Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

09.11.2017

AKTIONSPLAN CYBER-DEFENCE VBS (APCD)

AKTIONSPLAN CYBER-DEFENCE VBS (APCD)

VORWORT

Der vorliegende *Aktionsplan für Cyber-Defence* bezieht sich auf das VBS. Seine Erarbeitung begann im Juli 2016 mit einer Standortbestimmung, aufgrund derer eine Strategie festgelegt wurde. Nach deren Genehmigung im Oktober 2016 folgte ein Umsetzungsplan, der wiederum im Juni 2017 verabschiedet wurde.

Die Veröffentlichung dieses Aktionsplans erfolgt aufgrund eines Gesuchs, das gestützt auf das Öffentlichkeitsgesetz eingereicht wurde. Er umfasst technische Unterlagen mit zahlreichen klassifizierten Elementen, die bei einer teilweisen Schwärzung nicht mehr verständlich wären. Weil das VBS den Aktionsplan so verständlich wie möglich präsentieren möchte, hat es eine einfache und leicht zugängliche Version erstellt. Diese Version enthält, über die ursprüngliche Version hinaus, wo angezeigt auch Bezüge zum aktuellen Geschehen.

Die Dokumentation ist im Internet zugänglich unter:
http://www.vbs.admin.ch/de/verteidigung/schutz-vor-cyber-angriffen.html

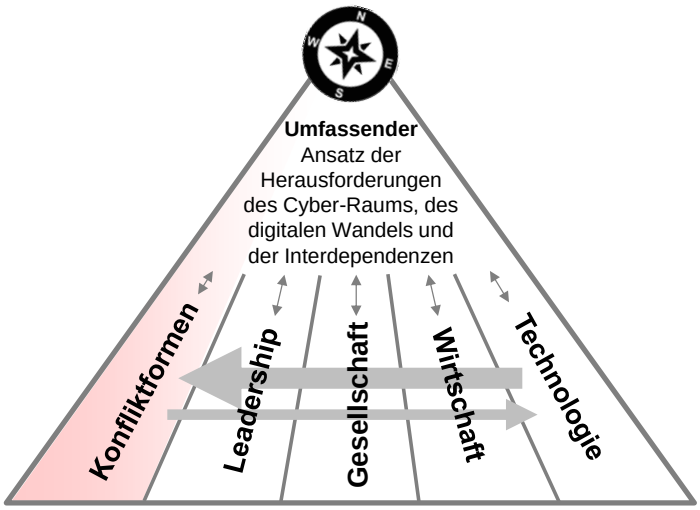
Abkürzungen

CERT	Computer Emergency Response Team
ISMS	Information Security Management System (gem. ISO 27000)
ENISA	European Network and Information Security Agency
LMS	Learning Management System
MELANI	Melde- und Analysestelle Informationssicherung
OIC	Operation Information Center
APCD	Aktionsplan Cyber-Defence VBS
SIPOL B	Bericht des Bundesrates über die Sicherheitspolitik der Schweiz
IOS	Informations- und Objektsicherheit (die IOS ist eine Abteilung des Generalsekretariats VBS)
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NDB	Nachrichtendienst des Bundes
IKT	Informations- und Kommunikationstechnologie

ÜBERSICHT

Die Herausforderungen des Cyber-Raums für die Sicherheitspolitik

Durch den technologischen Fortschritt und die Digitalisierung menschlicher Aktivitäten ist der Cyber-Raum entstanden. Unsere Gesellschaft ist unwiderruflich von ihm abhängig, und er bewirkt grundlegende Veränderungen unserer Lebensweise. Diese Entwicklung hat viel Positives, bringt aber auch laufend neue Risiken und Konfliktformen mit sich. Selbst die Natur der Konflikte wird dadurch verändert.



Cyber-Angriffe sind nicht mehr blosse durch Kleinkriminelle und Vandalen mit primitiven Mitteln verursachte geringfügige Störungen kurzer Dauer und geringer Reichweite. Sie sind heutzutage vielmehr komplexe Abläufe im Zusammenwirken einer bisher noch nie dagewesenen Vielfalt von immer professionelleren privaten und staatlichen Akteuren, die aus den unterschiedlichsten Beweggründen handeln und bereits im Frieden das zivile Umfeld für ihre Aktionen missbrauchen. Die Konsequenzen sind schwerwiegend. Auch wenn die Schweiz bisher keine grösseren Schäden zu beklagen hat, ist die Entwicklung der Herausforderungen im Cyber-Raum alarmierend, und eine ***ganzheitliche Vorgehensweise*** drängt sich auf. Das ist eine der grossen Herausforderungen für unsere Sicherheitspolitik.

Aufgaben des VBS im Cyber-Raum und Stand seiner Mittel

Mit der Entwicklung des Cyber-Raums und in Übereinstimmung mit der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS, die unter der Leitung des Eidgenössischen Finanzdepartements derzeit überarbeitet wird) will das VBS seine eigenen Systeme und Infrastrukturen schützen und verteidigen. Das ist eine Voraussetzung dafür, dass es jederzeit und unter allen Umständen seine Aufgaben erfüllen kann; dazu zählt auch die Unterstützung von Betreibern kritischer Infrastrukturen im Falle eines Cyber-Angriffs.

Die Mittel und Abläufe des VBS sind jedoch den Herausforderungen des Cyber-Raums nicht gewachsen, insbesondere im Fall zunehmender Anzahl und Komplexität von Cyber-Ereignissen. Dadurch wird auch das Potenzial beeinträchtigt, Betreiber kritischer Infrastrukturen bei Cyber-Angriffen zu unterstützen.

Der Cyber-Angriff gegen die RUAG im Jahr 2016 machte deutlich, dass im VBS ein Element zur strategischen Führung fehlte, um die Herausforderungen des digitalen Wandels ganzheitlich zu analysieren und rechtzeitig zu verstehen. Um diese Lücken zu schliessen, ordnete der Chef VBS 2016 die Ausarbeitung des Aktionsplans Cyber-Defence an, der bereits erste Wirkungen gezeitigt hat.

Strategie des VBS und Inhalt des Aktionsplans

Der Aktionsplan Cyber-Defence wurde vom VBS mit eigenen Mitteln und innerhalb seiner Kompetenzen geschaffen. Er wurde im Geist der NCS entwickelt. Er präjudiziert nicht deren Anpassung und wird auf sie abgestimmt. Einmal umgesetzt, wird dieser Aktionsplan Cyber-Defence das Schweizer Verteidigungsdispositiv im Kampf gegen Cyber-Bedrohungen erheblich verstärken.

Zur Erarbeitung des APCD gab der Chef VBS folgende Ziele vor:

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

- dem VBS als kritische Infrastruktur und innerhalb seiner Kompetenzen ermöglichen, die in Anzahl, Intensität und Komplexität zunehmenden Formen der Cyber-Bedrohung zu bewältigen, sowohl im Alltag als auch im Fall einer Krise oder eines Konflikts;
- die Cyber-Aspekte des Nachrichtendienstgesetzes (NDG) und des Militärgesetzes (MG) konkret umzusetzen;
- die Betreiber kritischer Infrastrukturen, die Opfer von Cyber-Angriffen wurden, bei Bedarf wirksam und nachhaltig zu unterstützen.

