CSS CYBER DEFENSE

Nationale Cybersicherheits-strategien im Vergleich – Herausforderungen für die Schweiz

Zürich, März 2019

Center for Security Studies (CSS), ETH Zürich

CSS ETH Zurich

ETH zürich

Autoren: Marie Baezner, Sean Cordey

Zusätzliche Recherche: Matteo Bonfanti, Robert Dewar, Jasper Frei und Fabien Merz
Layout: Miriam Dahinden-Ganzoni

© 2019 Center for Security Studies (CSS), ETH Zürich
Kontakt:
Center for Security Studies
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch
www.css.ethz.ch

Auftraggeber: Informatiksteuerungsorgan des Bundes ISB

Studie verfasst von: Center for Security Studies (CSS), ETH Zürich

ETH-CSS Projekt- und Qualitätsmanagement: Myriam Dunn Cavelty, stv. Leiterin CSS
und Andreas Wenger, Direktor des CSS.

Disclaimer: Die in dieser Studie wiedergegebenen Auffassungen stellen ausschliessliche
die Ansichten der betreffenden Autorinnen und Autoren dar.

Bitte zitieren als: Baezner, Marie; Cordey, Sean (2019): Nationale Cybersicherheitsstrategien
im Vergleich – Herausforderungen für die Schweiz
March 2019, Center for Security Studies (CSS), ETH Zürich.

Inhalt

Zusammenfassung

Die digitale Transformation zeichnet sich als eine der grossen Herausforderungen der kommenden Jahre ab. Sie bietet nicht nur vielfältige Vorteile, sondern birgt auch neuartige Risiken und schafft neue Verwundbarkeiten. Eine Mehrheit von Staaten hat begonnen, diesen unter dem Stichwort der «Cybersicherheit» durch die Entwicklung nationaler Strategien zu begegnen. Die Schweiz hat 2018 ihre zweite «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken» (NCS) veröffentlicht, in der sie wichtige Herausforderungen identifiziert, Verantwortlichkeiten umreisst und künftige Massnahmen skizziert. Die vorliegende Studie vergleicht die Cybersicherheitsstrategien Deutschlands, Finnlands, Frankreichs, Israels, Italiens und der Niederlande, um den schweizerischen Ansatz in einen breiteren internationalen Zusammenhang zu stellen und in einem Vergleich die wichtigsten zukünftigen Herausforderungen zu eruieren.

Im Zentrum stehen die Identifikation von Schlüsselstrategien, die Beschreibung von Hauptakteuren und ihren Aufgabenfeldern (insbesondere die Aufgabenverteilung zwischen zivilen und militärischen Behörden in den Bereichen «Sicherheit», «Verteidigung» und «Strafverfolgung») und die Identifikation von generellen Herausforderungen bei der Organisation nationaler Cybersicherheitspolitiken.

Die Cybersicherheitsstrategien weisen viele konzeptionelle Gemeinsamkeiten auf. Ihnen sind insbesondere sechs zentrale Aspekte gemeinsam: der holistische Ansatz, welcher sowohl nationale Sicherheit als auch sozioökonomische Anliegen umfasst; Verbindungen zu umfassenderen nationalen Sicherheitsstrategien; der zentrale Fokus auf die Entwicklung defensiver Cyberfähigkeiten; der hohe Stellenwert der internationalen Kooperation; die Betonung der notwendigen Zusammenarbeit mit dem Privatsektor und schliesslich die Notwendigkeit umfassenderer Sensibilisierung, Bildung und Information.

Die wichtigsten Unterschiede zwischen den untersuchten Ländern sind, wo Cybersicherheit im Rahmen staatlicher Strukturen angesiedelt wird und wer welche Verantwortlichkeiten trägt. Dies betrifft das Ausmass der Zentralisierung, die Beziehung zwischen zivilen und militärischen Kräften und die Aufgaben von Nachrichtendiensten und Stellen der Strafverfolgung. Die Gründe für die Unterschiede fussen grossmehrheitlich auf der politischen Kultur und der Organisation der politischen Systeme.

Angesichts eines globalen Bedrohungsumfelds stehen vergleichbare Staaten bei der Entwicklung, Umsetzung oder Aufrechterhaltung ihrer Strategien vergleichbaren Herausforderungen gegenüber. Wir haben acht solche Herausforderungen identifiziert:

- die (vertikale) Integration nationaler Cybersicherheit in den Rahmen der nationalen Sicherheit und/oder einer Gesamtstrategie, um nationale Ressourcen möglichst effizient zu steuern;
- die (horizontale) Koordination verschiedener Stellen, die sich um Cybersicherheit kümmern, wobei insbesondere die richtige Mischung zwischen Zentralisierung und Nutzung bestehender Kompetenzen zu finden ist;
- die Förderung internationaler Zusammenarbeit und die Ausbildung internationaler Verhaltensnormen in einem Umfeld, in dem sich geopolitische Verwerfungen intensiviert haben;
- die Schaffung solider und belastbarer Strukturen für das Krisenmanagement, einschliesslich effizienter Krisenkommunikation, sowie die Entwicklung einer guten Reaktionsfähigkeit auf schwerwiegende Vorfälle, die diesen Kommunikationsaspekt berücksichtigt;
- ein adäquates Lagebild und eine präzise Bedrohungsanalyse, die überzogenen Beurteilungen von Cyberbedrohungen gegenüber immun sind – trotz der Schwierigkeit, zuverlässige Daten zu sammeln;
- der Aufbau von Kapazitäten und die Ausgestaltung zukünftiger Bildungsangebote, um dem Personalmangel in der Cybersicherheit zu begegnen;
- ein Kooperationsrahmen mit der Privatwirtschaft, der Innovation nicht hemmt, aber nationale Sicherheit fördert sowie
- die Harmonisierung der Gesetzgebung und effiziente Strategien zur Bekämpfung von Cyberkriminalität.

Auch die Schweiz ist ebendiesen Herausforderungen ausgesetzt. Ein kleiner, aber wohlhabender Staat wie die Schweiz sollte gewährleisten, dass er ausreichend Mittel in die Cybersicherheit investiert, ohne die Reichweite und Rolle des Staats zu sehr auszudehnen, wenn er seine Zukunft in der digitalen Welt sichern möchte. Hierfür ist einerseits erforderlich, dass alle Teile der Regierung auf dasselbe übergeordnete Ziel hinarbeiten. Andererseits bietet sich eine besondere Berücksichtigung des Kapazitätsaufbaus und der Ausgestaltung von Bildungsangeboten als wohl fruchtbarster Ansatz an.

Einleitung

Länder in aller Welt sind bemüht, digitale Transformationsprozesse so zu gestalten, dass sie die Chancen dieses technologisch gesteuerten Wandels für ihre Gesellschaften jeweils optimal nutzen können. Allerdings beinhaltet die Verbreitung digitaler Technologien auch Risiken. Ihr technischer Unterbau ist aufgrund von technischen, wirtschaftlichen und politischen Faktoren unsicher und für eine Nutzung für kriminelle oder politische Zwecke anfällig. In Anbetracht der wachsenden Zahl interessanter Ziele und der aufgrund von starker Nachfrage immer ausgereifteren Fertigkeiten und Kompetenzen sind spektakuläre, kriminell motivierte Cyberverbrechen und die strategische Nutzung des Cyberspace zur alltäglichen Realität geworden.

Es ist daher unerlässlich, sich den Herausforderungen der Cybersicherheit zu stellen, wenn die digitale Transformation erfolgreich verlaufen soll. Die meisten Staaten überarbeiten folglich ihre Cybersicherheitsstrategien, um besser auf die Risiken vorbereitet zu sein, die sich in einem immer enger vernetzten und zugleich immer stärker politisierten und militarisierten Umfeld abzeichnen. Die zu bewältigenden Herausforderungen sind nicht ausschliesslich technischer Natur: Gross angelegte wirtschaftliche oder politische Cyberspionage, strategische Beeinflussungskampagnen und die Gefährdung kritischer Infrastrukturen von nationaler Bedeutung sind alles sicherheitspolitisch relevante Themen.

Die genaue Rolle des Staats und seiner Verwaltung in der Cybersicherheit muss allerdings in einem politischen Prozess bestimmt und sorgfältig definiert werden. Kritische Infrastrukturen befinden sich hauptsächlich in den Händen privater Akteure. Der Cyberspace kann als Allgemeingut bezeichnet werden, dessen Dynamik oder Nutzung von einem ganzen Ökosystem staatlicher und nichtstaatlicher Akteure geformt wird. Es gibt keine einzelne Lösung, die alle Probleme der Cybersicherheit beheben kann: In Anbetracht der vielfältigen Risiken, die digitale Technologien in sich bergen, sind die Festlegung von Verantwortlichkeiten und die Planung der Ressourcenzuteilung eine anspruchsvolle und komplexe Aufgabe der Politik.

Die Schweiz hat 2018 ihre zweite «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken» (NCS) veröffentlicht, in der die wichtigsten Herausforderungen und Verantwortlichkeiten auf diesem Gebiet dargestellt sind. Die vorliegende Studie vergleicht Politiken, Strukturen und Herausforderungen auf dem Gebiet der Cybersicherheit in sechs Ländern, um diese Bemühungen in Kontext zu setzen und zu validieren:[1]

- Finnland,
- Frankreich,
- Deutschland,
- Israel,
- Italien und
- die Niederlande.

Dieser Vergleich konzentriert sich insbesondere auf:

a die Art und den Inhalt wichtiger Strategien,

b die Rolle und Verantwortlichkeiten der wichtigsten Akteure und Stellen (Strafverfolgung, Militär, Nachrichtendienste und zivile Stellen) sowie

c die Herausforderungen, denen diese Staaten hinsichtlich der Cybersicherheit ausgesetzt sind.

Diese Studie baut auf primären Quellen wie öffentlichen nationalen Cybersicherheits- und Cyberabwehrstrategien sowie auf sekundären Quellen wie Medienartikeln und wissenschaftlicher Forschung auf. Alle der herangezogenen Dokumente sind öffentlich verfügbar. Es ist wichtig, den Kontext und die Ziele dieser Dokumente zu verstehen, die bestimmten Einschränkungen unterliegen:

- Erstens sagen nationale Cybersicherheitsstrategien wenig über die tatsächliche Bereitschaft eines Staats oder seiner tatsächlichen Aktivitäten aus, insbesondere in den Bereichen der nationalen Sicherheit und Verteidigung. Strategien sind vor allem Absichtserklärungen, die für ein vielfältiges einheimisch-internes und international-externes Publikum die künftige Richtung der nationalen Cybersicherheitsagenda vorgeben und signalisieren sollen. Deutschland und Frankreich haben sektorspezifische Umsetzungspläne (d.h. für die IT in der Verwaltung und für den Privatsektor), während der niederländische Umsetzungsplan noch im Schreibprozess ist. Im Fall vom Israel liegt kein Umsetzungsplan vor.

1 Die Auswahl dieser Länder erfolgte so, dass genügend unterschiedliche politische Systeme in der Analyse vertreten waren, es aber auch eine geographische Nähe zu der Schweiz gab. Israel wurde hinzugefügt, weil die Herangehensweise des Landes häufig als interessant vermerkt wird. Zudem musste sichergestellt sein, dass genügend öffentliches Material vorhanden war.

- Zweitens veröffentlichen Staaten oft nicht die genaue Höhe ihrer Ausgaben für die Cybersicherheit. Etwaigen Bekanntmachungen zum Umfang von «Cybertruppen» usw. sollte eine gewisse Skepsis entgegengebracht werden. Die Medien melden gelegentlich Schätzungen nationaler Ausgaben für die Cybersicherheit, aber diese werden im Allgemeinen von nationalen Sicherheitsausgaben extrapoliert und bilden die tatsächlichen Ausgaben für Cybersicherheit der jeweiligen Staaten nicht präzise ab. Die aktuelle Risikowahrnehmung wird am unmittelbarsten vom Militär und von (Auslands-)Geheimdiensten beeinflusst; allerdings sind die Aktivitäten beider staatlichen Dienste naturgemäss geheim, was die Erfassung von Informationen zu Ausgaben und Praktiken in diesem Umfeld äusserst schwierig gestaltet. Auch mehrere grosse, auf die Überwachung von Militärausgaben spezialisierte Projekte sind mit diesen Schwierigkeiten konfrontiert und verzichenten auf Angaben zu den Ausgaben für Cybersicherheit (darunter das Stockholm International Peace Research Institute (SIPRI), der Global Cybersecurity Index der Internationalen Fernmeldeunion (ITU) und Jane's Defence Budgets).

- Drittens ist die Cybersicherheit ein Querschnittsthema. Staaten weisen hierfür folglich kein zentrales Budget aus, sondern verteilen es auf mehrere Haushaltsposten. Diese Fragmentierung sowie unterschiedliche Definitionen der Cybersicherheit erschweren eine Beurteilung staatlicher Ausgaben in diesem Umfeld, sogar für die Staaten selbst.

Diese Studie umfasst drei Teile. Der erste Teil vergleicht die Entwicklung der Cybersicherheit, die wichtigsten politischen Prinzipien und die organisatorischen Strukturen in den verschiedenen Staaten. Der zweite Teil beschreibt acht gemeinsame Herausforderungen. Der dritte Teil macht Schlussfolgerungen für die Schweiz.

