Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

16. Januar 2025

Prüfbericht «Integration des NCSC ins VBS - Prozessprüfung»

IT-Prüfung I 2024-05

The Institute of Internal Auditors
IIA Switzerland

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

Frau
Bundesrätin Viola Amherd
Chefin VBS
Bundeshaus Ost
3003 Bern

Bern, 16. Januar 2025

Prüfbericht «Integration des NCSC ins VBS - Prozessprüfung»

Sehr geehrte Frau Bundesrätin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «Integration des NCSC ins VBS - Prozessprüfung» zukommen. Den vorliegenden Bericht haben wir mit unseren Ansprechpersonen besprochen. Die Stellungnahmen der Verwaltungseinheiten zu unserem Bericht sind in Kapitel 6 ersichtlich.

Diese Prüfung wurde in Übereinstimmung mit den internationalen Standards für die berufliche Praxis der internen Revision durchgeführt.

Sollten Sie Fragen zu unserem Bericht haben, stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Interne Revision VBS

[redacted]

Verteiler
– Generalsekretär VBS
– Staatssekretär SEPOS
– Direktor BACS

Leiter Interne Revision VBS

Interne Revision VBS
Schauplatzgasse 11
3003 Bern

Management Summary

Um die Cybersicherheit zu stärken, sollte das bisherige Nationale Zentrum für Cybersicherheit (NCSC) in ein Bundesamt überführt werden. Der Bundesrat beschloss an seiner Sitzung vom 2. Dezember 2022, dieses Bundesamt per 1. Januar 2024 im VBS anzusiedeln.

Die Interne Revision VBS (IR VBS) prüfte zur Einschätzung des Transformationsrisikos bei der Integration des NCSC ins VBS u. a. die Betriebsorganisation bzw. die entsprechenden Betriebsprozesse.

Die bestehende Organisation des NCSC wurde übernommen und mit dem Bereich «Planung und Steuerung» ergänzt, damit die Supportaufgaben, die Koordination der NCS etc. selbständig erfüllt werden können. Die rechtlichen Grundlagen wurden geschaffen, bevor das Bundesamt für Cybersicherheit (BACS) den operativen Betrieb im VBS per 1. Januar 2024 aufgenommen hat. Die Geschäftsordnung des BACS (GO BACS) wurde rückwirkend per 1. Mai 2024 in Kraft gesetzt. Das BACS hat die neuen Governance-Strukturen definiert und sich mit Aufnahme der operativen Tätigkeiten in die Strukturen und Gremien des VBS integriert.

Die Strategie des BACS vom 6. Mai 2024 basiert auf den vier strategischen Säulen «Cyberbedrohungen verständlich machen», «Mittel zur Verhinderung von Cyberangriffen zur Verfügung stellen», «Schäden aus Cybervorfällen reduzieren» sowie «Sicherheit von digitalen Produkten und Dienstleistungen erhöhen». Damit das BACS den Herausforderungen in der Cybersicherheit gerecht werden und die steigende Erwartungshaltung erfüllen kann, ist eine kontinuierliche Weiterentwicklung notwendig.

Seit dem Entscheid des Bundesrates im 2019 mit den damaligen NCSC ein Kompetenzzentrum zu schaffen, wurden die Mittel sukzessive erhöht, so dass 2025 etwa doppelt so viele Mittel zur Verfügung stehen wie noch 2020. Die Mittelerhöhung fand allerdings fast ausschliesslich beim Personalaufwand statt. Die Sachmittel sind seit 2019 unverändert geblieben. Ohne zusätzliche Finanzmittel während den nächsten Jahren kann das BACS die Weiterentwicklung der Anlaufstelle für Cyberbedrohungen nicht, wie in der Strategie BACS geplant, umsetzen. Damit könnte sich die externe Wahrnehmung und die Fähigkeit des BACS mittel- bis langfristig verschlechtern und zu Lücken im Cybersicherheitsdispositiv der Schweiz führen. Gespräche zur Ausfinanzierung des BACS ab 2025 sind innerhalb des VBS wie auch interdepartemental gegenwärtig am Laufen.

Mit dem Aufwuchs und dem Status eines eigenständigen Bundesamtes steigen auch die Ansprüche an die Governance, Risk & Compliance. Es sind angemessene und bewährte Betriebsprozesse geplant bzw. bereits umgesetzt worden. Die Fachprozesse (Kernaufgaben) haben sich mit der Überführung ins VBS nicht wesentlich geändert. Die Supportprozesse wurden neu aufgebaut und etabliert sowie mit Leistungen der Dienstleistungszentren Finanzen und Personal des Eidgenössischen Finanzdepartements (EFD) erweitert.

Damit das BACS seinen Kernauftrag umsetzen kann, ist es auf die Zusammenarbeit mit sicherheitsrelevanten Behörden innerhalb des Departements, der öffentlichen Verwaltung wie auch der Wirtschaft und Wissenschaft angewiesen. Die aufgaben- und zielorientierte Zusammenarbeit mit sicherheitsrelevanten Behörden war bereits im NCSC etabliert und wurde unverändert ins BACS übernommen. Obwohl die Zusammenarbeit als zielführend wahrgenommen wird, müssen noch vereinzelt Abgrenzungsfragen geregelt werden und sich deren praktische Umsetzung einspielen. Die Rollentrennung muss für alle klar und für den Krisenfall erprobt sein. Es muss auf bestehende Konzepte zurückgegriffen werden können. Die Prozesse der Zusammenarbeit sind zu formalisieren und zu institutionalisieren.