Der Aktionsplan Cyber-Defence legt die **Leistungen** des VBS fest, insbesondere für subsidiäre Einsätze der Armeemittel für die zivilen Behörden. Er definiert die **Prozesse** für einen optimalen Einsatz der Mittel. Er basiert auf einer **Architektur**, welche die Funktionen der Cyber-Defence logisch strukturiert. Weil die Herausforderungen und Krisen des Cyber-Raums komplex und bereichsübergreifend sind, definiert dieser Aktionsplan eine starke Steuerung und nennt alle nötigen **Fähigkeiten**, namentlich Führung, Antizipation, Schutz, Prävention, Reaktion, Aktion und Unterstützung der zivilen Behörden.

Umsetzung des Aktionsplans Cyber-Defence

Der Aktionsplan Cyber-Defence verlangt keine Revolution, zumal viele Massnahmen bereits ergriffen wurden. Er zielt auf eine **Optimierung** und **Verstärkung** der bestehenden Mittel des VBS, damit dieses mit Erfolg im Cyber-Raum agieren kann, auch im Fall einer grösseren Krise.

Es gibt drei Hauptbestrebungen, die wegen des raschen Wandels der Herausforderungen im Cyber-Raum laufend anzupassen sind: Als erstes geht es um eine **Steuerung** zur strategischen Führung des Bereichs, dann um den Ausbau der **operativen Mittel**. Dazu zählt die Erhöhung der Anzahl Mitarbeitenden von derzeit ca. 50 auf 150 bis zum Jahr 2020 durch VBS-interne Verschiebungen, und das trotz Spardruck. Schliesslich geht es darum, das Berufspersonal mit Milizangehörigen der Armee zu **verstärken**. Eine weitere Verstärkung ist die Kooperation des VBS mit Partnern im Rahmen eines *CYD-Campus*, der bereits ab 2018 erste Ergebnisse in der Vorausschau, in der gegenseitigen Zurverfügungstellung von Mitteln und in der Ausbildung zeitigen sollte. Die grösste Herausforderung des Aktionsplans Cyber-Defence wird darin bestehen, die richtigen Personen zu finden. Nach ersten Einschätzungen wird das VBS für diese Bestrebungen rund 2% seiner Ressourcen aufwenden müssen.

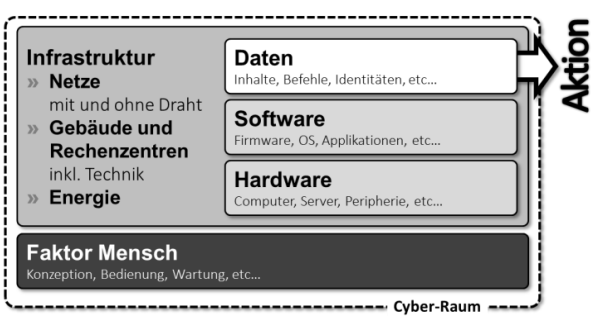
Ein zwingender erster Schritt

Die Verteidigung der Schweiz muss sich den unzähligen Herausforderungen des digitalen Wandels der Gesellschaft anpassen. Wegen des schnellen Wandels in diesem Bereich müssen auch die Cyber-Defence-Fähigkeiten rasch angepasst werden. 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. Der Aktionsplan Cyber-Defence ist aber weder eine vollständige Versicherung noch ein Endpunkt unserer Anstrengungen. Er dient dem VBS als erste Orientierungshilfe zur ständigen Anpassung an die Herausforderungen des Cyber-Raums, der zu einem **wichtigen Thema unserer Sicherheitspolitik** geworden ist.

INHALTSVERZEICHNIS

1 AUSGANGSLAGE

1.1 Der Cyber-Raum



Der Begriff *Cyber-Raum* bezeichnet die Umgebung, in der Daten gesammelt, gespeichert, benutzt und übermittelt werden. Aktivitäten im Cyber-Raum können auch physische Auswirkungen haben. Der Begriff umfasst aber weit mehr als die Informatik allein, denn diese benötigt immer auch Strom, Infrastrukturen und Personen. Der Cyber-Raum entwickelt sich sehr schnell und verändert nicht nur unsere Lebensweise, sondern auch die Natur der Konflikte. Er ist ein Schlüsselfaktor für Fortschritt auf vielen Gebieten, aber auch für kritische Verwundbarkeiten. Seine Hauptmerkmale sind die Komplexität, die Verflechtung, der Quasi-Wegfall zeitlicher und geografischer Grenzen, die Anonymität und damit verbunden die Schwierigkeit, Handlungen bestimmten Akteure zuzuordnen.

1.2 Bedrohungen und Gefahren im Cyber-Raum

Der Staat, die Wirtschaft und die Gesellschaft sind immer mehr auf globale digitale Netzwerke angewiesen. Sie sind von deren Funktionieren abhängig und bei Angriffen auf ihre Verfügbarkeit, Integrität und Vertraulichkeit entsprechend verwundbar. Die Möglichkeiten, diese Verwundbarkeiten für persönliche, kriminelle, terroristische und staatliche (militärische oder nachrichtendienstliche) Zwecke zu missbrauchen, sind praktisch unbegrenzt. Bei der Verteidigung des Cyber-Raums sind die unterschiedlichsten Akteure zu berücksichtigen, sowohl bezüglich Kompetenzen als auch Ressourcen. Die Palette reicht vom isolierten Amateur über kriminelle Netzwerke, die immer agiler und innovativer werden, bis zur Grossmacht, die über fast unbegrenzte Mittel verfügt.

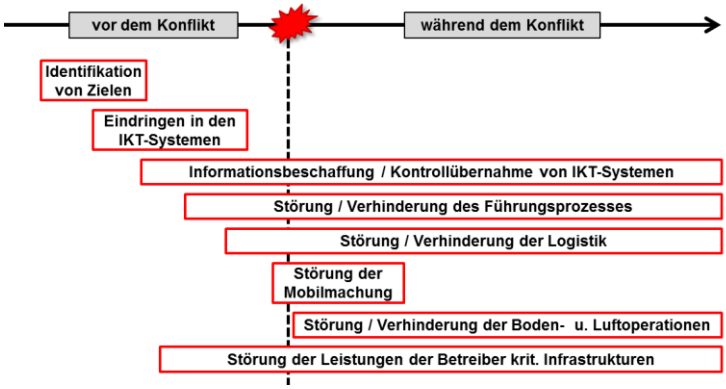
Innerhalb seiner angestammten Aufgaben unterscheidet das VBS vier Bereiche:

