Der Aktionsplan Cyber Defence des VBS (APCD)

Im Juli 2016 wurde, ausgelöst durch den im Januar aufgedeckten Cyber-Angriff auf die RUAG, eine Überprüfung des Cyber-Dispositivs des VBS angeordnet. Mit der Verabschiedung der Standortbestimmung und der Strategie Ende Oktober 2016 sowie des Umsetzungsplans im Juni 2017 ist der APCD entstanden.

Gérald Vernez

Was regelt dieser Aktionsplan Cyber Defence, wo ist er im nationalen Dispositiv verortet, was bedeutet «Subsidiarität» und welche Mittel werden aufgewendet? Der vorliegende Artikel stellt die wichtigsten Elemente dieses VBS-internen Plans[1] vor, der sich auf eigene Gesetzesgrundlagen und Mittel stützt.

Aufgaben und Stellung der Cyber-Verteidigung

Nebenstehende Abbildung 1 gibt einen Überblick über die Leistungen, für die das VBS im Bereich der Cyber-Sicherheit[2] zuständig ist. Diese ergeben sich aus der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS; welche durch den APCD ergänzt wird)[3] sowie aus der Umsetzung des Nachrichtendienstgesetzes[4] und des Militärgesetzes[5]. Ausserdem verleiht die Motion 17.3507[6], die im März vom Parlament angenommen wurde, den Elementen des APCD, welche die Armee betreffen, eine starke politische Legitimation.

Auf der Grundlage dieser Aufgaben und einer umfassenden Standortbestimmung wurde das folgende operative Ziel formuliert:

«Das VBS soll ein anerkannter Pol von Kompetenz für Cyber Defence sein. In enger Zusammenarbeit mit seinen Partnern, der Wirtschaft und den Hochschulen soll es quantitativ und qualitativ über genügend Mittel verfügen, um:

- *die eigenen IKT-Systeme und -Infrastrukturen jederzeit und unter allen Umständen gegen Cyber-Bedrohungen und -Angriffe zu schützen und zu verteidigen sowie ihre Resilienz sicherzustellen;*
- *militärische und nachrichtendienstliche Operationen im Cyber-Raum durchzuführen;*
- *zivile Behörden bei Cyber-Angriffen gegen kritische Infrastruktur zu unterstützen.»*

Die NCS betont das Prinzip der Eigenverantwortung als zentrales Element; die Cyber-Sicherheit ist deshalb dezentralisiert und liegt in der Verantwortung von Einzelpersonen, Unternehmen und Institutionen. Der Staat soll nur subsidiär eingreifen und im Falle der Armee nur dann, wenn die folgenden Kriterien erfüllt sind:

- Der Einsatz militärischer Mittel darf den Schutz und die Verteidigung der eigenen IKT-Systeme und -Infrastrukturen nicht beeinträchtigen;
- Der Einsatz militärischer Mittel für Dritte ist nur für Aufgaben möglich, die Fähigkeiten erfordern, welche die Armee für ihre originären Aufgaben selbst nutzen kann;

Abbildung 1: Aufgabenverteilung im Cyber-Raum

Leistungen des VBS zu Gunsten … \ Im Bereich von …	Cyber-Schutz	Cyber-Verteidigung	Aktionen im Cyber-Raum
Einzelpersonen	Eigenverantwortung	Im Ereignisfall greift die Strafverfolgungskette ein	
der Wirtschaft	Verantwortung der Firmen gem. Standards der Regulatoren und Branchen	Im Ereignisfall greift die Strafverfolgungskette ein; mögliche Unterstützung des VBS für Ereignisse von grosser Kritizität	
der Betreiber kritischer Infrastrukturen	Verantwortung der Operateure gem. Standards der Regulatoren und Branchen; Unterstützung des VBS für Prävention	Verantwortung der Operateure; der Nachrichtendienst des Bundes **kann** bei Cyber-Angriffen helfen; sind die Bedingungen erfüllt, **kann** die Armee unterstützen	
des VBS	Verantwortung des VBS gem. Bundesstandards und der erweiterten Bedürfnisse des VBS	Abwehr der eigenen IKT-Systeme und -Infrastrukturen	Informationsbeschaffung und Effekte im Cyber-Raum

