September 2020 · Dr. Sven Herpig

Die „Unabhängigkeit“ des Bundesamtes für Sicherheit in der Informationstechnik

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Inhalt

Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die wichtigste Behörde zur Gewährleistung und Verbesserung von IT- und Cybersicherheit in Deutschland. Jedoch wird seine für die Arbeit enorm wichtige fachliche Unabhängigkeit immer wieder angezweifelt. Die Kontroversen, die zu diesen Zweifeln führen, ergeben sich vor allem aus der Verortung des BSI innerhalb der Behördenlandschaft.

Das BSI wurde 1991 im Ressort des Bundesministeriums des Innern [jetzt „Bundesministerium des Innern, für Bau und Heimat“] (BMI) gegründet und ist aktuell die „Cyber-Sicherheitsbehörde des Bundes“1. Sie ist aus der Zentralstelle für das Chiffrierwesen, einem Arbeitsbereich des Bundesnachrichtendienstes (BND) entstanden.[2] Das BSI ist eine Obere Bundesbehörde im Ressort des Bundesministeriums des Innern, für Bau und Heimat. Seit der Amtsübernahme durch den aktuellen Präsidenten Arne Schönbohm 2016 wurde die Behörde kontinuierlich ausgebaut und ist mit mittlerweile über 1.400 Stellen und 163 Millionen Euro Jahresbudget[3] die größte Cybersicherheitsbehörde in der Europäischen Union.

Durch die immer weiter steigende Bedeutung der Digitalisierung aller Lebensbereiche im 21. Jahrhundert wurde das BSI zu einem wichtigen Akteur der deutschen Sicherheitspolitik. Um das BSI gibt es jedoch eine Kontroverse, die seit vielen Jahren sowohl in der politischen, als auch in der technischen Community diskutiert wird, und sogar Eingang in den aktuellen Koalitionsvertrag fand[4]: Ist das BSI unabhängig genug, um seiner Rolle[5] vollumfänglich nachkommen zu können? Oder gefährdet die Abhängigkeit der Behörde vom BMI das Vertrauensverhältnis anderer Akteure in das BSI und beeinträchtigt damit dessen Effektivität?

1 Bundesamt für Sicherheit in der Informationstechnik (2020): Das Bundesamt für Sicherheit in der Informationstechnik

2 Bundesamt für Sicherheit in der Informationstechnik (2003): Jahresbericht 2003

3 Bundesamt für Sicherheit in der Informationstechnik (2020): Kurzprofil des BSI (Stand: 1. April 2020)

4 Die Bundesregierung (2018): Koalitionsvertrag zwischen CDU, CSU und SPD

5 Hiermit ist explizit nicht der rechtliche Auftrag gem. § 3 BSIG gemeint, sondern die strategische Rolle als zentrale Cybersicherheitsbehörde in Deutschland’s Cybersicherheitsarchitektur.

Der Grund für diese Kontroverse liegt nicht nur in der Vergangenheit der Behörde, genauer: ihrer Entstehung aus dem BND und ihrer Zusammenarbeit mit dem Bundeskriminalamt (BKA). Schwerer wiegt die aktuelle Situation, in der der staatliche Umgang mit Schwachstellen in Hardware und Software ungeklärt ist und das BMI sowohl Behörden beheimatet die IT-Sicherheit fördern sollen, als auch solche, die von IT-Unsicherheit profitieren. Diese Aspekte werden im Folgenden erläutert. Darauf aufbauend werden unterschiedliche Modelle vorgestellt, wie das BSI durch weniger Abhängigkeit vom BMI seiner Rolle als Cybersicherheitsbehörde möglicherweise effektiver nachkommen kann.

Das BSI als Nationale Cybersicherheitsbehörde

Das BSI ist für den Schutz der IT-Systeme des Bundes verantwortlich, kooperiert mit den Cybersicherheitsbehörden der Länder und Wirtschaftsunternehmen, und informiert die Gesellschaft zu allen Themen der Cybersicherheit. Das BSI nimmt unterschiedliche Aufgaben wahr, vom operativen Schutz der Netze des Bundes, über die Zulassung von Software und Hardware für Verschlusssachen (eingestufte Dokumente und Informationen) bis hin zur Informationsaufbereitung für Bürger:innen und die Wirtschaft.[6] Zusätzlich soll die Behörde in der aktuellen Legislaturperiode Kompetenzen im Bereich des digitalen Verbraucherschutzes erhalten.[7] Das BSI ist die Heimat des Computer Emergency Response Teams des Bundes (CERT-Bund), des Mobile Incident Response Teams (MIRT), des IT-Krisenreaktionszentrums und des Nationalen Cyber-Abwehrzentrums (NCAZ).[8]

Während das BSI rechtlich gesehen nur die Cybersicherheitsbehörde des Bundes ist, wäre auf Basis seiner Aufstellung, also seines weiten Aufgabenspektrums gemäß BSI-Gesetz[9] und seiner umfassenden Ressourcenausstattung[10], die Beschreibung „Nationale Cybersicherheitsbehörde“ zutreffender. Hierzu trägt auch die zentrale Rolle bei, die das BSI in der deutschen Cybersicherheitsarchitektur einnimmt (siehe Abbildung 1).