- **Kampf gegen verbotenen Nachrichtendienst:** Cyber-Spionage wird für Nachrichtendienste auf der ganzen Welt immer wichtiger. Durch Aktivitäten im Cyber-Raum werden nicht nur die klassischen Spionagemethoden unterstützt, die immer noch zum Einsatz kommen, sondern neue, vergleichsweise günstige Möglichkeiten mit begrenzten Risiken genutzt. Die Vielfalt der Akteure führt dazu, dass nicht besonders raffinierte Angriffe mit im Internet frei verfügbaren Werkzeugen, die entsprechend leicht zu bekämpfen sind, genauso vorkommen wie Angriffe mit hochkomplexen, schwierig zu erkennenden Werkzeugen.
- **Kampf gegen Terrorismus:** Terroristische Gruppierungen verwenden soziale Medien zur Kommunikation und erreichen ein breites Publikum. Der Cyber-Raum ist für sie ein wesentliches Instrument zur Finanzierung, Rekrutierung, Ausbildung und Propaganda. Das Internet bietet ihnen aber auch immer mehr Angriffsmöglichkeiten. Zwar hatten solche Aktivitäten bis heute nur beschränkte Folgen, es ist aber davon auszugehen, dass terroristische Gruppierungen früher oder später die Fähigkeit erlangen werden, auch hochentwickelte Aktionen mit grossem Zerstörungspotenzial umzusetzen.
- **Schutz kritischer Infrastrukturen:** Die Betreiber kritischer Infrastrukturen sind mit der ganzen Palette von Cyber-Bedrohungen konfrontiert, wie Cyber-Spionage, Cyber-Sabotage oder Cyber-Kriminalität. Gegen kritische Infrastrukturen geführten Cyber-Angriffe können lebenswichtige Funktionen für die Gesellschaft beeinträchtigen und schwere Folgen sowie ungeahnte Kettenreaktionen zur Folge haben. Wie jede Störung zeigt, ist die Elektrizität ein besonders kritisches Element, da der Cyber-Raum, die Telekommunikation, die Finanz-

dienstleistungen, die gesamte Logistik, das Gesundheitssystem und Sicherheitssysteme davon abhängig sind.

- **Militärische Verteidigung:** Der Cyber-Raum ist zu einem echten militärischen Operationsgebiet geworden, und immer mehr Staaten bereiten sich darauf vor, dieses zu nutzen. Diese Entwicklung erfordert eine Anpassung, die mit der vor rund 100 Jahren erfolgten Ausdehnung der Kriegführung in den Luftraum zu vergleichen ist. Im Cyber-Raum geht es jedoch, wie auch in der Luft, nicht nur darum, sich auf einen Krieg vorzubereiten, sondern die ständige Verfügbarkeit, Integrität und Vertraulichkeit der Funktionen zu wahren, von denen wir abhängig sind. Die bislang vorherrschende Denkweise eines reaktiven, punktuellen Handelns muss einer Logik der Antizipation und Widerstandfähigkeit weichen, um parallel stattfindende und grössere Ereignisse bewältigen zu können.

Die Cyber-Angriffe von 2015 und 2016 gegen kritische Infrastrukturen in der Ukraine haben gezeigt, dass in einem modernen Konflikt solche Ziele zuerst anvisiert werden. In einer Gesellschaft wie der unseren, die von diesen Infrastrukturen abhängig ist, ist der Hebeleffekt solcher Angriffe besonders gross. Deshalb ist der bestmögliche Schutz wichtiger Infrastrukturen sicherzustellen, insbesondere im Elektrizitätsbereich. Cyber-Angriffe gegen das VBS und die Armee oder gegen Leistungserbringer, von denen sie abhängig sind, hätten eine sofortige Wirkung auf die Einsatzbereitschaft und folglich auch die Operationen. Die Folgen solcher Angriffe können von kleinen Störungen bis zur kompletten Blockierung aller oder Teilen der einsatzrelevanten Mittel reichen. Wie in der nebenstehenden Grafik dargestellt, ist Cyber-Defence bereits vor dem Konflikt wichtig.



1.3 Entwicklung der Cyber-Bedrohungen

Gemäss dem *World Economic Forum* betragen die Schäden der Cyber-Kriminalität für die Wirtschaft weltweit rund 450 Milliarden US-Dollar, was 0,82 Prozent des globalen Bruttoinlandprodukts entspricht. Obwohl es schwierig ist, genaue Zahlen vorzulegen, ist die Tendenz klar steigend. Beobachtungen zeigen, dass Angriffe – sowohl staatliche als auch von Privatpersonen – zunehmen. Wie sich in den Konflikten in der Ukraine und in Syrien zeigt, trägt die aktuelle geopolitische Situation zu einer immer aggressiveren Nutzung des Cyber-Raums bei. Es ist zu erwarten, dass die böswilligen Handlungen im Cyber-Raum immer raffinierter, massiver und andauernder werden. Die Tatsache, dass Aktionen im Cyber-Raum rasch und anonym durchgeführt werden können, führt dazu, dass sie in bewaffneten Konflikten immer wichtiger werden, einschliesslich der Beeinflussung, und noch vor der Verwendung eigentlicher Waffen.

Die Anzahl der Anwendungen und Systeme, die mit dem Internet verbunden sind (Internet der Dinge), und der Datentransfer in Clouds wächst stark. Die Sicherheit dieser Objekte ist gering. Die Benutzer können nicht bestimmen, welche Funktionen auf ihren Geräten durchgeführt werden, und ebenso wenig, welchen Weg die Informationen nehmen. Der Verlust von Kontrolle in Bezug auf sensible Abläufe und Daten ist unvermeidlich. Unter dem Druck zu sparen, zu optimieren und noch mehr Bedienerfreundlichkeit und Funktionen anzubieten, fördern der private und öffentliche Sektor Entwicklungen und Verhaltensweisen, die ihre eigenen Tätigkeiten gefährden.

Zusätzlich zu den oben genannten Elementen müssen auch das permanente und rasche Aufkommen neuer Technologien und deren – positive wie negative – Nutzungsmöglichkeiten beachtet und in einer laufenden Gesamtsicht berücksichtigt werden.

1.4 Aufgaben und Rechtsgrundlagen des VBS

Weil der Cyber-Raum ein Querschnittsthema ist, geht er über den Rahmen des VBS hinaus. Die folgende Tabelle erläutert die Aufgaben des VBS im Cyber-Bereich, auch um falsche Interpretationen und Erwartungen zu vermeiden. Sie berücksichtigt dort, wo sich ein Konsens klar abzeichnet, auch bereits Elemente des Informationssicherheitsgesetzes (ISG), das in Bearbeitung ist, und der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS), die unter der Leitung des Eidgenössischen Finanzdepartements zurzeit revidiert wird.

