April 2019 · Dr. Sven Herpig und Clara Bredenbrock

Cybersicherheits-politik in Deutschland

Akteure, Aufgaben und Zuständigkeiten.

Im Fokus: Das Cyber-Abwehrzentrum

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Inhalt

1. Hintergrund

Der erste Grundstein für die deutsche Cyber-Sicherheitsarchitektur wurde bereits 1986 gelegt. In diesem Jahr wurde in der Vorgängerorganisation des Bundesamts für Sicherheit in der Informationstechnik (BSI), der Zentralstelle für das Chiffrierwesen (ZfCh), "[...] eine Arbeitsgruppe aufgebaut, die sich vor dem Hintergrund der schnellen Entwicklung der IuK-Technik mit den Sicherheitsfragen beschäftigte"[1]. Am 1. Januar 1991 nahm das Bundesamt für Sicherheit in der Informationstechnik nach Ausgründung aus dem Bundesnachrichtendienst (BND) seine Arbeit auf.

In den öffentlichen Fokus geriet die staatliche Sicherheitsarchitektur dann insbesondere im Jahr 2011 durch die Veröffentlichung der Cyber-Sicherheitsstrategie für Deutschland[2]. Hierbei lag das Augenmerk vor allem auf dem neu zu schaffenden Nationalen Cyber-Abwehrzentrum (Cyber-AZ/NCAZ). Seitdem hat sich einiges getan: Cyber-Sicherheit ist für die Sicherheitspolitik in Deutschland ein elementarer Bestandteil geworden, weswegen einige neue Akteure hinzu gekommen sind. Hierzu zählen die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) und die Agentur für Innovation in der Cybersicherheit (ADIC). Jedoch gab es auch in der aktualisierten Version der Cyber-Sicherheitsstrategie für Deutschland 2016[3] keine grafische oder anderweitige Übersicht über die immer komplexer werdende Architektur deutscher Behörden im Cyber-Raum. Für eine effektive und effiziente deutsche Aufstellung im Cyber-Raum ist, gerade auch vor dem Hintergrund begrenzter Ressourcen[4], eine strukturierte politische Herangehensweise unverzichtbar.

Aus diesem Grund wollen wir im Rahmen unserer Arbeit zu Cyber-Sicherheitspolitik an der Stiftung Neue Verantwortung hierzu einen Beitrag leisten. In dieser Veröffentlichung stellen wir eine grafische Abbildung der staatlichen Cyber-Sicherheitsarchitektur, ein Abkürzungs- und Akteursverzeichnis sowie eine Erklärung der Verbindungen einzelner Akteure vor. Bis auf wenige Ausnahmen werden tiefergehende Länder- und Kommunalstrukturen, die internationale Ebene (UN, NATO, EU, etc.) sowie Akteure der Privatwirtschaft, Wissenschaft und Zivilgesellschaft nicht berücksichtigt. Am Ende der Publikation wird dem Cyber-Abwehrzentrum noch eine etwas detailliertere Analyse gewidmet.

Das Dokument wird auch zukünftig periodisch aktualisiert, um den neuesten Entwicklungsstand abzubilden. Die nächste Aktualisierung findet im Q3/2019 statt. Wir freuen uns daher über jeden Hinweis. Änderungs- und Er-

gänzungsvorschläge nimmt Dr. Sven Herpig gerne entgegen.

Die Verknüpfungen in der Visualisierung repräsentieren unterschiedliche Beziehungsaspekte und rangieren von der Entsendung von Mitarbeiter:innen in die verknüpfte Organisation über eine Mitgliedschaft im Beirat sowie finanziellen Zuwendungen bis hin zur Fach- und Rechtsaufsicht. Die Farben haben keine Bedeutung und dienen lediglich zur besseren Lesbarkeit.

Die erste Fassung dieser Veröffentlichung ist das Ergebnis der Arbeit von Dr. Sven Herpig und Tabea Breternitz.

2. Das Nationale Cyber-Abwehrzentrum

Politische Rahmenbedingungen

Die Gründung des „Nationalen Cyber-Abwehrzentrums“ (Cyber-AZ) wurde im Rahmen der 2011 verabschiedeten Cyber-Sicherheitsstrategie beschlossen.[5] Es handelt sich dabei um eine Informations- und Kooperationsplattform verschiedener Behörden mit dem Ziel, über eine intensivierte Zusammenarbeit Cyberangriffen vorzubeugen und ihnen entgegenzuwirken.[6] Das Cyber-AZ mit Sitz im Bundesamt für Sicherheit in der Informationstechnik (BSI) mit Sitz in Bonn ist keine eigenständige Behörde, sondern ein Zusammenschluss mehrerer Behörden. Diese tauschen sich zwar miteinander über die operative Cybersicherheit in Deutschland aus, verbleiben dabei aber jeweils in ihren Zuständigkeitsbereichen.[7] Die Art der Zusammenarbeit ist über Verwaltungsvereinbarungen zwischen den Behörden geregelt.[8] Diese Vereinbarungen können nach Anfragen gemäß Informationsfreiheitsgesetz (IFG)[1] online eingesehen werden.[9]

In dem 2013 geschlossenen Koalitionsvertrag vereinbarten CDU/CSU und SPD, die Kapazitäten des Cyber-AZ auszubauen. Auf Details, wie dieser Ausbau aussehen könnte, wurde jedoch erst in der Cyber-Sicherheitsstrategie für Deutschland 2016 eingegangen. Hier heißt es: *“Als ressortgemeinsame Institution wird es unter Federführung des Bundesministeriums des Innern zur zentralen Kooperations- und Koordinationsplattform fortentwickelt. Das Cyber-AZ soll zukünftig mit eigenen Bewertungs- und Auswertungsfähigkeiten ausgestattet sein und über ein aktuelles Cyber-Lagebild verfügen, das die Cyber-Sicherheitslage in Deutschland widerspiegelt.”* Inwiefern dieses Vorhaben umgesetzt wurde, ist mit den öffentlich verfügbaren Informationen schwer einzuschätzen. In der Cyber-Sicherheitsstrategie 2016 wurde auch erstmals explizit die Einbindung der Länder erwähnt. In den Koalitionsverhandlungen 2017 kam das Thema erneut auf, der 2018 beschlossene Koalitionsvertrag bleibt jedoch sehr allgemein in seinen Forderungen. Das BSI solle gestärkt werden und ebenso die *“Sicherheitsbehörden bei der Verfolgung und Prävention von Cyberkriminalität [durch die] Schaffung notwendiger rechtlicher, organisatorischer sowie technischer Rahmenbedingungen”*.[10] Die Forderung nach einer Stärkung des Cyber-Abwehrzentrums kam erst Anfang des Jahres 2019 wieder auf, nachdem im Januar private Daten, unter anderem von Mitgliedern des Bundestags, veröffentlicht wurden.[11]

1 Spezieller Dank gebührt Anna Biselli und Andre Meister für die IFG-Anfragen.

Aufbau und Arbeitsweise

Im Cyber-AZ arbeiten Vertreter:innen des Bundesamts für Sicherheit in der Informationstechnik (BSI), des Bundesamts für Verfassungsschutz (BfV), des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK), des Bundeskriminalamts (BKA), der Bundespolizei, des Zollkriminalamts, des Bundesnachrichtendienstes (BND), der Bundeswehr (Bw), des Bundesamts für den Militärischen Abschirmdienst (BAMAD), und der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zusammen. Die Behörden werden durch Verbindungspersonen im Cyber-AZ repräsentiert, die sich entweder dauerhaft oder anlassbezogen vor Ort befinden.[12] Das BSI stellt mit acht Mitarbeiter:innen den größten Teil der Ressourcen.[13] Die aufsichtführenden Betreiber der Kritischen Infrastrukturen (KRITIS) sind ebenfalls Teil des Cyber-AZ. Sprecher des Cyber-AZ ist BSI-Präsident Arne Schönbohm. In seiner Struktur ist das Cyber-AZ an das Gemeinsame Terrorabwehrzentrum angelehnt.[14]

Die Zusammenarbeit der Behörden im Cyber-AZ ist geprägt von seinem Selbstverständnis als Informations- und Kooperationsplattform. Die beteiligten Behörden bringen Erkenntnisse und Perspektiven aus ihren jeweiligen Fachgebieten ein, um Cyberangriffe bereits in einem frühen Stadium zu vermeiden. Sie tauschen sich über Schwachstellen in IT-Produkten, Verwundbarkeiten, Angriffsformen und Täterbilder aus.[15] Über den Informations- und Wissensaustausch können Risiken im Cyberraum ganzheitlich analysiert und bewertet werden. Am Ende dieses Prozesses steht dann eine konkrete Handlungsempfehlung, die auf den Erfahrungen und Kenntnissen der beteiligten Behörden beruht. Produkte, die das Cyber-AZ regelmäßig erarbeitet, sind einerseits die “Cyber-Lage”, ein tagesaktueller Lagebericht zum Thema Cybersicherheit, einen jährlich erscheinenden Tätigkeitsbericht, sowie Analysen konkreter Sachverhalte.[16] Dem Cyber-Sicherheitsrat (Cyber-SR) legt das Cyber-AZ in regelmäßigen Abständen anlassbezogene Empfehlungen vor.[17] Bei den Analysen des Cyber-AZ werden sowohl nachrichtendienstliche als auch polizeiliche Informationen einbezogen.[18]

Arbeitsweise und Struktur des Cyber-AZ haben sich seit seiner Gründung im Jahr 2011 weiterentwickelt.[19] Die Formen der Zusammenarbeit erstrecken sich von täglichen Lagebesprechungen über Arbeitsgruppen und -kreise bis Projektgruppen und Workshops – je nach Bearbeitungsdauer und Beschaffenheit der Themengebiete.[20] Die zu Beginn vorherrschende Struktur von assoziierten und Kernbehörden (Schalenmodell) wurde nach einiger Zeit, mit zunehmender Entwicklung hin zu einer Kooperationsplattform, aufgelöst.[21]