Cybersicherheits-strategien im Vergleich

Die vorliegende Studie vergleicht Politiken, Strukturen und Herausforderungen auf dem Gebiet der Cybersicherheit in Finnland, Frankreich, Deutschland, Israel, Italien und den Niederlanden. Die wichtigsten Parameter sind in der folgenden Tabelle zu sammengefasst:

	Finnland	**Frankreich**	**Deutschland**	**Italien**	**Israel**	**Niederlande**
Jahr der ersten publizierten Strategie	2013	2011	2011	2013	2011	2012
Jahr der aktuellen Strategie	2013	2015	2016	2017 (Nationaler Plan)	2015	2018
Separate Strategie für Verteidigung	Nein	Ja	Nein	Nein, aber Militär ist im Nationalen Plan 2017 abgedeckt	Nein	Ja
Definition von Cybersicherheit	Ja	Ja (in der NCSS 2011)	Ja	Nein	Ja	Ja
Federführung	UTVA und Sicherheitsausschuss (zivil)	Premierminister (zivil)	Innenminister (zivil)	Präsident des Ministerrats (zivil)	Premierminister (zivil)	Justiz- und Sicherheitsminister (zivil)
Organisationsstruktur	Zentral auf strategischer, dezentral auf operativer Ebene	Zentral	Dezentral	Mischung aus zentral und dezentral	Zentral	Dezentral
Defensive Cyberkapazitäten	Ja	Ja	Ja	Ja	Ja	Ja
Offensive Cyberkapazitäten (in der Strategie genannt)	Nein	Nein	Nein	Nein	Nein	Ja
Internationale Kooperation	Ja	Ja	Ja	Ja	Ja	Ja
Kooperation mit der EU	Ja	Ja	Ja	Ja	Nein	Ja
Kooperation mit der NATO	Ja	Ja	Ja	Ja	Nein	Ja
Kooperation mit der OSZE	Ja	Ja	Ja	Ja	Nein	Ja
Zusammenarbeit mit der Privatwirtschaft	Ja	Ja	Ja	Ja	Ja	Ja
Sensibilisierung/Bildung/ Information zur Cybersicherheit	Ja	Ja	Ja	Ja	Ja	Ja

Jeder Staat hat seine eigene politische Geschichte, seine eigenen Institutionen und seine eigenen politischen Entscheidungsprozesse, die in der Auseinandersetzung mit neuen politischen Fragen wie der Cybersicherheit zu wichtigen operativen Unterschieden führen. Es ist jedoch offensichtlich, dass zwischen diesen Staaten viele konzeptionelle Ähnlichkeiten bestehen. Im Folgenden stellen wir sowohl die Ähnlichkeiten als auch die Unterschiede zwischen diesen Staaten heraus, um ein besseres Verständnis nationaler Cybersicherheitsstrategien und der gemeinsamen Herausforderungen an Staaten in dieser Domäne zu ermöglichen.

Wichtige Dokumente und ihre Entwicklung

Alle sechs Staaten haben im Lauf der letzten zehn Jahre nationale Cybersicherheitsstrategien erarbeitet. Diese Entwicklung bestätigt sowohl ihre zunehmende Sensibilisierung gegenüber Bedrohungen aus dem Cyberspace als auch ihre Entschlossenheit, ihre Netze und Infrastrukturen gegenüber diesen Bedrohungen besser zu schützen. Die aktuellen Strategien sind das Ergebnis einer allgemeinen Entwicklung, die stark von spezifischen Ereignissen im Cyberspace mit internationaler Reichweite geprägt ist:[2]

Von den frühen 1990er Jahren bis in die Mitte der 2000er Jahre konzentrierte sich die Cybersicherheitspolitik auf den Schutz kritischer Infrastrukturen und staatlicher Netze gegen Cyberattacken. Die Cyberattacken auf estländische Institutionen 2007 und der Krieg zwischen Russland und Georgien 2008, der neben Bodenkämpfen auch Störungen des gegnerischen Cyberraums beinhaltete, verdeutlichten, dass das Konzept der Cybersicherheit nicht auf rein technische Aspekte begrenzt werden konnte.

Im Anschluss an diese Ereignisse begannen Staaten, ihr Konzept der Cybersicherheit von der technischen auf die politische Domäne auszuweiten. 2010 entdeckte die Welt Stuxnet, eine Schadsoftware zur Beschädigung von Zentrifugen in einer iranischen Nuklearanlage. Dieses Ereignis rückte sowohl das Interesse von Staaten an der Durchführung von Cyberoperationen als auch ihre entsprechenden Kapazitäten ins Rampenlicht und beschleunigte die Erstellung von nationalen Cybersicherheitsstrategien.

Seit 2013 konzentrieren sich diese Strategien zunehmend auf den Aufbau von Kapazitäten. Die Cybersicherheitsstrategie der Europäischen Union (EU) aus dem Jahr 2013 und die EU-Richtlinie zur Netz- und Informationssicherheit aus dem Jahr 2016 verlangen von Mitgliedstaaten darüber hinaus die Entwicklung nationaler Cybersicherheitsstrategien.

Es zeichnen sich sechs gemeinsame Elemente ab:

- Erstens verfolgen Staaten einen holistischen Ansatz für die Cybersicherheit, der technische Kapazitäten ebenso umfasst wie Bildung, Information und Sensibilisierung.

- Zweitens knüpfen Cybersicherheitsstrategien an weiter gefasste nationale Sicherheitsstrategien an und/oder bilden Teil davon.

- Drittens betonen Strategien vor allem die Notwendigkeit, dass Staaten defensive Cyberkapazitäten entwickeln müssen. Nur einer der analysierten Staat (die Niederlande[3]) gibt explizit bekannt, dass er offensive Kapazitäten entwickelt, um Cyberattacken begegnen zu können. Dies bedeutet natürlich nicht, dass andere Staaten nicht auch die Entwicklung solcher Kapazitäten beabsichtigen oder bereits über sie verfügen.

- Viertens betonen alle Strategien die Bedeutung internationaler Kooperation im Rahmen regionaler und internationaler Organisationen, um die Zusammenarbeit bei der Cybersicherheit zu verbessern. Alle Staaten ausser Israel sind Mitglieder der Europäischen Union und alle ausser Finnland und Israel sind Mitglieder der NATO. Entsprechend nennen alle Staaten ausser Israel die NATO als wichtigsten Partner bei der internationalen Zusammenarbeit im Umfeld der Cybersicherheit. Dies gilt auch für Finnland, das als Mitglied der Partnerschaft für den Frieden mit der NATO zusammenarbeitet. Darüber hinaus wurde die OSZE in den Strategien aller Mitglieder (mit Ausnahme der Niederlande) ausdrücklich erwähnt. Die UNO wird nur in der französischen, finnischen und niederländischen Strategie explizit erwähnt.

- Fünftens stellen alle Strategien die Notwendigkeit der Zusammenarbeit mit dem Privatsektor heraus (da viele kritische Infrastrukturen und Informationsgüter in privater Hand sind). Die Niederlande und Italien haben sich für einen Ansatz einer speziellen öffentlich-privaten Partnerschaft für die Cybersicherheit entschieden und Deutschland für eine auf die Betreiber kritischer Infrastrukturen begrenzte öffentlich-private Partnerschaft, während die restlichen hier untersuchten Staaten Branchen finanziell unterstützen, die aktiv zur Cybersicherheit beitragen.

- Sechstens betonen alle Staaten die Wichtigkeit einer Sensibilisierung für Fragen der Cybersicherheit auf allen Ebenen der Gesellschaft sowie die Notwendigkeit besserer Bildung und Information.

Ausser diesen breit gefassten Gemeinsamkeiten gibt es auch mehrere beachtenswerte Unterschiede:

- Finnland und Italien haben für ihr Verteidigungsministerium und ihre Streitkräfte keine separaten Strategien erarbeitet, sondern subsumieren deren Rolle und Ziele unter der allgemeinen, nationalen Cybersicher-

2 Kadri Kaska, *National Cyber Security Organisation: The Netherlands* (Tallinn: CCDCOE, 2015), https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_NETHERLANDS_032015_0.pdf

3 Ministerium für Justiz und Sicherheit, *National Cyber Security Agenda: A cyber secure Netherlands* (Den Haag: Ministerium für Justiz und Sicherheit, April 2018), S. 23, https://www.ncsc.nl/english/current-topics/national-cyber-security-agenda.html

heitsstrategie. Diese Integration der Streitkräfte in die Cybersicherheitsstrategie ist höchstwahrscheinlich auf politische und historische Pfadabhängigkeiten zurückzuführen, insbesondere die traditionell kollaborative, holistische und einvernehmliche Gestaltung der Sicherheitspolitik in beiden Staaten.

- Frankreich hat für das Innenministerium[4] und Verteidigungsministerium[5] separate Strategien veröffentlicht, die diesen Ministerien präzise Ziele vorgeben. Diese zusätzlichen Strategien entstanden wahrscheinlich aufgrund der spezifischen Aufgaben dieser Ministerien sowie des Wunsches, ihre Rolle in der Cybersicherheit präziser abzugrenzen und ihren Wirtschaftspartnern, anderen Ministerien und internationalen Partnern gegenüber ihre verschiedenen Ausrichtungen zu signalisieren[6].

- Während manche Staaten ältere Cybersicherheitsstrategien durch neue ersetzen, nutzt Italien seinen nationalen Strategierahmen für die Cybersicherheit aus dem Jahr 2013[7] als zentrales Strategiedokument, das anhand von nationalen Plänen[8] jeweils neu ausgerichtet wird. Dadurch ergeben sich flexiblere politische Gestaltungsmöglichkeiten.

- Die Niederlande haben bereits ihre dritte nationale Cybersicherheitsstrategie veröffentlicht und eine Reihe komplementärer Cybersicherheitsstrategien zu spezifischen Themen erarbeitet, insbesondere die Internationale Cyberstrategie 2017[9] und die Cyberstrategie für die Verteidigung 2015[10] (zweite niederländische Strategie). Die Vielzahl der Strategien in diesem Umfeld ist auf interne politische Auseinandersetzungen sowie die Tatsache zurückzuführen, dass jedes Ministerium seine Kompetenzen sichern möchte.

- Hinsichtlich der Terminologie hebt sich Frankreich durch die Verwendung des Begriffs «digitale Sicherheit» in der Strategie 2015[11] von den anderen Staaten ab, da dieser Begriff breiter gefasst ist als «Cybersicherheit» und auch online geführte Propaganda- und Desinformationskampagnen umfasst. Diese Änderung wurde im Kontext der Terrorattacken von 2015 und der wachsenden Propaganda des Islamischen Staats in sozialen Medien vorgenommen.

Rollen und Verantwortlichkeiten

Im Zusammenhang mit der Cybersicherheit übernehmen im Allgemeinen die obersten politischen Ebenen die politische und strategische Führung. Nationale Cybersicherheitsstrategien werden meistens vom Amt des Premierministers veröffentlicht, ausser in Deutschland und den Niederlanden, wo das Innenministerium bzw. das Ministerium für Justiz und Sicherheit für die Strategie verantwortlich ist.

Die Tatsache, dass die Thematik der Cybersicherheit auf der obersten politischen Ebene angesiedelt ist, betont nicht nur ihre Bedeutung, sondern auch die zivile Führung auf diesem Gebiet. Zivile Führung weist darauf hin, dass Staaten Cybersicherheit nicht als eng gefasste Frage der nationalen Sicherheit oder – noch enger – als militärische Frage verstehen, sondern vielmehr als ein sozioökonomisches Thema mit Ausstrahlung auf die gesamte Gesellschaft.

Ausser den Ämtern der Premierminister sind gewöhnlich die Innen- und Verteidigungsministerien als weitere Institutionen an der Cybersicherheit beteiligt. In den Niederlanden ist das Ministerium für Justiz und Sicherheit in Fragen der Cybersicherheit federführend, aber auch das Innen-, Verteidigungs- und Aussenministerium sind beteiligt[12]. In Finnland ist das Transport- und Kommunikationsministerium unter Beteiligung des Innen-, Verteidigungs- und Aussenministeriums für die Cybersicherheit verantwortlich. Bei der Abwehr von Cyberrisiken (defensiv) teilen sich zivile Stellen mit Verantwortung für die Verteidigung der Allgemeinheit die Führung mit den Streitkräften, die für die Verteidigung ihrer eigenen Infrastrukturen zuständig sind.

4 Innenministerium, *Stratégie de lutte contre les cybermenaces* (Paris: Innenministerium, 2017) *https://www.interieur.gouv.fr/content/download/101310/797848/file/Lutte-contre-les-cybermenaces.pdf*

5 Verteidigungsministerium, *Pacte Cyber Défense* (Paris: Verteidigungsministerium, Februar 2014) *http://www.defense.gouv.fr/content/download/237708/2704474/file/Pacte%20D%C3%A9fense%20Cyber-1.pdf*

6 Jean-Yves Le Drian, *Présentation du Pacte Cyber Défense* (Paris: Verteidigungsministerium, Februar 2014) *https://www.defense.gouv.fr/english/actualites/articles/presentation-du-pacte-defense-cyber*

7 Präsident des Ministerrats, *Nationaler Rahmen für Cybersicherheit* (Rom: Präsident des Ministerrats, Dezember 2013) *https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf*

8 Präsident des Ministerrats, *Nationaler Plan für Schutz im Cyberspace und IKT-Sicherheit* (Rom: Präsident des Ministerrats, Dezember 2013) *https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf*; Präsident des Ministerrats, *Piano nazionale per la protezione cibernetica e la sicurezza informatica* (Rom: Präsident des Ministerrats, März 2017) *https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf*

9 Aussenministerium, *«Building Digital Bridges» International Cyber Strategy – Towards an integrated international cyber policy* (Den Haag: Aussenministerium, Februar 2017), *https://www.government.nl/binaries/government/documents/parliamentary-documents/2017/02/12/international-cyber-strategy/International+Cyber+Strategy.pdf*

10 Verteidigungsministerium, *The Defence Cyber Strategy* (Den Haag: Verteidigungsministerium, Februar 2015), *https://english.defensie.nl/topics/cyber-security/defence-cyber-strategy*

11 Premierminister, *Stratégie Nationale Pour la Sécurité Du Numérique* (Paris: Premierminister, Oktober 2015), *https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques*

12 Ministerium für Justiz und Sicherheit, *National Cyber Security Agenda: A cyber secure Netherlands* (Den Haag: Ministerium für Justiz und Sicherheit, April 2018), *https://www.ncsc.nl/english/current-topics/national-cyber-security-agenda.html*

Bei den für diese Studie analysierten Staaten stellten wir verschiedene Grade der Zentralisierung fest:

- Frankreich, wo die nationale Agentur für Cybersicherheit (Agence nationale de la sécurité des systèmes d'information/ANSSI) die wichtigste Organisation darstellt, ist stark zentralisiert; allerdings sind die französischen Strukturen der Strafverfolgung stärker fragmentiert, da dieses Feld von verschiedenen Akteuren abgedeckt wird, deren Aufgaben auch den Kampf gegen Cyberkriminalität beinhalten.

- In Finnland ist zwar auf strategischer Ebene eine Zentralisierung beim Präsidenten und Ministerkomitee für Aussen- und Sicherheitspolitik (UTVA) gegeben, aber auf operativer Ebene ist die Cybersicherheit stärker fragmentiert.

- Israel weist seit der Gründung der Cyber-Direktion 2018 den höchsten Grad institutioneller Zentralisierung defensiver Aspekte der Cybersicherheit auf.

- Italiens institutionelle Struktur beinhaltet eine Mischung aus Zentralisierung und Dezentralisierung: Sie ist insofern zentralisiert, als der Präsident des Ministerrats bei Fragen der Cybersicherheit die primäre politische Verantwortung trägt. Die Strukturen unterhalb dieser Ebene sind allerdings dezentralisiert, da verschiedene, miteinander interagierende Stellen für die Cybersicherheit zuständig sind und zur Cybersicherheitsstrategie Beiträge leisten.