	Cyber-Schutz[1]	**Cyber-Verteidigung**	**Aktion im Cyber-Raum**
Für Bürger / Einzelperson	Jeder ist für den eigenen Schutz verantwortlich.	Bei Zwischenfällen greifen die Strafverfolgungsbehörden ein.	Nicht anwendbar
Für die Wirtschaft	Jedes Unternehmen ist für seinen Schutz verantwortlich. Spezifische Normen können von einzelnen Sektoren oder Behörden erlassen werden.	Jedes Unternehmen ist für seine Verteidigung verantwortlich. Bei Zwischenfällen greifen die Strafverfolgungsbehörden ein. VBS-Unterstützung möglich bei hoher Kritikalität (politischer Entscheid).	
Für kritische Infrastrukturen	Jede kritische Infrastruktur ist für ihren Schutz verantwortlich. Spezifische Normen können von einzelnen Sektoren oder Behörden erlassen werden. Zusammenarbeit zur Prävention sind mit dem Nachrichtendienst des Bundes und der Armee etabliert.	Jede kritische Infrastruktur ist für ihre Verteidigung verantwortlich. Der Nachrichtendienst des Bundes kann im Falle eines Cyber-Angriffs Unterstützung leisten (unter Umständen mit offensiven Gegenmassnahmen). Wenn gewisse Bedingungen erfüllt sind, kann auch die Armee unterstützen.	
Für das VBS	Das VBS ist für seinen eigenen Schutz verantwortlich. Es wendet die Normen des Bundes und die eigenen für seine spezifischen Bedürfnisse an.	Das VBS ist für die eigene Verteidigung (bei Bedarf mit offensiven Gegenmassnahmen) verantwortlich.	Das VBS stellt die Fähigkeiten sicher, die seine Ämter und die Armee zur Erfüllung ihrer originären Aufgaben benötigen.

Ein Rechtsgutachten der Direktion für Völkerrecht (EDA) und des Bundesamts für Justiz (EJPD) zeigte 2009, dass die Rechtsgrundlagen nur für eine passive Verteidigung reichen. Das im September 2016 in einer Volksabstimmung angenommene Nachrichtendienstgesetz und das im März 2016 vom Parlament genehmigte Militärgesetz schliessen die im Gutachten erwähnten Lücken für eine aktive Verteidigung. Die rechtlichen Rahmenbedingungen für das VBS sind nun definiert und werden nachfolgend zusammengefasst:

[1] Arbeitsdefinitionen: *Cyber-Schutz:* Gesamtheit der Massnahmen zum Schutz der IKT-Systeme und -Infrastrukturen vor Cyber-Risiken und zur Sicherstellung ihrer Resilienz. *Cyber-Verteidigung:* Gesamtheit der Massnahmen zur Erkennung, Identifizierung und Reaktion auf Bedrohungen und Angriffe auf die IKT-Systeme und -Infrastrukturen, gegebenenfalls durch offensive Gegenmassnahmen. *Aktionen im Cyber-Raum:* Gesamtheit der Massnahmen, die gegen einen Gegner im Cyber-Raum ergriffen werden, um Nachrichten zu beschaffen oder die Verfügbarkeit oder Integrität seiner IKT-Systeme und -Infrastrukturen zu beeinträchtigen.

Armee		Normale Lage (Ausbildungsdienst, Unterstützungsdienst)[2]
Cyber-Schutz		erlaubt
Cyber-Verteidigung	passiv	
	aktiv	im Fall eines Cyber-Angriffs gegen die Armee möglich, aber bewilligungspflichtig (Art. 100 al. 1 lit. c MG)
Aktion im Cyber-Raum	passiv	erlaubt
	aktiv	nicht erlaubt

Nachrichtendienst des Bundes		In allen Lagen
Cyber-Schutz		erlaubt
Cyber-Verteidigung	passiv	
	aktiv	im Fall eines Cyber-Angriffs gegen kritische Infrastrukturen möglich, aber bewilligungspflichtig (Art. 26 al. 1 lit. d Ziff. 2 NDG; Art. 37 al. 1 NDG)
Aktion im Cyber-Raum	passiv	erlaubt
	aktiv	bewilligungspflichtig (Inland gem. Art. 26, lit. d)

1.5 Personelle Mittel des VBS

In der Cyber-Sicherheit geht es oft um die personellen Mittel. In seiner Stellungnahme zur Interpellation 17.3103[3] gab der Bundesrat dazu wie folgt Auskunft: „[…] *Ressourcen im Rahmen der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken. Zu diesem Zweck verfügt der Bund über rund 86 Stellen (50 beim VBS, 20 beim EJPD, 10 beim EFD, 2 beim EDA, 2 beim WBF und 2 beim UVEK), davon waren 30 vor dem Entscheid des Bundesrates vom 26. April 2017 befristet. Diese Stellen ermöglichen die Bearbeitung der täglichen Vorfälle. Die im sicherheitspolitischen Bericht 2016 erläuterte Zunahme der Intensität und der Folgen der Cyber-Bedrohungen erfordert jedoch eine erneute Überprüfung, die im Rahmen der Revision der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken vorgesehen ist. Im Rahmen seines Aktionsplans Cyber-Defence hat das VBS bereits angekündigt, seine Personalbestände bis 2020 bedeutend zu erhöhen.“*

Es wäre allerdings falsch, sich nur auf die Anzahl Stellen zu fokussieren. Die technischen Werkzeuge, die Abläufe, das personelle Netzwerk, das Vertrauen, die Qualität des Informationsaustausches und der von der Miliz eingebrachte Nutzen sind ebenfalls Faktoren, die bei der Beurteilung der Stärke des Dispositivs berücksichtigt werden müssen. Obwohl das VBS über qualifiziertes Berufspersonal verfügt, ist es allein mit diesem derzeit nur möglich, seinen Cyber-Schutz und seine Cyber-Verteidigung in der normalen Lage sicherzustellen. Wegen Ressourcenmangel ist es hingegen nicht möglich, mehrere gleichzeitige, komplexe oder lang andauernde Vorfälle zu bewältigen. Auch im Hinblick auf Unterstützungsbeiträge ist die Armee aktuell nur in der Lage, punktuell Leistungen zu erbringen.

Bezüglich Milizpersonals wird mit dem aktuellen System das vorhandene Potenzial nicht ausgeschöpft; es braucht ein spezifisches Verfahren zur besseren Erkennung, Prüfung, Vorbereitung und Rekrutierung von geeigneten Personen, wie beispielsweise beim Programm *SPHAIR* der Luftwaffe.[4] Arbeiten in diese Richtung sind im Gang. Diese zeigen auch, dass das *klassische* System mit Rekrutenschule und Wiederholungskursen nicht geeignet ist: Einen Informatiker kann man nicht in vier Monaten ausbilden. Im Moment werden die Armeeangehörigen isoliert rekrutiert und eingesetzt, und sie haben keine Möglichkeit, eine militärische Karriere im Cyber-Bereich zu machen, wie dies im militärischen Nachrichtendienst der Fall ist.

[2] Im Aktivdienst gelten zusätzlich die Regeln des humanitären Völkerrechts.

[3] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173103

[4] Ein Rechtsgutachten des Bereichs Recht VBS vom 26. August 2014 zeigt, dass Bürger mit einem Invaliditätsgrad bis 40 Prozent bei der Cyber-Verteidigung ihren Dienst leisten könnten, wo vor allem intellektuelle Fähigkeiten gefragt sind.

Der Einsatz von Durchdienern ist hilfreich, es handelt sich aber um junge Armeeangehörige mit noch wenig Reife, Erfahrung und Ausbildung, die eng geführt werden müssen. Es müssen flexible und differenzierte Einsatzmodelle, mit Berufspersonal zur Führung, ins Auge gefasst werden, wie sie schon in der Vergangenheit, zum Beispiel im damaligen Strategischen Nachrichtendienst, praktiziert wurden.