Das BSI ist als primäre Institution für die Cyber- und IT-Sicherheit Deutschlands verantwortlich. Um diese Rolle einnehmen zu können, müssen die unterschiedlichen Arbeitsbereiche des BSI mit allen politischen, behördlichen, wirtschaftlichen und gesellschaftlichen Akteuren vertrauensvoll zusammenarbeiten können.[11] Fehlt ein solches Vertrauensverhältnis, oder ist es beschädigt, versiegen möglicherweise Informationskanäle, die wichtige Daten weitergeben (zum Beispiel Informationen über bisher unbekannte Schwachstellen) oder es wird den Sicherheitsempfehlungen der Behörde nicht mehr gefolgt (zum Beispiel technisch-organisatorische Best Practices oder Update-Empfehlungen).

6 Bundesamt für Sicherheit in der Informationstechnik (2020): Organisationsplan

7 Andre Meister (2020): IT-Sicherheitsgesetz 2.0 – Seehofer will BSI zur Hackerbehörde ausbauen

8 Stiftung Neue Verantwortung (2020): Akteure und Zuständigkeiten in der deutschen Cybersicherheitspolitik

9 Bundesministerium der Justiz und für Verbraucherschutz und Bundesamt für Justiz (2020): Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)

10 Bundesamt für Sicherheit in der Informationstechnik (2020): Kurzprofil des BSI (Stand: 1. April 2020)

11 Bundesamt für Sicherheit in der Informationstechnik (2017): Digitale Gesellschaft: smart & sicher

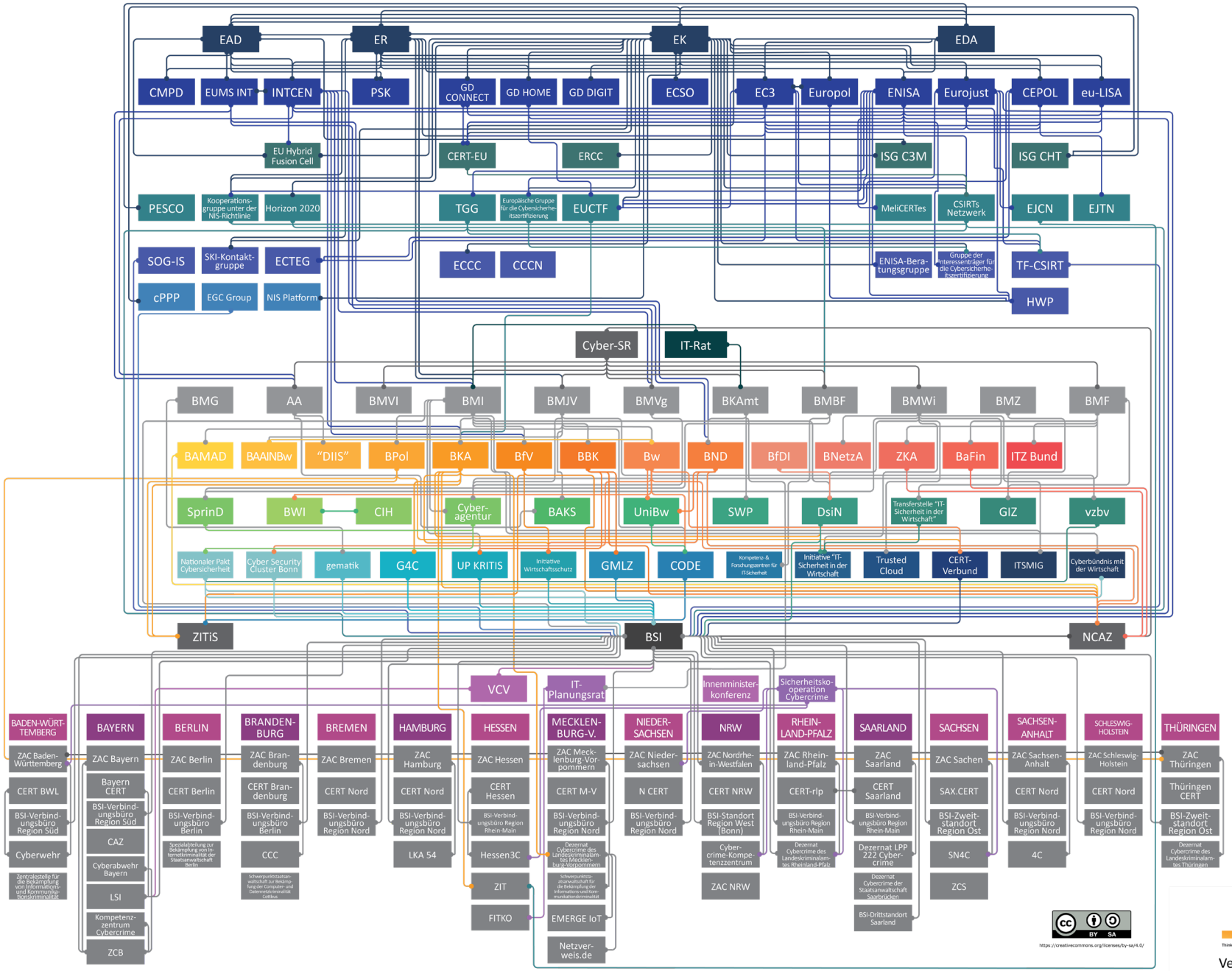
STAATLICHE CYBERSICHERHEITSARCHITEKTUR

Abbildung 1

EUROPÄISCHE UNION

BUND

LÄNDER



Version: März 2020

Zum Aufbau und zur Wahrung eines Vertrauensverhältnis ist es wichtig, dass das BSI seiner Aufgabe, der Stärkung der Cyber- und IT-Sicherheit in Deutschland, unabhängig nachkommen kann, und sich nicht entgegengesetzten Interessen unterordnen muss. Letzteres wird in einigen, für die Arbeit des BSI relevanten Bereichen, als durchaus kontrovers betrachtet. Es besteht die Annahme, dass Cyber- und IT-Sicherheit im Zweifelsfall weniger Priorität genießen als andere Maßnahmen der öffentlichen Sicherheit. Cyber- und IT-Sicherheit sind aber elementare Grundbedingungen für öffentliche Sicherheit, zum Beispiel in Form sicherer Endgeräte und starker Verschlüsselung. Eine Schwächung der Verschlüsselung von Kommunikationsmitteln, wie 2019 vom BMI gefordert, würde daher nicht nur zur Schwächung der Cyber- und IT-Sicherheit, sondern auch zur Gefährdung der öffentlichen Sicherheit führen.[12]

12 Unbekannt (2019): Offener Brief an das Bundesministerium des Innern, für Bau und Heimat

Das BSI zwischen BND-Vergangenheit und Schadsoftware-Entwicklung

Der Bundestagsausschuss für Inneres und Heimat hat die Kontroverse um das BSI bereits am 08.04.2019 zum Thema gemacht. In seiner Stellungnahme als Sachverständiger[13] äußerte sich der Autor damals wie folgt:

Gleichzeitig wird spätestens seit Verabschiedung der Cybersicherheitsstrategie für Deutschland 2016 eine starke Konvergenz öffentlicher Sicherheit (u.a. auch durch den Einsatz von Hacking-Werkzeugen) und IT-Sicherheit vorangetrieben. Um einen singulären Fokus des BSI auf IT-Sicherheit zu wahren und eine entsprechende vertrauenswürdige und effektive Zusammenarbeit mit anderen staatlichen und nicht-staatlichen Stellen zu gewährleisten, sollten verschiedene Modelle der Unabhängigkeit des BSI vom Bundesministerium des Innern, für Bau und Heimat (BMI) geprüft werden.

