Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Generalsekretariat VBS
Digitalisierung und Cybersicherheit DCS

Del CYD VBS, 27.01.2021

Schlussbericht
Aktionsplan Cyberdefence VBS

Öffentliche Fassung

Inhaltsverzeichnis

1 Ausgangslage 3

2 Basis für die Beurteilung des APCD 3

2.1 Strategische Ziele 3

2.2 Umsetzungsziele 3

3 Gesamtbeurteilung des APCD 4

3.1 Fokus «Architektur» 4

3.2 Fokus «Strategische Aufgaben» 6

3.3 Fokus «Umsetzungsmassnahmen» 7

4 Verbesserungsmassnahmen 9

5 Bilanz und Ausblick 10

1 Ausgangslage

In den letzten Jahren hat Cybersicherheit stark an Bedeutung gewonnen, insbesondere nachdem die Bundesverwaltung mehrmals Opfer von Cyberangriffen wurde. Infolge des Cyberangriffs auf die RUAG 2016 erteilte der damalige Chef VBS den Auftrag, einen «Aktionsplan Cyberdefence VBS» (APCD) für die Periode 2017-2020 zu erstellen.

Der Zweck des vorliegenden Abschlussberichtes ist die Beurteilung der Zielerreichung des Aktionsplan Cyberdefence VBS. Der Abschlussbericht legt dar, welche Massnahmen umgesetzt wurden, in wie fern die Ziele erreicht werden konnten und in welchen Bereichen noch Lücken bestehen. Die «Strategie Cyberdefence VBS» wird für den Zeitraum 2021-2024 die Nachfolge des APCD sicherstellen.

2 Basis für die Beurteilung des APCD

Die Umsetzung des APCD erfolgte bis Ende 2020. Für die Messung der Ergebnisse wurden die **strategischen Ziele** (Ziff. 2.1) **und die Umsetzungsziele** (Ziff. 2.2) bewertet. Die Beurteilung basiert auf einer Selbsteinschätzung der Fachexperten der Verwaltungseinheiten des VBS (VE-VBS), da im Rahmen des APCD keine formalen Kriterien definiert worden sind.

2.1 Strategische Ziele

Die Ziele des APCD aus dem Jahr 2017 lauten wie folgt:

In enger Zusammenarbeit mit seinen Partnern, der Wirtschaft und den Hochschulen will das VBS ein anerkannter Pol von Kompetenzen im Bereich der Cyberabwehr werden. Es soll über quantitativ und qualitativ ausreichende Mittel verfügen, um die folgenden Ziele erreichen zu können:

- Dem VBS, als Betreiber kritischer Infrastrukturen und innerhalb seiner Kompetenzen ermöglichen, die in Anzahl, Intensität und Komplexität zunehmenden Formen der Cyberbedrohung zu bewältigen, sowohl im Alltag als auch im Falle einer Krise oder eines Konflikts;
- Die Cyberaspekte des Nachrichtendienstgesetzes (NDG) und des Militärgesetzes (MG) konkret umsetzen;
- In der Lage sein, die Betreiber kritischer Infrastrukturen, die Opfer von Cyberangriffen wurden, bei Bedarf wirksam und nachhaltig zu unterstützen.

2.2 Umsetzungsziele

Nebst den oben aufgeführten strategischen Zielen enthält die 2018 revidierte Fassung des APCD zusätzlich drei Umsetzungsziele:

- Die bestehenden Mittel zur Gewährleistung eines wirksamen Schutzes der VBS-Infrastrukturen zu optimieren;
- Das VBS befähigen, sich wirksam zu verteidigen und im Bedarfsfall ein glaubwürdiger Erbringer von Unterstützungsleistungen zu sein;
- Das VBS zu stärken und zu befähigen, auch im Konfliktfall im Cyberraum handlungsfähig zu sein.

