenden Rechts im Cyberraum
- Intensivierung von Kooperationen mit der Europäischen Union und der Industrie

Dargestellte Cyberbedrohungen:

k.A.

Hauptakteure:

- NATO Computer Incident Response Capability (NCIRC)
- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)
- NATO Communications and Information Systems School (NCISS)
- Cyber Defence Committee
- NATO Industry Cyber Partnership (NICP)

Ansprechpartner

Katrin Rohmann
Partner | Government &
Public Services Industry Leader
Tel: +49 (0)30 2546 8127
krohmann@deloitte.de

Peter J. Wirnsperger
Partner | Cyber Risk Leader
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Autoren

Knut Schönfelder
Senior Manager | Cyber Risk
Tel: +49 (0)40 32080 4447
kschoenfelder@deloitte.de

André Roosen
Manager | Cyber Risk
Tel: +49 (0)30 2546 8327
aroosen@deloitte.de

Kaan Sahin
Consultant | Cyber Risk
Tel: +49 (0)30 2546 85245
ksahin@deloitte.de

Deloitte.

Stand 09/2018