Die Kontroverse reicht jedoch viel weiter zurück. Es gibt immer noch Personen, wenn auch sehr wenige, die dem BSI nicht vertrauen, weil es vor fast 30 Jahren aus einer Arbeitseinheit des BND hervorgegangen ist. Da der BND zum Beispiel durch offensive Cyberoperationen nachrichtendienstliches Material sammelt und in der Vergangenheit sogar über eine Firma manipulierte Verschlüsselungstechnik in der ganzen Welt vertrieben hat[14], bestehe die Annahme, dass eine Güterabwägung zwischen Cyber- und IT-Sicherheit und öffentlicher Sicherheit[15] zum Nachteil der Cyber- und IT-Sicherheit, dem Auftrag des BSI, ausfallen könnte.

Seit der Gründung des BSI 1991 sind BSI und BND jedoch getrennt und operieren in unterschiedlichen Ressorts, das BSI im Ressort des Bundesministeriums des Innern, für Bau und Heimat und der BND im Bereich des Bundeskanzleramts. Auch die Anzahl der Mitarbeiter:innen, die vor knapp drei Jahrzehnten aus der Zentralstelle für das Chiffrierwesen in das BSI übernommen wurde und dort heute noch tätig ist, dürfte sehr klein sein. Lediglich eine örtliche Überschneidung hat lange Zeit, möglicherweise bis heute, Bestand gehabt. Das Amt für Militärkunde, eine „abgetarnte Außenstelle“ des BND teilt sich anscheinend am Nippenkreuz 19 in Bonn[16] eine Liegenschaft mit einem Dienstgebäude des BSI[17].

13 Sven Herpig (2019): Sachverständigenstellungnahme für die Sitzung des Bundestagsausschusses für Inneres und Heimat am 08.04.2019 zum Thema „IT-Sicherheit“

14 Elmar Theveßen, Peter F. Müller und Ulrich Stoll (2020): „Operation ‚Rubikon‘“

15 Matthias Schulze und Daniel Voelsen (2019): Nationale Sicherheit vs. IT-Sicherheit

16 Armin E. Möller (2011): Das Amt für Militärkunde in Bonn: Geheimhaltung gehört zum Geschäft

17 Bundesamt für Sicherheit in der Informationstechnik (2020): Standort Bonn-Mehlem

Ein jüngeres Ereignis wird häufiger als Argument für eine Unabhängigkeit des BSI vom BMI angeführt[18]: Das BSI hätte das BKA bei der Programmierung einer Schadsoftware – auch bekannt als „Bundestrojaner“ oder „Staatstrojaner“ unterstützt[19]. Laut Netzpolitik.org hat das BSI, statt seinem Auftrag nachzukommen und die IT-Systeme in Deutschland sicherer zu machen, sein Wissen genutzt, um anderen Behörden zu helfen, in IT-Systeme einzudringen. Stand 2020 verneint das BSI, Schwachstellen zum offensiven Einsatz an andere Behörden weitergegeben zu haben.[20] Eine wohlwollende Lesart wäre, dass das BSI dem BKA lediglich dabei half, die Schadsoftware sicherer zu machen, damit keine Kriminellen, Nachrichtendienste oder andere Dritte die Ermittlungen des BKA gefährden können. Das würde zwar nicht dem gesetzlichen Auftrag des BSI widersprechen, wohl aber seiner strategischen Rolle: Denn eigentlich soll die Behörde vor Schadsoftware schützen und nicht Schadsoftware sicherer machen.