- Deutschland und die Niederlande besitzen dezentrale Strukturen. In Deutschland ist diese Dezentralisierung auf das föderale politische System zurückzuführen.

Beziehungen zwischen der zivilen und militärischen Domäne

In den meisten Ländern sind die zivilen und militärischen Domänen der Cybersicherheit getrennt und verfügen jeweils über ihre eigenen Institutionen, Strategien, Aufgaben und Personal. Die Streitkräfte sind im Allgemeinen hauptsächlich für den Schutz ihrer eigenen Infrastrukturen sowie den Aufbau offensiver und defensiver Kapazitäten verantwortlich.

In manchen Fällen wird eine Kooperation zwischen zivilen und militärischen Stellen erwähnt:

- In Frankreich findet eine Kooperation im Rahmen der Operativen Sicherheitszentrale für Informationssysteme (Centre d'opération pour la sécurité des systèmes d'information/COSSI) der ANSSI-Analysegruppe und der Analysezentrale für defensive Cyberoperationen (Centre d'analyse en lutte informatique défensive/CALID) der Streitkräfte statt. Die Zusammenarbeit zwischen den beiden Institutionen beinhaltet den Austausch von Informationen und CALID unterstützt COSSI im Fall einer Cyberattacke auf Verteidigungsunternehmen. COSSI und CALID haben ihre Zentrale im selben Gebäude, um ihre Zusammenarbeit zu fördern[13].

- In den Niederlanden findet die Zusammenarbeit auf der Ebene der Joint SIGINT Cyber Unit (JSCU) statt, die den Inlands- und Auslandsgeheimdienst (AIVD) sowie den Militärischen Geheimdienst (MIVD) umfasst. Sowohl der AIVD als auch der MIVD verfügen über separate Budgets, separate Hierarchien und separates Personal, arbeiten aber im selben Gebäude, teilen Informationen über Vorfälle und arbeiten in manchen Fällen nach Bedarf auch zusammen[14].

- In Finnland findet die Zusammenarbeit über den Sicherheitsausschuss (TK) unter dem Vorsitz des Verteidigungsministers sowie das staatliche Lagezentrum (GOVSITCEN) beim Amt des Premierministers auf einer höheren Ebene statt. Streitkräfte und Zivilisten tauschen im TK Informationen zur Planung und Erarbeitung nationaler Sicherheitsstrategien und im GOVSITCEN Informationen zu Bedrohungen aus, um eine umfassende situative Sensibilisierung für den Cyberspace zu bewirken[15].

- In Israel ist die dem Amt des Premierministers direkt zugeordnete Cyber-Direktion für den Austausch von Informationen zuständig.

Eine Zusammenarbeit besteht zum Teil auch zwischen den Streitkräften und dem privaten Sektor. Diese Art der Kooperation findet hauptsächlich zwischen Streitkräften und privaten, kritische Infrastrukturen verwaltenden Akteuren statt, um solche Infrastrukturen gegen Cyberattacken zu schützen.

13 Verteidigungsministerium, *Pacte Cyber Défense* (Paris: Verteidigungsministerium, Februar 2014) http://www.defense.gouv.fr/content/download/237708/2704474/file/Pacte%20D%C3%A9fense%20Cyber-1.pdf; Pascal Brangetto, *National Cyber Security Organisation: France* (Talinn: CCDCOE, 2015), S. 12, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_FRANCE_032015_0.pdf

14 Kadri Kaska, *National Cyber Security Organisation: The Netherlands* (Talinn: CCDCOE, 2015), p. 17, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_NETHERLANDS_032015_0.pdf

15 Vgl. Sean Cordey, «Finland», in *National Cybersecurity and Cyberdefense policy snapshots* (Zürich, Center for Security Studies, September 2018), http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefense_Policy_Snapshots_Collection_1.pdf

Cybersicherheit in den Streitkräften

Die Cybersicherheit in den Streitkräften ist in allen sechs Staaten ähnlich organisiert. In jedem Land finden sich Cybersicherheits-Stellen auf den obersten Kommandoebenen, oft direkt unterhalb des Oberbefehlshabers der Streitkräfte. Diese Konstellation zeigt, dass sich die Staaten der Bedeutung von Fragen der Cybersicherheit für alle Teile der Streitkräfte bewusst sind.

Diese Priorisierung und Zentralisierung der Cybersicherheit bei Militärs ist vor allem bei den NATO-Mitgliedern zu erkennen. Alle in unserer Studie untersuchten NATO-Mitglieder gründeten zwischen 2014 und 2017 Cyber-Kommandostellen. Es ist unklar, ob der Anreiz zur Schaffung von Cyber-Kommandostellen von der NATO oder NATO-Mitgliedern ausging, aber diese Stellen bilden unter NATO-Mitgliedern einen klaren, allgemeinen Trend. Das Ziel der Cyber-Kommandostellen ist die Zentralisierung und Überwachung defensiver Cyberaktivitäten der Streitkräfte. Finnland ist kein NATO-Mitglied und hat noch keine Cyber-Kommandostelle geschaffen, zieht dies aber in Erwägung. In Israel war die Schaffung einer einheitlichen Cyber-Kommandostelle geplant; es wurde jedoch letztendlich beschlossen, die Trennung zwischen defensiven militärischen Kapazitäten (Direktion C4I) einerseits und der Fernmeldeaufklärung und Durchführung von Cyberattacken (Einheit 8200 der Direktion des militärischen Nachrichtendienstes) andererseits beizubehalten[16].

Alle Streitkräfte haben ihre offiziellen militärischen IT-Notfallteams (Computer Emergency Response Teams/CERTs), die jeweils ihre eigenen Netze schützen. Italien verfügt über ein zentrales CERT für das gesamte Militär, das von weiteren CERTs für die einzelnen militärischen Bereiche ergänzt wird.

Die Rolle der Nachrichtendienste

Die Rolle der Nachrichtendienste wird in nationalen Cybersicherheitsstrategien aufgrund der sensiblen, geheimen Natur ihrer Tätigkeit oft nicht ausdrücklich erwähnt. Wenn Nachrichtendienste in Strategiedokumenten Erwähnung finden, dann um sie innerhalb des breiteren nationalen Rahmens der Cybersicherheit zu positionieren. Sofern ihre Rolle beschrieben wird, geht es um Spionageabwehr und ein Situationsbewusstsein für Cyberbedrohungen. Nachrichtendienste stehen oft unter ziviler Aufsicht und sind damit den obersten politischen Ebenen unterstellt, zum Beispiel dem Premierminister, Kanzler, Verteidigungs- oder Innenminister.

Drei länderspezifische Beobachtungen sind hier erwähnenswert:

- In Frankreich ist die Generaldirektion für innere Sicherheit (Direction Générale de la Sécurité Intérieure/DGSI) hinsichtlich Überwachungsstrukturen von der Generaldirektion für äussere Sicherheit (Direction Générale de la Sécurité Extérieure/DGSE) abhängig. Die DGSI baut jedoch eigene Infrastrukturen auf, um unabhängig zu werden[17].

- In Israel verfügen die Nachrichtendienste (d.h. Aman für das Militär, Mossad für das Ausland und Shin Beth für das Inland) mutmasslich über offensive Cyberkapazitäten.

- In Italien sammelt und koordiniert die Abteilung für Sicherheitsinformationen (Dipartimento delle Informazioni per la Sicurezza/DIS) Informationen über Cybersicherheit vom Auslandsnachrichtendienst (Agenzia Informazioni e Sicurezza Esterna/AISE) und Inlandsnachrichtendienst (Agenzia Informazioni e Sicurezza Interna/AISI).

Strafverfolgung

Strafverfolgungsbehörden sind in Cybersicherheit eingebunden, da sie Cyberkriminalität und durch den Cyberspace ermöglichte Kriminalität ermitteln und bekämpfen. In allen für diese Studie untersuchten Staaten sind die Aufgaben und Strukturen der Strafverfolgungsbehörden von denen anderer Institutionen der Cybersicherheit und vor allem von militärischen Institutionen getrennt, wie das in demokratischen Ländern nicht anders zu erwarten ist[18]. Ihre spezifischen Aufgaben bestehen in der Prüfung und Ermittlung illegaler Internetinhalte, durch den Cyberspace ermöglichter Kriminalität und Cyberkriminalität sowie in der Sensibilisierung für diese Bedrohungen und der Gefahrenabschätzung. In allen Staaten besteht eine Trennung zwischen den Einheiten, die für die Suche und Überwachung illegaler Internetinhalte bzw. die Cyberkriminalität verantwortlich sind. Darüber hinaus bezieht z.B. Deutschland Spezialeinheiten für die organisierte Kriminalität in Ermittlungen von Cyberkriminalität mit ein. Europäische Staaten arbeiten bei der Cyberkriminalität über EUROPOL auf europäischer Ebene zusammen; alle Staaten kooperieren international über Interpol.

16 Judah Ari Gross, *Army beefs up cyber-defense unit as it gives up idea of unified cyber command* (Jerusalem: The Times of Israel, Mai 2017), *https://www.timesofisrael.com/army-beefs-up-cyber-defense-unit-as-it-gives-up-idea-of-unified-cyber-command*

17 Jacques Follorou, *Pris dans leurs rivalités, les services français ont privilégié leurs liens avec la NSA et le GCHQ* (Paris: Le Monde, Dezember 2016), *https://www.lemonde.fr/pixels/article/2016/12/10/pris-dans-leurs-rivalites-les-services-francais-ont-privilegie-leurs-liens-avec-la-nsa-et-le-gchq_5046755_4408996.html*

18 Italien bildet hier eine Ausnahme, da die Carabinieri eine militärische Kraft mit Polizeiaufgaben darstellen.

Drei Beobachtungen zu Besonderheiten einzelner Staaten sind erwähnenswert:

- In Frankreich und Italien ist die Strafverfolgung fragmentiert. Dies ist auf bestehende Strukturen zurückzuführen, die zusätzlich mit der Bekämpfung von Cyberkriminalität und durch den Cyberspace ermöglichter Kriminalität betraut wurden.

- Italien verfügt über eine Spezialeinheit, das Nationale Antikriminalitäts-Informationszentrum zum Schutz kritischer Infrastrukturen (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche/CNAIPIC), das Cyberkriminalität gegen kritische Infrastrukturen bekämpft.

- Die deutschen und niederländischen Strafverfolgungsbehörden haben Kooperationsplattformen mit dem privaten Sektor entwickelt. In Deutschland fungiert die Zentrale Ansprechstelle Cybercrime (ZAC) als Kontaktstelle für Firmen, die kriminellen Cyberattacken ausgesetzt sind. In den Niederlanden wurde die niederländische Electronic Crimes Task Force von den Strafverfolgungsbehörden als öffentlich-private Partnerschaft mit dem Privatsektor errichtet.

Wichtigste Herausforderungen

Da das Bedrohungsumfeld der meisten hier untersuchten Staaten ähnlich ist, sind alle ihre Regierungen hinsichtlich der Entwicklung, Implementierung und Aufrechterhaltung umfassender, holistischer Cybersicherheitsstrategien mit einer Reihe von Herausforderungen konfrontiert.

Wir haben acht wichtige Herausforderungen identifiziert:

1. die (vertikale) Integration nationaler Cybersicherheitsstrategien in den Rahmen der nationalen Sicherheit und/oder einer Gesamtstrategie;

2. die (horizontale) Koordination der verschiedenen Stellen im Umfeld der Cybersicherheit;

3. internationale Kooperation und Normenbildung;

4. Krisenmanagement;

5. Lagebild und Analyse von Cyberbedrohungen;

6. Aufbau von Kapazitäten, Bildung, Information und Sensibilisierung;

7. Schaffung eines funktionierenden Kooperationsrahmens mit dem Privatsektor und

8. Harmonisierung der Gesetzgebung.

1. Integration (vertikal)

Die Integration nationaler/internationaler Visionen und Zielsetzungen für die Cybersicherheit in den breiteren Rahmen nationaler Sicherheit bereitet Staaten Schwierigkeiten. Hierzu zählt auch der konzeptionelle Übergang von der Auffassung der Cybersicherheit als technisches Problem zu ihrer Betrachtung als politische Herausforderung. Cybersicherheit ist ein Querschnittsthema, das sich mit vielen anderen – teilweise älteren – Politikbereichen überschneidet, darunter die Informationssicherheit, der Schutz kritischer Infrastrukturen und die allgemeine Verteidigung. Diese Bereiche sind von einer Vielzahl etablierter Strategien, Gesetze, Regelungen und politischer Abläufe gekennzeichnet. Die Herausforderung besteht nun darin, alle bestehenden Politiken, die häufig voneinander isoliert sind, zu koordinieren und zu integrieren, um einen kohärenten, vernetzten und straffen Rahmen oder eine Gesamtstrategie zu schaffen. Eine Auffassung und Behandlung der Cybersicherheit als separates Thema, das nicht mit vorhandenen Politiken integriert wird, ist zu vermeiden.

2. Koordination (horizontal)

Die zweite Herausforderung hängt mit der Definition und effizienten Umsetzung von Politiken und Massnahmen zusammen. Schwierigkeiten ergeben sich aus der Heterogenität der Akteure in der Cybersicherheit und Cyberabwehr auf vertikaler (nationaler, regionaler, lokaler) oder horizontaler (ziviler und militärischer, öffentlicher und privater) Ebene. Zu den zu koordinierenden Aspekten zählen die Institutionalisierung der Zusammenarbeit zwischen öffentlichen Stellen, die erforderliche Veränderung bestimmter, oft tief verwurzelter bürokratischer Gewohnheiten und Routinen, das Mainstreaming des Dialogs und der verwendeten Terminologie unter allen Akteuren, die Abstimmung verschiedener operativer Logiken des privaten (gewinnorientierten) und öffentlichen (gemeinwohlorientierten) Sektors sowie die Entwicklung neuer technischer Kenntnisse und Kapazitäten mit begrenzten Ressourcen und Erfahrungen. Die Abstimmung divergierender Interessen und Positionen der verschiedenen Akteure kann viel Zeit, Energie und Mittel beanspruchen und von Konkurrenzdenken geprägt sein – dies gilt insbesondere bei einer Verteilung oder Neuverteilung von Ressourcen, die häufig zu bürokratischem Gerangel um Budgets und Kompetenzen führt (zum Beispiel in Israel[19]). Darüber hinaus können komplexe bürokratische Verantwortlichkeits- und Kontrollstrukturen (wie beispielsweise bei den für die Cyberkriminalität zuständigen Stellen in Frankreich und Italien) eine effiziente übergeordnete Überwachung beinahe unmöglich machen.