Ein Lenkungskreis entscheidet über thematische Schwerpunkte der Arbeit und richtet die verschiedenen Arbeitsgruppen ein.[22]

Dem Cyber-Abwehrzentrum kommt eine bedeutende Rolle in der Cybersicherheitsarchitektur Deutschlands zu. Ähnlich wie der Cyber-Sicherheitsrat auf politisch-strategischer Ebene relevante Akteure zusammenbringt, bietet das Cyber-AZ eine behördenübergreifende Plattform für die operative Zusammenarbeit. Da die deutsche Cybersicherheitsarchitektur nicht auf dem Reissbrett geplant wurde, erfüllt es damit eine essenzielle Funktion bezüglich der Koordinierung und Kommunikation zwischen der Vielzahl an Behörden, die in Deutschland für Cybersicherheit sorgen sollen. Vor Schaffung des Cyber-Abwehrzentrums gab es das in dieser Form nicht.[23]

Kritik

Die bisherige Kritik an dem Cyber-AZ setzt sowohl an seinen Produkten (Lagebericht, Analysen ...) als auch an dem Zusammenschluss selbst an. In der Kooperation verschiedener Behörden wird eine Vermischung polizeilicher und nachrichtendienstlicher Tätigkeiten und damit ein Verstoß gegen das Trennungsgebot von Polizei und Geheimdiensten gesehen.[24] Weiterhin wurde in einem internen Bericht des Bundesrechnungshofs im Jahr 2014 scharfe Kritik gegenüber dem Cyber-AZ geäußert. Nicht nur sei die Plattform mit unzureichenden Kapazitäten ausgestattet, um die formulierten Ziele zu erfüllen, es sei auch fraglich, was das Ergebnis der Zusammenarbeit ist. Zudem fehle es an Handlungskompetenzen und es sei unklar, was im Falle eines Cyberangriffs tatsächlich geschehe.[25] Die geäußerte Kritik ist nicht zuletzt der Tatsache geschuldet, dass das Cyber-AZ seit seiner Gründung nicht nur die unterschiedlichen Erwartungshaltungen der beteiligten Behörden zu vereinen versucht, sondern auch deren unterschiedliche Arbeitsweisen, "Kulturen" und den jeweiligen Grad der Bereitwilligkeit, ihr Wissen zu teilen.[26] Konträre Herangehensweisen im Umgang mit Cyberangriffen (unter anderem "Beratungskultur" versus "Verfolgungskultur"[27]) erschweren eine reibungslose Zusammenarbeit ebenso wie eine verhaltene Bereitschaft, eigene Kenntnisse und Informationen zu teilen.

Mit Blick auf die Strukturen und die Außenwirkung wurde zudem der große Einfluss des BSI auf das Cyber-AZ kritisiert. Nicht nur stellt das Amt einen großen Teil der Mitarbeiter:innen, häufiger Kritikpunkt war auch die Einseitigkeit des Inputs. BfV und BBK haben nach eigener Auskunft nur wenig Informationen eingebracht; etwa 98% stammten zu Beginn vom BSI.[28] Es ist fraglich, ob dies allein dem BSI zum Vorwurf gemacht werden kann, jedoch

verdeutlicht es das Verbesserungspotenzial des Cyber-AZ in seiner Funktion als Informations- und Austauschplattform.

In der Gesamtschau dieser Kritikpunkte wird deutlich, dass die behördenübergreifende Zusammenarbeit im Cyber-AZ einen Spagat zwischen der Einhaltung des Trennungsgebots einerseits und einem effektiven und ausbalancierten Informationsfluss andererseits meistern muss.[29]

Letztlich stellte sich auch wiederholt die Frage nach der Zusammenarbeit mit und Abgrenzung zu anderen Einrichtungen innerhalb des BSI, wie dem CERT-Bund und dem IT-Lagezentrum.[30] Da diese Institutionen bereits an ähnlichen Themen arbeiten, wurde befürchtet, dass es hier zu unnötigen Dopplungen der Arbeit kommen könnte.[31] Klarer Schwerpunkt von Lagezentrum und CERT ist es jedoch, unmittelbar und konkret auf Vorfälle zu reagieren, die Situation zu bewältigen und die technische Sicherheit wiederherzustellen. Das Cyber-AZ hingegen konzentriert sich eher auf Informationsaustausch und Maßnahmenkoordinierung.[32]

Das Cyber-Abwehrzentrum Plus

Seit der Gründung des Cyber-AZ hat sich die Gefahren- und Behördenlandschaft weiterentwickelt. Es ist deshalb folgerichtig, dass das Cyber-Abwehrzentrum zu einem Cyber-Abwehrzentrum+ (Plus) ausgebaut werden soll.[33] Sowohl die geplante stärkere Anbindung an die Länderebene, als auch die bedarfsgerechte Zusammenarbeit mit ausgewählten Firmen sind sinnvolle Strategien. Ersteres könnte auch dem Vorhaben mancher Bundesländer, eigene Landesämter für Sicherheit in der Informationstechnik (LSI) zu errichten, entgegenwirken. Während Computer Emergency Response Teams (CERTs) auf Länderebene einen wichtigen (technischen) Dreh- und Angelpunkt für IT-Sicherheit darstellen, droht der Aufbau von eigenständigen LSIs den ohnehin schon problematischen Fachkräftemangel in der öffentlichen Verwaltung[34] weiter zu verschärfen und Parallelstrukturen zu schaffen.

Eine Erweiterung des Cyber-AZ ist dann am zielführendsten, wenn das Cyber-AZ weiterhin beim Bundesamt für Sicherheit in der Informationstechnik verankert bliebe, welches qua gesetzlicher Grundlage “die zentrale Meldestelle für die Zusammenarbeit der Bundesbehörden in Angelegenheiten der Sicherheit in der Informationstechnik”[35] ist. Die bisher geringen personellen Ressourcen des Cyber-AZ werden durch die breite und tiefe technische Expertise der Fachkräfte im BSI, auf die Zugriff besteht, aufgewogen. Gleichzeitig beherbergt das BSI mit dem Nationalen IT-Lagezentrum, welches im

Krisenfall zum IT-Krisenreaktionszentrum anwächst, das zentrale Element für die technische Bearbeitung und Koordinierung von IT-Sicherheitsvorfällen.

Aktuell werden verschiedene Modelle und Anbindungen des Cyber-AZ+ diskutiert. Gegen eine Angliederung des Cyber-AZ+ an Bundeswehr, Geheimdienste oder Polizeien spricht nicht nur die dort weniger ausgeprägte Fachkenntnis, sondern auch der mögliche Vertrauensverlust seitens wichtiger Kooperationspartner in der Industrie, der Wissenschaft, der Gesellschaft und sogar unter den Behörden. Die kulturellen und rechtlichen Rahmenbedingungen der Polizeien und Nachrichtendienste können herausfordernd sein. Wenn Polizeien Informationen zu einer Straftat erlangen, müssen sie unmittelbar Ermittlungen einleiten (Legalitätsprinzip), im nachrichtendienstlichen Bereich werden Informationen hingegen oft zurückgehalten, um die Aufklärung oder Gegenspionage zu ermöglichen. Auf das BSI treffen keine der beiden Aspekte zu, das dortige Leitbild ist die Stärkung der IT-Sicherheit. Eine mögliche Angliederung des Cyber-AZ+ an die Bundeswehr scheidet schon allein deswegen aus, da bisher kein Cyberangriff auf Deutschland die Schwelle für eine militärische Reaktion überschritten hat. Das BSI steht für die Gewährleistung von technischer IT-Sicherheit und wäre demnach weiterhin prädestiniert als erste Anlaufstelle des Cyber-AZ+. Cybersicherheitspolitik wurde in Deutschland bisher vor allem durch den Fokus auf IT-Sicherheit und einer strikten Trennung der zivilen und militärischen Domäne geprägt. Die Priorität sollte nach wie vor darin bestehen, IT-Systeme und Netzwerke zu schützen, statt Aufklärung, Strafverfolgung oder anderweitige repressive Maßnahmen auszubauen.