18 Deutscher Bundestag (2019): Experten vermissen klare Strategie der IT-Sicherheit

19 Andre Meister (2015): Geheime Kommunikation: BSI programmierte und arbeitete aktiv am Staatstrojaner, streitet aber Zusammenarbeit ab

20 Andre Meister (2020): Der Staat sollte alle IT-Sicherheitslücken schließen. Manche lässt er lieber offen.

Behördlicher Umgang mit Schwachstellen braucht Regeln und Vertrauen

Die Unterstützung des BSI bei der Entwicklung von Schadsoftware wäre problematisch für das Vertrauensverhältnis zwischen der Behörde auf der einen und IT-Sicherheitsforscher:innen und Unternehmen auf der anderen Seite.[21] Schließlich geben IT-Sicherheitsforscher:innen das Wissen über Schwachstellen in Hardware und Software an das BSI weiter, damit die Behörde dafür sorgt, dass der Hersteller das Produkt über Updates sicherer macht. Es handelt sich hierbei um einen der wichtigsten Prozesse im digitalen Ökosystem – selbst das BMI bezeichnet Schwachstellen als „Seuche der modernen IT“[22]. BKA, Bundesamt für Verfassungsschutz (BfV) und Bundespolizei (BPol) hingegen setzen Schadsoftware und/oder digitale forensische Werkzeuge ein, die als Funktionsprinzip offene Schwachstellen ausnutzen müssen. Je mehr Schwachstellen in Software und Hardware nicht geschlossen sind, umso einfacher wird es für diese Behörden, solche Werkzeuge einzusetzen. Sollten IT-Sicherheitsforscher:innen aber Zweifel daran haben, dass das BSI seiner Aufgabe nachkommt, damit diese Schwachstellen geschlossen werden können, könnte der Informationsfluss abnehmen oder sogar versiegen. Auch das Verhältnis der Behörde zur Wirtschaft, könnte dadurch großen Schaden nehmen. Das betrifft insbesondere die Beziehung zwischen dem BSI und Wirtschaftsverbänden oder Firmen, denn diese stellen einen wichtigen Kooperationspartner der Behörde für IT-Sicherheit dar. Das wäre sehr problematisch für die IT- und Cybersicherheit in Deutschland – und darüber hinaus. Unter Betrachtung der aktuellen Bedrohungslage[23], von nachrichtendienstlichen Aktivitäten bis Cyberkriminalität, ist es daher dringend geboten, dass IT-Sicherheitsforscher:innen und Unternehmen und das BSI uneingeschränkt vertrauensvoll zusammenarbeiten können.

Generell ist der Umgang mit Schwachstellen durch deutsche Behörden ein heikles Thema, was durch die Bundesregierung noch nicht effektiv angegan-

21 Vgl. zum Beispiel Linus Neumann (2015): Chaos Computer Club – Stellungnahme zum Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) und Stiftung Neue Verantwortung (2020): Vorläufige Bewertung des Referentenentwurfs zum IT-Sicherheitsgesetz 2.0 vom 07.05.2020 und Empfehlungen, siehe v. a. „5. Schwachstellenmanagement und -meldewesen“ und „6. Untersuchung der Sicherheit in der Informationstechnik“.

22 Sven Herpig (2019): Sachverständigenstellungnahme für die Sitzung des Bundestagsausschusses für Inneres und Heimat am 08.04.2019 zum Thema „IT-Sicherheit“

23 Bundesamt für Sicherheit in der Informationstechnik (2019): Die Lage der IT-Sicherheit in Deutschland und Bundeskriminalamt (2019): Bundeslagebild Cybercrime

gen wurde. Ein „nationales Schwachstellenmanagement“[24] was den operativen Umgang mit diesen Informationen transparenter und verbindlicher regeln würde, wurde bis heute nicht implementiert.[25] Die unübersichtlichen rechtlichen Regelungen zum strategischen Umgang mit Schwachstellen in einem aktuellen Gesetzesentwurf[26] tun ihr Übriges zur vorherrschenden Skepsis. Nichts davon setzt Anreize, Informationen über Schwachstellen an das BSI weiterzuleiten.

24 Sven Herpig (2020): Deutschland braucht ein behördenübergreifendes IT-Schwachstellenmanagement

25 Sven Herpig (2020): Eine vertane Chance für die IT-Sicherheit in Deutschland

26 Stiftung Neue Verantwortung (2020): Vorläufige Bewertung des Referentenentwurfs zum IT-Sicherheitsgesetz 2.0 vom 07.05.2020 und Empfehlungen, siehe v. a. „5. Schwachstellenmanagement und -meldewesen“ und „6. Untersuchung der Sicherheit in der Informationstechnik“.