Die Aufgaben und Kompetenzen der drei Verwaltungseinheiten (VE) Generalsekretariat VBS (GS-VBS), Staatssekretariat für Sicherheitspolitik SEPOS und BACS bezüglich Informations- und Cybersicherheit sind im Informationssicherheitsgesetz (ISG) und der dazugehörigen Ausführungsverordnung geregelt. Mit der Inkraftsetzung der Cybersicherheitsverordnung (CSV) voraussichtlich im zweiten Quartal 2025 werden die Aufgaben des BACS weiter präzisiert. Das BACS wurde in die Prozesse des VBS eingebunden und es findet ein regelmässiger Austausch zwischen den Vertreterinnen und Vertretern der VE statt. *Die IR VBS empfiehlt dem Generalsekretariat VBS (GS-VBS) – nach Abschluss des finalen vom Bundesrat beauftragten Evaluationsberichts über die Funktionsweise der Fachstelle Informationssicherheit des Bundes und Etablierung der Strukturen – das Thema der Cybersicherheit gesamtheitlich zu beurteilen. Dabei soll u. a. analysiert werden, ob innerhalb des VBS Prozesse weiter vereinfacht, Schnittstellen abgebaut und zusätzliche Kosten in Querschnittsbereichen eingespart werden können. Hierfür ist vom GS-VBS eine unabhängige Stelle einzusetzen.*

Das Subsidiaritätsprinzip ist ein zentrales Element des schweizerischen Staatsrechts. Das BACS ist verantwortlich für die Kernaufgaben im Bereich Cybersicherheit sowie die Koordination mit allen beteiligten Stellen. Die Aufgaben des BACS konzentrieren sich ausschliesslich auf die zivile Cybersicherheit und sind damit klar abgegrenzt von den Aufgaben des Nachrichtendienstes des Bundes (NDB) und den Zuständigkeiten der Armee im Bereich der Cyberdefence. Das Postulat «VBS. Subsidiarität und Cybersicherheit» (22.3368) hat den Bundesrat beauftragt, in einem Bericht darzulegen, wie der Subsidiaritätsbegriff im VBS neu geprüft wird und wie dieser insbesondere in der Zusammenarbeit mit den Sicherheitsdienstleistungen im Cyberbereich anzuwenden ist.

Gegenwärtig fehlt es im Cyberbereich an einer Rechtsgrundlage, damit das BACS auf einem vereinfachten Weg Unterstützungsleistungen vom Kommando Cyber (Kdo Cy) erhalten kann. Die IR VBS begrüsst, dass die Schaffung von rechtlichen Grundlagen geprüft werden soll, um solche Unterstützungsleistungen im Cyberbereich inskünftig zu vereinfachen.

1 Ausgangslage

Das heutige Bundesamt für Cybersicherheit (BACS) hat sich unter der Bezeichnung Nationales Zentrum für Cybersicherheit (NCSC) als zentrale Anlaufstelle für Cybersicherheitsfragen in der Schweiz etabliert und war bis Ende 2023 im Generalsekretariat des Eidgenössischen Finanzdepartement (GS-EFD) angesiedelt. Das NCSC war verantwortlich für die Koordination der nationalen Cyberstrategie (NCS), die Unterstützung öffentlicher und privater Akteure bei der Prävention und Bewältigung von Cybervorfällen sowie die Förderung der Zusammenarbeit zwischen verschiedenen Sektoren im Sinne einer Public Privat Partnership. Trotz seiner zentralen Rolle operierte das NCSC relativ unabhängig von anderen sicherheitsrelevanten Behörden und hatte begrenzte Durchsetzungsmöglichkeiten. Die personelle und technische Ausstattung des NCSC war nicht immer ausreichend, um den wachsenden Anforderungen gerecht zu werden.

Die Cybersicherheit in der Schweiz ist fragmentiert, mit verschiedenen Bundesämtern und Kantonen, die unterschiedliche Aspekte abdecken. Diese Eigenständigkeit und Eigenverantwortung u. a. bei den Kantonen sind auf den Föderalismus zurückzuführen, welcher hierzulande tief verankert ist. Dies führt zu Herausforderungen bei der Koordination und Reaktionsfähigkeit auf nationale Cyberbedrohungen.

In den vergangenen Jahren hat die Cybersicherheit auf allen Ebenen stark an Bedeutung gewonnen. Sie ist ein zentraler Faktor für den Wirtschaftsstandort Schweiz und für die Sicherheit der Bevölkerung im digitalen Raum. Auch in der nationalen und internationalen Aussen- und Sicherheitspolitik spielt die Cybersicherheit eine wichtige Rolle. Die Gewährleistung der Cybersicherheit ist daher zu einer unverzichtbaren Aufgabe des Bundes geworden.

Um die Cybersicherheit zu stärken, sollte das bisherige NCSC in ein Bundesamt überführt werden. Der Bundesrat beschloss an seiner Sitzung vom 2. Dezember 2022, dieses Bundesamt per 1. Januar 2024 im VBS anzusiedeln. Dazu startete das VBS am 30. Januar 2023 das Projekt «Überführung des NCSC in ein Bundesamt für Cybersicherheit (BACS)». Die Aufgaben zu den Haupt-Meilensteinen 2023 wurden erfolgreich umgesetzt. Das BACS hat den operativen Betrieb per 1. Januar 2024 planmässig aufgenommen.

Die Vision des BACS ist es, die Cybersicherheit in der Schweiz in enger Zusammenarbeit mit allen relevanten Akteuren zu verbessern: «Das Bundesamt für Cybersicherheit (BACS) legt das Fundament für eine sichere Nutzung digitaler Dienstleistungen und Infrastrukturen in der Schweiz und befähigt die Schweiz, zu einem der führenden Länder bezüglich sicherer Digitalisierung zu werden.»[1]

[1] Bundesamt für Cybersicherheit BACS, Strategie des BACS (admin.ch) (Stand: 12.09.2024)

Das BACS richtet seine Leistung entlang vier strategischer Säulen aus:

1) Cyberbedrohungen verständlich machen.
2) Mittel zur Verhinderung von Cyberangriffen zur Verfügung stellen.
3) Schäden aus Cybervorfällen reduzieren.
4) Sicherheit von digitalen Produkten und Dienstleistungen erhöhen.