3. Internationale Kooperation

Eine dritte Herausforderung betrifft die internationale Kooperation im Kontext einer dezentralen, fragmentierten Governanzstruktur für die Cybersicherheit (und das Internet allgemein) und dem Einhalten von Normen für gutes oder verantwortliches Verhalten im Cyberspace. Erstere ist für die Multiplikation von Prozessen verantwortlich, die dazu geführt hat, dass Cyberdiplomatie höhere (personelle, wirtschaftliche und politische) Ressourcen beansprucht und eine höhere Wichtigkeit einnimmt. Dies ist vor allem für Staaten mit begrenzten diplomatischen Corps problematisch (zum Beispiel Finnland). Gleichzeitig gestalten aktuelle geopolitische Spannungen den Dialog, die Vertrauensbildung, die Zusammenar-

19 Lior Tabansky & Isaac Ben Israel, *Cybersecurity in Israel* (New York: Springer Briefs in Cybersecurity, 2015), *https://www.springer.com/de/book/9783319189857*

beit und die Krisenprävention schwierig. Vor allem aber verbreitert sich derzeit die Kluft zwischen dem kollektiven Streben der internationalen Gemeinschaft nach grösserer Stabilität und den tatsächlichen offensiven Praktiken mancher Staaten, da der Konkurrenzkampf um Einfluss im Cyberspace weiterhin andauert.

4. Krisenmanagement

Die vierte Herausforderung betrifft drei zusammenhängende Themen: die Aufrechterhaltung effizienter Krisenkommunikation, den Aufbau klarer Strukturen für die Krisenkommunikation und die Entwicklung ausreichender Kapazitäten für die Reaktion auf Vorfälle. Im Fall einer grösseren Cyberkrise ist der effiziente, kontinuierliche Fluss von Informationen zwischen den verantwortlichen öffentlichen und privaten Stellen für eine angemessene Reaktion entscheidend, kann sich aber ohne institutionalisierte Informationskanäle schwierig gestalten. Die öffentliche Kommunikation kann darüber hinaus sowohl für den öffentlichen als auch für den privaten Sektor problematisch und sensibel sein und sogar kontraproduktiv wirken, wenn sie nicht angemessen organisiert wird. Eine grundlegende Schwierigkeit liegt hierbei darin, dem privaten Sektor die richtigen Anreize zu bieten, um bei Vorfällen staatliche Stellen zu benachrichtigen, Unterstützung anzufordern und zusammenzuarbeiten. Das Fehlen klar definierter, bewährter Führungsstrukturen kann die Reaktionsfähigkeit des Staats zusätzlich behindern. Gleichzeitig sind Notfallplanungen und Übungen auf gesamtstaatlicher Ebene aufgrund der bereichsübergreifenden Natur der Thematik und der Vielzahl der beteiligten Akteure äusserst komplex (und kostspielig). Schliesslich bereiten die Qualifizierung und Aufrechterhaltung von ausreichend Personal, das auf Vorfälle angemessen reagieren kann und auf Abruf bereitsteht, Schwierigkeiten.

5. Lageanalyse

Die fünfte Herausforderung besteht einerseits im Aufbau und in der Aufrechterhaltung eines konstanten, ebenso holistisch wie detailorientierten Lageanalyse mit besonnener Risikobeurteilung und andererseits in der Sicherstellung effizient und effektiv koordinierter Informationsflüsse zwischen allen Informationen sammelnden und aggregierenden (zivilen und militärischen) Akteuren, zum Beispiel Nachrichtendienste, nationale Cybersicherheitszentren oder die Streitkräfte. In diesem Kontext besteht schon seit langem das Risiko, Cyberbedrohungen überzubewerten und Katastrophenszenarien zu viel Gewicht zu geben. Auch ein nicht einheitliches Bild der Bedrohungslage in den verschiedenen Diensten, die Informationen sammeln, ist ein zu berücksichtigendes Risiko. Ohne die Herausforderungen der Digitalisierung verharmlosen zu wollen, bilden auch unverhältnismässige Auffassungen von Risiken keine gute Basis für Lösungen. Die Frage des Gleichgewichts zwischen Freiheitsrechten (zum Beispiel Persönlichkeitsrechten) und Sicherheit behält in allen Demokratien eine entscheidende Bedeutung. Entscheidend ist eine eigenständige Analysefähigkeit, die Risiken im nationalen Kontext identifiziert und dadurch deren Bearbeitung erst ermöglicht.

6. Bildung und Information sowie Aufbau von Kapazitäten

Eine weitere Herausforderung besteht im Aufbau von Kapazitäten und in der Bereitstellung relevanter Bildung und Information. Diese Problematik wird immer dringlicher, da bereits heute in der Cybersicherheit enormer Arbeitskräftemangel besteht (etwa 142.000 im EMEA-Gebiet und 2,93 Mio. weltweit[20]), der wahrscheinlich noch drastischer werden wird. Dieser Mangel betrifft nicht nur Fachkräfte für die Cybersicherheit, sondern auch GeneralistInnen, technische SpezialistInnen, politische EntscheidungsträgerInnen und AkademikerInnen, die eine reibungslose Funktion des privaten und öffentlichen Sektors ermöglichen. Eine weitere Herausforderung besteht in der Gewinnung und in der Bindung von Nachwuchskräften, vor allem im öffentlichen Sektor, der im Vergleich zum privaten Sektor (unter finanziellen und Karriereaspekten) als weniger attraktiv gilt. Längerfristig sind in diesem Kontext eventuell auch weitere politische Fragen zu berücksichtigen, zum Beispiel die stete Herausforderung, einen holistischen, partizipativen nationalen Rahmen für Initiativen zum Kapazitätsaufbau zu schaffen, koordinieren und begleiten; die Sicherstellung, dass Bildungsinhalte mit dem schnellen Wandel in der Cybersicherheit und ihrem operativen Umfeld Schritt halten; die kontinuierliche Schulung der Beschäftigten im öffentlichen Dienst zum sicheren Umgang mit dem Cyberspace sowie potenziell auch die Weiterentwicklung bestehender Zertifizierungen; und schliesslich die Schaffung neuer, nicht-traditioneller Qualifikationen wie zum Beispiel digitale Badges. Mit dieser Herausforderung ist auch das Problem der Sensibilisierung verbunden – nicht nur in der öffentlichen Verwaltung, sondern auch generell im privaten Sektor (zum Beispiel von CEOs oder KMU), unter der politischen Elite (d.h. von ParlamentarierInnen) und der Allgemeinheit. Vielen Staaten bereitet es Schwierigkeiten, Lücken zu identifizieren, Ziele zu definieren und Mechanismen zu entwickeln, um eine Kultur des Datenschutzes, der Datensicherheit und der Cybersicherheit zu schaffen.

20 ISC2, *Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens* (2018), https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx

7. Öffentlich-private Partnerschaften

Die Mehrheit der kritischen Infrastrukturen befinden sich in der Hand des Privatsektors. Daher ist die Frage öffentlich-privater Partnerschaften für die politische Entscheidungsfindung zur Cybersicherheit von zentraler Bedeutung. Regierungen sind bemüht, einen angemessenen Rahmen für diese Zusammenarbeit zu definieren und ein Gleichgewicht zwischen einem präskriptiven, staatlich orientierten und einem kooperativen, marktorientierten Ansatz zu finden. Öffentlich-private Partnerschaften bilden heute jedoch Eckpfeiler der meisten nationalen Cybersicherheitsstrategien und fungieren als zentrale Plattformen, um sowohl traditionellen als auch nicht-traditionellen Sicherheitsbedrohungen gemeinsam mit dem privaten Sektor zu begegnen. Dennoch bleiben viele Herausforderungen bestehen[21], darunter die anhaltende Unklarheit hinsichtlich der Einzelheiten solcher Partnerschaften, die allgemeine Schwierigkeit der Festlegung von Normen, fehlende Anreize für den privaten Sektor, sich an Fragen der nationalen Sicherheit zu beteiligen, und die Problematik, den Kosten-Nutzen-Rahmen privater Akteure zugunsten eines auf das Gemeinwohl abgestellten Rahmens zu erweitern. Dies alles verursacht mangelnde Klarheit bei Verantwortlichkeiten, Verantwortungsbereitschaft und Autorität.

8. Gesetzgebung und Regulierung

Schliesslich besteht eine Reihe rechtlicher Herausforderungen, insbesondere die Identifizierung von Rechtslücken, die Harmonisierung von Gesetzen und Rechtsordnungen im Zusammenhang mit dem Cyberspace und Cyberaktivitäten, die Regulierung des privaten Sektors, die Frage der Verschlüsselung und strafrechtlicher Ermittlungen sowie die dynamische Veränderung des technischen Umfelds. Darüber hinaus bleibt die Messbarkeit eines Erfolgs wie überall in Fragen der öffentlichen Ordnung und ihrer Überprüfung komplex.

21 Madeline Carr, *Public–private partnerships in national cyber-security strategies* (London: Royal Institute of International Affairs, 2016), *https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf*

Schlussfolgerung und Herausforderungen für die Schweiz

Die zwei Strategien zum Schutz der Schweiz vor Cyberrisiken (NCS 2012 und 2018) weichen im Wesentlichen nicht von den sechs Strategien ab, die für diese Studie verglichen wurden. Gefahren werden ähnlich beurteilt und dieselben Fragen und erforderlichen Massnahmen werden als besonders dringlich erkannt. Die Schweiz ist daher in verschiedenem Ausmass denselben acht Herausforderungen ausgesetzt.

1. Integration: In der NCS kommt eine holistische Perspektive der Cybersicherheit zum Ausdruck, die sich auch in der «Nationalen Strategie zum Schutz kritischer Infrastrukturen» (SKI) sowie der Strategie «Digitale Schweiz» wiederspiegelt. Eine Einbettung in eine übergeordnete Strategie fehlt allerdings, auch wenn die bundesrätlichen Berichte in der Aussen- und Sicherheitspolitik als strategische Leitplanke dienen könnten. Eine strategische Vision für technologische Themen ist jedoch unerlässlich, wenn sich die Schweiz in einer sich schnell entwickelnden und digitalisierenden Welt effektiv positionieren möchte.

2. Koordination: Die NCS berücksichtigt die verschiedenen bürokratischen Einheiten und deren Rollen und Verantwortlichkeiten. Darüber hinaus ist ein Kompetenzzentrum Cybersicherheit im Aufbau, die von einer/einem Delegierten für Cybersicherheit geleitet werden soll. Mithilfe dieser neuen Struktur sollte die Herausforderung der Koordination zwischen verschiedenen Akteuren – auch ausserhalb der Regierung – einfacher zu bewältigen sein, aber die Gefahr eines bürokratischen Kompetenzgerangels und suboptimaler Lösungen bleibt bestehen und die neuen Strukturen müssen sich erst noch bewähren. Zudem ist die Cybersicherheit kein isoliertes Thema, sondern muss auf sinnvolle Weise in andere Politikbereiche eingebettet werden. Die Schaffung von Parallelstrukturen nur für Cyberfragen ist dabei nicht unbedingt zielführend.

3. Internationale Kooperation: Die Schweiz beteiligt sich an den wichtigsten internationalen Aktivitäten zur Normenbildung im Umfeld der Cybersicherheit. Diese Bemühungen könnten jedoch noch intensiviert werden und die Position Genfs als Zentrum der Überlegungen zur Cybersicherheit liesse sich weiter stärken. Dieser Raum ist dabei nicht konkurrenzlos. Auch andere Staaten verwenden umfangreiche (finanzielle und diplomatische) Ressourcen, um sich in der Entwicklung von Normen zu positionieren. Ebenso gilt es zu überlegen, die Schulung des diplomatischen Corps im Bereich der Cyber-Themen zu verstärken.

4. Krisenmanagement: Gutes Krisenmanagement und insbesondere gute Krisenkommunikationsfähigkeiten bleiben im Zusammenhang mit grösseren Cybervorfällen eine wichtige politische Herausforderung. Auch wenn Cyberaspekte in den etablierten Krisenmanagement-Stäben (wie beispielsweise dem Bundesstab Bevölkerungsschutz/BSTB) integriert sind, bleibt die Handhabung von Cybervorfällen erfahrungemäss eine grosse politische Herausforderung, gerade weil das Wissen über die Täterschaft und den erfolgten Schaden schwierig abzuschätzen ist. Übungen, die mehrere Verantwortungsbereiche mit einbeziehen, sind hier von höchster Bedeutung. Da zu erwarten ist, dass die meisten national relevanten Cybervorfälle eine politische Dimension beinhalten, ist es von zentraler Bedeutung, dass die Cybersicherheit als politische und nicht nur als technische Verantwortung aufgefasst wird.

5. Lageanalyse: Die Verfügbarkeit guter cyberforensischer Kapazitäten ist für Staaten ebenso entscheidend wie die Fähigkeit, verschiedene Nachrichtenquellen zu einem Gesamtbild zu integrieren. Die Schweiz ordnet Gefahren allgemein umsichtig ein, aber die Gefahrenabschätzung bleibt aufgrund der Vielzahl von Unwägbarkeiten hinsichtlich der Absichten ausländischer Akteure und der dynamischen technischen Entwicklung eine permanente Herausforderung.

6. Bildung: Für Staaten, die gut vorbereitet in die digitale Zukunft gehen möchten, besteht die wohl wichtigste Herausforderung darin, weiterhin in breit gefasste Forschung, Bildung, Information und Innovationskraft zu investieren. Ein holistischer Ansatz für die Cybersicherheit bedeutet, diese nicht lediglich eng als Informatikproblem zu verstehen, sondern sie viel umfassender als gesellschaftliches, politisches und wirtschaftliches Thema aufzufassen (wie das teilweise in der Strategie «Digitale Schweiz» sowie der Botschaft zur Förderung von Bildung, Forschung und Innovation angedacht ist). So kann die Cybersicherheit als Voraussetzung verstanden werden, die Möglichkeiten der Digitalisierung optimal zu nutzen: also auch als Chance für eine nachhaltige Transformation der Schweizer Wirtschaft.

7. Öffentlich-private Partnerschaften: Die Schweiz verfügt über ein bewährtes Modell für öffentlich-private Partnerschaften in der Cybersicherheit, das sich allerdings zum Grossteil auf freiwillige Teilnahme

stützt. Es wird künftig wichtig sein, sich auch mit anderen Modellen, inkl. regulativen Massnahmen wie Meldepflichten auseinanderzusetzen, oder auch mit der Setzung finanzieller Anreize in bestimmten Bereichen und der Übernahme von Verantwortung durch den Staat bei spezfischen Vorfällen. Dabei ist eine Herausforderung, diese so zu gestalten, dass funktionierende öffentlich-private Partnerschaften nicht gefährdet werden.