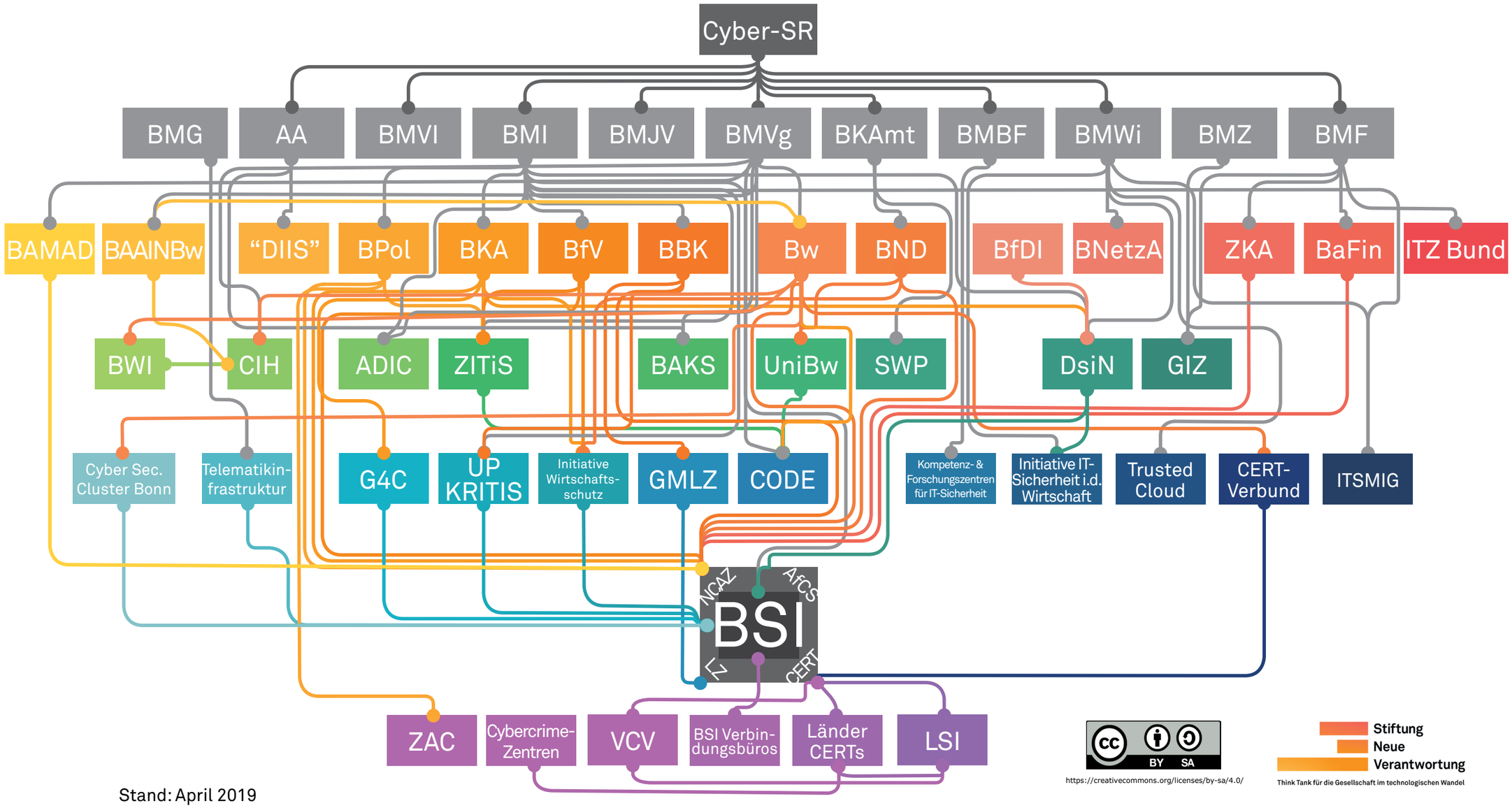
Die Erweiterung zu einem Cyber-Abwehrzentrum+ muss daher auch die am Cyber-AZ geäußerte Kritik berücksichtigen. Die Kritik ist in weiten Teilen nachvollziehbar und in einigen Bereichen sind die Probleme von der Bundesregierung hausgemacht. Die Benennung einer Informations- und Kooperationsplattform (Stand: bei der Gründung 2011) als “Abwehrzentrum” ruft in Verbindung mit der damaligen und aktuellen Ressourcen- und Aufgabenzuteilung unerfüllbare Erwartungen hervor. Dabei war es nie das Ziel dieser Institution, Cyber-Angriffe abzuwehren. Dafür gibt es in den jeweiligen Zuständigkeitsbereichen Behörden wie das Bundesamt für Sicherheit in der Informationstechnik, das Bundeskriminalamt, die Bundeswehr oder auch das Bundesamt für Verfassungsschutz. Sie alle sind Behörden, die im Cyber-AZ vertreten sind. Das tatsächliche Anliegen des Cyber-AZ war bisher in erster Linie, die wichtigen staatlichen Akteure an einen Tisch zu bringen, um den Austausch zwischen ihnen zu ermöglichen. Das ist eine zentrale Aufgabe, bei der schwer zu beurteilen ist, ob das Cyber-AZ ihr gerecht geworden ist.

Dieser Austausch kann aber auch kritisch betrachtet werden: Wie funktioniert diese Zusammenarbeit zwischen Behörden mit polizeilichen und nachrichtendienstlichen Befugnissen im Cyber-Abwehrzentrum unter Einhaltung des Trennungsgebotes im Detail? Dazu gibt es öffentlich keine Informationen. Mehr Transparenz über die konkrete Zusammenarbeit der Behörden im Cyber-Abwehrzentrum ist hier zwingend notwendig.

Fazit und rechtliche Verankerung

Analog zur Gründung der Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITiS)[36], gibt es auch für das Cyber-Abwehrzentrum bisher kein Errichtungsgesetz. Die Vertreter:innen der im Cyber-Abwehrzentrum vertretenen Behörden handeln auf Basis der Rechtsgrundlage ihrer jeweiligen Behörden. Die Fach- und Rechtsaufsicht sowie die etwaige parlamentarische und juristische Kontrolle gestalten sich analog. Die nötigen Zuständigkeiten und Befugnisse liegen schon jetzt bei den entsprechenden Behörden, sodass diese Fragen in einem Errichtungsgesetz nicht erst geklärt werden müssten. Der Schwerpunkt des Errichtungsgesetzes wäre daher die Verankerung des Cyber-AZ+ und die strukturelle Zusammenarbeit der verschiedenen Behörden (unter anderem Art, Umfang und Modus Operandi des Informationsaustausches). Eine solche Ausgestaltung des Errichtungsgesetzes würde vermutlich eine Grundgesetzesänderung voraussetzen (z. B. Verlagerung der Gefahrenabwehr im Cyberraum von Landes- auf Bundesebene). Auch zur Förderung der Transparenz und Einbettung des Cyber-Abwehrzentrums in die bestehende Kontrollarchitektur des Bundes wäre es sinnvoll, eine entsprechend klare Rechtsgrundlage für dieses Exekutivhandeln zu schaffen. Auch würde das dazu beitragen, dass die Öffentlichkeit besser versteht, worin die Rolle des Cyber-AZ liegt und woran man dort arbeitet – was wiederrum dessen Akzeptanz stärken würde. Dies ist vor allem dann wichtig, wenn die Zusammenarbeit mit Akteuren aus Industrie und Ländern im Rahmen der Cyber-AZ+ Konzeption ausgebaut werden soll und damit das Cyber-AZ seiner wichtigen Rolle im Herzen der deutschen Cybersicherheitsarchitektur sinnvoll nachkommen kann.

Staatliche Cybersicherheitsarchitektur



Stand: April 2019

Stiftung Neue Verantwortung
Think Tank für die Gesellschaft im technologischen Wandel

4. Akteure und Abkürzungen

AA	Auswärtiges Amt
ADIC	Agentur für Innovation in der Cybersicherheit
AfCS/ACS	Allianz für Cyber-Sicherheit
BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAKS	Bundesakademie für Sicherheitspolitik
BAMAD	Bundesamt für den Militärischen Abschirmdienst
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BKAmt	Bundeskanzleramt
BMBF	Bundesministerium für Bildung und Forschung
BMF	Bundesministerium für Finanzen
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern, für Bau und Heimat
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BMVg	Bundesministerium der Verteidigung
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BMWi	Bundesministerium für Wirtschaft und Energie
BMZ	Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung
BND	Bundesnachrichtendienst
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

BPol	Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik
BWI	Bundesweite IT-Systemhaus GmbH
Bw	Bundeswehr
CERT	Computer Emergency Response Team des Bundes (CERT-Bund) und Bürger-CERT
CERT-Verbund	
CIH	Cyber Innovation Hub
CODE	Forschungsinstitut Cyber Defence
Cybercrime-Zentren	*Cybercrime-Akteure in den Bundesländern, u. a. Hessen 3C und ZCB (Bayern)*
Cyber Security Cluster Bonn	Cyber Security Cluster Bonn e.V.
Cyber-SR	Cyber-Sicherheitsrat
DIIS	*Deutsches Institut für Internet Sicherheit / Deutsches Institut für Cyber-Sicherheit (in Planung)*
DsiN	Deutschland sicher im Netz e.V.
G4C	German Competence Centre against Cyber Crime
GIZ	Gesellschaft für Internationale Zusammenarbeit
GMLZ	Gemeinsames Melde- und Lagezentrum
Initiative IT-Sicherheit in der Wirtschaft	
Initiative Wirtschaftsschutz	
ITSMIG	IT Security made in Germany
ITZBund	Informationstechnikzentrum Bund
Kompetenz- und Forschungszentren für IT-Sicherheit	
Länder-CERTs	
LSI	Landesamt für Sicherheit in der Informationstechnik Bayern

LZ	Nationales IT-Lagezentrum
NCAZ / Cyber-AZ	Nationales Cyber-Abwehrzentrum
SWP	Stiftung Wissenschaft und Politik
Trusted Cloud	Kompetenznetzwerk Trusted Cloud
UniBw	Universität der Bundeswehr München
UP KRITIS	Umsetzungsplan Kritische Infrastrukturen
VCV	Verwaltungs-CERT-Verbund
ZAC	Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich
ZKA	Zollkriminalamt

5. Erläuterung

Agentur für Innovation in der Cybersicherheit (ADIC)
Die Einrichtung der Agentur für Innovation in der Cybersicherheit (ADIC) wurde im Koalitionsvertrag 2018 beschlossen. Sie wird unter der Federführung des BMI und BMVg sowie mithilfe eines IT-Sicherheitsfonds die "technologische Innovationsführerschaft" im Bereich der sicherheitsrelevanten Schlüsseltechnologien gewährleisten. Die Cyberagentur soll als Inhousegesellschaft gegründet werden und ihren Sitz in Leipzig/Halle haben.
Die ADIC wird unter Federführung des BMI und BMVg eingerichtet.[37]

Allianz für Cyber-Sicherheit (AfCS/ ACS)
Die Allianz für Cyber-Sicherheit (AfCS/ ACS) bietet einen vertrauensvollen Austausch zwischen den Mitgliedern und dem BSI zu Cyber-Bedrohungen, Schutzmaßnahmen und Vorfallsmanagement. Außerdem erhalten die Mitglieder Informationen zum Ausbau ihrer Cyber-Sicherheitskompetenzen. Mitglied kann jede Institution mit Sitz in Deutschland werden.
Die AfCS ist eine Public-Private-Partnership von BSI und BITKOM mit Wirtschaft, Behörden, Forschung und Wissenschaft.[38]