1.6 Sensibilisierung und Ausbildung

Die Informations- und Objektsicherheit (IOS) ist für die integrale Sicherheit im VBS zuständig. Sie führt unter anderem Sensibilisierungskampagnen durch, auch zur Informatiksicherheit. Wie die Organisationseinheit *Cyber-Defence Armee*, ist die IOS bei Seminaren der militärischen Kaderschulen präsent und bietet verschiedene Ausbildungssequenzen im LMS[5] an. Die Organisationseinheit *Cyber-Defence Armee* führt seinerseits unter dem Titel *ATTENZ!UN* Sensibilisierungskampagnen durch. Soweit sie kann, ist sie auch an Ausstellungen und Veranstaltungen der Armee präsent und schult die militärischen Einheiten im Einsatz gemäss deren operativen Bedürfnissen. Die Cyber-Organisationseinheiten des VBS nehmen auch an internationalen Übungen teil, wie *Cyber Coalition* (NATO), *Locked Shield* (CCDCoE[6], Tallinn) und *Cyber Storm,* und organisieren die nationale Übung *Cyber Pakt.* Der Sicherheitsverbund Schweiz, dessen Geschäftsstelle im Generalsekretariat VBS angesiedelt ist, führte 2016 die Übung *Popula* durch.

Die Einheitlichkeit und Abstimmung dieser Aktivitäten ist aber noch nicht zufriedenstellend. In der Armee entspricht die Ausbildung noch nicht dem aktuellen Stand der Cyber-Bedrohungen, und der Unterbestand bei den für die Cyber-Defence zuständigen Einheiten erlaubt es nicht, die von der Truppe benötigten Produkte in erforderlicher Quantität und Qualität zu liefern.

1.7 Steuerung und Führung

Verstärkung der Schutzmassnahmen

Die Informations- und Objektsicherheit bereitet für die / den Generalsekretär(in) des VBS die Sicherheitsvorschriften auf, es fehlt ihr aber ein konsolidiertes Bild der Cyber-Bedrohungen. Dadurch kommt es zu Verzögerungen und Divergenzen zu den Technologien und den Anwendungspraktiken der Nutzerinnen und Nutzer. Es bestehen Unstimmigkeiten zwischen den verschiedenen Weisungen, und deren Umsetzung ist mangelhaft.

Um die Problematik der Sicherheit der militärischen und zivilen IKT-Systeme und -Infrastrukturen des VBS generell anzugehen, führt die Informations- und Objektsicherheit für die Verwaltungseinheiten des VBS ein Informationssicherheits-Managementsystem (ISMS) nach ISO-Norm 27000 ein. Es sind auch Arbeiten im Gange bezüglich der Architektur und Topologie der Netzwerke. Diese Bemühungen sowie die Einführung eines kontinuierlichen Verbesserungsprozesses werden zur Erhöhung des Sicherheitsniveaus beitragen. Mit dem *Fachorgan Informationssicherheit* (FINS) verfügt die Informations- und Objektsicherheit über ein Gremium, die diese Massnahmen steuert und in der die Sicherheitsverantwortlichen der Verwaltungseinheiten zusammenkommen. Das neue Informationssicherheitsgesetz (ISG), das ca. 2019 in Kraft treten soll, wird die Wirksamkeit dieser Arbeiten noch deutlich steigern. Das VBS wird so bei den Schutzmassnahmen schrittweise von einer Logik der Konformität (*compliance*) zu einer Logik der Wirksamkeitskontrolle übergehen. Die Modernisierung der IKT-Systeme und -Infrastrukturen des VBS[7] ist Teil der laufenden allgemeinen Bemühungen zur Verbesserung der Sicherheit.

---

5 Learning Management System (E-Learning-Plattform)

6 Cooperative Cyber Defence Centre of Excellence; Dieses Forschungszentrum, das keine operativen Aufgaben wahrnimmt, ist bei der NATO akkreditiert. Es befindet sich in Tallinn, Estland.

7 http://www.vtg.admin.ch/de/aktuell/themen/programme-projekte/ikt-systeme-der-armee.html und https://www.efk.admin.ch/de/publikationen/wirtschaft-verwaltung/informatikprojekte/942-pruefung-des-ikt-schluesselprojekts-fitania-eidgenoessisches-departement-fuer-verteidigung-bevoelkerungsschutz-und-sport-d.html

Das Bundesamt für Bevölkerungsschutz (BABS) erstellt im Rahmen der NCS Risiko- und Verwundbarkeitsanalysen für die kritischen Sektoren. Es führt ein Inventar der kritischen Infrastrukturen, das als Grundlage für die Planung und Umsetzung der nötigen Sicherheitsmassnahmen und die Verbesserung der Resilienz dient. Das BABS koordiniert zudem die Umsetzung der Nationalen Strategie zum Schutz kritischer Infrastrukturen (SKI), die den Bereich *Information und Kommunikation* als kritischen Sektor ausweist und dort auch Cyber-Risiken thematisiert.

Führung der Projekte

Der Schutz vor Cyber-Risiken wird noch nicht bei allen Beschaffungsprojekten als zwingend erforderlich erachtet. Bei den Übungen *Conex* und *Stabante* in 2015 wurden organisatorische Schwachstellen erkannt, die sich aus der ungenügenden Berücksichtigung dieses Aspekts ergaben. In der Praxis gibt es aber Fortschritte, so zum Beispiel beim Projekt zur Beschaffung eines neuen Kampfflugzeugs[8]. Die Umsetzung von Projekten im Bereich Cyber-Sicherheit ist auch wegen des Mangels an qualifiziertem Personal und einem generell ungenügenden Verständnis von Cyber-Risiken noch zu langsam. Die bestehenden Prozesse erlauben keine rasche Reaktion; die Umsetzung von Projekten muss deshalb beschleunigt werden, um rechtzeitig auf allfällige Ereignisse reagieren zu können.

Operative Koordination

Das *Operation Information Center* der *Melde- und Analysestelle Informationssicherung* (MELANI OIC) ist eine Organisationseinheit des Nachrichtendienstes des Bundes, die mit dem Informatiksteuerungsorgan des Bundes (ISB) zusammenarbeitet, das im Eidgenössischen Finanzdepartement angesiedelt ist. Es stellt die operative Koordination der Akteure des Bundes im Bereich Cyber-Sicherheit und der kritischen Infrastrukturen sicher. Seine Hauptaufgabe ist die Analyse der Cyber-Bedrohungslage. Es stellt den Informationsaustausch zwischen 200 Betreibern von kritischen Infrastrukturen – einschliesslich der Leistungserbringer der Bundesverwaltung und der Armee – sicher, ebenso wie die operative und analytische Unterstützung dieser 200 Stellen unmittelbar nach einem Cyber-Vorfall, sofern es sich um eine Situation handelt, die nicht im üblichen Rahmen behoben werden kann oder die andere kritische Dienstleister bedroht.