3 Gesamtbeurteilung des APCD

3.1 Fokus «Architektur»

Zur Strukturierung der Aufgaben, Mittel und Prozesse der beteiligten VE-VBS wurde eine Architektur mit vier Funktionsbereichen definiert (Abbildung 1). Diese Architektur hat sich weitgehend **als zweckmässig erwiesen**.

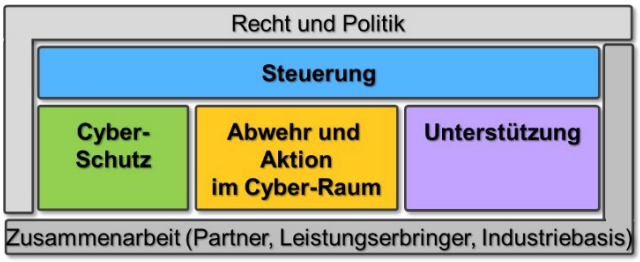

Abbildung 1 – Architektur des APCD

- **Steuerung**

  Mit der vierteljährlichen Konferenz Cyberdefence unter dem Vorsitz des Generalsekretärs VBS, der Schaffung der Stelle eines Delegierten VBS für Cyberdefence und seit Anfang 2020 der neuen Abteilung «Digitalisierung und Cybersicherheit»[1] verfügt das VBS über funktionierende Steuerungsinstrumente. Zusätzlich ist das VBS auf der strategischen Ebene im Rahmen des Cyberausschusses des Bundesrats, der Kerngruppe Cyber und des Steuerungsausschusses NCS vertreten. In diesen Gremien ist der Nachrichtendienst des Bundes (NDB) für die umfassende Bedrohungsbeurteilung (Lagedarstellung) zuständig.

- **Cyberschutz**

  Mit der Umsetzung der vom APCD gesetzten Ziele wurden im Bereich Cyberschutz massgebliche Fortschritte erzielt. Dazu zählt z.B. die Schaffung einer permanenten Überwachung der Netzwerke und Systeme mit der seit Ende 2019 neu geschaffenen Stelle eines *Chief Information Security Officer* (CISO) bei der FUB und des ihm unterstellten *Cyber Fusion Centers* (CFC), das u.a. aus dem militärischen *Computer Emergency Response Team* (milCERT) und dem neuen *Security Operations Center* (SOC) besteht.

- **Abwehr u. Aktion im Cyberraum**

  Der **Nachrichtendienst des Bundes** (NDB) hat wiederholt gezeigt, dass er Cyberangriffe auf Schweizer Interessen antizipieren, frühzeitig erkennen, verhindern und einem Akteur zuordnen kann (Attribution). Er bedient Entscheidungsträger auf föderaler und kantonaler Ebene mit Lagebeurteilungen. Die bestehenden Fähigkeiten müssen noch weiter ausgebaut werden, damit alle sicherheitspolitisch relevanten Cyberangriffe auf die Schweiz antizipiert, frühzeitig erkannt, verhindert und attribuiert werden können. 2019 wurde im Direktionsbereich *Steuerung und Lage*

[1] Zuerst als «Cyber, Informatik und Informationssicherheit (CII)» konstituiert, hat diese Abteilung die Aufgaben der ehemaligen Informations- und Objektsicherheit (IOS) im Bereich der Informationssicherheit wie auch des Bereichs Cyberdefence VBS übernommen.

(NDBS) die Funktion Steuerung für den Bereich *Cyber* geschaffen. Eine weitere Konsolidierung fand im NDB Themenbereich Cyber mit der Kreierung eines Ressorts *Cyber* (ehemals Cyber NDB) statt. Dieses besteht aus einem *Analysebereich* (operative Analyse CY), einem *technischen Analysebereich* (technische Analyse CY) und einem Bereich für *Research and Development*. Der Bedarf an der Stärkung des Bereichs *OSINT*[2] wurde im Rahmen der NCS 2 identifiziert. Die Besetzung der Stellen wird anfangs 2021 erfolgen. Der Bereich der technischen Analyse wurde schon teilweise gestärkt.