Das BACS als Kompetenzzentrum des Bundes für Cybersicherheit koordiniert die Umsetzung der NCS und ist erste Anlaufstelle für die Verwaltung, Wirtschaft, Bildungseinrichtungen und Bevölkerung bei Cyberfragen. Es nimmt Meldungen zu Cybervorfällen entgegen und unterstützt insbesondere Betreiberinnen von kritischen Infrastrukturen (BKI) bei der Bewältigung. Zudem erstellt das BACS technische Analysen zur Bewertung und Abwehr von Cybervorfällen und Cyberbedrohungen sowie zur Identifikation und Behebung von Schwachstellen beim Schutz der Schweiz vor Cyberbedrohungen.

2 Auftrag, Methodik und Abgrenzung

Die Chefin VBS erteilte der Internen Revision (IR VBS) am 4. Juni 2024 den Auftrag, zur Einschätzung des Transformationsrisikos bei der Integration des NCSC ins VBS u. a. die Betriebsorganisation bzw. die entsprechenden Betriebsprozesse zu prüfen.

Im Rahmen dieses Prüfauftrages führte die IR VBS strukturierte Befragungen mit den für die Integration und Umsetzung verantwortlichen Personen beim BACS durch. Zudem wurden weitere Vertreterinnen und Vertreter innerhalb des Departements wie auch der Bundesverwaltung sowie aus der Industrie befragt, welche in ihrer Funktion mit dem BACS zusammenarbeiten (u. a. Generalsekretariat VBS, Staatssekretariat für Sicherheitspolitik SEPOS, Nachrichtendienst des Bundes, Kommando Cyber, Bundesamt für Polizei fedpol, Steuerungsausschuss NCS). Ergänzend analysierte die IR VBS Dokumente, welche ihr zur Verfügung gestellt wurden. Des Weiteren zog die IR VBS externe, öffentlich zugängliche Unterlagen bei.

Die Feststellungen bilden den Zustand der Integration ins VBS bis zum Abschluss der Prüfungshandlungen per Mitte Oktober 2024 ab. Darauf basieren auch die Beurteilungen und Empfehlungen. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach Abschluss der Prüfungsdurchführung.

3 Unterlagen und Auskunftserteilung

Die Interviewpartnerinnen und Interviewpartner des BACS sowie weiterer Stellen innerhalb und ausserhalb der Bundesverwaltung haben der IR VBS die notwendigen Auskünfte umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen standen dem Prüfteam vollumfänglich zur Verfügung. Die IR VBS dankt für die gewährte Unterstützung.

4 Rechtliche Verankerung

Die rechtlichen Grundlagen wurden geschaffen, bevor das BACS den operativen Betrieb im VBS per 1. Januar 2024 aufgenommen hat. Einerseits wurde die Regierungs- und Verwaltungsorganisationsverordnung (RVOV)[2] vom 25. November 1998 entsprechend angepasst. Andererseits wurde das BACS in die Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (OV-VBS)[3] vom 7. März 2003 in Artikel 15*a* aufgenommen, wo die Funktionen zur Verfolgung der Ziele beschrieben werden. Auch in der Geschäftsordnung VBS (GO VBS) vom 21. Dezember 2023 wurden die notwendigen Anpassungen vorgenommen.

Beurteilung

Die rechtlichen Grundlagen wurden geschaffen, damit das BACS den operativen Betrieb im VBS per 1. Januar 2024 aufnehmen konnte.

5 Governance und Ressourcenmanagement

5.1 Betriebsorganisation

An seiner Sitzung vom 19. April 2023 hat der Bundesrat Beschlüsse zu den Ressourcen gefällt. Die eingestellten Personal- und Sachmittel für das ehemalige NCSC in der Höhe von 13,7 Millionen Franken wurden vom GS-EFD ins BACS im VBS verschoben. Damit das BACS die Supportaufgaben im Bereich Controlling, Finanzen, Beschaffung, Personal, Informatik und Recht eigenständig wahrnehmen kann, hat der Bundesrat entschieden, per 1. Januar 2024 das Budget um 0,8 Millionen Franken aufzustocken. Diese Supportaufgaben wurden in der Vergangenheit durch die Geschäftsstelle des NCSC in Zusammenarbeit mit dem GS-EFD wahrgenommen, dem das NCSC als Bereich angegliedert war.

Das BACS hat seine operative Tätigkeit planmässig per Anfang 2024 aufgenommen. Die wichtigsten Supportstellen konnten im Jahresverlauf geschaffen und etabliert werden. Bis Ende 2024 werden alle bei der Schaffung des Bundesamts gesprochenen zusätzlichen Stellen besetzt sein. Des Weiteren wurde eine Strategie erarbeitet. Diese wurde am 6. Mai 2024 öffentlich kommuniziert.[4]

Die Geschäftsordnung des BACS (GO BACS) wurde rückwirkend per 1. Mai 2024 in Kraft gesetzt. In Ausführung von Artikel 9 der gültigen GO BACS wurde zudem das Unterschriften-

[2] SR **172.010.1** - Regierungs- und Verwaltungsorganisationsverordnung (RVOV) vom 25. November 1998

[3] SR **172.214.1** - Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (OV-VBS) vom 7. März 2003

[4] Bundesamt für Cybersicherheit BACS, Strategie des BACS (admin.ch) (Stand: 12.09.2024)

reglement BACS finalisiert und freigegeben. Das BACS hat die neuen Governance-Strukturen definiert und sich mit Aufnahme der operativen Tätigkeiten in die Strukturen und Gremien des VBS integriert.