Auswärtiges Amt (AA)
Das Auswärtige Amt (AA) setzt sich im Rahmen seiner Cyber-Außenpolitik für internationale Cyber-Sicherheit, universelle Menschenrechte im digitalen Raum, sowie die Nutzung wirtschaftlicher Chancen durch die Digitalisierung ein. Dafür wurde 2011 der Koordinierungsstab für Cyber-Außenpolitik im Auswärtigen Amt geschaffen.
Das AA ist im Cyber-SR vertreten. Es strebt die Gründung des Deutschen Instituts für Internet Sicherheit (DIIS) an und stellt im Wechsel mit dem BMVg die Leitung der BAKS.[39]

Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw)
Hauptaufgabe des Bundesamtes für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) ist die Ausstattung des deutschen Militärs. Dies erfolgt sowohl durch Gerätschaften als auch durch IT-Systeme. Die Systeme werden teilweise vom BAAINBw eigenständig entwickelt, getestet und betrieben und in anderen Fällen in Auftrag gegeben. Es trägt somit Mitverantwortung dafür, die Bundeswehr bestmöglich vor Cyberangriffen zu schützen.
Das BAAINBw gehört zum Geschäftsbereich des BMVg. Es versorgt die Bw mit Ausrüstung und ist im Steuerungsboard des CIH vertreten.[40]

Bundesakademie für Sicherheitspolitik (BAKS)
Die Bundesakademie für Sicherheitspolitik (BAKS) ist die zentrale Weiterbildungsstätte des Bundes für Sicherheitspolitik. In unterschiedlichen Veranstaltungsformaten, wie z. B. dem "Berliner Forum zur Cyber-Sicherheit", setzt sie sich mit den sicherheitspolitischen Herausforderungen im digitalen Raum auseinander.
Die BAKS gehört zum Geschäftsbereich des BMVg. Präsident und Vizepräsident kommen abwechselnd aus BMVg und AA.[41]

Bundesamt für den Militärischen Abschirmdienst (BAMAD)
Das Bundesamt für den Militärischen Abschirmdienst (BAMAD) ist eine Bundesoberbehörde und der militärische Nachrichtendienst des Bundes. Im Rahmen von 2017 durchgeführten Umstrukturierungsmaßnahmen wurde der Militärische Abschirmdienst (MAD) als BAMAD direkt dem Bundesministerium der Verteidigung unterstellt. Zu den Aufgaben des dritten und kleinsten Nachrichtendienstes, neben dem Bundesnachrichtendienst (BND) und dem Bundesamt für Verfassungsschutz (BfV), zählen Extremismus- sowie Terrorismusabwehr sowie die Bekämpfung von (Cyber-) Spionage und Sabotage in der Bundeswehr.
Das BAMAD gehört zum Geschäftsbereich des BMVg und ist im Cyber-AZ vertreten.[42]

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
Die Aufgabe der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ist es ein funktionsfähiges, integres und stabiles Finanzsystem in Deutschland zu gewährleisten. Im Bereich der Wirtschaftskriminalität sieht die BaFin für Versicherer, Finanzdienstleister und Banken eine zunehmende Gefahr durch Cyber-Kriminalität.
Die BaFin gehört zum Geschäftsbereich des BMF und ist im Cyber-AZ vertreten.[43]

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) übernimmt eine wichtige Funktion im Gesamtkonzept der nationalen Sicherheitsarchitektur. In diesem Rahmen beschäftigt es sich zunehmend auch mit den Risiken von Cyber-Angriffen auf kritische Infrastrukturen. Das BBK ist im Cyber-AZ vertreten und sein Personal besetzt das Gemeinsame Melde- und Lagezentrum (GMLZ).
Die BBK gehört zum Geschäftsbereich des BMI und ist im GMLZ, UP KRITIS und Cyber-AZ vertreten.[44]

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Aufgabe die Sicherheit in der Informationstechnik des Bundes zu stärken. Als Behörde mit höchster technischer Expertise fördert es darüber hinaus die Informations- und Cyber-Sicherheit in Verwaltung, Wirtschaft und Gesellschaft durch zahlreiche Aktivitäten, Kooperationen und Initiativen. Um sich regional noch stärker zu vernetzen, baut das BSI aktuell deutschlandweit Verbindungsbüros auf.
Das BSI gehört zum Geschäftsbereich des BMI. In ihm beherbergt sind u.a. Cyber-AZ, AfCS, LZ, CERT-Bund und das Bürger-CERT.[45]

Bundesamt für Verfassungsschutz (BfV)
Das Bundesamt für Verfassungsschutz (BfV) untersucht, wie neue technische Möglichkeiten beispielsweise von Extremisten, Terroristen oder ausländischen Nachrichtendiensten genutzt werden, um in Deutschland Spionage, politische Desinformation oder Computersabotage zu betreiben. Das BfV versucht Cyber-Angriffe auf staatliche und private Einrichtungen abzuwehren und aufzuklären.
Das BfV gehört zum Geschäftsbereich des BMI. Es ist im Cyber-AZ und der Initiative Wirtschaftsschutz vertreten und greift auf die Expertise von ZITiS zurück.[46]

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) berät und kontrolliert die Daten- und Informationsverarbeitung der öffentlichen Stellen des Bundes, sowie nicht-öffentlicher Stellen. Sie ist in der Ausübung ihres Amtes unabhängig und unterliegt nur der parlamentarischen Kontrolle durch den Bundestag.
Die BfDI ist im Beirat der DsiN vertreten.[47]

Bundeskanzleramt (BKAmt)
Das Bundeskanzleramt (BKAmt) unterstützt den / die Bundeskanzler:in bei ihrer inhaltlichen Arbeit. Dazu unterhält es durch seine “Spiegelreferate” engen Kontakt zu den Bundesministerien. Mit Themen der Cyber-Sicherheit kommt es u. a. bei der Dienst- und Fachaufsicht des BND und der Finanzierung der SWP in Berührung.
Das BKAmt ist im Cyber-SR vertreten und ihm ist der BND nachgeordnet. Aus seinem Haushalt wird die institutionelle Zuwendung an die SWP gezahlt.[48]

Bundeskriminalamt (BKA)
Das Bundeskriminalamt (BKA) hat als Zentralstelle der deutschen Polizei sein Aufgabenfeld der nationalen Verbrechensbekämpfung auch auf den Cy-

ber-Raum ausgeweitet. Es klärt Straftaten im Cyber-Raum auf, ermittelt und versucht Cyber-Kriminalität vorzubeugen.
Das BKA gehört zum Geschäftsbereich des BMI. Es ist im Cyber-AZ, sowie im G4C und der Initiative Wirtschaftsschutz vertreten. Es ist im DsiN Beirat und greift auf die Expertise von ZITiS zurück.[49]

Bundesministerium der Justiz und für Verbraucherschutz (BMJV)
Das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) ist vor allem ein Gesetzgebungsministerium, das auch andere Bundesministerien bei ihren Rechtsetzungsvorhaben unterstützt. Innerhalb der Bundesregierung ist es für die wirtschaftliche Verbraucherpolitik zuständig. In diesem Rahmen beschäftigt es sich u. a. mit Themen wie dem Schutz von Bürgern und Onlinehändlern vor Cyber-Kriminalität oder Onlinemobbing.
Das BMJV ist im Cyber-SR vertreten.[50]

Bundesministerium der Verteidigung (BMVg)
Das Bundesministerium der Verteidigung (BMVg) ist für die militärische Verteidigung Deutschlands und somit auch für die Verteidigung Deutschlands im Cyber-Raum verantwortlich. Dafür setzt das BMVg auf nationale und internationale Kooperationen und Partnerschaften, zum Beispiel mit dem Cyber Innovation Hub oder dem Cooperative Cyber Defense Centre of Excellence der NATO. Im Ministerium ist die Abteilung Cyber- und Informationstechnik (CIT) für den Bereich Cyber-Verteidigung federführend zuständig.
Das BMVg ist im Cyber-SR vertreten. Ihm ist die Bw nachgeordnet und die BAKS gehört zu seinem Geschäftsbereich. ADIC soll unter Federführung des BMVg eingerichtet werden.[51]

Bundesministerium des Innern, für Bau und Heimat (BMI)
Das Bundesministerium des Innern, für Bau und Heimat (BMI) ist u. a. für die Sicherheit im Cyber-Raum zuständig. Die vom BMI vorgelegte "Cyber-Sicherheitsstrategie für Deutschland 2016" wurde im November 2016 vom Kabinett verabschiedet und bildet den ressortübergreifenden, strategischen Rahmen der Bundesregierung. Das BMI koordiniert die Umsetzung der Cyber-Sicherheitsstrategie durch den Bundesbeauftragten für Informationstechnik, der auch Vorsitzender des Cyber-Sicherheitsrates ist.
Das BMI ist im Cyber-SR vertreten. Seinem Geschäftsbereich sind BPol, BKA, BSI, BfV und BBK zugeordnet. Auf ein Erlass des BMI hin, wurde 2017 ZITiS gegründet. Das BMI ist in den Initiativen UP KRITIS, DsiN (Beirat), sowie der AfCS vertreten. ADIC soll unter Federführung des BMVg eingerichtet werden.[52]

Bundesministerium für Bildung und Forschung (BMBF)
Das Bundesministerium für Bildung und Forschung (BMBF) finanziert als Teil der Digitalen Agenda drei Kompetenzzentren für IT-Sicherheitsforschung. Mit dem CISPA (Saarbrücken), CRISP (Darmstadt) und KASTEL (Karlsruhe) soll die deutsche Forschungskapazität im Bereich der Cyber-Sicherheit nachhaltig erhöht werden.
Das BMBF ist im Cyber-SR vertreten und fördert die Kompetenzzentren für IT-Sicherheit.[53]