In der **Gruppe Verteidigung** (Gruppe V) wurden die Stellen mit dem APCD der FUB zwar zugewiesen aber die Rahmenbedingungen, die Anzahl Mitarbeitende und das Budget konnten nicht in Einklang gebracht werden. Durch den aktuellen Anstellungsstopp können die noch geplanten APCD-Stellen somit erst im 2021/22 aufgebaut werden. Zu den wichtigsten Entwicklungen in der Gruppe V gehört die Schaffung eines Cyberlehrgangs, welcher seit 2018 bereits zum fünften Mal durchgeführt werden konnte und in welchem bis anhin ca. 100 Milizangehörige ausgebildet wurden. Weiter wurde die *Cyber Training Range* (CTR) der Armee zur simulationsgestützten Ausbildung von Cyberspezialisten Ende 2020 in Betrieb genommen. Mit dem Start der beiden Projekte zur Schaffung von mobilen Einsatzmitteln (MCM) und zum Aufbau eines *Cyber Training Centers* (CTC) wurden zusätzliche, wichtige Massnahmen getroffen. Die Koordination des Bereichs Cyber mit den anderen Operationssphären beim Kommando Operationen wurde verbessert und letztlich wurde entschieden, die Synergien zwischen NDB und FUB im Bereich der technischen Analyse zu stärken. Die Abdeckung der sich aus diesen vielen Entwicklungen ergebenden Immobilien-Bedürfnisse wurden ebenfalls laufend sichergestellt.

- **Unterstützung**

  Im Verlauf der Umsetzung des APCD wurden die Fähigkeiten von armasuisse Wissenschaft und Technologie (ar W+T) bei der Beobachtung der technologischen Entwicklung sowie der Forschung und Entwicklung eigener Lösungen erkannt. Die Schaffung des CYD-Campus zur Erweiterung des ursprünglich vorgesehenen Dispositivs konnte ausgelöst werden und ist mittlerweile operationell. Wie die ersten konkreten Ergebnisse zeigen, erlaubt die enge Zusammenarbeit mit den ETHs (insb. mit der Schaffung von Labors in Zürich und Lausanne) rasche Fortschritte. Der DEFTECH[3]-Prozess von ar W+T zur Verfolgung der Technologieentwicklungen hat sich bewährt.

  Zur Stärkung der Kompetenzen und der Interoperabilität mit den Partnern ist die Ausbildung zentral. Hier konnten wesentliche Fortschritte erzielt werden. Auf strategischer und technisch-operativer Ebene führte das VBS mehrere Übungen durch oder beteiligt sich seit vielen Jahren daran. Dazu gehören z.B. *strategische Führungsübungen* (SFU), *Sicherheitsverbundübungen* (SVU), *Cyber Pakt*, *Locked Shields*, *Cyber Coalition*, *ENISA Cyber Europe Exercise* und *Cyberstorm* (*Interna-*

[2] Open Source Intelligence

[3] Defence Future Technologies

tional Watch and Warning Network, IWWN). Die Analyse zeigt, dass eine Erweiterung des bestehenden Bildungssystems unerlässlich ist, um den Herausforderungen (insbesondere die Komplexität und die rasante Entwicklung) der Digitalisierung und somit der Cybersicherheit gerecht zu werden.

3.2 Fokus «Strategische Aufgaben»

Die Erfüllung der vom APCD gesetzten strategischen Ziele (Ziff. 2.1) können wie folgt beurteilt werden:

- **Sicherheit und Abwehr bei den eigenen IKT-Systemen und -Infrastrukturen in allen Lagen**

  Die vorhandenen Mittel ermöglichen den Verwaltungseinheiten des VBS, den alltäglichen Cyberbedrohungen zu begegnen. Viele Massnahmen sind zur Stärkung der eigenen Cybersicherheit (qualitativ) im Aufbau.