Beurteilung

Die Prüfung ergab ein positives Gesamtbild bezüglich der umgesetzten Betriebsorganisation. Die bestehende Organisation des NCSC wurde übernommen und mit dem Bereich «Planung und Steuerung» ergänzt, damit die Supportaufgaben, die Koordination der NCS etc. selbständig erfüllt werden können.

5.2 Strategie und Weiterentwicklung

Die Strategie des BACS vom 6. Mai 2024 basiert auf den vier strategischen Säulen «Cyberbedrohungen verständlich machen», «Mittel zur Verhinderung von Cyberangriffen zur Verfügung stellen», «Schäden aus Cybervorfällen reduzieren» sowie «Sicherheit von digitalen Produkten und Dienstleistungen erhöhen». Sie stellt eine konsequente Weiterführung der bisherigen Dienstleistungen dar und orientiert sich an der Dachstrategie, der NCS.

Das BACS prüft laufend, wie die Strukturen optimiert werden können. Im Rahmen des Entwicklungsplanes hat das BACS eine Selbsteinschätzung des Reifegrades in den vier strategischen Säulen vorgenommen. Daraus abgeleitet wurden Varianten erarbeitet, die aufzeigen, welche Ressourceninvestitionen nötig sind, um den Reifegrad weiter zu verbessern.

Die Chefin VBS hat an der Amtsleitungssitzung vom 30. Januar 2024 beschlossen, den Ausbau des BACS zur Umsetzung der Meldepflicht zu beginnen und diesen allenfalls zu etappieren. Der Reifegrad bei den strategischen Säulen soll gesamthaft angehoben werden.

Beurteilung

Damit das BACS den Herausforderungen in der Cybersicherheit gerecht werden und die steigende Erwartungshaltung erfüllen kann, ist eine kontinuierliche Weiterentwicklung notwendig. Die IR VBS begrüsst den Entscheid, den Ausbau des BACS zur Umsetzung der Meldepflicht rasch in Angriff zu nehmen und den Reifegrad mittelfristig über alle strategischen Säulen hinweg anzuheben.

5.3 Finanzen und Ressourcen

Mit der Überführung vom NCSC zu einem Bundesamt im VBS wurden Supportstellen, aber keine weiteren finanziellen Mittel für bestehende und noch nicht finanzierte sowie neu beschlossene Aufgaben für die Cybersicherheit gesprochen. Für die Supportaufgaben wurde dem BACS per 1. Januar 2024 eine Budgeterhöhung um 0,8 Millionen Franken zugespro-

chen. Der Mehrbedarf im Sach- und Betriebsaufwand fürs Jahr 2024 kann durch den Minderbedarf im Personalaufwand aufgrund von Vakanzen und gestaffelter Rekrutierung im laufenden Jahr gedeckt werden.

Seit dem Entscheid des Bundesrates im 2019 mit den damaligen NCSC ein Kompetenzzentrum zu schaffen, wurden die Mittel sukzessive erhöht, so dass 2025 etwa doppelt so viele Mittel zur Verfügung stehen wie noch 2020. Die Mittelerhöhung fand allerdings fast ausschliesslich beim Personalaufwand statt, wobei sich der Personalbestand von 2020 bis 2025 von 28 auf 67 Mitarbeitende erhöhen wird. Das BACS konnte früher, als NCSC im EFD, nur durch den permanenten Einsatz von nicht ausgeschöpften gesprochenen Personalmitteln von rund 2 Millionen Franken die dringend notwendigen Sachausgaben finanzieren. Für das heutige Bundesamt sind personelle Mittel im Umfang von 11,7 Millionen Franken bewilligt, die Sachmittel sind aber seit 2019 unverändert geblieben. In der gleichen Zeit sind die Cyberbedrohungen stark angestiegen und der Bedarf aus Wirtschaft und Bevölkerung an Unterstützung durch das BACS wurde massiv höher. Im Jahr 2020 hat das NCSC rund 11'000 Meldungen entgegengenommen, im 2023 waren es bereits 50'000.

Ohne die zusätzlichen Finanzmittel während den nächsten Jahren kann das BACS die Weiterentwicklung der Anlaufstelle für Cyberbedrohungen nicht, wie in der Strategie BACS geplant, umsetzen. Zudem erfordert die Einführung der Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen per 1. Januar 2025 Mehrmittel, die dem BACS zum Prüfungszeitpunkt nicht zugesprochen wurden. Gegenwärtig laufen intensive interdepartementale Gespräche auf mehreren Stufen, um diesen Umstand zu regeln. Aufgrund der zu ergreifenden Sparmassnahmen in der Bundesverwaltung ist eine Lösung zurzeit nicht absehbar.

Beurteilung

Mit der Einführung der Meldepflicht für Cyberangriffe auf kritische Infrastrukturen werden die Aufgaben des BACS zunehmen. Dadurch wird sich die Anzahl der vom BACS erhaltenen Meldungen weiter erhöhen. Auch in den strategischen Säulen 2 (Cyberangriffe verhindern) und 3 (Schäden reduzieren) müssen zusätzliche Leistungen erbracht werden. Sollte das BACS ab 2025 nicht ausfinanziert sein, besteht das Risiko, dass beschlossene Aufgaben und Leistungen nicht mehr vollumfänglich wahrgenommen werden können. Ohne Ausbau der Ressourcen müssten wohl dazu Leistungen in den Säulen 1 (Bedrohungen verständlich machen) und 4 (sichere Produkte und Dienstleistungen) abgebaut werden. U. a. könnte die Weiterentwicklung der Anlaufstelle für Cyberbedrohungen nicht wie geplant umgesetzt werden und Schwachstellen des Bundes könnten nicht mehr mittels «Bug Bounty»-Programmen identifiziert werden. Ferner könnten sich die externe Wahrnehmung und Fähigkeit des BACS mittel- bis langfristig verschlechtern und zu Lücken im Cybersicherheitsdispositiv der Schweiz führen.