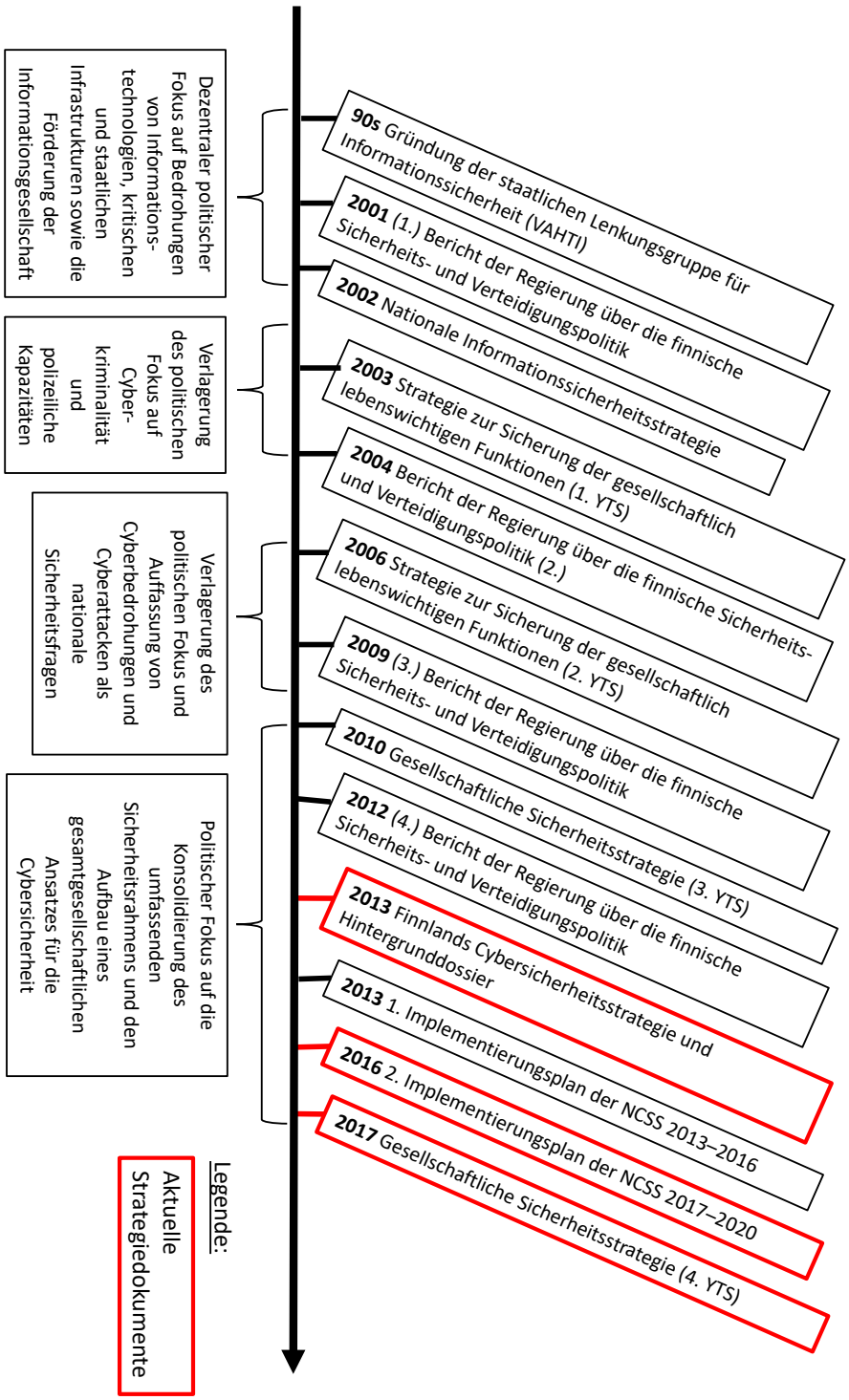
8. Gesetzgebung: Technologische Herausforderungen sind einem schnellen Wandeln unterworfen, die die Gesetzgebung vor Schwierigkeiten stellen. Cyberkriminelle sind innovativ, und Rechtssysteme haben zuweilen Schwierigkeiten, mit ihnen Schritt zu halten. Neben der Verfügbarkeit guter cyberforensischer und analytischer Kapazitäten der Strafverfolgung ist daher auch der Austausch von Informationen wichtig, zum Beispiel zwischen kantonalen Polizeibehörden.

Wie eingangs erwähnt ist die Höhe der Cyberbudgets anderer Staaten unklar. In Anbetracht der vielfältigen Aktivitäten ist jedoch offensichtlich, dass das Thema ernst genommen wird, vor allem weil eine so positive Entwicklung wie die Digitalisierung von der Fähigkeit staatlicher Akteure abhängt, für ihre Gesellschaften ein gewisses Mass an Cybersicherheit zu schaffen, respektive das Umfeld so zu gestalten, dass mehr Cybersicherheit ermöglicht und gefördert wird. Ausserdem sind politische Akteure im Allgemeinen desto eher bereit Geld auszugeben, je ernster ein Thema genommen wird. Die Schweiz wendet in diesem Bereich hingegen (noch) keine hohen Ausgaben auf. Am vorteilhaftesten sind Investitionen in den Aufbau von Kapazitäten, die Bildung, Forschung und Information, da diese langfristige Vorteile für alle schaffen. Ergänzend muss sichergestellt werden, dass die verschiedenen Stellen der Verwaltung wissen, was sie zu tun haben, und auf ein gemeinsames, übergeordnetes Ziel hinarbeiten.

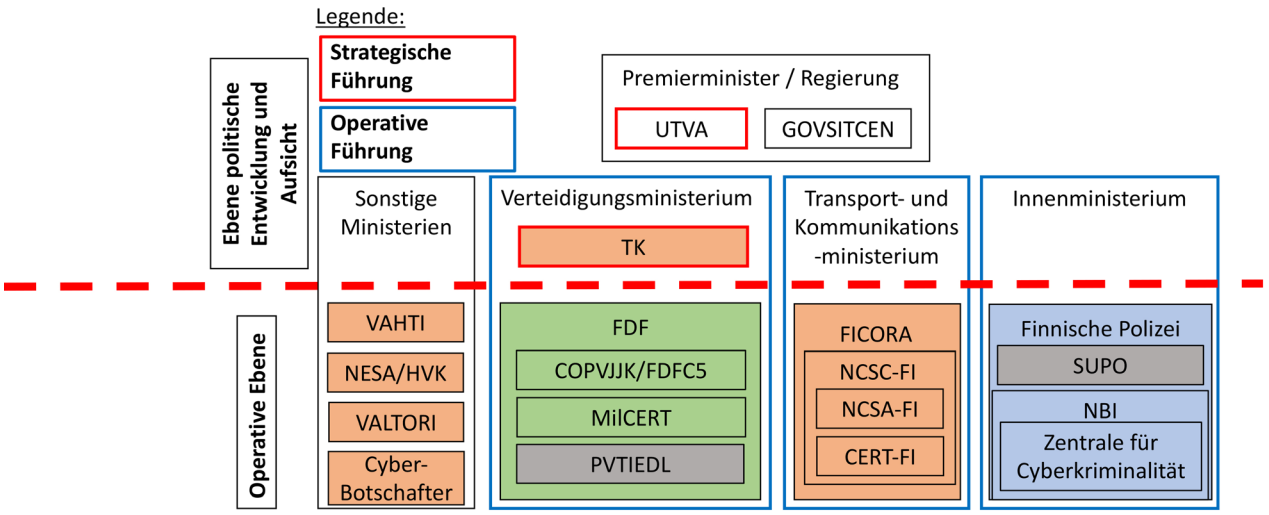
Anhang

Länderinformation Finnland

1. Wichtige Strategiedokumente und Entwicklung



2. Organisation, wichtige Organe und Verantwortlichkeiten



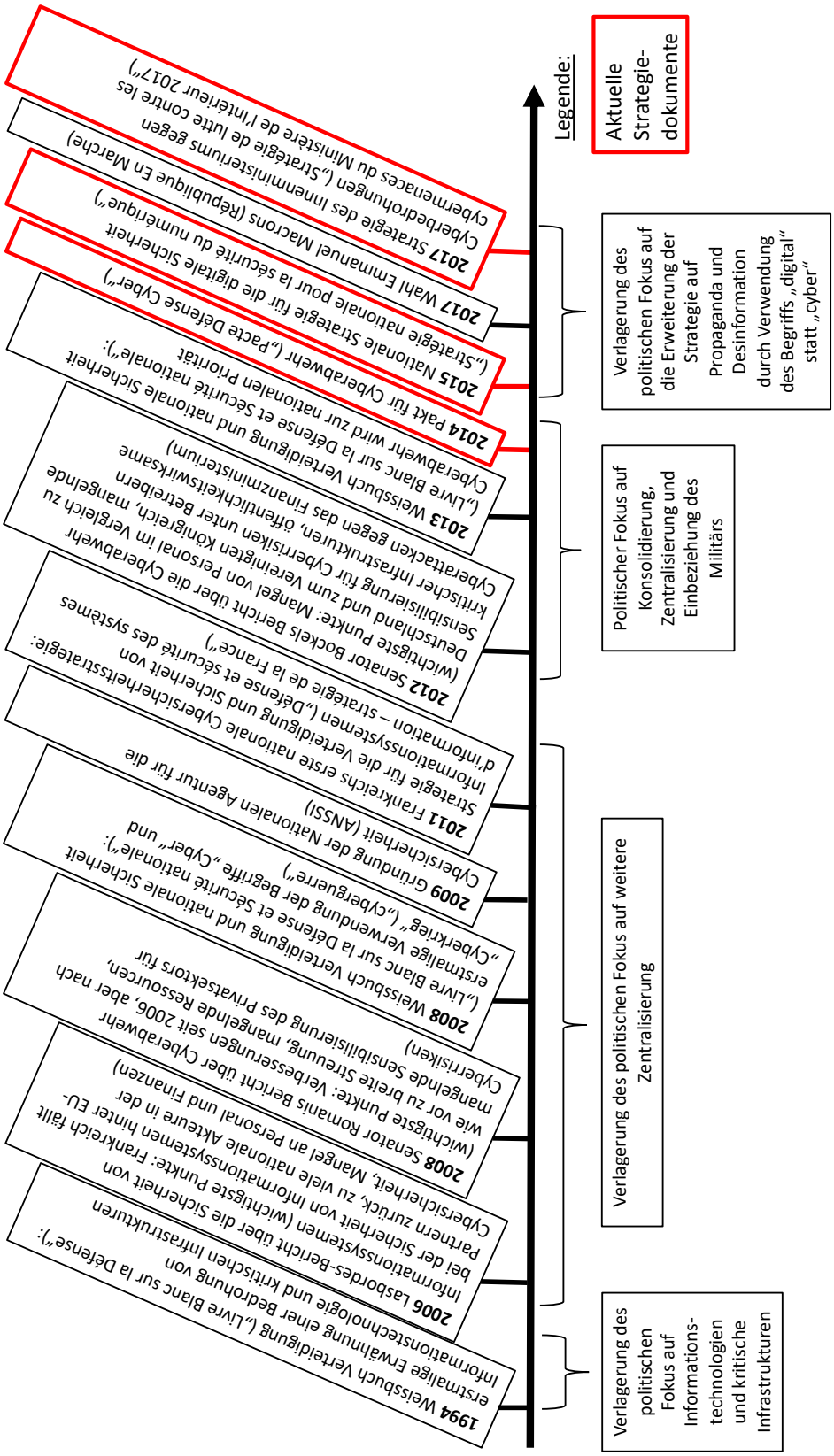
Cybersicherheit	Cyberkriminalität	Cyberabwehr	Nachrichtendienste
TK: - Kollegialbehörde für umfassende Sicherheitspolitik - Entwicklung, Koordination und Begleitung der NCSS	**NBI:** - Bekämpfung, Ermittlung und Verhinderung von Cyber- und Onlinekriminalität - Beurteilung der Bedrohungslage durch Cyberkriminalität - Koordination und Durchführung der strafrechtlichen Erkenntnisgewinnung zwischen Polizei-, Zoll- und Grenzschutzbehörden - Funktion als nationale und internationale Kooperationszentrale	**FDFC5 – Cyberabteilung:** - Schutz von Datennetzen und Infrastrukturmanagement von Diensten - Entwicklung defensiver und offensiver Cyberkapazitäten - Erarbeitung, Pflege und Verbreitung von Informationen zur Cyberabwehr und Cyber-Bedrohungslage	**SUPO:** - Nachrichtendienst und Spionageabwehr
NCSC-FI: - Informations- und Kommunikationssicherheit - Operative Unterstützung und Reaktion - Erarbeitung von Lagebildern			**PVTIEDL:** - Militärischer Nachrichtendienst und militärische Gegenspionage - Sammlung von Geodaten und meteorologischen Informationen