- **Originäre Aufgaben des NDB und der Gruppe V**

  Im Umgang mit Cyberrisiken leistet der NDB gestützt auf das NDG einen massgebenden Beitrag zur Antizipation, frühzeitigen Erkennung und Vorbeugung von Cyberangriffen auf Schweizer Interessen. Er hat die Fähigkeit, staatliche Cyberangriffe zu identifizieren und zuzuordnen (Attribution). Er bedient Entscheidungsträger auf föderaler und kantonaler Ebene mit umfassenden nachrichtendienstlichen Informationen und mit Beurteilungen der Cyberbedrohungen (Cyberlage). Der NDB ist die erste Verteidigungslinie im Cyberdefence-Dispositiv. Die Armee selbst (vor allem FUB ZEO) verfügt bereits über breite Kompetenzen im Cyberbereich und wird von den Streitkräften der umliegenden Staaten als valider Partner in diesem Bereich angesehen.

- **Unterstützung der Betreiber kritischer Infrastrukturen bei Cyberangriffen**

  Der NDB leistet unter anderem Unterstützung im Bereich des Bedrohungsbildes, mit Erreichbarkeit rund um die Uhr oder mit Beratung bei Vorfällen. Dasselbe gilt für die Präventionsarbeit bei sensiblen Unternehmen und Dienstleistern. Das Nachrichtendienstgesetz ist ein geeigneter Rahmen, um diese im Fall von Cyberangriffen zu unterstützen. Das VBS bietet immer mehr Bildungs- und Beratungsangebote für die Betreiber von kritischen Infrastrukturen und ihre Partner an.

3.3 Fokus «Umsetzungsmassnahmen»

In der revidierten Fassung des APCD vom 17.12.2018 wurden 11 Massnahmen getroffen. Die folgende Tabelle fasst ihren Umsetzungsstand zusammen.

Teilprojekte [Verantwortlich]	**Massnahmen** [Originaltext von 17.12.2018]	**Stand**[5] [Erläuterungen]
1) Informationssicherheit [GS-VBS]	Die Funktion *Planung und Steuerung* der Architektur verwirklichen. Die Entwicklung des Informationsschutzgesetzes (ISG) und die Implementierung des Integralen Sicherheits-Management-Systems VBS berücksichtigen.	Die ehemalige IOS wurde in die neue Abteilung «Digitalisierung und Cybersicherheit» überführt und reorganisiert; das ISG[4] wurde vom Eidgenössischen Parlament erst in der Wintersession 2020 angenommen; das zentrale ISMS.VBS wird 2021 überarbeitet.
2) Zelle Cyberdefence VBS (CYD VBS) [GS-VBS]	Die Funktionen *Strategische Steuerung* und *Strategische Analyse* der Architektur verwirklichen. Die Empfehlungen der Internen Revision VBS berücksichtigen. Das Kontinuum zwischen Cyberschutz und Cyber-Vtg durch enge Zusammenarbeit mit IOS sicherstellen. Die Kohärenz zwischen CYD-VBS, Beirat CYD VBS und CYD-Campus sicherstellen.	Die Zelle des « Delegierten des VBS für Cyberdefence » ist gut etabliert und anerkannt. Sie wird personell verstärkt.
3) Cyber-Mittel des NDB [NDB]	Die Funktionen Cyberdefence der zivilen kritischen Infrastrukturen und Nachrichtendienstlichen Cyber-Aktionen der Architektur konkretisieren.	Der im APCD identifizierte Personalbedarf zur nachhaltigen Früherkennung, Verhinderung und Attribution von sicherheitsrelevanten Cyberangriffen soll gemäss Entscheid des GS VBS mehrheitlich über die NCS 2 finanziert werden. Die Personalverstärkung im Bereich OSINT wurde im Rahmen der NCS geregelt.