Bundesministerium für Finanzen (BMF)
Das Bundesfinanzministerium (BMF) ist vorrangig für die Steuer-, Haushalts- und Europäische Finanzpolitik zuständig. Es entwickelt zum Beispiel gemeinsam mit nationalen und internationalen Partnern Mindeststandards für die Cyber-Sicherheit in der Finanzdienstleistungsbranche.
Das BMF ist im Cyber-SR vertreten. Ihm nachgeordnet ist das ZKA und es hat außerdem die Rechts- und Fachaufsicht über die BaFin. BMZ und BMF sind Gesellschafter der GIZ.[54]

Bundesministerium für Gesundheit (BMG)
Das Bundesministerium für Gesundheit (BMG) ist vor allem für die Leistungsfähigkeit der Gesetzlichen Krankenversicherung sowie der Pflegeversicherung verantwortlich. Mit dem E-Health-Gesetz soll eine digitale Infrastruktur mit höchsten Sicherheitsstandards im Gesundheitswesen geschaffen werden.
Das BMG hat die gematik mit dem Aufbau einer Telematikinfrastruktur beauftragt, die Voraussetzung für eine sichere Vernetzung des Gesundheitswesens ist.[55]

Bundesministerium für Verkehr und digitale Infrastruktur (BMVI)
Das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) ist für die Verkehrsinfrastruktur, -planung, -sicherheit sowie die digitale Infrastruktur verantwortlich. Aufgrund der sich daraus ergebenden Verantwortung für die zivile Notfallvorsorge bzw. Gefahrenabwehr, entwickelt das BMVI seine Krisenszenarien auch hinsichtlich möglicher Cyber-Angriffe auf digitale Infrastrukturen weiter.
Das BMVI ist im Cyber-SR vertreten.[56]

Bundesministerium für Wirtschaft und Energie (BMWi)
Das Bundesministerium für Wirtschaft und Energie (BMWi) hat es sich zum Ziel gesetzt für Wirtschaft, Gesellschaft und Staat den Zugang zu einer sicheren und vertrauenswürdigen IT zu schaffen, damit diese von der Digitalisierung bestmöglich profitieren können. Das BMWi setzt sich dabei vor allem

für IT-Sicherheit in der Industrie 4.0 ein.
Das BMWi ist im Cyber-SR vertreten. Es hat die Initiative IT-Sicherheit in der Wirtschaft und Trusted Cloud ins Leben gerufen. Es ist im Beirat von DsiN vertreten; die BNetzA gehört zum Geschäftsbereich.[57]

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ)
Das Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ) ist für die Entwicklungszusammenarbeit der Bundesregierung verantwortlich. Dabei entwickelt das BMZ auch gesicherte IT-Lösungen für Partnerländer und unterstützt Cyber Capacity Building durch Bildungsprogramme vor Ort.
Das BMZ ist der wichtigste Auftraggeber der GIZ und neben dem BMF einer der beiden Gesellschafter.[58]

Bundesnachrichtendienst (BND)
Der Bundesnachrichtendienst (BND) ist der Auslandsnachrichtendienst der Bundesrepublik Deutschland und handelt im Auftrag der Bundesregierung. Im Ausland erfasst er Angriffe, die der Cyber-Spionage oder -Sabotage in Deutschland dienen sollen und warnt betroffene Akteure im Inland entsprechend vor, damit Abwehrmechanismen eingeleitet werden können. Bekannt ist dieser Teil seiner Arbeit auch unter dem Akronym SSCD - SIGINT Support to Cyber Defense.
Der BND gehört zum Geschäftsbereich des BKAmt. Er ist an der Initiative Wirtschaftsschutz beteiligt und im Cyber-AZ vertreten. Sein Personal wird u.a. an der UniBw ausgebildet.[59]

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA)
Die Bundesnetzagentur (BNetzA) ist vorrangig für Regulierungs- und Wettbewerbsfragen in den Bereichen Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen zuständig. Da die Bedeutung von Cyber-Sicherheit in diesen Bereichen zunehmend an Bedeutung gewinnt, kümmert sich die BNetzA auch um IT-Sicherheitsanforderungen in den entsprechenden Sektoren.
Die BNetzA gehört zum Geschäftsbereich des BMWi. Gemeinsam mit dem BSI hat sie den IT-Sicherheitskatalog herausgebracht, zu dessen Umsetzung alle Betreiber von Gas- und Stromnetzen verpflichtet sind.[60]

Bundespolizei (BPol)
Die Bundespolizei (BPol) übernimmt Aufgaben im Bereich des Grenzschutzes, der Luftsicherheit, Bahnpolizei und Kriminalitätsbekämpfung. Da illegale Aktivitäten immer stärker auch im Internet oder mithilfe von Infor-

mationstechnik ausgeübt werden, bekämpft die BPol zunehmend auch Internet-Kriminalität.
Die BPol gehört zum Geschäftsbereich des BMI. Sie ist im Cyber-AZ vertreten und greift auf die Expertise von ZITiS zurück. Die ZAC sind bei den Polizeien des Bundes und der Länder angesiedelt.[61]

Bundeswehr (Bw)
Die Bundeswehr (Bw) ist u. a. für die Landes- und Bündnisverteidigung verantwortlich. Um dieser Aufgabe im digitalen Zeitalter gerecht zu werden, wurde im April 2017 der neue militärische Organisationsbereich Cyber- und Informationsraum (CIR) aufgestellt. Neben Heer, Luftwaffe und Marine ist die neue Organisation ganzheitlich für die Verteidigung des Cyber- und Informationsraums verantwortlich.
Die Bw gehört zum Geschäftsbereich des BMVg. Sie bildet Teile ihres Personals an der UniBw aus und ist im Cyber-AZ sowie im CERT-Verbund vertreten.[62]

Bundesweite IT-Systemhaus GmbH (BWI)
Die BWI ist eine Gesellschaft des Bundes und sowohl IT-Dienstleister der Bundeswehr als auch ein IT-Dienstleistungszentrum des Bundes. Im Rahmen des Herkules-Großprojektes wurde die Bundeswehr-IT durch die BWI umfassend modernisiert. An der Gesellschaft und dem Großprojekt waren auch IBM und Siemens beteiligt. Ende des Jahres 2016 endeten jedoch sowohl das Projekt Herkules als auch die Beteiligung der beiden Firmen und die BWI wurde zu einer reinen Bundesgesellschaft. Schwerpunkte der Arbeit sind das Betreiben und Modernisieren von nichtmilitärischen Informations- und Kommunikationstechniken der Bundeswehr und die Unterstützung in den Bereichen Logistik und Administration. Die BWI ist unter anderem auch für das Software-Management und die IT-Sicherheit der von ihr betriebenen IT-Infrastruktur verantwortlich.
Die BWI GmbH ist eine Bundesgesellschaft und IT-Systemhaus für Bw und Bund.[63]

CERT-Bund / Bürger-CERT
Das Computer Emergency Response Team (CERT) des Bundes ist Notfallteam und Anlaufstelle für alle Bundesbehörden im Falle eines sicherheitsrelevanten IT-Vorfalls. Das Bürger-CERT ist ein Warn- und Informationsdienst für Privatpersonen, die vom Bürger-CERT neutral und kostenlos über aktuelle Sicherheitslücken informiert werden.
Das CERT des Bundes ist im BSI aufgehangen und kooperiert im Rahmen des Verwaltungs-CERT-Verbunds (VCV) mit den Länder-CERTs.[64]

CERT-Verbund
Der CERT-Verbund ist eine Allianz deutscher Sicherheits- und Computer-Notfallteams, die sich in Unternehmens-, Kommerziellen-, Akademischen- und Verwaltungs-CERTs auf Bundes- und Länderebene zusammengeschlossen haben.
Im CERT-Verbund sind u.a. die Bw und das BSI (mit dem CERT-Bund) vertreten.[65]

Cyber Innovation Hub (CIH)
Um die Konkurrenzfähigkeit der Bundeswehr im Bereich Cyber und IT zu garantieren, bietet der Cyber Innovation Hub (CIH) der Bundeswehr eigenen Mitarbeiter:innen in Zusammenarbeit mit Startups eine Plattform zum Erforschen und Weiterentwickeln von innovativen Technologien. Durch die Verknüpfung von Bundeswehr und Startups sollen Ideen schneller verwirklicht und fortschrittliche Technologien besser umgesetzt werden können. Die Soldat:innen arbeiten gemeinsam mit Zivilpersonen vor allem auch an der Entwicklung von disruptiven Technologien für die Bundeswehr.
Der CIH ist dem BMVg zugeordnet und dem Steuerungsboard gehören Vertreter:innen von Bw, BAAINBw sowie BWI an.[66]

Cybercrime-Zentren
13 der 16 Bundesländer haben inzwischen Cybercrime-Zentren aufgebaut, die für die Bekämpfung und Aufklärung von Cyber-Kriminalität zuständig sind. Die Cybercrime-Zentren sind organisatorisch überwiegend im Polizeibereich der entsprechenden Landeskriminalämter oder bei den Staatsanwaltschaften aufgehangen.
Die Cybercrime-Zentren kooperieren mit den entsprechenden Länder-CERTs.[67]

Cyber Security Cluster Bonn e.V.
Der Cyber Security Cluster Bonn e.V. ist ein Zusammenschluss von verschiedenen, in der Bonner Region ansässigen Institutionen, unter anderem dem BSI, dem Kommando Cyber- und Informationsraum der Bundeswehr, der Hochschule Bonn-Rein-Sieg und dem Fraunhofer-Institut. Auch die Deutsche Telekom, die Industrie- und Handelskammer, die Stadtverwaltung und Vertreter der Bonner Wirtschaft sind Mitglieder. Ziel ist es, die geographische Nähe zu nutzen, um die Zusammenarbeit zu intensivieren und sowohl Fachkräfte anzuziehen als auch gemeinsam an konkreten Projekten im Bereich der Cybersicherheit zu arbeiten.
Das BSI und das Kommando Cyber- und Informationsraum der Bundeswehr sind Mitglieder im Cyber Security Cluster Bonn e.V.[68]