3. Akronyme

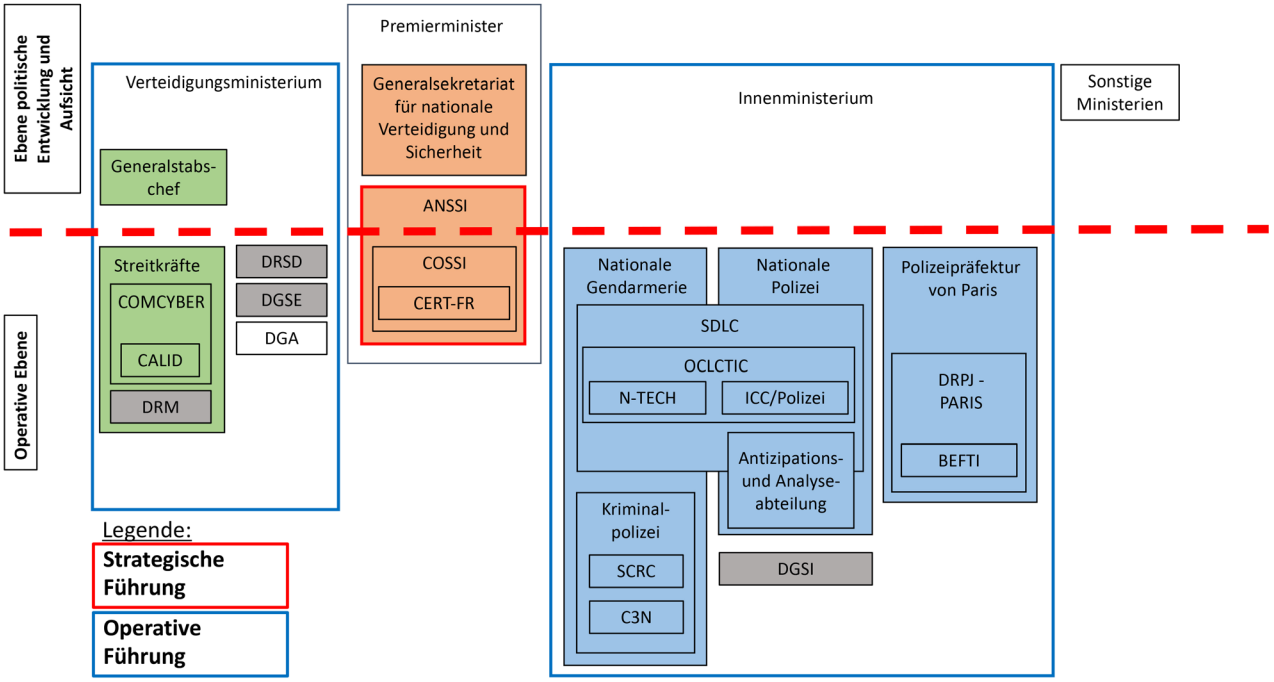
Akronym	Finnisch	Deutsch
FDF	Försvarsmakten	Finnische Streitkräfte
FICORA	Viestintävirasto	Finnische Telekommunikations-Aufsichtsbehörde
GOV-CERT	-	Staatliches CERT (IT-Notfallteam)
GOVSITCEN	-	Staatliches Lagezentrum
HTAO	-	Büro des Botschafters für hybride Bedrohungen
NCSA-FI	-	Finnische Nationalbehörde für Kommunikationssicherheit
NCSC-FI	Kyberturvallisuuskeskus	Nationales Zentrum für Cybersicherheit
NCSS	Suomen kyberturvallisuusstrategia	Nationale Cybersicherheitsstrategie
NESA/HVK	Huoltovarmuuskeskus	Nationale Behörde für Krisenversorgung
PVJJK/ FDFC5A	Puolustusvoimien johtamisjärjestelmäkeskus	Finnische Streitkräfte – Abteilung C5
SUPO	Suojelupoliisi	Finnischer Sicherheits- und Nachrichtendienst
TK	Turvallisuuskomitea	Sicherheitsausschuss
UTVA	Valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta	Kabinettsausschuss für Aussen- und Sicherheitspolitik
VAHTI	Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä	Staatliche Lenkungsgruppe für Informationssicherheit
VALTORI	Valtion tieto- ja viestintätekniikkakeskus	Staatliche IKT-Zentrale
YTS	Yhteiskunnan turvallisuusstrategia	Gesellschaftliche Sicherheitsstrategie

Länderinformation Frankreich

1. Wichtige Strategiedokumente und Entwicklung



2. Organisation, wichtige Organe und Verantwortlichkeiten



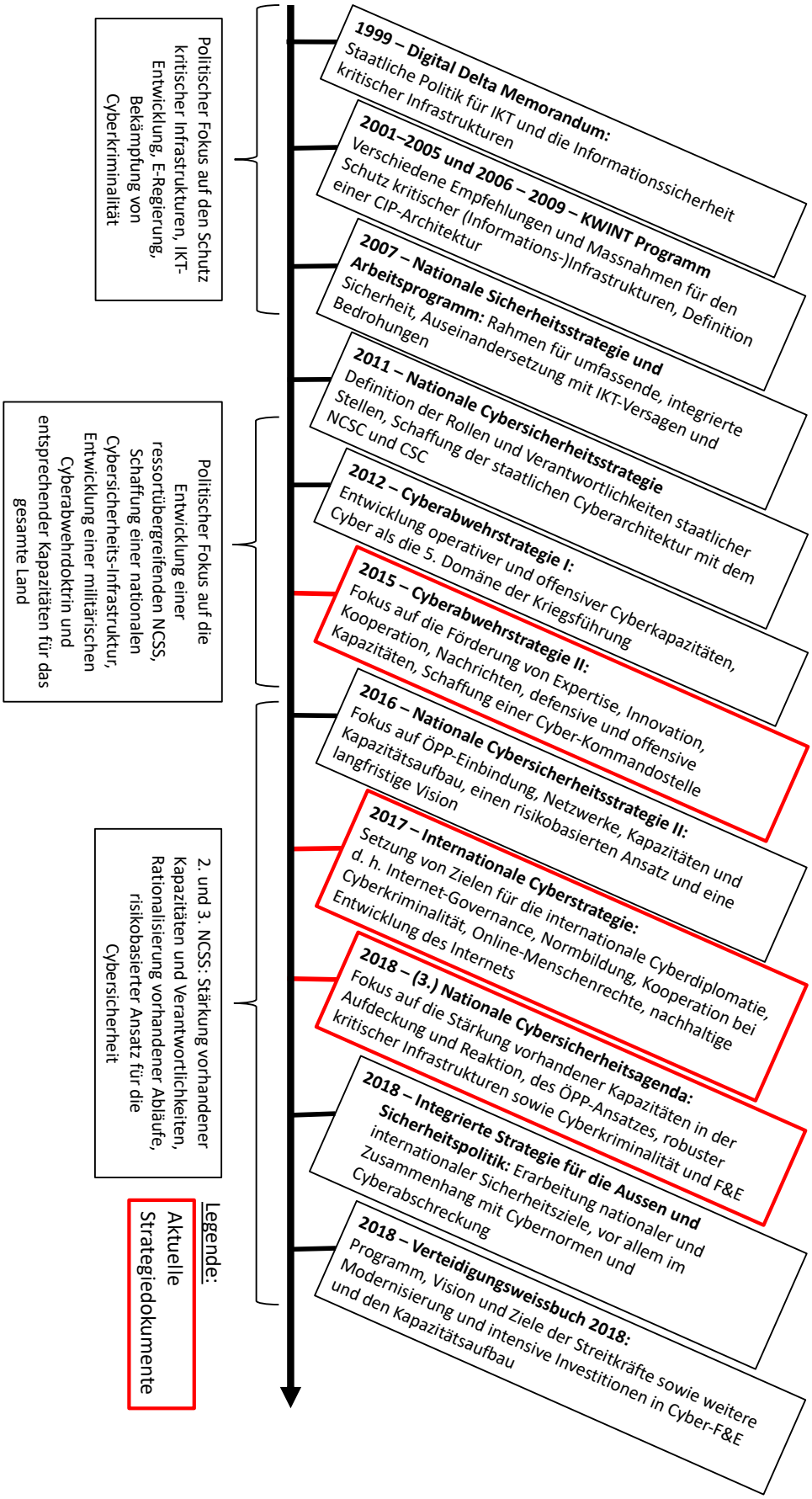
Cybersicherheit	Cyberkriminalität	Cyberabwehr	Nachrichtendienste
ANSSI: - Zentralisierung, Koordination und Beratung der Regierung - Unterstützung des Privatsektors - Förderung der Sicherheit kritischer Infrastrukturen - Sensibilisierung der Öffentlichkeit, Bildung und Information	**OCLCTIC:** - Ermittlungen im Zusammenhang mit Hacking, illegalen Inhalten und Onlinebetrug - Technische Entwicklung - Bildung, Information und Expertise - Nationaler Ansprechpartner	**COMCYBER:** - Zentralisierung und Koordination aller Stellen der Cyberabwehr - Durchführung offensiver und defensiver Cyberoperationen	**DGSI:** - Gegenspionage - Ermittlungen bei Cyberattacken gegen kritische und staatliche Infrastrukturen
COSSI: - Analyse von Bedrohungen und Systemanfälligkeiten - Entwicklung von Reaktionen auf Attacken - Leistung dringender technischer Unterstützung	**Antizipations- und Analyseabteilung:** - Entwicklung von Reaktionen auf Cyberattacken für nichtkritische Infrastrukturen - Sensibilisierung der Öffentlichkeit für Cyberbedrohungen	**CALID:** - Funktion als operative Zentrale der Streitkräfte - Durchführung und Überwachung von Cyber-Reaktionen	**DGSE:** - Cyber-Überwachung
	C3N: - Bereitstellung von Bildung, Information, Schulungen, Forschung, Überwachung und Ermittlungen		**DRM:** - Militärischer Nachrichtendienst
			DRSD: - Schutz von Personal, Informationen, Material und Infrastruktur - Überwachung des Cyberspace - Spionageabwehr - Sensibilisierung

3. Akronyme

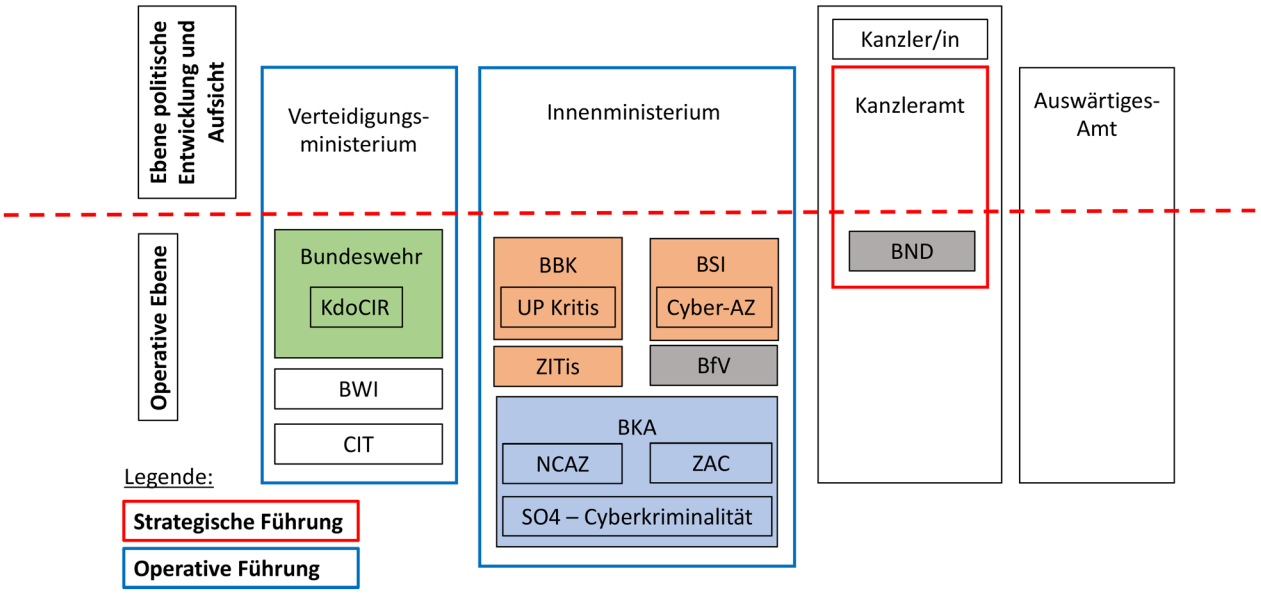
Akronym	Französisch	Deutsch
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information	Nationale Agentur für Cybersicherheit
BEFTI	Brigade d'Enquête sur les Fraudes aux Technologies de l'Information	Ermittlungsbrigade für Betrug und Informationstechnologien
C3N	Centre de lutte contre les Criminalités Numériques	Zentrale gegen digitale Kriminalität
CALID	Centre d'Analyse de Lutte Informatique Défensive	Analysezentrale für defensive Cyberoperationen
CERT-FR	-	Französisches CERT (IT-Notfallteam)
COMCYBER	Commandement des Cyberdéfense	Cyber-Kommandostelle
COSSI	Centre Opérationnel de Sécurité des systèmes d'Information	Operative Sicherheitszentrale für Informationssysteme
CRAC	Centre de Recherche et d'Analyse du Cyberespace	Forschungs- und Analysezentrum für den Cyberspace
DCPJ	Direction Centrale de la Police Judiciaire	Zentraldirektion der Kriminalpolizei
DGA	Direction Générale de l'Armement	Generaldirektion für Rüstungsbeschaffung
DGSE	Direction Générale de la Sécurité Extérieure	Generaldirektion für äussere Sicherheit
DGSI	Direction Générale de la Sécurité Intérieure	Generaldirektion für innere Sicherheit
DRM	Direction du Renseignement Militaire	Direktion des militärischen Nachrichtendiensts
DRPJ-PARIS	Direction Régionale de la Police de Paris	Regionale Polizeidirektion für Paris
DRSD	Direction du Renseignement et de la Sécurité de la Défense	Direktion für Nachrichtendienste und Sicherheit der Verteidigung
ICC/Polizei	Investigateur en Cyber-Criminalité	Ermittlungsstelle für Cyberkriminalität
OCLCTIC	Office Central de Lutte contre la Criminalité liée aux Technologies de l'information et de la Communication	Zentralstelle für die Bekämpfung von Informations- und Kommunikations-Kriminalität
SCRC	Service Central du Renseignement Criminel	Zentrales Kriminalamt
SDLC	Sous-Direction de la Lutte contre la Cybercriminalité	Abteilung zur Bekämpfung von Cyberkriminalität