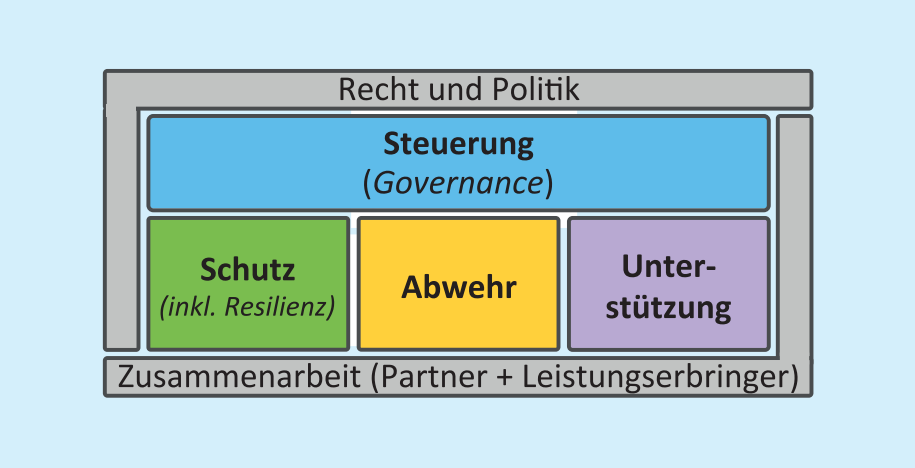


Abbildung 2: Funktionelle Architektur.

- Die Armee leistet technische Unterstützung für die Zivilbehörden nur dann, wenn diese ihre eigenen Mittel erschöpft haben.

Das VBS – ein System

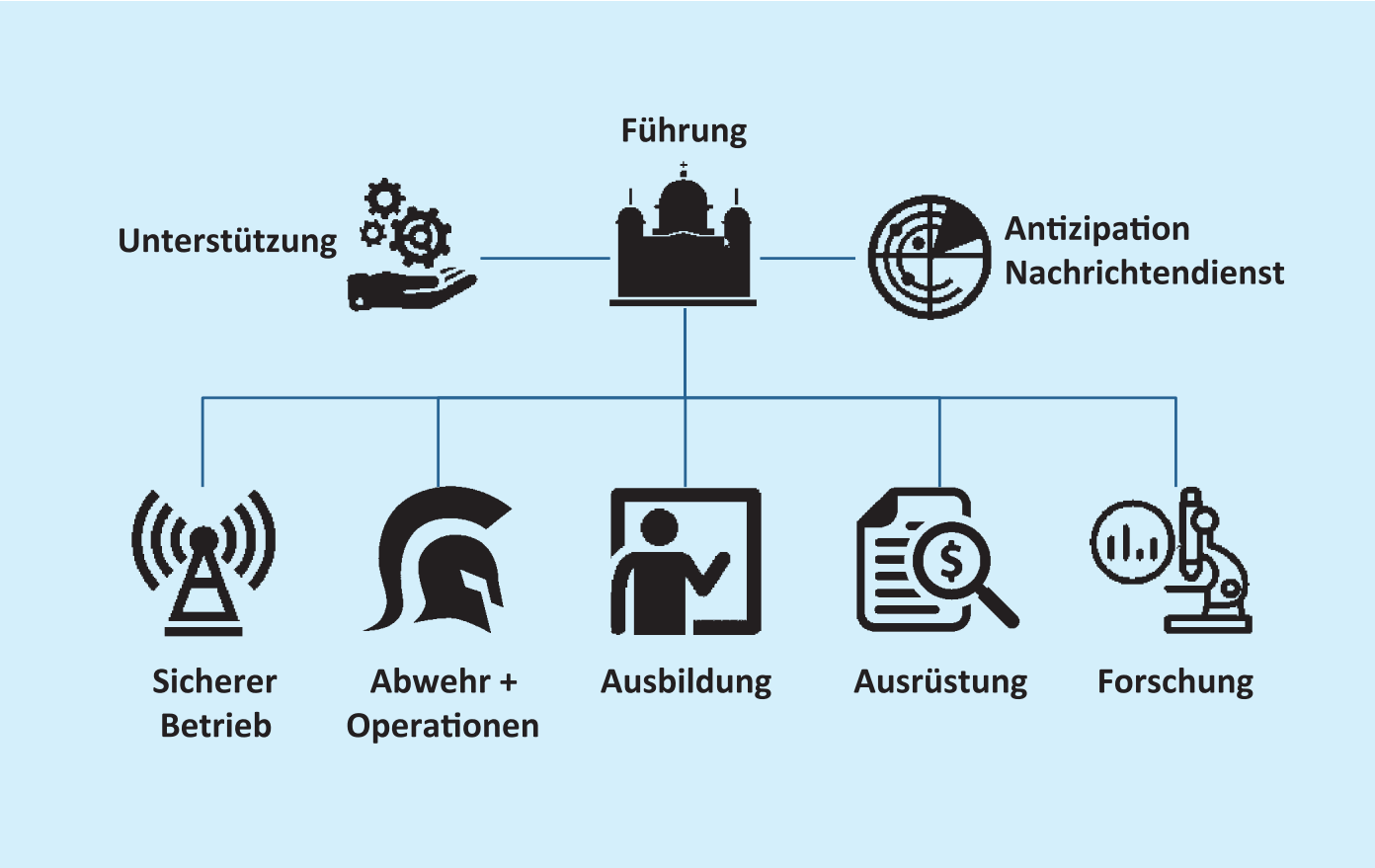
Das Dispositiv des VBS für die Cyber-Verteidigung umfasst verschiedene Funktionen, die in obenstehend abgebildeter Architektur (Abbildung 2) eingebettet sind. Es wird von handlungsleitenden Regeln und unterstützenden Kooperationen umrahmt und umfasst vier Schlüsselbereiche: Die Steuerung stellt die kohärente Gesamtsicht sicher, der Schutz umfasst den sicheren Betrieb der IKT-Systeme und Infrastrukturen des VBS, die Abwehr umfasst die Aktionen im Cyber-Raum und die Unterstützung schafft günstige Voraussetzung in den Bereichen Antizipation, Kompetenzen und Fähigkeiten sowie Ausbildung und Training.