Cyber-Sicherheitsrat (Cyber-SR)
Der nationale Cyber-Sicherheitsrat (Cyber-SR) wurde 2011 im Zuge der Cyber-Sicherheitsstrategie mit dem Ziel eingerichtet, als strategischer Ratgeber der Bundesregierung langfristige Handlungsnotwendigkeiten und Trends der Cyber-Sicherheit zu identifizieren und entsprechende Impulse anzuregen. Er bringt Vertreter der Bundesebene, der Länder und aus der Wirtschaft zusammen.
Im Cyber-SR sind BMI, BKAmt, AA, BMVg, BMWi, BMJV, BMF, BMBF und BMVI vertreten.[69]

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)
Die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) hilft der Bundesregierung bei der Realisierung ihrer Ziele zur internationalen Entwicklungszusammenarbeit. Sie unterstützt die Förderung von Informations- und Kommunikationstechnologien und plant in Zukunft auch Cyber-Sicherheit als Element der traditionellen Entwicklungszusammenarbeit aufzunehmen.
BMZ und BMF sind Gesellschafter der GIZ.[70]

Deutsches Institut für Internet Sicherheit / Cyber-Sicherheit (DIIS)
In der Cyber-Sicherheitsstrategie für Deutschland 2016 wurde die Gründung eines *Deutschen Instituts für Cyber-Sicherheit (DIIS)* angekündigt. Das Institut soll unterschiedliche Akteure einbeziehen, um an Cyber-Sicherheitsthemen mit Bezug zu internationaler Stabilität und Krisenprävention zu arbeiten. Dabei soll es Regierungen als internationaler Ansprechpartner zur Verfügung stehen.
Das DIIS soll vom AA gegründet werden.[71]

Deutschland sicher im Netz e.V. (DsiN)
Deutschland sicher im Netz e.V. (DsiN) wurde im Rahmen des 1. Nationalen IT-Gipfels gegründet, um die Bevölkerung, sowie kleine und mittlere Betriebe über IT-Sicherheit aufzuklären. In Kooperation mit seinen Mitgliedern und Partnern betreibt DsiN verschiedene Initiativen und Projekte, um konkrete Hilfestellungen für IT-Sicherheit zu leisten.
Das BMI, BMWi, BSI, BKA und BfDI sind im DsiN Beirat vertreten. DsiN kooperiert mit der Initiative IT-Sicherheit in der Wirtschaft.[72]

Forschungsinstitut Cyber Defence (CODE)
Das Forschungsinstitut Cyber Defence (CODE) an der Universität der Bundeswehr wurde vom BMVg mit dem Ziel gegründet, innovative technische Neuerungen für Bundeswehr und Bund zum Schutz von Daten, Software und Systemen zu verwirklichen. Darüber hinaus ist das interdisziplinäre, unabhängige Forschungsinstitut an die wissenschaftliche Aus-, Fort- und Weiter-

bildung der Universität der Bundeswehr angebunden. Hier baut es ein intersektorales Cyber-Cluster auf.
CODE ist das Forschungsinstitut Cyber Defence an der UniBw, wo Bw Personal wissenschaftlich ausgebildet wird. Es befindet sich in geografischer Nähe zur ZITiS.[73]

Gemeinsames Melde- und Lagezentrum (GMLZ)
Das Gemeinsame Melde- und Lagezentrum (GMLZ) hat die Aufgabe für Bund, Länder und Fachbehörden ein einheitliches Lagebild für den Bevölkerungsschutz abzubilden. Dafür verfolgt und bewertet es rund um die Uhr relevante Geschehnisse im In- und Ausland und berichtet im täglichen Lagebericht oder gezielten Lagemeldungen.
Das GMLZ übernimmt nachts die Aufgaben des LZ. Das BBK ist im GMLZ vertreten.[74]

German Competence Centre against Cyber Crime (G4C)
Das German Competence Centre against Cyber Crime (G4C) ist ein Verein, der unterschiedliche Akteure in einer strategischen Allianz gegen Cyber-Kriminalität zusammenbringt. Durch einen täglichen Informationsaustausch zwischen den behördlichen Kooperationspartnern und den Mitgliedern, können diese geeignete Schutzmaßnahmen entwickeln.
Das G4C kooperiert mit dem BKA und dem BSI.[75]

Informationstechnikzentrum Bund (ITZBund)
Das ITZBund ist IT-Dienstleister der Bundesverwaltung. Es ist 2016, als Teil einer Gesamtstrategie mit dem Ziel einer konzentrierten Bündelung der IT-Kapazitäten des Bundes, aus drei Vorgängerbehörden gegründet worden: der Bundesstelle für Informationstechnik (BIT), der dem Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) nachgeordneten Bundesanstalt für IT-Dienstleistungen (DLZ-IT BMVI) und dem Zentrum für Informationsverarbeitung und Informationstechnik (ZIVIT). Das ITZBund gehört zum Geschäftsbereich des Bundesministeriums der Finanzen und soll unter anderem auch den Schutz vor Cyberangriffen verbessern.
Das ITZBund gehört zum Geschäftsbereich des Bundesministeriums der Finanzen.[76]

Initiative IT-Sicherheit in der Wirtschaft
Die Initiative IT-Sicherheit in der Wirtschaft ist eine Initiative des BMWi für kleine und mittlere Unternehmen. Eine Vielzahl von Aktivitäten werden von der Initiative gebündelt. Die Mitglieder des Steuerkreises sind IT-Experten aus Verwaltung, Wissenschaft und Wirtschaft und beraten die Initiative IT-Sicherheit in der Wirtschaft bei der Umsetzung ihrer Projekte.

Die Initiative IT-Sicherheit in der Wirtschaft ist eine Initiative des BMWi. In ihrem Rahmen wird u. a. das "Bottom-Up" Projekt von DsiN betrieben.[77]

Initiative Wirtschaftsschutz
Die Initiative Wirtschaftsschutz hat das Ziel den Schutz wichtiger Unternehmenswerte der deutschen Wirtschaft zu verbessern. Das BMI koordiniert die Zusammenarbeit von staatlichen Stellen und Wirtschaftsverbänden. Die Initiative bietet ein umfangreiches Schutzkonzept aus Maßnahmen, Handlungsempfehlungen und Seminaren.
Die Initiative Wirtschaftsschutz arbeitet auf staatlicher Seite mit dem BND, BfV, BKA und dem BSI zusammen.[78]

IT Security made in Germany
Das Vertrauenszeichen "IT Security made in Germany" wurde 2005 gemeinsam durch das BMI, das BMWi sowie Vertreter der deutschen IT-Sicherheitswirtschaft ins Leben gerufen. Seit 2011 wird der Verein in Form der TeleTrusT-Arbeitsgruppe "ITSMIG" fortgeführt. Ziel ist es, die gemeinsame Außendarstellung der organisierten deutschen IT-Sicherheitswirtschaft zu koordinieren und die Zusammenarbeit zu verbessern.
Bei der Etablierung von ITSMIG haben das BMI und das BMWi unterstützt. Beide Ministerien sind im Beirat der Arbeitsgruppe vertreten.[79]

Kompetenznetzwerk Trusted Cloud (Trusted Cloud)
Das Kompetenznetzwerk Trusted Cloud (Trusted Cloud) ist aus dem gleichnamigen Programm des BMWi entstanden, welches ein Gütesiegel für Cloud Services entwickelt und etabliert hat. Trusted Cloud dient als neutrale und branchenübergreifende Plattform für den Austausch zwischen Cloud-Anbietern und Anwendern.
Trusted Cloud wurde durch das BMWi ins Leben gerufen.[80]

Kompetenz- und Forschungszentren für IT-Sicherheit
Die drei Kompetenz- und Forschungszentren für IT-Sicherheit in Saarbrücken, Darmstadt und Karlsruhe sind Bestandteil der Digitalen Agenda des BMBF. Mit der Gründung der drei Forschungszentren hat die Bundesregierung die Forschung und Entwicklung im Bereich Cyber-Sicherheit und Schutz der Privatsphäre maßgeblich ausgeweitet.
Die drei Kompetenz- und Forschungszentren für IT-Sicherheit werden durch das BMBF gefördert.[81]

Länder-CERTs
Die Länder-CERTs sind die Computer Emergency Response Teams der einzelnen Bundesländer. Im Rahmen des Verwaltungs-CERT-Verbunds (VCV) kooperieren Bund und Länder beim Aufbau und Betrieb der Länder-CERTs.
Die Länder-CERTs kooperieren mit dem CERT-Bund im BSI.[82]

Landesamt für Sicherheit in der Informationstechnik Bayern (LSI)
Das Landesamt für Sicherheit in der Informationstechnik Bayern (LSI) hat sich mit seiner Gründung im Dezember 2017 den Schutz staatlicher IT-Infrastrukturen zur Aufgabe gemacht. Es soll Kommunen und Bürger beratend unterstützen.
Das LSI ist Mitglied im VCV, beheimatet das Bayern-CERT und kooperiert mit dem BSI.[83]

Nationales Cyber-Abwehrzentrum (NCAZ/ Cyber-AZ)
Das Nationale Cyber-Abwehrzentrum (NCAZ oder Cyber-AZ) hat die Aufgabe die operative Zusammenarbeit hinsichtlich verschiedener Gefährdungen im Cyber-Raum zwischen staatlichen Stellen zu optimieren und entsprechende Schutz- und Abwehrmaßnahmen zu koordinieren. Dafür werden im Cyber-AZ, welches im BSI angesiedelt ist, alle Informationen zu Cyber-Angriffen auf IT-Infrastruktur gebündelt. Aktuell wird in der Regierung eine Ausweitung zum sogenannten “Cyber-AZ Plus” diskutiert.
Das Cyber-AZ ist eine Kooperationsplattform zwischen BSI, BPol, BKA, BfV, BBK, BND, Bw, ZKA, BaFin und BAMAD.[84]