Aufgrund dessen, dass gegenwärtig Gespräche innerhalb des VBS wie auch interdepartemental zur Ausfinanzierung des BACS ab 2025 am Laufen sind, verzichtet die IR VBS auf die Abgabe einer Empfehlung.

5.4 Betriebsprozesse

Während in Artikel 15*a* Absatz 2 der OV-VBS enumerativ festgehalten wird, welche Funktionen das BACS wahrnimmt, um die Ziele als Kompetenzzentrum des Bundes für Cybersicherheit zu verfolgen, sind in Kapitel 5 des Informationssicherheitsgesetzes (ISG)[5] vom 18. Dezember 2020 sowie in der Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee (Informationssicherheitsverordnung, ISV)[6] vom 8. November 2023 die Aufgaben und Kompetenzen vom BACS stipuliert. Des Weiteren werden in der Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV)[7] u. a. die Aufgaben des BACS spezifiziert. Diese wird voraussichtlich im zweiten Quartal 2025 in Kraft treten.

Die Fachprozesse (Kernaufgaben) haben sich mit der Überführung ins VBS nicht wesentlich geändert. Aus diesem Grund konnten die vorhandenen Dokumentationen vom NCSC übernommen und entsprechend angepasst werden. Da das BACS die Supportaufgaben im Bereich Finanzen, Controlling, Beschaffung, Personal, Informatik und Recht seit dem 1. Januar 2024 mehrheitlich eigenständig wahrnimmt, wird die Dokumentation der relevanten Prozesse laufend ergänzt und optimiert. Die Supportprozesse wurden neu aufgebaut und etabliert sowie mit Leistungen der Dienstleistungszentren Finanzen und Personal des EFD erweitert.

Des Weiteren wurde die Richtlinie für das interne Kontrollsystem (IKS) erstellt und per 30. April 2024 in Kraft gesetzt. Die IKS-relevanten Geschäftsprozesse wurden mehrheitlich dokumentiert und entsprechende Kontrollen implementiert. Auch werden aktuell die Fachprozesse für die Meldepflicht für kritische Infrastrukturen beurteilt, überarbeitet und dokumentiert. Die Geschäftsprozesse werden laufend ergänzt und bei Bedarf aktualisiert. Das Risikomanagement (RM) befindet sich – in enger Abstimmung mit dem RM Departement sowie der Koordinationsstelle RM Bund – gegenwärtig im Ausbau.

Beurteilung

Es sind angemessene und bewährte Betriebsprozesse geplant bzw. bereits umgesetzt worden. Doch mit dem Aufwuchs und dem Status eines eigenständigen Bundesamtes steigen auch die Ansprüche an die Governance, Risk & Compliance. Das BACS muss nun sicherstellen, dass die Dokumentationen zeitnah erstellt bzw. überarbeitet und anschliessend regelmässig aktualisiert werden. Aufgrund dessen, dass die Geschäftsprozesse und die dazugehörigen Dokumentationen gegenwärtig erarbeitet und finalisiert werden, verzichtet die IR VBS auf die Abgabe einer Empfehlung.

---

5 SR **128** - Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG)

6 SR **128.1** - Verordnung vom 8. November 2023 über die Informationssicherheit in der Bundesverwaltung und der Armee (Informationssicherheitsverordnung, ISV)

7 Der Bundesrat, Bundesrat eröffnet Vernehmlassung zur Cybersicherheitsverordnung (Stand: 19.11.2024)

5.5 Zusammenarbeit mit sicherheitsrelevanten Behörden

Cybersicherheit ist ein Querschnittsthema, das nicht einer einzelnen sicherheitsrelevanten Behörde zugeordnet werden kann. Dies gilt besonders für die Schweiz, die durch föderalistische Strukturen geprägt ist. Damit das BACS seinen Kernauftrag umsetzen kann, ist es auf die Zusammenarbeit mit sicherheitsrelevanten Behörden innerhalb des Departements, der öffentlichen Verwaltung wie auch der Wirtschaft und Wissenschaft angewiesen. Unter Berücksichtigung der rechtlichen Grundlagen, die unabhängig von der organisatorischen Zugehörigkeit gelten, sollen mit der Integration ins VBS Schnittstellen abgebaut und Synergien genutzt werden. Nachfolgend wird die Zusammenarbeit des BACS mit einer Auswahl an sicherheitsrelevanten Behörden aufgeführt. Daneben gibt es noch eine Vielzahl weiterer Ausschüsse, Gremien etc., in denen das BACS vertreten ist, welche aber nicht näher beschrieben werden.