Das BMI zwischen IT-Sicherheit und -Unsicherheit

Die Kontroversen über die BND-Vergangenheit, die Mitentwicklung des „Bundestrojaners“ und den Umgang mit Schwachstellen sind nur Symptome für einen grundlegenden Mangel an Vertrauen. Die Ursache liegt in der aktuellen Struktur der Exekutive, genauer: dem Aufgabenzuschnitt des BMI. In diesem Ressort sind nämlich nicht nur das BSI, sondern auch mehrere Behörden beheimatet, die teilweise von einer Schwächung der Cyber- und IT-Sicherheit profitieren.

Im Ressort des BMI sind neben dem BSI auch das BKA, das BfV und die Bundespolizei (BPol). Diese drei Behörden profitieren aus genannten Gründen von IT-Unsicherheit, zum Beispiel in Form von (unter Verschluss gehaltenen) offenen Schwachstellen. Hinzu kommt die Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITiS), deren Auftrag es ist, die von den Polizeien und Nachrichtendiensten entsprechend benötigten digitalen Werkzeuge und Dienstleistungen zu beschaffen. Jede dieser dafür benötigten, offenen Schwachstellen kann aber gleichzeitig auch von organisierter Kriminalität und ausländischen Nachrichtendiensten und Militärs ausgenutzt werden. Das bringt die Sicherheitsbehörden – im Gegensatz zum BSI, das einen klaren IT-Schutzauftrag hat – in eine Zwickmühle, da das BKA auch für den Schutz vor Cyberkriminalität und das BfV auch für den Schutz vor Cyberspionage und -sabotage zuständig sind.

Ein Großteil dieser teils gegensätzlichen Aufgaben, inklusive der Fachaufsicht über das BSI, sind sogar beim BMI in der gleichen Abteilung beheimatet: Der Abteilung Cyber- und Informationssicherheit (CI).[27] Es ist leicht vorstellbar, dass es hier zu Interessenkonflikten rund um Cyber- und IT-Sicherheit und öffentliche Sicherheit kommt. Die Weisung an das BSI, das BKA bei der Programmierung einer Schadsoftware zu unterstützen, war möglicherweise der Beweis dafür. Das bedeutet, dass aktuell elementare sicherheitspolitische Güterabwägungen auf Abteilungsleiter:innenebene getroffen werden. Eine wissenschaftlich-fundierte Momentaufnahme aus 2019 zeigt, dass das BSI als „besonders kompetent und rechtschaffen“ angesehen wird, während für das BMI, die Nachrichtendienste und Polizeien im Bezug auf IT-Sicherheit eher das Gegenteil gilt.[28] Eine Lösung dieses Zielkonflikts wäre daher eine neue institutionelle Struktur, die es dem BSI erlaubte, seiner Aufgabe als von den Polizeien und Nachrichtendiensten unabhängigen Nationalen Cybersicherheitsbehörde nachzukommen.

27 Bundesministerium des Innern, für Bau und Heimat (2020): Organisationsplan

28 Bundesamt für Sicherheit in der Informationstechnik (2017): Digitale Gesellschaft: smart & sicher

Reform des BSI für mehr Unabhängigkeit

Aktuell befindet sich das BSI im Ressort des BMI und unterliegt dessen Fachaufsicht, Rechtsaufsicht und Dienstaufsicht. Diese unterscheiden sich wie folgt[29]:

- *Fachaufsicht ist die Aufsicht über die Recht- und Zweckmäßigkeit des Verwaltungshandelns.*
- *Bei der Rechtsaufsicht ist die Befugnis der aufsichtsführenden Behörde darauf beschränkt, die Rechtmäßigkeit des Verwaltungshandelns zu überprüfen.*
- *Dienstaufsicht bezieht sich auf Beschäftigte, Organisationseinheiten oder Aufbau und Abläufe. Sie zielt insbesondere auf persönliche Pflichterfüllung der Beschäftigten, die hiermit in Verbindung stehende innere Ordnung und den Dienstbetrieb der nachgeordneten Organisationseinheit.*

Betrachtet man die Aufsicht als Basis der Abhängigkeit des BSI vom BMI, ergeben sich unterschiedliche Optionen für eine institutionelle Aufstellung des BSI, die die Behörde unabhängig von den entgegengesetzten Interessen der Sicherheitsbehörden im Ressort des BMI machen würde.

Das BSI als Informationssicherheitsbeauftragter des Bundes

Im Sicherheitsbereich ist es eine grundlegende Regel, dass Informationssicherheitsbeauftragte nicht den IT-Beauftragten, deren Arbeit sie kontrollieren sollen, unterstellt sein sollten.[30] Das gilt daher auch analog für die IT des Bundes. Das BSI als Informationssicherheitsbeauftragter des Bundes sollte daher nicht dem Beauftragten der Bundesregierung für Informationstechnik[31], zuständig für die Bundes-IT, unterstellt sein. Nur so kann das BSI seine Kontrollaufgabe gegenüber der Bundes-IT unabhängig ausüben. Aktuell ist der Beauftragte der Bundesregierung für die Informationstechnik jedoch für die Abteilung CI des BMI zuständig, die die Aufsicht über das BSI hat. Das BSI müsste daher aus der Abteilung CI herausgelöst werden und unabhängig