Nationales IT-Lagezentrum (LZ)
Das Nationale IT-Lagezentrum (LZ) im BSI hat die Aufgabe 24 Stunden täglich ein IT-Lagebild zu erstellen, um auftretende IT-Sicherheitsvorfälle für staatliche Stellen und Wirtschaftsunternehmen schnell einschätzen zu können und wenn nötig darauf zu reagieren. Nachts übernimmt das GMLZ die Funktion. Cyberangriffe sollen rechtzeitig entdeckt und vorbeugende Maßnahmen früh ergriffen werden. Dies wird über konstantes Monitoring und Auswerten von verschiedenen Quellen erreicht, die in der Gesamtschau eine möglichst umfassende Übersicht zu der IT-Sicherheitlage in der Bundesrepublik liefern. Die Kapazitäten und Strukturen des LZ erlauben es ihm zudem, gegebenenfalls zum IT-Krisenreaktionszentrum aufzuwachsen.
Das LZ arbeitet eng mit dem GMLZ, CERT-Bund und Cyber-AZ zusammen.[85]

Stiftung Wissenschaft und Politik (SWP)
Die Stiftung Wissenschaft und Politik (SWP) berät Bundestag und Bundesregierung, sowie internationale Organisationen zu außen- und sicherheitspolitischen Fragen und ist dabei politisch unabhängig. Ihre Forschung umfasst

auch Digitalisierungs- und Cyber-Sicherheitsthemen.
Die SWP erhält ihre institutionelle Zuwendung vom BKAmt.[86]

Umsetzungsplan Kritische Infrastrukturen (UP KRITIS)
Der Umsetzungsplan Kritische Infrastrukturen (UP KRITIS) hat die Aufgabe, die Versorgung durch Kritische Infrastrukturen zu erhalten. Dafür dient UP KRITIS als öffentlich-private Kooperation zwischen staatlichen Stellen, Betreibern Kritischer Infrastrukturen und ihren Verbänden. Da Informations- und Kommunikationstechnik einen immer größerer Bestandteil von Kritischen Infrastrukturen darstellt, kommt ihrem Schutz eine zentrale Rolle zu.
Im Rahmen des UP KRITIS kooperieren von staatlicher Seite BMI, BSI und BBK.[87]

Universität der Bundeswehr München (UniBw)
Die Universität der Bundeswehr München (UniBw) bildet Offiziere und Offiziersanwärter wissenschaftlich aus. Die Studiengänge umfassen aktuell unter anderem Informatik, Cyber-Sicherheit, Mathematical Engineering und Wirtschaftsinformatik.
Die UniBw bildet Bw Personal wissenschaftlich aus und beheimatet CODE als fakultätsübergreifendes Forschungszentrum.[88]

Verwaltungs-CERT-Verbund (VCV)
Der Verwaltungs-CERT-Verbund (VCV) ist eine Plattform zum gegenseitigen Informationsaustausch zwischen dem CERT Bund und den vorhandenen Länder-CERTs. So soll die IT-Krisenprävention und -reaktion gestärkt und die IT-Sicherheit in der öffentlichen Verwaltung verbessert werden.
Am VCV beteiligt sind das BSI, Länder CERTs, sowie das LSI.[89]

Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft (ZAC)
Die Zentralen Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft (ZAC) stehen Unternehmen präventiv und reaktiv im Falle von Internetstraftaten zur Verfügung. In jedem Bundesland ermitteln speziell ausgebildete Polizeibeamte gemeinsam mit IT-Spezialisten.
Die ZAC sind u.a. bei der BPol angesiedelt.[90]

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)
Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) entwickelt, forscht, unterstützt und berät die deutschen Sicherheitsbehörden in den folgenden Bereichen: Digitale Forensik, Telekommunikationsüberwachung, Krypto- und Big-Data-Analyse. Darüber hinaus arbeitet ZITiS auch zu technischen Fragen im Bereich der Kriminalitätsbekämpfung, Ge-

fahren- und Spionageabwehr.
ZITiS wurde vom BMI gegründet. Sie versorgt BKA, BfV und BPol mit ihrer Expertise. Sie ist auf dem Campus der UniBw angesiedelt und befindet sich so auch in geographischer Nähe zu CODE.[91]

Zollkriminalamt (ZKA)
Das Zollkriminalamt (ZKA) gehört zum Geschäftsbereich des BMF und ist für die Prävention und Aufklärung von mittlerer, schwerer und organisierter Zollkriminalität verantwortlich. Dabei koordiniert das ZKA die Ermittlungen der einzelnen Zollfahndungsämter und kann in besonderen Fällen auch eigene Ermittlungen aufnehmen. Dies erstreckt sich auch auf den Cyber-Raum.
Das ZKA ist dem BMF nachgeordnet und ist im Cyber-AZ vertreten.[92]

Gut zu wissen

Wenn Sie Fragen rund um IT-Sicherheit haben, können Sie kostenlos beim Bundesamt für Sicherheit in der Informationstechnik die Hotline des *BSI für Bürger* anrufen. Die Damen und Herren dort sind Montag bis Freitag von 8:00 Uhr bis 18:00 Uhr unter 0800 274 1000 erreichbar.[93]

IT-Sicherheit versus Cybersicherheit: IT-Sicherheit hat eine relativ enge Definition. Diese folgt dem ; der Schutz der Vertraulichkeit (*Confidentiality*), Integrität (*Integrity*) und Verfügbarkeit (*Availability*) von Daten.[94] Im Verlauf der letzten Dekade nahm vor allem im anglo-amerikanischen, aber auch europäischen Raum der Gebrauch des Wortes im Vergleich zu IT-Sicherheit zu. *Cybersicherheit* ist breiter angelegt als *IT-Sicherheit* und umfasst zusätzlich auch sozio-kulturelle, politische, rechtliche und weitere Dimensionen.[95] Zusätzlich wird in Deutschland unter *Cybersicherheit* offiziell spätestens seit der Cyber-Sicherheitsstrategie für Deutschland 2016 nicht mehr nur noch die Erhöhung von IT-Sicherheit in den vorgenannten Dimensionen, sondern auch der Einsatz von offensiven Cyberwerkzeugen zur Herstellung der öffentlichen Sicherheit verstanden - unter anderem durch den *Einsatz des Bundestrojaners*[96] oder *Aktiver Cyberabwehr*.[97]

Es heißt jetzt Cybersicherheit ohne Bindestrich. Die Bundesregierung hat bis circa 2016/2017 bei Begriffen mit den Bindestrich verwendet, dies geht u.a. aus dem Glossar der *Cyber-Sicherheitsstrategie für Deutschland 2016* hervor.[98] Spätestens seit 2018 werden Begriff mit Cyber zusammengeschrieben, wie die Benennung der neuen Referate in der Abteilung Cyber- und Informationssicherheit im Bundesministerium des Innern, für Bau und Heimat[99] oder der *Agentur für Innovation in der Cybersicherheit* belegen.[100]

Cyberveranstaltungen. Mit der wachsenden Relevanz des Themas IT- und Cybersicherheitspolitik steigt auch die Anzahl der Veranstaltungen in dem Bereich. Schon allein für Deutschland ist es schwer die Vielzahl an Konferenzen und weiteren Ereignissen zu überblicken. Um hier etwas mehr Übersicht zu schaffen, hat die Stiftung Neue Verantwortung hierfür einen entsprechenden Kalender online gestellt. Er ist unter cyber-veranstaltungen.de zu finden.

Was ist eigentlich “Aktive Cyberabwehr” (auch bekannt als “Hackbacks”)? Zu diesem Thema haben wir anhand von Veröffentlichungen und Hintergrundgesprächen eine kurze Handreichung mit Definition und Maßnahmenübersicht entwickelt.

Referenzen

1 Bundesamt für Sicherheit in der Informationstechnik, Jahresbericht 2003.
2 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2011.
3 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.
4 Julia Schütze, Warum dem Staat IT-Sicherheitsexpert:innen fehlen.
5 Bundesministerium der Verteidigung, Nationales Cyber-Abwehrzentrum.
Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2011.
6 Heise Online, Jeden Tag drei bis fünf Fälle für das Cyber-Abwehrzentrum.
7 Bundesamt für Sicherheit in der Informationstechnik, Cyber-Abwehrzentrum.
8 Deutscher Bundestag - Antwort der Bundesregierung auf eine Kleine Anfrage, Die Strategie der Bundesregierung zur Bekämpfung der Internetkriminalität - Das Nationale Cyber-Abwehrzentrum.
9 FragDenStaat, Kooperationsvereinbarungen zum Nationalen Cyber-Abwehrzentrum.
FragDenStaat, Evaluierungen Nationales Cyber-Abwehrzentrum (Cyber-AZ).
10 Koalitionsvertrag zwischen CDU, CSU und SPD, Ein neuer Aufbruch für Europa Eine neue Dynamik für Deutschland Ein neuer Zusammenhalt für unser Land 2018.
11 Zeit Online, Bundesinnenministerium kündigt “Cyber-Abwehrzentrum plus” an.
12 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Durchführungserläuterungen zum Dokument “Auftrag und Arbeitsweise”.
13 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Durchführungserläuterungen zum Dokument “Auftrag und Arbeitsweise”.
14 Heise Online, Bundesregierung beschließt Cyber-Sicherheitsstrategie.
15 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Auftrag und Arbeitsweise.
16 Bundesamt für Sicherheit in der Informationstechnik, Cyber-Abwehrzentrum.
17 Deutscher Bundestag - Antwort der Bundesregierung auf eine Kleine Anfrage, Die Strategie der Bundesregierung zur Bekämpfung der Internetkriminalität - Das Nationale Cyber-Abwehrzentrum.
18 Bundesamt für Sicherheit in der Informationstechnik, Cyber-Abwehrzentrum.
19 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Auftrag und Arbeitsweise.
20 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Auftrag und Arbeitsweise.
21 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Auftrag und Arbeitsweise.
22 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Auftrag und Arbeitsweise.
23 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Betreff: “Erfahrungsbericht Nationales Cyber-Abwehrzentrum”.
24 Spiegel Online, Internet-Wacht am Rhein.
25 tagesschau.de, Kaum Kompetenz, kaum Akzeptanz.