Führung der militärischen Cyber-Verteidigung

Die Angriffe von 2016 haben ein ungenügendes Niveau bei der Führung, eine mangelnde Vorbereitung für eine rasche Reaktion auf Anomalien sowie Lücken bei der Überwachung gewisser Systeme offengelegt. Ein 2013 geschaffener militärischer Stab[9] verstärkt das Berufspersonal bezüglich Kompetenzen und Durchhaltefähigkeit; er ermöglicht die Einbettung des Cyber-Bereichs in die militärischen Aktivitäten auf operativer Ebene, aber auch hier sind weitere Fortschritte nötig. Das Thema *Cyber* wurde in die militärischen Reglemente wie die *Taktische Führung* und die *Operative Führung* eingearbeitet, und Standardverfahren wurden definiert; diese Dokumente müssen jedoch laufend aufgrund der aus praktischen Erfahrungen gewonnenen Erkenntnisse nachgeführt und verbessert werden.

1.8 Zusammenarbeit

Schutz der Gruppe Verteidigung

Die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) fordert die Betreiber von kritischen Infrastrukturen zur Zusammenarbeit mit ihren Partnern und Leistungserbringern auf. Für ihre eigenen Aufgaben hat die Armee die kritischen Leistungserbringer identifiziert, deren Nichtverfügbarkeit ihre Operationen

[8] Bericht der Expertengruppe Neues Kampfflugzeug, http://www.vbs.admin.ch/content/vbs-internet/de/die-schweizer-armee/sicherheit-im-luftraum.download/vbs-internet/de/documents/verteidigung/sicherheitluftraum/Bericht-Luftverteidigung-der-Zukunft-d.pdf

[9] Nur das VBS verfügt über einen solchen Stab; seine Mitglieder bringen spezifische Kenntnisse mit.

beeinträchtigen würde; sie hat mit diesen Partnern Kooperationen zur Prävention[10] von Cyber-Risiken etabliert. Damit das VBS in der Lage ist, das komplexe Thema der Cyber-Sicherheit längerfristig zu bewältigen, muss es sich aber auch auf industrielle und akademische Partner abstützen; eine genaue *Kartografie* fehlt diesbezüglich aber noch.

Zivile ausländische Partner

Bei der Spionageabwehr im Cyber-Bereich besteht hoher Kooperationsbedarf. Cyber-Vorfälle haben immer eine internationale Komponente, und kein Land kann im Alleingang erfolgreich sein. Der Nachrichtendienst des Bundes (inkl. MELANI OIC) hat eine lange Tradition internationaler nachrichtendienstlicher Kooperation, auch zu Cyber-Bedrohungen. Nebst dem regelmässigen Austausch mit Partnerdiensten beteiligt er sich seit Jahren an den Arbeiten verschiedener Fachgremien und unterhält seine Kontakte auch durch die Teilnahme an Übungen wie *Cyber Storm* (USA) oder *Cyber Europe* (ENISA).

Militärische ausländische Partner

Die Armee unterhält Beziehungen mit mehreren ausländischen Streitkräften. Dieser Austausch ist wichtig, um die Kenntnisse zu erweitern und Vergleiche anzustellen. Die Kontakte sind wegen der verfügbaren Ressourcen limitiert; es besteht jedoch die Absicht, sie weiterzuentwickeln. Mit dem Cooperative Cyber-Defence Centre of Excellence wird die Zusammenarbeit verstärkt. Die Schweiz ist dort bereits mit Praktikanten engagiert und strebt den Status einer *Contributing Nation* bei diesem Forschungszentrum an.

Forschungs- und universitäre Einrichtungen

In der Schweiz gibt es zahlreiche sehr kompetente akademische Institutionen (Bildung, Forschung und Innovation). Von wenigen Ausnahmen abgesehen, bleiben diese jedoch für die Entwicklung der Fähigkeiten für Cyber-Defence weitgehend ungenutzt. Das VBS hat 2015 für die NCS ein erstes Inventar zusammengestellt und wird demnächst die Schweizerische Akademie der technischen Wissenschaften (SATW) mit einer Aktualisierung beauftragen. Das VBS vergibt zudem verschiedene Forschungsaufträge und Unterstützungsmandate an Hochschulen auf technischen[11] und nicht-technischen Gebieten, z.B. an das *Center for Security Studies* (CSS) der ETH Zürich. Experten des VBS unterstützen Forschungsarbeiten von Studierenden (Bachelor, Master, Doktorat) und engagieren sich als Coach oder Jurymitglied bei Wettbewerben wie der *Cyber Student Challenge,* die vom *Geneva Center for Security Policy* (GCSP) organisiert wird. Die Armee unterstützt seit kurzem *Swiss Cyber Storm*, eine Veranstaltung zur Entdeckung und Förderung junger Talente.

2 PLANUNGSRAHMEN FÜR DEN AKTIONSPLAN CYBER-DEFENCE

Folgende Elemente bildeten den Rahmen für die Erstellung des Aktionsplans.

Operatives Ziel

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;

[10] Im Krisenfall ersetzen die üblichen operativen Prozesse diese Kooperationen.

[11] Zum Beispiel der gemeinsam entwickelte neuartige Ansatz zur Erkennung von gezielten Cyber-Angriffen: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-67019.html

- militärische und nachrichtendienstliche Operationen im Cyber-Raum durchzuführen;
- zivile Behörden bei Cyber-Angriffen gegen kritische Infrastruktur zu unterstützen.

Zeitliches Ziel

Drei Schlüsseletappen wurden definiert:

- bis Ende 2018 die bestehenden Mittel zu optimieren, um einen wirksamen Schutz der IKT-Infrastrukturen des VBS zu gewährleisten und die Revision der NCS zu unterstützen;
- bis Ende 2018 das VBS zu befähigen, sich wirksam zu verteidigen und ein glaubwürdiger Leistungserbringer zu sein, der um Hilfe ersuchende Behörden unterstützen kann (Subsidiarität);
- bis Ende 2020 das VBS zu befähigen, auch im Fall einer grösseren Krise im Cyber-Raum handlungsfähig zu sein.

Leitlinien

Die Entwicklung orientierte sich an folgenden spezifischen Elementen:

- Beschränkung auf die Aufträge, Kompetenzen und Mittel des VBS (gemäss den gesetzlichen Grundlagen und der Aufgabenanalyse unter 1.4);
- Ausrichtung an der vom EFD gesteuerten NCS;
- Entwicklung flexibler und nachhaltiger Lösungen, die kontinuierlich und langfristig anpassungsfähig sind;
- Formulierung der Aufgaben der Einheiten des VBS, um den Schutz, die Verteidigung und die Widerstandsfähigkeit der eigenen IKT-Systeme und -Infrastrukturen jederzeit und unter allen Umständen sicherzustellen;
- Formulierung der Aufgaben der Armee, um ihre (subsidiäre) Unterstützung kritischer Infrastrukturen, die Opfer eines Cyber-Angriffs wurden, sowie ihre Aufgaben im Konflikt- oder Kriegsfall zu gewährleisten;
- Konzentration der Mittel, strukturell und organisatorisch oder bezüglich der Abläufe, sofern ein Nutzen erwiesen ist;
- Aufbau einer soliden Zusammenarbeit mit der Industrie und Institutionen in den Bereichen Bildung, Forschung und Innovation;
- Regelung der Steuerung, der Abläufe, der Ausbildung und des Einsatzes der Miliz und Definition des Ressourcenbedarfs gemäss dem Ambitionsniveau sowie Beiträge zur Wiederherstellung einer Sicherheitskultur.