Fünf der sieben Verwaltungseinheiten des VBS wirken direkt am APCD mit:

- das Generalsekretariat des VBS (GS-VBS), namentlich mit dem Delegierten VBS für Cyber Defence sowie der Bereich Informations- und Objektsicherheit (IOS);
- der Nachrichtendienst des Bundes (NDB) mit verschiedenen Stellen, darunter dem bei ihm angesiedelten Teil der Melde- und Analysestelle Informationssicherung (MELANI);
- die Armee, insbesondere mit der Führungsunterstützungsbasis, welche die Systeme und Infrastrukturen des VBS betreibt und über die technisch-operativen Fähigkeiten und Kompetenzen verfügt;
- das Bundesamt für Bevölkerungsschutz, das für die Strategie zum Schutz kritischer Infrastrukturen verantwortlich und durch die NCS mit Risikoanalysen beauftragt ist;
- armasuisse, die für die Beschaffung zuständig ist und deren Abteilung Wissenschaft und Technologie (W+T) eine zentrale Rolle in der Entwicklung und Antizipation spielt.

Von aussen mag dies den Anschein einer Zerstückelung erwecken. Tatsächlich verfügt das VBS so aber über ein umfassendes Instrumentarium (siehe Abbildung 3), welches es dank seiner Steuerung

Abbildung 3: das VBS als gesamter Leistungserbringer. Grafiken: VBS



situativ und mit konzentrierter Wirkung einsetzen kann.

Umsetzung des APCD

Das VBS sorgt heute schon für Sicherheit im Cyber-Bereich und mit dem APCD soll die aktuelle Lage in Bezug auf Mittel, Abläufe sowie Kompetenzen und Fähigkeiten optimiert und verstärkt werden. Der angestrebte Sollzustand ist bis Ende 2020 zu erreichen, und die Kosten dürften nach aktuellem Kenntnisstand pro Jahr rund zwei Prozent der Ressourcen des VBS ausmachen. Bis zur Zielerreichung stehen grosse Arbeiten an, diverse Beispiele erlauben jedoch Optimismus:

- **Krisenbewältigung:** Das VBS kann sich auf sein grosses Stabs-Know-how abstützen und verfügt über beachtliche Verstärkung in Form seines Milizkaders; mithilfe der in den letzten Jahren gesammelten Erfahrungen, insbesondere im Zusammenhang mit den Angriffen gegen die RUAG 2016 sowie gegen die Armee im Sommer 2017, wurden Abläufe eingerichtet, welche Mittel und Aktionen auf technischer und politischer Ebene zusammenbringen; dank diesem Erfahrungsschatz erreichten die Experten von EDA und VBS bei der Übung Locked Shields 2018 im strategischen Teil den ersten Rang;

«Der Aktionsplan Cyber Defence des VBS ist kein Endpunkt, sondern dient dem VBS als erste Orientierungshilfe zur Anpassung an die Herausforderungen des Cyber-Raums.»