26 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Betreff: “Weiterentwicklung Nationales Cyber-Abwehrzentrum”.
27 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Durchführungserläuterungen zum Dokument “Auftrag und Arbeitsweise”.
28 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Betreff: “Erfahrungsbericht Nationales Cyber-Abwehrzentrum”.
29 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Betreff: “Weiterentwicklung Nationales Cyber-Abwehrzentrum”.
30 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Betreff: “Cyber-AZ”.
FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Workshop “Abgrenzung CERT, IT-LZ, Cyber-AZ”.
FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Cyber-AZ Präsentation.
31 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Durchführungserläuterungen zum Dokument “Auftrag und Arbeitsweise”.
32 FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Workshop “Abgrenzung CERT, IT-LZ, Cyber-AZ”.
FragDenStaat, Antwort des Bundesamtes für Sicherheit in der Informationstechnik, Cyber-AZ Präsentation.
33 tagesschau.de, “Cyber-Abwehrzentrum plus” geplant.
34 Julia Schütze, Warum dem Staat IT-Sicherheitsexpert:innen fehlen.
35 Bundesamt für Sicherheit in der Informationstechnik, Bundesgesetzblatt Teil I Nr. 54, Jahrgang 2009, Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes.
36 taz, Backdoor im Gesetz.
37 Bundesministerium des Innern, Agentur für Innovation in der Cybersicherheit.
Bundesministerium der Verteidigung, Technologiesouveränität erlangen – die neue Cyberagentur.
Bundesministerium der Verteidigung, BMVg und BMI geben Standort für neue Cyberagentur bekannt.
38 Bundesamt für Sicherheit in der Informationstechnik, Allianz für Cyber-Sicherheit - Über uns.
39 Auswärtiges Amt, Cyber-Außenpolitik.
40 Das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr, Das BAAINBw.
41 Bundesakademie für Sicherheitspolitik, Cyber-Realität zwischen Freiheit und Sicherheit.
42 Bundesamt für den Militärischen Abschirmdienst, Über uns.
43 Bundesanstalt für Finanzdienstleistungsaufsicht, Aufgaben & Geschichte der BaFin.
44 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Gemeinsames Melde- und Lagezentrum von Bund und Ländern.
45 Bundesamt für Sicherheit in der Informationstechnik, Bundesgesetzblatt Teil I Nr. 54, Jahrgang 2009, Gesetz zur Stärkung der Sicherheit in der Informationstech-

nik des Bundes.
Bundesamt für Sicherheit in der Informationstechnik, Themen.
46 Bundesamt für Verfassungsschutz, Cyberangriffe.
47 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Aufgaben.
48 Bundeskanzleramt, Chef des Bundeskanzleramtes.
49 Bundeskriminalamt, Straftaten im Internet.
50 Bundesministerium der Justiz und für Verbraucherschutz, Aufgaben und Organisation.
Bundesministerium der Justiz und für Verbraucherschutz, Schutz von Bürgern und Onlinehandel vor Cyberkriminalität.
Bundesministerium der Justiz und für Verbraucherschutz, Wir dürfen Cybermobbing nicht ignorieren.
51 Bundesministerium der Verteidigung, Cybersicherheit.
Bundesministerium der Verteidigung, Cyber Innovation Hub.
Koalitionsvertrag zwischen CDU, CSU und SPD, Ein neuer Aufbruch für Europa Eine neue Dynamik für Deutschland Ein neuer Zusammenhalt für unser Land 2018.
52 Bundesministerium des Innern, für Bau und Heimat, IT & Cybersicherheit.
Bundesministerium des Innern, für Bau und Heimat, Cyber-Sicherheitsstrategie für Deutschland.
Koalitionsvertrag zwischen CDU, CSU und SPD, Ein neuer Aufbruch für Europa Eine neue Dynamik für Deutschland Ein neuer Zusammenhalt für unser Land 2018.
53 Kompetenz- und Forschungszentren für IT-Sicherheit, Über uns.
54 Bundesfinanzministerium, Themen.
Bundesfinanzministerium, Grundelemente zur Cyber-Sicherheit.
55 Bundesministerium für Gesundheit, E-Health-Gesetz.
Bundesministerium für Gesundheit, Aufgaben und Organisation.
56 Bundesministerium für Verkehr und digitale Infrastruktur, Krisenmanagement.
57 Bundesministerium für Wirtschaft und Energie, IT-Sicherheit.
Bundesministerium für Wirtschaft und Energie, IT-Sicherheit für die Industrie 4.0.
58 Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, Grundsatzfrage: Warum brauchen wir Entwicklungspolitik?
Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, Glossar - Digitalisierung und nachhaltige Entwicklung.
59 Bundesnachrichtendienst, Die Arbeit.
Bundesnachrichtendienst, Cybersicherheit.
60 Bundesnetzagentur, Aufgaben und Struktur.
Bundesnetzagentur, IT-Sicherheit im Energiesektor.
61 Bundespolizei, Startseite.
Bundespolizei kompakt, 04/2015.
62 Bundeswehr, Auftrag und Aufgaben der Bundeswehr.
Bundeswehr, Das Kommando Cyber- und Informationsraum.
63 Bundesweite IT-Systemhaus GmbH, Unternehmensbroschüre.
64 Bundesamt für Sicherheit in der Informationstechnik, CERT-Bund.
65 Deutscher CERT-Verbund, Startseite.

66 Bundesministerium der Verteidigung, Cyber Innovation Hub.
67 Secupedia, Nationales Cyber-Abwehrzentrum.
68 Cyber Security Cluster Bonn, Über uns.
69 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.
70 Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) GmbH, Bundesregierung.
Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) GmbH, IKT-Förderansatz der GIZ.
Hintergrundgespräche, 2018.
71 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.
72 Deutschland sicher im Netz, Presse.
73 Universität der Bundeswehr München, Forschungsinstitut CODE.
74 Bundesministerium des Innern, für Bau und Heimat, Das Gemeinsame Melde- und Lagezentrum von Bund und Ländern.
75 German Competence Centre against Cyber Crime e.V. (G4C), Über uns.
76 Informationstechnikzentrum Bund, Über uns.
77 Bundesministerium für Wirtschaft und Energie, Steuerkreis.
Bundesministerium für Wirtschaft und Energie, Erste Berufsschulen in Niedersachsen setzen auf Bottom-Up für mehr IT-Sicherheit im Mittelstand.
78 Initiative Wirtschaftsschutz, Aktuelles.
79 TeleTrust, IT Security made in Germany.
80 Bundesministerium für Wirtschaft und Energie, Das Kompetenznetzwerk Trusted Cloud.
81 Kompetenz- und Forschungszentren für IT-Sicherheit, Über uns.
82 Niedersächsisches Computer Emergency Response Team N-CERT, 2016, Kooperation der CERTS im Verwaltungs-CERT-Verbund (VCV).
83 Landesamt für Sicherheit in der Informationstechnik Bayern, Startseite.
84 Bundesamt für Sicherheit in der Informationstechnik, Cyber-Abwehrzentrum.
85 Bundesamt für Sicherheit in der Informationstechnik, Nationales IT-Lagezentrum.
86 Stiftung Wissenschaft und Politik, Cyber-Sicherheit.
Stiftung Wissenschaft und Politik, Über uns.
87 Internetplattform zum Schutz Kritischer Infrastrukturen, Zusammenarbeit im Rahmen des UP KRITIS.
Internetplattform zum Schutz Kritischer Infrastrukturen, UP KRITIS: Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen.
88 Universität der Bundeswehr München, Hintergrundinformationen.
89 Niedersächsisches Computer Emergency Response Team N-CERT, 2016, Kooperation der CERTS im Verwaltungs-CERT-Verbund (VCV).
90 Der Polizeipräsident in Berlin, Zentrale Ansprechstelle Cybercrime für die Wirtschaft im LKA Berlin.
Bundeskriminalamt, Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft.

91 Zentrale Stelle für Informationstechnik im Sicherheitsbereich, Aufgaben & Ziele.
92 Der Zoll, Die Aufgaben des Zolls.
93 Bundesamt für Sicherheit in der Informationstechnik, BSI für Bürger.
94 Bundesamt für Sicherheit in der Informationstechnik, Glossar.
95 Sven Herpig, Anti-War and the Cyber Triangle.
96 Netzpolitik.org, Bundestrojaner.
97 Sven Herpig, Hackback ist nicht gleich Hackback.
98 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.
99 Bundesministerium des Innern, Organisationsplan.
100 Bundesministerium der Verteidigung, Technologiesouveränität erlangen – die neue Cyberagentur.

Über die Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Neue Technologien verändern Gesellschaft. Dafür brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhängige Denkfabrik, in der konkrete Ideen für die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlägen zu unterstützen, führen unsere Expertinnen und Experten Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prüfen Ideen radikal.

Über den Autor

Sven Herpig ist Leiter für Internationale Cyber-Sicherheitspolitik. Hierzu gehört das transatlantische Expert:innen-Netzwerk Transatlantic Cyber Forums (TCF), das von der Europäischen Kommission geförderte EU Cyber Direct (EUCD) und die dauerhafte Analyse der deutschen Innen-, Sicherheits- und Verteidigungspolitik im Cyber-Raum.

Bei der SNV befasst Sven sich vorrangig mit der deutschen Cyber-Sicherheitsarchitektur, Staatlichem Hacken (u. a. dem “Bundestrojaner”) und IT-Schwachstellenmanagement, dem Schutz der Wahlen in vernetzten Gesellschaften, Angriffen auf Machine Learning Anwendungen und der Resilienz-Strategie der Europäischen Union.

So erreichen Sie den Autor
Dr. Sven Herpig
Projektleiter für Internationale Cyber-Sicherheitspolitik
sherpig@stiftung-nv.de
+49 (0)30 81 45 03 78 91

Impressum

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Free Download:

www.stiftung-nv.de