3 ARCHITEKTUR DES AKTIONSPLANS CYBER-DEFENCE

3.1 Fähigkeiten

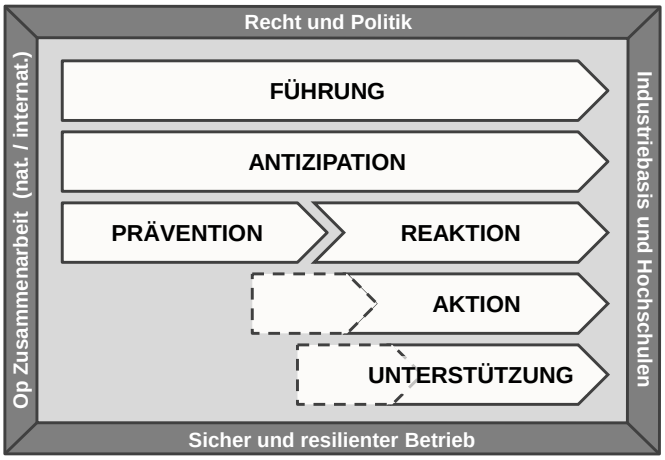
Der Aktionsplan Cyber-Defence ist in einem Gesamtrahmen zu betrachten, der folgende Elemente umfasst:

- der **rechtliche Rahmen** (Gesetze, Verordnungen) und die politischen Entscheide (Bundesratentscheide, Befehle, Weisungen, parlamentarische Vorstösse, Empfehlungen der Aufsichtsorgane, Strategien wie sicherheitspolitischer Bericht, Nationale Strategie zum Schutz der Schweiz gegen Cyber-Risiken und Nationale Strategie zum Schutz der kritischen Infrastrukturen);
- ein **Kooperations-Netzwerk** in der Schweiz und im Ausland, um Informationen zu Bedrohungen, bewährten Methoden etc. auszutauschen;

- ein **Netzwerk** der in der Schweiz **verfügbaren Kompetenzen** (in erster Linie) in der technologischen Industriebasis und in den Hochschulen;
- ein **Fundament** an sicheren und widerstandsfähigen IKT-Systemen und -Infrastrukturen (eigene und externe Leistungen, auf die das VBS angewiesen ist), damit die Mittel für Cyber-Defence auf vitale Leistungen konzentriert werden können.

Um das strategische Ziel im oben beschriebenen Kontext zu erreichen, muss das VBS über folgende Fähigkeiten verfügen und sie verbessern:

- **Führung** der Massnahmen und Aktionen auf allen betroffenen Stufen, kontinuierlich und unter allen Umständen, sowie Koordination mit externen Stellen und Partnern zu Aufgaben, die das VBS direkt betreffen;
- **Antizipation** der Entwicklung von Bedrohungen und Vorfällen im Cyber-Bereich, um rechtzeitig die nötigen Entscheidgrundlagen zu haben;



- **Prävention**, um die Angriffsflächen des VBS gegenüber Cyber-Risiken zu verringern;
- **Reaktion**, um mögliche Folgen bei Vorfällen zu beschränken, wenn nötig auch durch offensive Gegenmassnahmen;
- **Aktion** im Cyber-Raum zugunsten der eigenen Operationen zur Verteidigung oder für den Nachrichtendienst;
- **Unterstützung** der zuständigen zivilen Behörden, primär zum Schutz kritischer Infrastrukturen.

3.2 Grundsätze zu den Zuständigkeiten innerhalb des VBS

Die folgenden Grundsätze regeln die Aktivitäten im VBS:

Steuerung

- Weil zahlreicher Stellen innerhalb und ausserhalb des VBS involviert sind, erfolgt die Steuerung der Cyber-Sicherheit auf politischer Ebene.

Schutz im Cyber-Raum

- Das Prinzip der Eigenverantwortung aller Stellen ist zentral; das VBS ist nur für den Schutz der eigenen Systeme, Infrastrukturen und Prozesse verantwortlich.
- Das VBS definiert die Spezifikationen und zertifiziert die sensiblen Komponenten, die zur Implementierung von Hochsicherheitslösungen erforderlich sind, von denen es abhängig ist.
- Gemäss der NCS kooperieren die Verwaltungseinheiten des VBS, insbesondere der Nachrichtendienst des Bundes[12] und die Armee, mit den Betreibern kritischer Infrastrukturen, von denen sie abhängig sind, zur Stärkung ihrer Antizipations- und Präventionsmassnahmen.

[12] Gem. die Bundesratsentscheide von 2004 und 2007 und der besondere Auftrag dies in enger Zusammenarbeit mit dem EFD zu tun.

Verteidigung im Cyber-Raum

- Cyber-Angriffe gegen die Bevölkerung und die Wirtschaft sind Sache der zuständigen Behörden des Bundes und der Kantone. Der Nachrichtendienst des Bundes erfüllt seine originären Aufgaben der Prävention und Erkennung. Im Fall von staatlichen Cyber-Angriffen gegen die Bevölkerung oder die Wirtschaft in den vom Nachrichtendienstgesetz definierten Gebieten (z.B. Spionage oder Terrorismus) ist der Nachrichtendienst des Bundes zuständig für die Identifizierung dieser Angriffe und ihrer Täter sowie die Verteidigung potenzieller Ziele.
- Die Armee ist für die Verteidigung der eigenen IKT-Systeme und -Infrastrukturen verantwortlich. In Friedenszeiten sind aktiven Gegenmassnahme (Abwehr) der Armee zur Verteidigung ihrer eigenen IKT-Systeme und -Infrastrukturen genehmigungspflichtig[13].
- Wenn zivile kritische Infrastrukturen mit Cyber-Angriffen konfrontiert sind, obliegen allfällige aktive Gegenmassnahmen, um diese zu stoppen, dem Nachrichtendienst des Bundes und sind genehmigungspflichtig.[14]
- Gem. Vorgaben der politischen Behörden kann die Armee den Nachrichtendienst des Bundes oder andere zivile Behörden unterstützen. Diese Unterstützung kann auf der Grundlage von Leistungsvereinbarungen (insbesondere mit dem Nachrichtendienst des Bundes) oder subsidiär erfolgen.

Aktionen im Cyber-Raum

- Der Nachrichtendienst des Bundes nimmt seine originären nachrichtendienstlichen Aufgaben mit Bezug zum Cyber-Raum auf der Grundlage des Nachrichtendienstgesetzes wahr.
- Die Armee ist in der Lage, - wie in den anderen Operationssphären (Luft, Land, elektromagnetischer Raum) - Cyber-Aktionen gegen feindliche IKT-Systeme und -Infrastrukturen im Konfliktfall durchzuführen (in Übereinstimmung mit dem humanitären Völkerrecht).