[4] Informationssicherheitsgesetz

Teilprojekte [Verantwortlich]	**Massnahmen** [Originaltext von 17.12.2018]	**Stand**[5] [Erläuterungen]
4) Cyber-Mittel der Armee [Armee]	Die Funktionen *Militärische Cyberaktion* und *Militärische Cyberdefence* der Architektur konkretisieren.	Umgesetzt. Strukturelle Änderungen im Bereich Cyberdefence wurden im Rahmen der Ausrichtung zum Kdo Cyber bereits getroffen.
5) CYD-Campus [ar W+T, GS-VBS]	Die Funktionen *Technologisches Monitoring* Cyber, *Entwicklung und Anwendungen* sowie *Ausbildung und Training* der Architektur konkretisieren; ar W+T integrieren; den Zeitraum 2018-2019 vorrangig abdecken und so rasch wie möglich operativ werden.	Umgesetzt.
6) Entwicklung und Management des Berufspersonals [GS-VBS]	Die quantitative und qualitative Verstärkung der Personalbestände sicherstellen; sie werden durch interne Neuzuweisungen generiert; dazu wird es notwendig sein: - mögliche Verschiebungen oder Aufgabenverzichte in Betracht zu ziehen, ohne die Weiterentwicklung der A oder Beschaffungen zu gefährden; - gleichzeitig die vom Parlament angeordnete Reduktion der Personalbestände umsetzen; - einen regelmässigen und geordneten Personalaufbau bevorzugen, um den Aufwand für Rekrutierung, Integration, Schulung u. Org. zu minimieren.	Die Auslegeordnung mittels APCD im Bereich Personal hat zu einer wichtigen personellen Verstärkung geführt, die mit der Strategie Cyber VBS weitergeführt werden soll.
7) Entwicklung und Management des Milizpersonals [Armee]	Die Rekrutierung, Führung und Entwicklung von Milizpersonal sicherstellen; namentlich die Erfahrungen aus dem SPHAIR-Programm und den Wettbewerben wie Swiss Cyber Storm berücksichtigen; mit dem Teilprojekt 5 synchronisieren; die Bedürfnisse in die AO 19 aufnehmen.	Operativ. Mit dem Cyberlehrgang und der regelmässigen Integration von «Quereinsteigern» werden die Bestände gem. Motion Dittli 17.3507 schrittweise erhöht . Die neuen Strukturen (Cyber Bat und Fachstab) sind in der Revision der Armeeorganisation enthalten.
8) Ausbildung und Sensibilisierung des Personals [Armee]	Die Aus- und Weiterbildung der verschiedenen Personalkategorien des VBS sicherstellen (ausser beim NDB, der seine Mitarbeitenden selbst ausbildet); mit den Teilprojekten 5, 6, und 7 synchronisieren.	Die Ausbildung und Sensibilisierung des Personals konnte gestärkt werden. Das Gesamtkonzept gem. der revidierten Fassung des APCD ist noch ausstehend.

Teilprojekte [Verantwortlich]	**Massnahmen** [Originaltext von 17.12.2018]	**Stand**[5] [Erläuterungen]
9) Infrastrukturen CYD [Armee]	Die notwendigen Räumlichkeiten zur Verfügung stellen und mit dem Teilprojekt 5 synchronisieren.	Umgesetzt und laufend ausgebaut.
10) Militärischer reglementarischer Rahmen [Armee]	Es geht darum - die Schnittstellen zwischen Armee und NDB zu regeln; - Art. 100, Abs. 1, Lit. c MG in einer Verordnung umzusetzen; - die doktrinale Grundlage fertig zu stellen und in einem Reglement der Armee umzusetzen; - die neue Organisation in die Geschäftsordnung der FUB umzusetzen; - eine Cyberrichtlinie des Chefs der Armee ausarbeiten, um das Funktionieren der Cybersphäre in der Armee zu regeln.	Umgesetzt und laufend weiterentwickelt.
11) Kontinuierliche Verbesserung [GS-VBS]	Es geht darum, die kontinuierliche Verbesserung des Dispositivs des VBS für Cyberdefence mit einem geeigneten Verfahren zur Messung der Fortschritte sicherzustellen.	Wie die zurzeit in Erarbeitung stehende Strategie Cyberdefence zeigt, funktioniert dieser Prozess. Aufgrund der späten Bereitstellung von genehmigten Personalressourcen konnten genaue Messinstrumente noch nicht etabliert werden.