Staatssekretariat für Sicherheitspolitik (SEPOS)
In Artikel 51 Absatz 6 der ISV wird ausgeführt, dass das BACS gewisse Aufgaben und Kompetenzen der Fachstelle des Bundes für Informationssicherheit – in der ebenfalls per 1. Januar 2024 neu geschaffenen Verwaltungseinheit (VE) SEPOS – bis Mitte 2025 wahrnimmt. Zusammen mit der Anpassung der OV-VBS führen die neuen Rechtsgrundlagen im ISG sowie deren Ausführungsverordnung zu Änderungen der Prozesse und der Zuständigkeiten im Bereich Cybersicherheit. Während die normativen Grundlagen geschaffen wurden, werden die Modalitäten dieser Zusammenarbeit bis Mitte 2025 etabliert. Der Bundesrat hat das VBS im Zusammenhang mit dem Umsetzungsrecht ISG beauftragt, die Modalitäten der Zusammenarbeit zwischen dem SEPOS (Fachstelle des Bundes für Informationssicherheit) und dem BACS bis Ende 2024 in einem Evaluationsbericht festzuhalten. Diese Arbeiten sind gegenwärtig im Gang (siehe Abschnitt 5.6).

Bundesamt für Polizei fedpol
Die Cyber-Strafverfolgung im fedpol des Eidgenössischen Justiz- und Polizeidepartements (EJPD) besteht in der Koordination bzw. im Informationsaustausch auf nationaler und internationaler Ebene sowie in der Vornahme von Ermittlungen in eigener Zuständigkeit. Die Zusammenarbeit hat sich mit der Integration ins VBS nicht wesentlich geändert. Die Aufgaben und Verantwortlichkeiten sind genügend klar definiert. Es wird weiterhin auf etablierte Prozesse zum Informationsaustausch abgestützt. Für das fedpol besteht Klärungsbedarf hinsichtlich der Zuständigkeit für die Koordination bei grösseren Cybersicherheitsvorfällen, die auch die Bundesverwaltung betreffen.

Steuerungsausschuss der Nationalen Cyberstrategie (StA NCS)
Der StA NCS setzt sich aus Vertretungen der Bundesverwaltung, der Kantone, der Wirtschaft, der Hochschulen und der Zivilgesellschaft zusammen und hat u. a. die Aufgabe, die Prioritäten und Zeitpläne für die Umsetzung der Massnahmen zu definieren, den Fortschritt bei der Umsetzung der Massnahmen laufend zu beurteilen und für die laufende Weiterentwicklung der NCS zu sorgen. Zum Prüfungszeitpunkt hat der StA NCS zweimal getagt und

die Zusammenarbeit mit dem BACS wird bislang als positiv wahrgenommen. An diesen Sitzungen ist das BACS standardmässig eingeladen. Zudem findet ein regelmässiger Austausch zwischen der Präsidentin des StA NCS und der Direktion des BACS statt. Der StA NCS bekommt heute vom BACS die notwendige fachliche und administrative Unterstützung, um die mandatierten Aufgaben wahrzunehmen.

Nachrichtendienst des Bundes (NDB)
Der NDB ist ein sicherheitspolitisches Instrument der Schweiz. Seine Aufgaben sind in Artikel 6 des Bundesgesetzes über den Nachrichtendienst (Nachrichtendienstgesetz, NDG)[8] vom 25. September 2015 definiert. Bereits im zweiten Halbjahr 2023 haben sich der Direktor des NDB sowie der designierte Direktor BACS geeinigt, die ihrem Auftrag am besten entsprechende Aufgaben- und Ressourcenaufteilung weiter zu verfolgen. Dem BACS wurden alle Tätigkeiten übertragen, die dem operativen Austausch mit BACS-Partnern sowie der Aufbereitung und Auswertung des BACS-Informationsaufkommens dienen. Diese Aufgabenverschiebung bewahrt die operative Integrität und Funktionsfähigkeit beider VE und führt innerhalb beider Organisationen zu einem Mehrwert. Artikel 76*a* revISG[9] klärt die Rollenteilung zwischen dem BACS und dem NDB (Absatz 1) sowie den Inhalt und die Art und Weise der Informationsübermittlung an den NDB, die Strafverfolgungsbehörden und die kantonalen Stellen, die für Cybersicherheit zuständig sind (Absätze 2 bis 4). Die Zusammenarbeit zwischen dem NDB und BACS wird von den Beteiligten als zielführend wahrgenommen.

Kommando Cyber (Kdo Cy; Armee)
Während der Kernauftrag des BACS darin besteht, die Cybersicherheit im zivilen Bereich zu stärken, besteht die Kernleistung des Kdo Cy der Armee im Cyber und elektromagnetischen Raum darin, Informationen und Services auf der eigenen, einsatzkritischen Informations- und Kommunikationstechnologie (IKT) ortsunabhängig zur Verfügung zu stellen und zu schützen. Die Funktionen und Zuständigkeiten des Kdo Cyber sind in Artikel 96 und Artikel 100 Absatz 1 Buchstabe c des Bundesgesetzes über die Armee und die Militärverwaltung (Militärgesetz, MG)[10] vom 3. Februar 1995, Artikel 11 Buchstabe d OV-VBS und in der Verordnung über die militärische Cyberabwehr (MCAV)[11] vom 30. Januar 2019 (insbesondere Art. 4 MCAV) geregelt. Der Austausch zwischen diesen beiden VE erfolgt regelmässig über alle Ebenen mit periodischen Gesprächen auf der Stufe Direktion (siehe auch Abschnitt 5.7). Die Aufgaben und Verantwortlichkeiten sind für das Kdo Cy während der normalen Lage klar geregelt.[12] Auch wird die Zusammenarbeit mit dem BACS als zielführend wahrgenommen. In

8 SR **121** - Bundesgesetz vom 25. September 2015 über den Nachrichtendienst (Nachrichtendienstgesetz, NDG)

9 BBl **2023** 84 - Botschaft zur Änderung des Informationssicherheitsgesetzes (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen)

10 SR **510.10** - Bundesgesetz vom 3. Februar 1995 über die Armee und die Militärverwaltung (Militärgesetz, MG)

11 SR **510.921** - Verordnung vom 30. Januar 2019 über die militärische Cyberabwehr (MCAV)

12 BBl **2007** 8293 - Weisungen über organisatorische Massnahmen in der Bundesverwaltung zur Bewältigung besonderer und ausserordentlicher Lagen

Absprache mit dem SEPOS – und unter Einbezug des BACS – erarbeitet das Kdo Cy gegenwärtig «High-Level Use Cases», welche definieren sollen, wie die Aufgaben und Kompetenzen im Falle einer besonderen respektive ausserordentlichen Lage geregelt werden könnten.