Länderinformation Deutschland

1. Wichtige Strategiedokumente und Entwicklung



2. Organisation, wichtige Organe und Verantwortlichkeiten



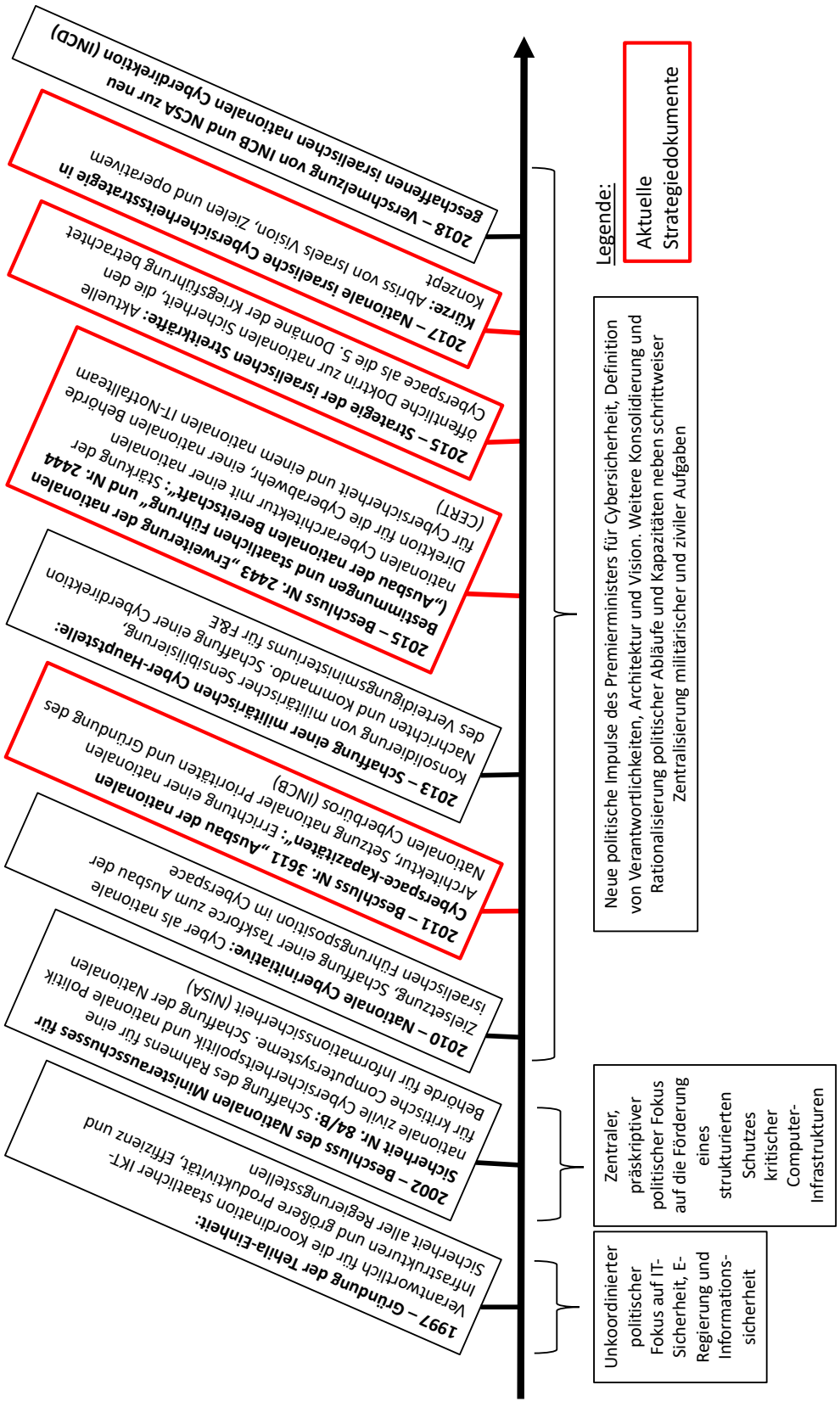
Cybersicherheit	Cyberkriminalität	Cyberabwehr	Nachrichtendienste
Kanzleramt: - Zentralstelle für Cyberabwehr und Sicherheitspolitik	**NCAZ:** - Gemeinsame Abwehrplattform verschiedener ziviler und militärischer Stellen - Teilung von Informationen - Sammlung von Nachrichten - Gefahrenabschätzung	**KdoCIR:** - Unterstützung des Schutzes kritischer Infrastrukturen - Entwicklung defensiver und offensiver Kapazitäten - Durchführung von Computer Network Operations (CNO) und Aufgaben der elektronischen Kriegsführung - Ermittlung bei Propaganda und Desinformation - Erfassung militärischer Nachrichten und Cyber-Gefahrenabschätzung	**BfV:** - Nachrichtendienst und Spionageabwehr - Aufrechterhaltung eines mobilen Einsatzteams
BSI: - Informationssicherheit und Schutz staatlicher IT - Operative Unterstützung und Reaktion auf Vorfälle - Erarbeitung der NCSS	**ZAC:** - Zentraler Ansprechpartner für Cyberkriminalität		**BND:** - Nachrichtendienst - Cyberspionage und Spionageabwehr
ZITis: - IT-Governance	**SO4 – Cybercrime:** - Ermittlung - Nationale und internationale Kooperationszentrale		
BBK: - Schutz kritischer Infrastrukturen - ÖPP mit Betreibern wichtiger kritischer Infrastrukturen			

3. Akronyme

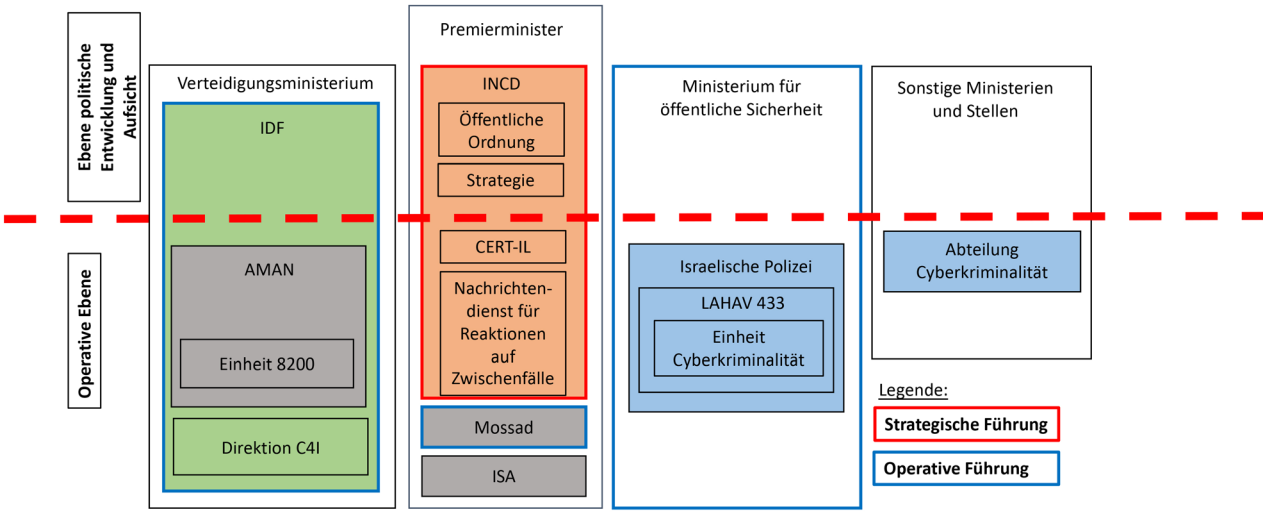
Akronym	Deutsch
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BMI	Bundesministerium des Inneren
BMVg	Bundesministerium der Verteidigung
BND	Bundesnachrichtendienst
BSI	Bundesamt für Sicherheit in der Informationstechnik
-	Bundeswehr
BWI	Bundeswehr Informationstechnik GmbH
CIT	Abteilung Cyber/ IT
Cyber-AZ	Nationales Cyber-Abwehrzentrum
KdoCIR	Kommando Cyber- und Informationsraum
NCAZ	Nationales Cyber-Abwehrzentrum
SO4-Cyber-crime	Gruppe SO 4 – Cybercrime der Abteilung Schwere und Organisierte Kriminalität (SO)
UP Kritis	Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen
ZAC	Zentrale Ansprechstelle Cybercrime
ZITis	Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Länderinformation Israel

1. Wichtige Strategiedokumente und Entwicklung



2. Organisation, wichtige Organe und Verantwortlichkeiten



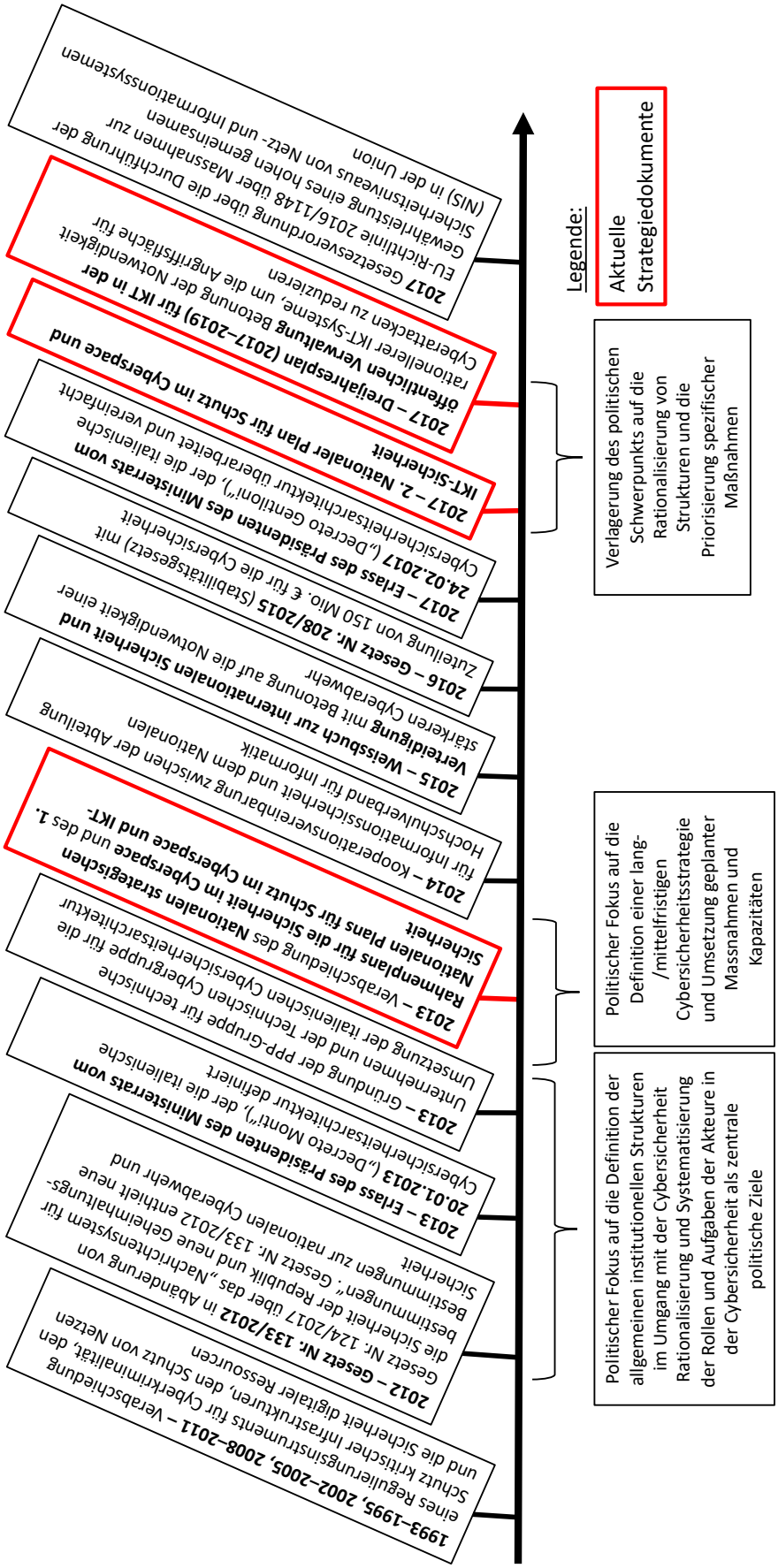
Cybersicherheit	Cyberkriminalität	Cyberabwehr	Nachrichtendienste
INCD: - Entwicklung, Koordination und Implementierung der NCSS - Durchführung und Implementierung operativer ziviler Abwehraktionen - Beratung des Premierministers und anderer Behörden - Schutz kritischer Informationsinfrastrukturen	**LAHAV 433:** - Ermittlung, Bekämpfung und Prävention von Cyberkriminalität - Entwicklung digitaler forensischer Expertise und Kapazitäten - Strafrechtliche Erkenntnisgewinnung - Technische Unterstützung für Polizeieinheiten und Ermittler	**Direktion C4I:** - Koordination und Durchführung defensiver, proaktiver und offensiver Cyberoperationen - Koordination von Cyberabwehr-Initiativen der IDF - Schutz eigener Infrastrukturen, Systeme und Netze - Förderung und Erweiterung von Bildung, Information und Fertigkeiten im Umfeld der Cyberabwehr	**AMAN:** - Erfassung und Verarbeitung militärischer Nachrichten - Durchführung von Kriegsoperationen im Cyberspace (Einheit 8200)
CERT-IL: - Management von Zwischenfällen - Austausch von Nachrichten - Best Practice für Cybersicherheit - Sensibilisierung - Ansprechpartner bei Bedrohungen			**ISA:** - Innere Sicherheit und Nachrichten - Spionageabwehr und Spionage
			Mossad: - Nachrichtendienst - Geheime Operationen, Terrorismusabwehr

3. Akronyme

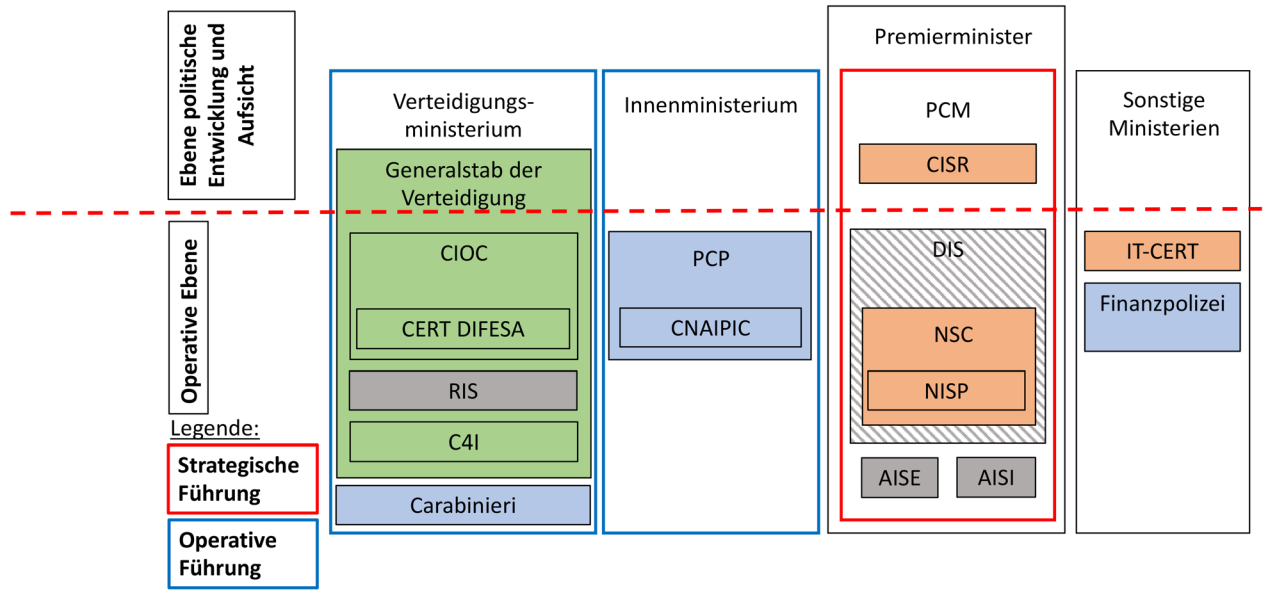
Akronym	Hebräisch	Deutsch
AMAN	Agaf HaModi'in	Direktion des militärischen Nachrichtendiensts
CERT-IL		Nationales CERT (IT-Notfallteam) Israels
IDF	Tsva ha-Hagana le-Yisra'el	Israelische Streitkräfte
INCB		Nationales Cyberbüro
INCD	Ma'arach	Nationale Cyberdirektion Israels
ISA	Shabak/Shin Beth	Israelische Agentur für Innere Sicherheit
Maf'at	Maf'at	Verwaltung für die Rüstungsentwicklung und technische Infrastruktur
Mossad	HaMossad leModi'in uleTafkidim Meyuhadim	Geheimdienst und Stelle für Sonderoperationen
NCSA		Nationale Behörde für Cybersicherheit