4 Verbesserungsmassnahmen

Aus der obigen Beurteilung ergeben sich folgende Erkenntnisse, welche in die neue Strategie Cyberdefence VBS einfliessen:

- **Steuerung**: Die Vorgaben sind zu vereinfachen, an die künftigen Herausforderungen der Digitalisierung anzupassen und die diesbezügliche Governance sowie die entsprechenden Aufgaben, Kompetenzen und Verantwortlichkeiten zu überarbeiten.
- **Cyberschutz**: Die Schutz- und Abwehrmassnahmen bei Angriffen müssen in Einklang gebracht werden; dazu gehört auch die Umsetzung der Empfehlungen der EFK von Ende 2019.
- **Abwehr und Aktion im Cyberraum**: Die Fähigkeiten zur Attribution sollen ausgebaut werden, sodass alle sicherheitspolitisch relevanten Cyberangriffe zugeordnet werden können. Die Abstimmung des Cyberbereichs mit anderen Operationssphären (Boden-, Luft- und elektromagnetischer Raum) soll weiterentwickelt werden. Die Kompetenzen der vorhandenen Mittel und der Durchhaltefähigkeit sollen ausgebaut werden.
- **Unterstützung**: Es ist ein umfassenderes, auf Stufe Departement koordiniertes Ausbildungs- und Sensibilisierungssystem zu etablieren, das den künftigen Her-

ausforderungen der Digitalisierung gerecht wird. Dazu müssen sich alle Akteure in diesen Prozessen systematisch mit der Thematik befassen.

- **Kommunikation**: Um das VBS als attraktiven Arbeitgeber im Cyberbereich zu positionieren, soll mit angepassten Kommunikationsprodukten auf die Ausbildungs- und Karriereangebote hingewiesen werden. Zusätzlich soll die Rolle des VBS im Bereich Cyberdefence bekannter werden.

5 Bilanz und Ausblick

Der APCD hat eine beachtenswerte Umgestaltung des VBS im Bereich Cyber eingeleitet und zu massgeblichen Verbesserungen geführt. Das VBS hat mit der Umsetzung der Massnahmen und der Koordination von Kompetenzen und Kapazitäten deutlich an Kohärenz gewonnen. Die interdepartementale Zusammenarbeit ist wichtig. Das VBS verfügt heute über gute Fähigkeiten, um hochstehende Leistungen (Abbildung 2) zu erbringen und kann als verlässlicher Partner auf ein zuverlässiges Netzwerk im In- und Ausland zurückgreifen.

Abbildung 2: Übersicht der Leistungen des VBS

Nicht alle Ziele des APCD konnten vollständig erreicht werden. Dies insbesondere aufgrund der Komplexität und der raschen Veränderungen im Cyberbereich.

Mittels der «Gesamtkonzeption Cyber» zur Definition des künftigen Kommandos Cyber der Armee sowie der neuen «Strategie Cyberdefence VBS» werden die in diesem Bericht teilweise erreichte Ziele systematisch adressiert und das Gesamtsystem weiterentwickelt.

Für den Schlussbericht:

Generalsekretariat VBS

Gérald Vernez
Delegierter Cyberdefence VBS

Signaturerklärung: Schlussbericht Aktionsplan Cyberdefence VBS (APCD)

Digital signiert von Vernez Gerald PC0PYS
Bern, 2021-01-27 (mit Zeitstempel)

Zur Kenntnis genommen:

Generalsekretär VBS

Digital signiert von Eder
Anton 2P0YWL
2021-02-09 (mit Zeitstempel)

Toni Eder