29 Bundesministerium des Innern (2008): Grundsätze zur Ausübung der Fachaufsicht der Bundesministerien über den Geschäftsbereich

30 Zum Beispiel Bundesamt für Sicherheit in der Informationstechnik (2017): BSI-Standard 200-2 und Bundesanstalt für Finanzdienstleistungsaufsicht (2018): IT-Sicherheit: Aufsicht konkretisiert Anforderungen an die Kreditwirtschaft und ISACA Germany (2016): Implementierungsleitfaden ISO/IEC 27001:2013

31 Der Beauftragter der Bundesregierung für Informationstechnik (2020): Der Beauftragte der Bundesregierung für Informationstechnik

vom Beauftragten der Bundesregierung für Informationstechnik im BMI verortet werden, wie zum Beispiel der Beauftragte für den Datenschutz im BMI.

Das BSI wäre in diesem Fall zwar noch immer im Ressort des BMI, aber unabhängiger von den Sicherheitsbehörden und ein effektiveres Kontrollorgan des Beauftragten der Bundesregierung für Informationstechnik. Gleichzeitig wäre dieses Modell leicht umzusetzen, da es lediglich eine ressortinterne Umstrukturierung mit möglichen Anpassungen des BSI-Gesetzes beinhalten würde.

Ausschließlich Rechtsaufsicht durch das BMI

Die Aufsicht des BMI über das BSI könnte auf eine reine Rechtsaufsicht reduziert werden. Damit würde das BMI weiterhin als Kontrollorgan des BSI fungieren, hätte aber keine (inhaltliche) Weisungsbefugnis ihm gegenüber mehr. So könnte das BMI das BSI zum Beispiel nicht mehr anweisen das BKA bei der Programmierung einer Schadsoftware zu unterstützen. Dies könnte im BSI-Gesetz verankert werden und analog zum Gesetz über die Statistik für Bundeszwecke lauten: „Für sie gelten die Grundsätze der Neutralität, Objektivität und fachlichen Unabhängigkeit“[32]. Diese Aspekte, die für eine wissenschaftliche und unpolitische Erarbeitung von Statistiken notwendig sind, treffen in großen Teilen auch für die Cyber- und IT-Sicherheit zu. Als Beispiel kann hier die Verschlüsselungsdebatte[33] angeführt werden: Nach wissenschaftlichen Erkenntnissen führt eine Schwächung der Verschlüsselung für den Zugriff durch Sicherheitsbehörden zu weniger Cyber- und IT-Sicherheit. Das ist belegt und darf daher nicht politisiert werden.[34]

Hierbei handelt es sich um ein Modell, dass der Option „das BSI als Informationssicherheitsbeauftragter des Bundes“ ähnelt und mit ihr kombiniert werden kann. Es würde die Unabhängigkeit des BSI vom BMI verbessern, ohne es aus dem Ressort zu lösen.

32 Bundesministerium der Justiz und für Verbraucherschutz (2020): Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz – BStatG)

33 Unbekannt (2019): Offener Brief an das Bundesministerium des Innern, für Bau und Heimat

34 Zum Beispiel Bruce Schneier (2015): A ‘Key’ for Encryption, Even for Good Reasons, Weakens Security, Amie Stepanovich and Michael Karanicolas (2018): Why An Encryption Backdoor for Just the “Good Guys” Won’t Work oder Michael Hayden (2016): The Pros and Cons of Access to Encrypted Files

Ressortwechsel des BSI

Eine naheliegende Option wäre der Übergang des BSI aus dem Ressort des BMI in ein anderes Ressort. In der Exekutive gibt es derzeit kein Ministerium für Digitales oder Ähnliches, sondern lediglich eine Staatsministerin für Digitalisierung beim Bundeskanzleramt. Allerdings würde eine Ansiedlung des BSI im Bereich des Bundeskanzleramts aufgrund der dortigen Verortung des BND zu ähnlichen Herausforderungen führen wie die aktuelle Verortung des BSI im BMI. Denkbar wären stattdessen zum Beispiel das Bundesministerium für Wirtschaft und Energie (BMWi) oder das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI). Jedoch würde sich auch in diesem Fall eine Abhängigkeit des BSI vom jeweiligen Ministerium ergeben. Aktuell steht eine Kontroverse über Cyber-/IT-Sicherheit und öffentlicher Sicherheit im Raum. Bei Ansiedlung im BMWi wäre beispielsweise eine Kontroverse über zu hohe IT-Sicherheitsstandards und damit verbundene Kosten für die deutsche Wirtschaft denkbar. Es wäre zu prüfen, ob solche Abhängigkeiten das Vertrauen in die Arbeit und Rolle des BSI weniger negativ beeinflussen würden als es in der aktuellen Situation der Fall ist. In diesem Zusammenhang wäre auch die mögliche Gründung eines Ministeriums für Digitales in der kommenden Legislaturperiode zu betrachten.