Beurteilung

Der Schutz vor Cyberbedrohungen ist eine gemeinsame Verantwortung von Wirtschaft, Gesellschaft und Staat. Innerhalb des Departements nehmen die VE verschiedene Aufgaben im Bereich Cyber wahr. Die aufgaben- und zielorientierte Zusammenarbeit mit sicherheitsrelevanten Behörden war bereits im NCSC etabliert und wurde unverändert ins BACS übernommen. Aus Sicht der IR VBS funktioniert die Zusammenarbeit weiterhin gut. Insbesondere auf fachlicher Ebene wird vertrauensvoll mit allen Anspruchsgruppen zusammengearbeitet. Obwohl die Zusammenarbeit als zielführend wahrgenommen wird, müssen noch vereinzelt Abgrenzungsfragen geregelt werden und sich deren praktische Umsetzung einspielen. Die Rollentrennung muss für alle klar und für den Krisenfall erprobt sein. Diese Trennung und die klaren Verantwortlichkeiten sind v. a. bei Cybervorfällen von zentraler Bedeutung, um zentrale Anlaufstellen und eine klare Aufgabenteilung bzw. -zuweisung zu haben, welche sich in herausfordernden Phasen bewähren. Es muss auf bestehende Konzepte zurückgegriffen werden können. Die Prozesse der Zusammenarbeit sind zu formalisieren und zu institutionalisieren.

5.6 Synergien im Bereich der Cybersicherheit im VBS

Die Aufgaben und Kompetenzen der drei VE Generalsekretariat VBS (GS-VBS), SEPOS und BACS bezüglich Informations- und Cybersicherheit sind im ISG und der dazugehörigen Ausführungsverordnung geregelt. Mit der Inkraftsetzung der CSV voraussichtlich im zweiten Quartal 2025 werden die Aufgaben des BACS weiter präzisiert.

Das BACS sowie das SEPOS sind im VBS seit dem 1. Januar 2024 im operationellen Betrieb. Während die Modalitäten der Zusammenarbeit zwischen dem SEPOS (Fachstelle des Bundes für Informationssicherheit) und dem BACS bis Ende 2024 in einem Evaluationsbericht festgehalten werden, wird im GS-VBS gegenwärtig die Sicherheitsgovernance VBS erarbeitet. Dabei ist bei den Aufgabenbereichen der jeweiligen VE zwischen den drei Ebenen National, Bund und Departement zu unterschieden.

Das BACS wurde in die Prozesse des VBS eingebunden und es findet ein regelmässiger Austausch zwischen den Vertreterinnen und Vertretern der VE statt.

Beurteilung

Aktuell übernehmen neben dem BACS auch das GS-VBS sowie das SEPOS Aufgaben, welche sich mit der Cybersicherheit auseinandersetzen. Innerhalb des VBS könnten möglicherweise Prozesse weiter vereinfacht, Schnittstellen reduziert und Kosten in Querschnittsbereichen eingespart werden.

Ob die drei Prinzipien der Wirksamkeit, Sparsamkeit und Wirtschaftlichkeit in der öffentlichen Verwaltung und des Verwaltungsmanagements mit der Integration des NCSC ins VBS ihre erhoffte Wirkung hinsichtlich Synergieeffekte entfalten bzw. bereits nachweislich unter Beweis gestellt haben, kann zum Prüfungszeitpunkt noch nicht abschliessend beantwortet werden (siehe Abschnitt 5.5).

Empfehlung 1: Synergien im Bereich der Cybersicherheit im VBS

Die IR VBS empfiehlt dem Generalsekretariat VBS (GS-VBS) – nach Abschluss des finalen vom Bundesrat beauftragten Evaluationsberichts über die Funktionsweise der Fachstelle Informationssicherheit des Bundes und Etablierung der Strukturen – das Thema der Cybersicherheit gesamtheitlich zu beurteilen. Dabei soll u. a. analysiert werden, ob innerhalb des VBS Prozesse weiter vereinfacht, Schnittstellen abgebaut und zusätzliche Kosten in Querschnittsbereichen eingespart werden können. Hierfür ist vom GS-VBS eine unabhängige Stelle einzusetzen.

5.7 Subsidiarität im Bereich der Cybersicherheit

Das Subsidiaritätsprinzip ist ein zentrales Element des schweizerischen Staatsrechts. Dieses besagt, dass Aufgaben primär von der kleinsten staatlichen Ebene übernommen werden. Gemäss Artikel 43*a* der Bundesverfassung der Schweizerischen Eidgenossenschaft (BV)[13] vom 18. April 1999 übernimmt der Bund demnach nur die Aufgaben, welche die Kraft der Kantone übersteigt oder einer einheitlichen Regelung durch den Bund bedürfen. Im Bereich der inneren Sicherheit sind Bund und Kantone gemeinsam zuständig (Art. 57 BV), wobei die Verantwortung grundsätzlich bei den Kantonen liegt.