Länderinformation Italien

1. Wichtige Strategiedokumente und Entwicklung



2. Organisation, wichtige Organe und Verantwortlichkeiten



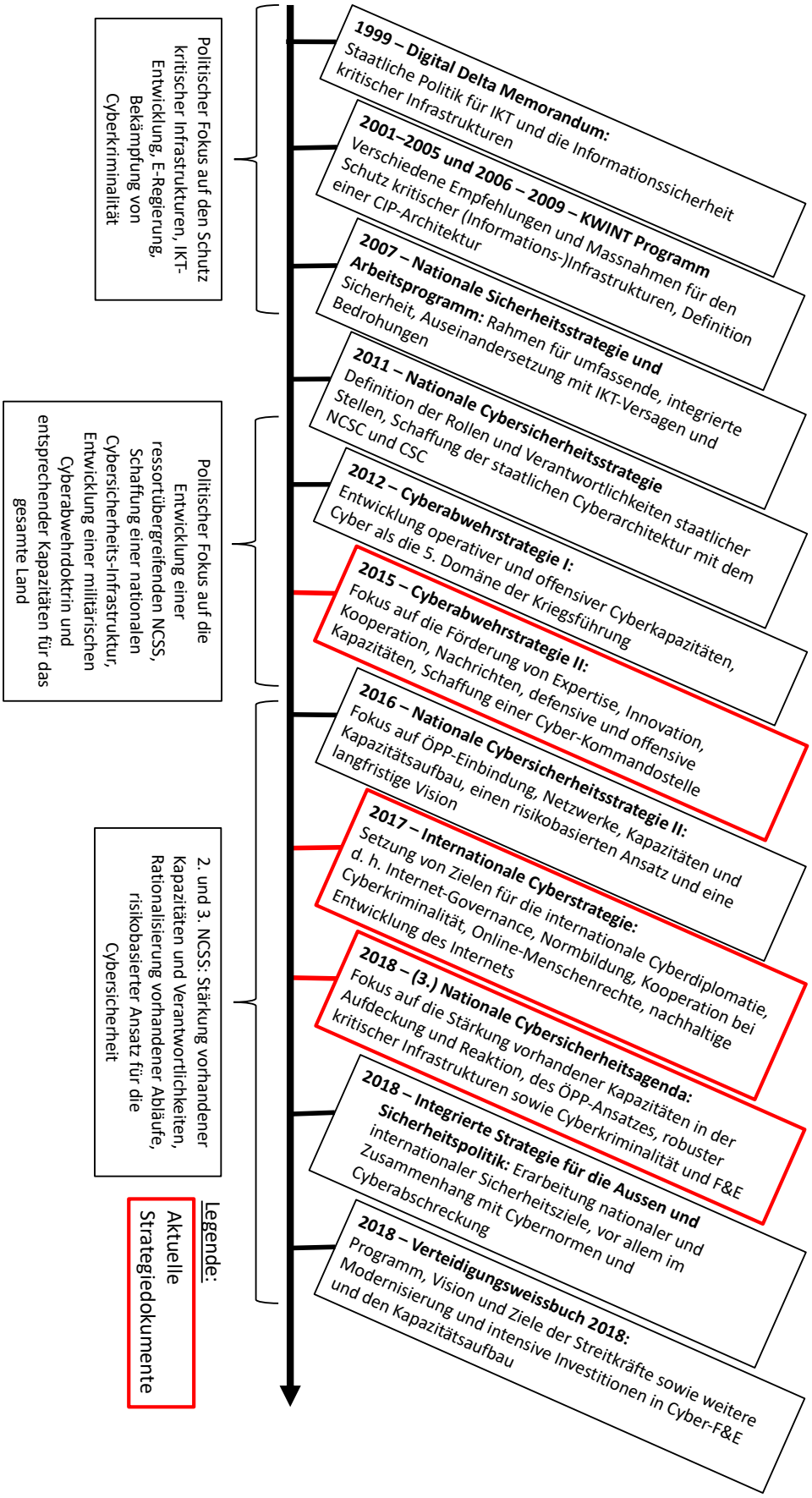
Cybersicherheit	Cyberkriminalität	Cyberabwehr	Nachrichtendienste
NSC: - Koordination staatlicher Initiativen - Prävention, Risikobewertung, Risikominderung, Reaktion auf Vorfälle und Krisenmanagement	**PCP:** - Bekämpfung, Ermittlung und Verhinderung von Cyber- und Onlinekriminalität - Abschätzung von Cyberkriminalität und Bedrohungen - Funktion als nationale und internationale Kooperationszentrale - Schutz kritischer Infrastrukturen	**CIOC:** - Schutz militärischer Netze, Dienste und Infrastrukturen - Entwicklung defensiver und offensiver Cyberkapazitäten - Lagebilder zur Cyberabwehr, Bedrohungsabschätzung - Reaktion auf Krisen	**DIS:** - Koordination und Austausch von Nachrichten - Gefahrenabschätzung - Sensibilisierung, Bildung, Information - Nationaler Ansprechpartner für Cybervorfälle
PCM: - Kollegialbehörde für Sicherheitspolitik - Entwicklung, Koordination und Begleitung der NCSS	**Carabinieri:** - Ermittlung von Telematik-Kriminalität	**C4I:** - Operative Planung und Cyberoperationen - Kommando, Kontrolle, Telekommunikationen und IKT	**RIS:** - Militärischer Nachrichtendienst und militärische Gegenspionage
CISR: - Beratung zu legislativen Fragen und Best Practice - Förderung von Zusammenarbeit, Informationsaustausch und ÖPP			**AISE/AISI:** - Äusserer/innerer Nachrichtendienst und Gegenspionage

3. Akronyme

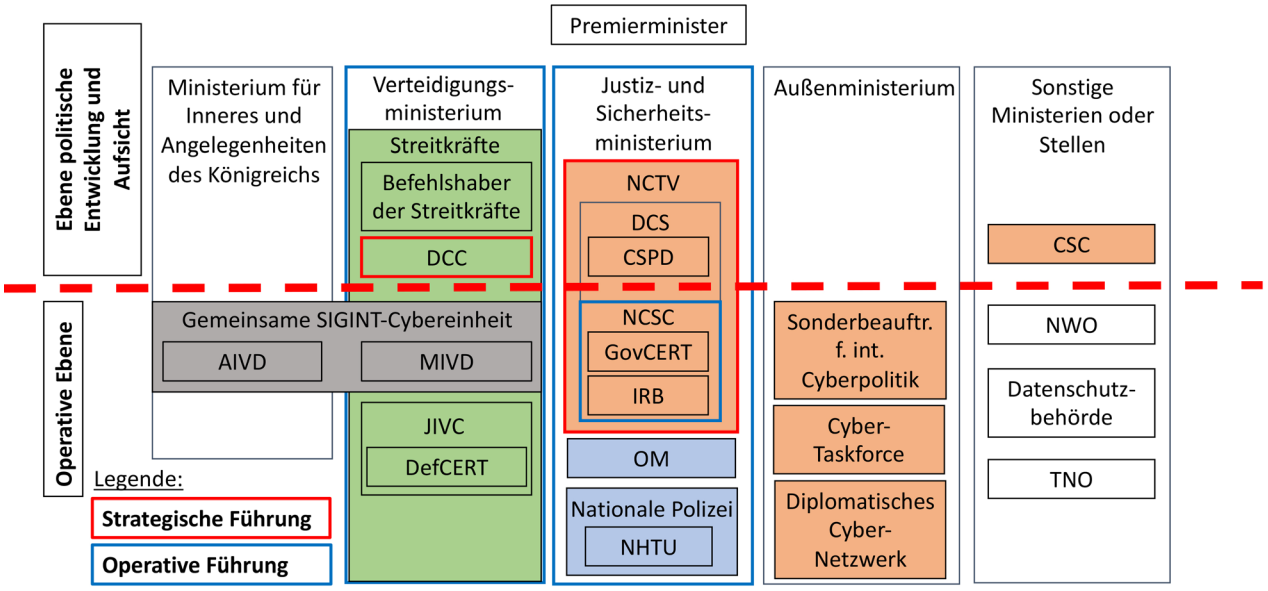
Akronym	Italienisch	Deutsch
AISE	Agenzia Informazioni e Sicurezza Esterna	Agentur für äussere Sicherheit und Nachrichten
AISI	Agenzia Informazioni e Sicurezza Interna	Agentur für innere Sicherheit und Nachrichten
C4I	Comando C4 Difesa	Abteilung für Kommando, Kontrolle, Kommunikation, Computer- und Informationssysteme
CERT-DIFESA	Computer Emergency Response Team per le Forze Armate	CERT (IT-Notfallteam) für die Streitkräfte
CERT-N	Computer Emergency Response Team Nazionale	Italienisches CERT (IT-Notfallteam)
CERT-PA	Computer Emergency Response Team per la Pubblica Amministrazione	CERT (IT-Notfallteam) für die öffentliche Verwaltung
CIOC	Comando Interforze Operazioni Cibernetiche	Gemeinsames Kommando für kybernetische Operationen
CISR	Comitato Interministeriale per la Sicurezza della Repubblica	Interministerieller Ausschuss für die Sicherheit der Republik
CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche	Nationales Antikriminalitäts-Informationszentrum zum Schutz kritischer Infrastrukturen
DIS	Dipartimento delle Informazioni per la Sicurezza	Abteilung für Informationssicherheit
IT-CERT		Italienisches CERT (IT-Notfallteam)
NSC	Nucleo per la Sicurezza Cibernetica	Cybersicherheitseinheit
NP cyber	Piano nazionale per la protezione cibernetica e la sicurezza informatica	Nationaler Plan für Schutz im Cyberspace und IKT-Sicherheit
PCP	Polizia Postale e delle Comunicazioni	Post- und Kommunikationspolizei
PCM	Presidenza del Consiglio dei ministri	Präsident des Ministerrats
NISP	Nucleo Interministeriale Situazione e Pianificazione	Interministerielle Lage- und Planungsstelle
RIS	Reparto Informazioni e Sicurezza	Informations- und Sicherheitsabteilung

Länderinformation Niederlande

1. Wichtige Strategiedokumente und Entwicklung



2. Organisation, wichtige Organe und Verantwortlichkeiten



Cybersicherheit	Cyberkriminalität	Cyberabwehr	Nachrichtendienste
NCTV: - Nexus für Sicherheitspolitik - Gefahrenabschätzung - Policy-Cluster - Förderung der Widerstandsfähigkeit gegen Cyberattacken	**NHTU:** - Prävention, Ermittlung und strafrechtliche Verfolgung gewöhnlicher, High-Tech- und Online-Kriminalität - Nationale und internationale Kooperationszentrale - ÖPP für den Informationsaustausch mit dem Finanz- und Privatsektor	**DCC:** - Koordination von Cyberoperationen, Nachrichten und Entwicklung defensiver/offensiver Kapazitäten - Förderung und Management von Cyber-Expertise und -Information in den Streitkräften	**AIVD/MIVD – Joint Cyber SIGINT:** - Gegenspionage - Cyberspionage und Spionageabwehr - Militärischer Nachrichtendienst, Abschätzung von Cyberbedrohungen
NCSC: - Operative Koordination und Unterstützung im Krisenfall - Zentrale für Information, Beratung und Expertise			
CSC: - ÖPP mit Beratungs- und Aufsichtsfunktionen über die NCSS - Sensibilisierung, Forschung und Entwicklung		**JIVC** - Schutz und Überwachung von militärischen Netzen, IT-Diensten und -Systemen - Beurteilungen der Widerstandsfähigkeit/ Anfälligkeit - Reaktion auf Krisen	

3. Akronyme

Akronym	Niederländisch	Deutsch
AIVD	Algemene Inlichtingen- en Veiligheidsdienst	Allgemeiner Nachrichten- und Sicherheitsdienst
CSC	Cyber Security Raad	Rat für Cybersicherheit
CSPD	-	Abteilung für Cybersicherheitspolitik
DCS	-	Direktion für Cybersicherheit
DCC	Defensie Cyber Commando	Defensive Cyber-Kommandostelle
DefCERT	-	Niederländisches Verteidigungs-CERT (IT-Notfallteam)
NCSC	Nationaal Cyber Security Centrum	Nationales Zentrum für Cybersicherheit
IRB	-	Ausschuss für IKT-Einsätze
JSCU	-	Gemeinsame SIGINT-Cybereinheit
JIVC	Joint IV Commando	Gemeinsame Organisation für Informationsmanagement
MIVD	Militaire Inlichtingen- en Veiligheidsdienst	Militärischer Nachrichten- und Sicherheitsdienst
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid	Nationaler Koordinator für Sicherheit und Terrorismusbekämpfung
NHTU	-	Nationale Stelle zur Bekämpfung von High-Tech-Kriminalität
NWO	Nederlandse Organisatie voor Wetenschappelijk Onderzoek	Niederländische Organisation für Wissenschaft und Forschung
OM	Openbaar Ministerie	Staatsanwaltschaft
TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek	Niederländische Organisation für angewandte wissenschaftliche Forschung

CSS
ETH Zurich

Das **Center for Security Studies (CSS) der ETH Zürich** ist ein Kompetenzzentrum für schweizerische und internationale Sicherheitspolitik. Es bietet sicherheitspolitische Expertise in Forschung, Lehre und Beratung. Das CSS fördert das Verständnis für sicherheitspolitische Herausforderungen. Es arbeitet unabhängig, praxisrelevant und wissenschaftlich fundiert.