Es ist denkbar, dass diese Option die Kooperation zwischen den Sicherheitsbehörden, die vor allem für die operative Arbeit – beispielsweise Analysen von Sicherheitsvorfällen – elementar ist, gefährdet. Bisher sind mit dem BSI, BKA, BfV sowie der BPol wesentliche (operative) Akteure der deutschen Cybersicherheitsarchitektur auf Bundesebene im selben Ressort angesiedelt. Das führt – zumindest in der Theorie – zu kurzen Abstimmungswegen und einer zentralen Entscheidungsinstanz – in Form des Innenministers. Lediglich die Bundeswehr (Bw) und der BND sind in anderen Ressorts angesiedelt. Jedoch gibt es für die ressortübergreifende (operative) Zusammenarbeit bei Cybersicherheit auf Bundesebene das NCAZ. Über diese Informationsdrehscheibe und Kooperationsplattform könnte so auch die Zusammenarbeit vorangetrieben werden, wenn das BSI größere Unabhängigkeit vom BMI genießt. Betrachtet man die bisherige Aufstellung des NCAZ ist es jedoch fraglich, ob diese Rolle in der Praxis erfüllt werden kann.[35] Es fehlt nach wie vor zum Beispiel eine klare, transparente rechtliche Grundlage für den Informationsaustausch und die Kooperation der Behörden. Eine Unabhängigkeit des BSI könnte daher – trotz Existenz des NCAZ – zu einer weniger effektiven Kooperation der Sicherheitsbehörden bei gemeinsamen Vorhaben führen. Ein Ressortwechsel sollte daher direkt mit einer Reform des NCAZ verbunden werden.

35 Sven Herpig (2019): Sachverständigenstellungnahme für die Sitzung des Bundestagsausschusses für Inneres und Heimat am 08.04.2019 zum Thema „IT-Sicherheit“

Die stark technischen und operativen Bereiche des BSI liefern die Informationen, die die Grundlage für die Arbeit vieler anderer Bereiche bilden. Es ist denkbar, dass bei dieser Option Teile des BSI im BMI verbleiben (zum Beispiel die operative Cyberabwehr mit dem CERT-Bund, dem IT-Lagezentrum und den MIRTs), während andere Bereiche im neuen Ressort angesiedelt werden. Eine Solche Aufspaltung des BSI gilt es zu verhindern, da die Zusammenarbeit der unterschiedlichen mehr und weniger technischen und operativen Bereiche im BSI zu einer elementaren Wertschöpfungskette führen. Diese über Ressortgrenzen hinweg aufzuteilen würde die Effektivität und Effizienz in der Zusammenarbeit negativ beeinflussen.

Weiterhin könnte durch einen Ressortwechsel die Verhandlungsposition des BSI innerhalb der verschiedenen IT-(Sicherheits-)Gremien geschwächt werden. Im IT-Planungsrat ist das BSI derzeit beispielsweise in Form des Beauftragten der Bundesregierung für Informationstechnik auch indirekt durch das BMI vertreten.[36] Bei Unabhängigkeit des BSI vom BMI wäre das BSI im IT-Planungsrat zunächst gar nicht mehr vertreten und müsste seine Teilnahme neu aushandeln.

Das BSI als Oberste Bundesbehörde

Das BSI könnte von einer Oberen zu einer Obersten Bundesbehörde werden, wie zum Beispiel der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) – der bis 2016 im Ressort des BMI war – oder der Bundesrechnungshof.[37] Hierdurch würde dem BSI ein Höchstmaß an fachlicher Unabhängigkeit zugestanden, eine Kontrolle könnte dann zum Beispiel wie beim BfDI durch das Parlament erfolgen.[38]

Gemäß dieser Option könnte das BSI direkt mit anderen Behörden an Digitalisierungsprojekten zusammenarbeiten, ohne, dass das BMI hierüber informiert werden muss (vgl § 26 GGO39). Hierdurch könnte auch die Zusammenarbeit mit Institutionen, die eine verfassungsrechtliche Unabhängigkeit genießen, wie zum Beispiel dem Bundestag oder dem Bundesverfassungsgericht, erleichtert werden. Beispielsweise wurde im Rahmen der Aufarbeitung

36 IT-Planungsrat (2020): Zusammensetzung des IT-Planungsrats

37 Bundeszentrale für politische Bildung (2009): Verwaltung des Bundes

38 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2017): Anlage zur BfDI-Pressemitteilung für den 26. Tätigkeitsbericht zum Datenschutz

39 Bundesregierung (2020): Gemeinsame Geschäftsordnung der Bundesministerien GGO

des Cyberangriffs auf den Bundestag 2015 deutlich, wie wichtig für solche Institutionen eine transparente und unabhängige Rolle bei entsprechenden Dienstleistungen ist.[40]

Hinzu kommt, dass der Status als Oberste Bundesbehörde dem BSI erlauben würde, mehr Einfluss auf legislative Vorhaben im Bereich IT- und Cybersicherheit zu nehmen und gegenüber den Sicherheitsbehörden klar als Verfechter der deutschen Cyber- und IT-Sicherheit aufzutreten.[41]

Als Oberste Bundesbehörde wäre auch eine, im Vergleich zum aktuellen Status als Obere Bundesbehörde, bessere Gehalts- und Besoldungsstruktur für die Mitarbeiter:innen der Behörde denkbar. Dies würde allerdings den Mangel an IT-Spezialist:innen nicht beheben, solange das starre Laufbahnsystem im öffentlichen Dienst nicht signifikant geändert wird.[42] Jedoch könnte die Unabhängigkeit von den Sicherheitsbehörden über ein erhöhtes Vertrauen die Attraktivität der Behörde als Arbeitgeber, gerade für die technische Community, steigern.