Das BACS ist verantwortlich für die Kernaufgaben im Bereich Cybersicherheit sowie die Koordination mit allen beteiligten Stellen. Die Aufgaben des BACS konzentrieren sich ausschliesslich auf die zivile Cybersicherheit und sind damit klar abgegrenzt von den Aufgaben des NDB und den Zuständigkeiten der Armee im Bereich der Cyberdefence (siehe Abschnitt 5.5). Das BACS übernimmt keine Aufsichts- oder Regulierungsaufgaben von Fachbehörden in den Sektoren. Es arbeitet eng mit den Fachämtern zusammen und stellt ihnen sein Fachwissen im Bereich Cybersicherheit zur Verfügung. Die Zuständigkeit für die Cyberstrafverfolgung liegt primär bei den Kantonen. Seitens des Bundes sind das fedpol und die Bundesanwaltschaft (BA) dafür verantwortlich. Die Kantone gestalten ihre Organisation der Cybersicherheit eigenständig und passen sie an ihre individuellen Bedürfnisse an. Die übergeordnete interkantonale Koordination zu Themen der Cybersicherheit findet über die Kantonale Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) statt. Die Zusammenarbeit mit dem Bund wird durch den Sicherheitsverbund Schweiz (SVS) koordiniert und gefördert.[14]

[13] SR **101** - Bundesverfassung der Schweizerischen Eidgenossenschaft (BV) vom 18. April 1999

[14] Der Bundesrat, «Nationale Cyberstrategie (NCS)» vom April 2023, S. 9-10

Das Postulat «VBS. Subsidiarität und Cybersicherheit» (22.3368)[15] hat den Bundesrat beauftragt, in einem Bericht darzulegen, wie der Subsidiaritätsbegriff im VBS neu geprüft wird und wie dieser insbesondere in der Zusammenarbeit mit den Sicherheitsdienstleistungen im Cyberbereich anzuwenden ist. In diesem Bericht vom 20. September 2024[16] wird nun festgehalten, dass das VBS sowohl im militärischen als auch im zivilen Bereich über ausgeprägte Cyberkompetenzen verfügt. Eine Zusammenarbeit zwischen dem militärischen Teil des Kdo Cy und dem BACS bei der Bewältigung eines kritischen Cybervorfalls kann jedoch nur unter den Voraussetzungen des Assistenzdienstes der Armee erfolgen. Dazu gehört, dass der Bundesrat über diesen Einsatz entscheidet. Bei Cybervorfällen müssen Spezialistinnen und Spezialisten schnell eingesetzt werden können. Dieser Entscheidungsweg erfordert jedoch Zeit und kann damit eine effiziente Zusammenarbeit zwischen dem BACS und dem Kdo Cy bei zeitkritischen Einsätzen erschweren.

Der Bundesrat kommt in seinem Bericht zum Schluss, dass die Schaffung von rechtlichen Grundlagen geprüft werden soll, um solche Unterstützungsleistungen im Cyberbereich zu vereinfachen. Das VBS wurde beauftragt, dem Bundesrat bis Ende 2026 Varianten zum weiteren Vorgehen zu unterbreiten. Bei den Rechtsgrundlagen muss berücksichtigt werden, dass das BACS in der normalen Lage die Gesamtverantwortung für Einsätze trägt, bei der es durch das Kdo Cy unterstützt wird. Die Trennung zwischen zivilen und militärischen Interessen muss bestehen bleiben. Auch muss die Vertraulichkeit von Meldungen ans BACS gewährleistet werden.

Beurteilung

Die Ereignisse in den Sommermonaten 2024 haben gezeigt, dass das VBS über einen Einsatz der Armee bei Katastrophen – wie etwa schweren Unwettern im Inland – entscheiden kann. Im Cyberbereich fehlt es an einer Rechtsgrundlage, damit das BACS auf einem solchen vereinfachten Weg Unterstützungsleistungen vom Kdo Cy erhalten kann. Aus diesem Grund begrüsst die IR VBS, dass die Schaffung von rechtlichen Grundlagen geprüft werden soll, um solche Unterstützungsleistungen im Cyberbereich inskünftig zu vereinfachen.

[15] 22.3368 | VBS. Subsidiarität und Cybersicherheit | Geschäft | Das Schweizer Parlament (Stand: 12.09.2024)

[16] Der Bundesrat, «VBS. Subsidiarität und Cybersicherheit - Bericht des Bundesrates in Erfüllung des Postulates 22.3368 Sicherheitspolitische Kommission NR vom 9. Mai 2022» vom 20. September 2024

6 Stellungnahmen

Generalsekretariat (GS-VBS)
Das GS-VBS ist mit den Empfehlungen einverstanden.

Staatssekretariat für Sicherheitspolitik (SEPOS)
Nous sommes d'accord avec la recommandation, dans le sens d'optimiser et de simplifier les processus pour créer des synergies et éliminer d'éventuels doublons. En revanche, l'exercice ne devrait pas consister à remettre en question les tâches et les compétences clairement définies dans le nouveau cadre légal. La clarté des tâches constitue, en effet, un facteur critique pour la sécurité. Nous pensons également qu'il faut laisser encore le temps aux unités concernées de s'établir, avant de lancer une telle analyse. L'exercice du rapport d'évaluation a montré qu'il est difficile d'évaluer une unité alors qu'elle n'est pas encore complètement opérationnelle. C'est pourquoi, nous sommes de l'avis que cette évaluation devrait être lancée une fois que le SEPOS aura repris les tâches du BACS selon l'art. 51 al. 6 de l'ordonnance sur la sécurité de l'information et sera complètement opérationnel. Seulement à ce moment-là, une analyse des processus pourra être pertinente.

Bundesamt für Cybersicherheit (BACS)
Das BACS dankt für die Möglichkeit, Stellung zu nehmen. Wir zeigen uns mit dem Bericht und den Einschätzungen einverstanden.