- **Ausbildung:** Das VBS setzt über die Armee zahlreiche Sensibilisierungsaktionen um und schult sein Personal und die Angehörigen der Armee in den Grundlagen der Cyber-Hygiene; die Führungsunterstützungsbasis hat vor Kurzem einen Lehrgang für Cyber-Security-Spezialisten lanciert, welchen die Armeeangehörigen mit einer Berufsprüfung abschliessen können; das GS-VBS seinerseits führte in den letzten drei Jahren die Übung Cyber-Pakt durch; damit wurde die Mittel des VBS, zusammen mit Partnern aus anderen Departementen und Betreibern von für das VBS wichtigen kritischen Infrastrukturen, trainiert;
- **Technisch-operative Fähigkeiten:** Nach Erreichen des angestrebten Soll-Zustands werden dem VBS eine beträchtliche Anzahl Mitarbeitende[7] zur Verfügung stehen; diese Mittel werden hinsichtlich Kompetenzen und Durchhaltefähigkeit mit bis zu 600 Angehörigen der Armee verstärkt, ein Bestand, der in sechs bis sieben Jahren erreicht sein soll; ein aufschlussreicher Anhaltspunkt (wenn auch Vergleiche immer etwas Zufälliges haben) ist ausserdem der 13. Rang von 22, den unser Team an der Übung Locked Shields 2018 erreicht hat, nachdem es sich seit 2017 qualitativ enorm gesteigert hat;
- **Entwicklung und Antizipation:** Mit armasuisse Wissenschaft und Technologie verfügt das VBS über eine «Mini-DARPA[8]», die gut mit der Forschung vernetzt ist und konkrete Projekte umsetzt; mit dem Projekt CYD-Campus (Cyber-Defence-Campus) wird zudem ein agiles Netzwerk entstehen, welches die Kompetenzen und Fähigkeiten des VBS verstärken wird.

«Dass bisher keine grösseren Angriffe erfolgt sind, ist kein Grund dafür, das Problem langsam anzugehen.»

Herausforderungen

An sich ständig verändernden Variablen und Unbekannten mangelt es nicht; präzise Prognosen sind daher unmöglich. Die Umsetzung des APCD ist somit zunächst vor allem Führungssache, wobei mit dem Fachkräftemangel, den Ausmassen des Problems, einer lückenhaften Standortbestimmung und ständig neuen Verwundbarkeiten, aber auch zahlreichen privaten und öffentlichen Initiativen jongliert werden muss. Zudem darf die Umsetzung des APCD die laufende Armeereform (WEA) und das für die Erneuerung der Mittel zum Schutz des Luftraums zentrale Projekt «Air2030» nicht gefährden. Der Aktionsplan Cyber Defence des VBS ist daher kein Endpunkt unserer Anstrengungen, sondern dient dem VBS als erste Orientierungshilfe zur Anpassung an die Herausforderungen des Cyber-Raums, der zu einem wichtigen und dringlichen Thema der Sicherheitspolitik geworden ist. Dass bisher keine grösseren Angriffe erfolgt sind, ist kein Grund dafür, das Problem langsam anzugehen. Böswillige Akteure nützen bereits heute unsere Sicherheitslücken aus und könnten uns im Falle eines Konflikts massiven Schaden zufügen. ■

1 https://www.vbs.admin.ch/content/vbs-internet/de/die-schweizer-armee/schutz-vor-cyber-angriffen.download/vbs-internet/de/documents/verteidigung/cyber/Aktionsplan-Cyberdefense-d.pdf
2 Dieser Begriff beschreibt den angestrebten Zustand in Bezug auf die IT-Situation, in dem die Risiken dank einer Reihe von passiven und aktiven Massnahmen auf ein tragbares Niveau reduziert worden sind.
3 Der Bundesrat hat das Eidgenössische Finanzdepartement mit der Erarbeitung und der Steuerung ihrer Umsetzung betraut: https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/ncs_strategie.html
4 Bundesgesetz über den Nachrichtendienst (NDG, Art. 26 Abs. 1 Bst. d Ziff. 2 und Art. 37 Abs. 1).
5 Bundesgesetz über die Armee und die Militärverwaltung (MG, Art. 100 Abs. 1 Bst. c)
6 17.3507 Motion Dittli – Ein Cyber-Defence-Kommando mit Cyber-Truppen für die Schweizer Armee: https://www.parlament.ch/de/ratsbetrieb/suche-curiavista/geschaeft?AffairId=20173507; die auf den Änderungen der Sicherheitspolitischen Kommission des Nationalrats beruhende Fassung findet sich unter: https://www.parlament.ch/centers/kb/Documents/2017/Kommissionsbericht_SiK-N_17.3507_2017-10-30.pdf
7 Die Übung wird vom Cooperative Cyber Defence Centre of Excellence in Tallinn (Estland) durchgeführt.
8 Die Defense Advanced Research Projects Agency ist die Forschungsagentur des US-Verteidigungsministeriums, die neue Technologien für die militärische Verwendung entwickelt.

Gérald Vernez
MAS ETH SPCM
Delegierter VBS
für Cyber-Defence
1580 Avenches