Weiterhin müsste das BSI jedoch selbst für mehr Personal und Ressourcen eintreten und hätte nicht, wie jetzt, das BMI als Fürsprecher für den Haushalt. Auch wenn das Thema Cyber- und IT-Sicherheit in den nächsten Jahren vermutlich wenig an Relevanz verlieren wird, so hat die Behörde in den letzten Jahren einen massiven Personalaufbau erfahren, was die zukünftige Verhandlungsposition des BSI nicht unbedingt positiv beeinflussen dürfte.

Analog zum „Ressortwechsel des BSI“ würde das BSI bei diesem Modell vor den gleichen Herausforderungen bezüglich der Kooperation mit den Sicherheitsbehörden, einem möglichen Verbleib von Teilbereichen des BSI im BMI, sowie der geschwächten Verhandlungsposition in den IT-(Sicherheits-)Gremien, stehen.

40 Frankfurter Allgemeine Zeitung (2015): Verfassungsschutz klärt Hackerangriff nicht auf

41 Sven Herpig (2018): Warum sollte die Polizei Instagram-Passwörter bekommen?

42 Julia Schuetze (2018): Warum dem Staat IT-Sicherheitsexpert:innen fehlen

Empfehlung

Es ist an der Zeit, dass sich die Bundesregierung der Kontroverse annimmt, und dem Bundesamt für Sicherheit in der Informationstechnik mehr Unabhängigkeit einräumt. Davon würde die Cyber- und IT-Sicherheit in Deutschland sicherlich profitieren, da das BSI so seine Rolle – vor allem in (vertrauensvoller) Zusammenarbeit mit anderen Akteuren – effektiver ausüben könnte.

Die hier vorgeschlagenen Modelle und die entsprechenden Vor- und Nachteile sollen lediglich als erster Aufschlag für eine tiefere, inhaltliche Auseinandersetzung mit dem Thema hin zu einem idealtypischen Modell dienen. Zusätzlich bedarf es neben einer dedizierten rechtlichen Betrachtung für jedes dieser Modelle auch weiteren inhaltlichen Analysen. Während es zu den Themen Vertrauensbeziehungen, Umgang mit Schwachstellen, Fachkräftemangel, dem Spannungsfeld von Cyber-/IT-Sicherheit und öffentlicher Sicherheit, sowie der Rolle von Informationssicherheitsbeauftragten bereits belastbare Policy-Forschung gibt, müssten bei anderen Aspekten, wie zum Beispiel der Aufstellung des NCAZ, noch weitere Analysen angefertigt werden. Diese Grundlagen wären vor allem wichtig, wenn ein „Ressortwechsel des BSI“ oder „das BSI als Oberste Bundesbehörde“ angestrebt würden.

Zur zeitnahen Umsetzung stünden „das BSI als Informationssicherheitsbeauftragter des Bundes“, „ausschließlich Rechtsaufsicht durch das BMI“ oder eine Kombination aus diesen Optionen zur Debatte. Währenddessen gilt es, die Policy-Grundlagenarbeit in den genannten Punkten weiter voranzutreiben. So könnte der Erfolg des gewählten Modells von einem unabhängigen Expert:innengremium beurteilt werden und je nach Ergebnis mittelfristig eins der anderen Modelle, „Ressortwechsel des BSI“ oder „das BSI als Oberste Bundesbehörde“, umgesetzt werden.

Die Rolle des BSI in der deutschen Cybersicherheitsarchitektur ist von elementarer strategischer Natur für die Cybersicherheitspolitik und damit indirekt auch für die Sicherheits-, Außen-, Wirtschafts-, und Digitalpolitik. Die Policy-Frage zur Unabhängigkeit des BSI muss daher, unabhängig davon, wie sich die Bundesregierung entscheidet, in der für 2021 geplanten Cybersicherheitsstrategie adressiert werden.

Danksagung
Ein besonderer Dank geht an die deutsche Cybersicherheitspolitik Community für die wie immer hervorragende Unterstützung bei der Erstellung dieser Kurzanalyse.

Über die Stiftung Neue Verantwortung

Die Stiftung Neue Verantwortung (SNV) ist ein gemeinnütziger Think Tank, der an der Schnittstelle von Technologie und Gesellschaft arbeitet. Die Kernmethode der SNV ist die kollaborative Entwicklung von Politikvorschlägen und -analysen. Die Expert:innen der SNV arbeiten nicht allein, sondern entwickeln und testen Ideen gemeinsam mit Vertreter:innen aus Politik und Verwaltung, Technologieunternehmen, Zivilgesellschaft und Wissenschaft. Unsere Expert:innen arbeiten unabhängig von Interessengruppen und Parteien. Unsere Unabhängigkeit gewährleisten wir durch eine Mischfinanzierung, zu der viele verschiedene Stiftungen, öffentliche Mittel und Unternehmensspenden beitragen.

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, sowie der Verwundbarkeit von Künstlicher Intelligenz gegen Cyberangriffe.

So erreichen Sie den Autor

Dr. Sven Herpig
Leiter für Internationale Cybersicherheitspolitik
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:
Jan Klöthe