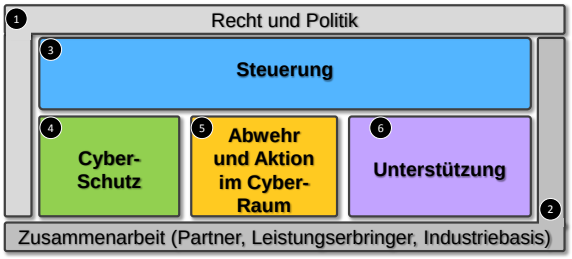
3.3 Unterstützungsleistungen der Armee (subsidiär)

Wenn die Armee mit Aufgaben ausserhalb ihres originären Handlungsfeldes betraut ist, müssen die folgenden Kriterien erfüllt sein, bevor sie diese erfüllt:

1. Das Engagement militärischer Mittel darf den Schutz und die Verteidigung der eigenen IKT-Systeme und -Infrastrukturen nicht beeinträchtigen.
2. Das Engagement militärischer Mittel für Dritte ist nur für Aufgaben möglich, die Fähigkeiten erfordern, welche die Armee für ihre originären Aufgaben selbst nutzen kann.
3. Die Armee leistet technische Unterstützung für die Zivilbehörden nur dann, wenn diese ihre eigenen Mittel erschöpft haben.
4. Jeder Auftrag an die Armee, der die Kriterien 1 bis 3 überschreitet, kann nur dann ausgeführt werden, wenn die Armee die dazu erforderlichen Ressourcen erhält.

3.4 Funktionale Architektur

Eine detaillierte Analyse und die Erfahrungen des VBS seit 2002 im operativen Cyber-Bereich sowie die Strukturierung der unter Kap. 3.1 und 3.2 aufgeführten Kapazitäten und Kompetenzen führten zur Schaffung



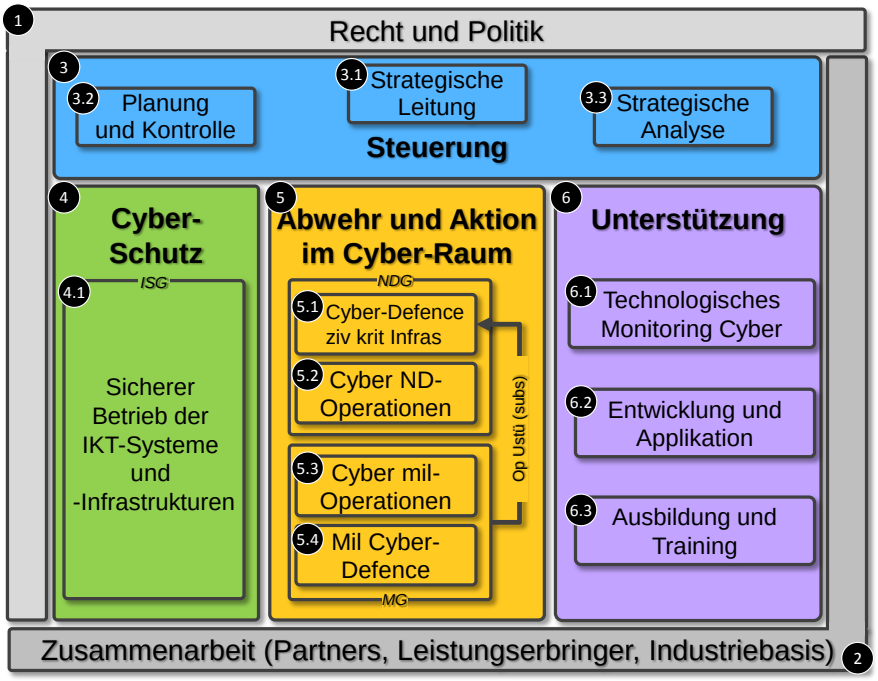
[13] Art. 100 al. 1 lit. c MG; die Verordnung dazu sollte Mitte 2018 in Kraft treten.
[14] Art. 26 al. 1 lit. d Ziff. 2 NDG; Art. 37 al. 1 NDG

der funktionalen Architektur. Diese Architektur fügt sich in den höheren normativen Rahmen ❶ und wird von allen Kooperationen ❷ des Cyber-Bereichs unterstützt.

Sie besteht aus vier Bereichen:

- Die **Steuerung** ❸, die auf strategischer Stufe des VBS günstige Bedingungen für die Entwicklung und den Einsatz der operativen Mittel schafft und mit ihren Planungs- und Kontrolltätigkeiten (inkl. gemäss künftiger ISG) dafür sorgt, dass das gewünschten Sicherheitsniveau erreicht wird.
- Der **Cyber-Schutz** ❹, wo die originären Leistungen der VBS-Verwaltungseinheiten erbracht werden und sich die Betreiber der IKT-Systeme und -Infrastrukturen des VBS befinden und die unter ❸ genannten Sicherheitsvorschriften umsetzen.
- Die **Aktion und Abwehr im Cyber-Raum** ❺, wo der Nachrichtendienst des Bundes und die Armee im operativen Cyber-Bereich für ihre eigene Verteidigung und ihre originären Aufgaben (nachrichtendienstliche Tätigkeiten und militärische Operationen) tätig sind.
- Die **Unterstützung** ❻, bei der Wissen, Personal, Fähigkeiten und technische Fähigkeiten flexibel für andere Bereiche bereitgestellt werden (❸,❹,❺).

Diese Bereiche sind nach der folgenden Abbildung und Tabelle in **Funktionen** unterteilt.



	Funktionen	Beschreibung der Aufgaben und Verantwortlichkeiten
Steuerung	3.1 Strategische Leitung	Festlegung der Strategie für Cyber-Sicherheit. Schaffung von Rahmenbedingungen für die Prävention von Cyber-Krisen, deren Management sowie die Bewältigung deren Folgen (Massnahmen) auf Ebene VBS.
	3.2 Planung und Kontrolle	Gestützt auf einem klaren Bild der Cyber-Herausforderungen, Definition der Sicherheitsmassnahmen und Kontrolle ihrer Anwendung (z.B. durch Inspektionen und Audits).
	3.3 Strategische Analyse	Kontinuierliche strategische Analyse der Cyber-Herausforderungen; Erarbeitung einer Gesamtschau für das VBS unter Berücksichtigung von Politik, Strategie, Technologie, Forschung, Doktrin, Ereignissen usw., insbesondere durch Aggregation der Produkte aus den Bereichen 4, 5 und 6, um rechtzeitig über die Grundlagen für strategische Entscheidungen zu verfügen.

	Funktionen	Beschreibung der Aufgaben und Verantwortlichkeiten
Schutz (Rahmen *in prep.* Informationsschutzgesetz)	4.1 Sicher[15] Betrieb der IKT-Systeme und Infrastrukturen des VBS	Umsetzung von Sicherheitsrichtlinien nach Funktion 3.2, um das Sicherheitsniveau und die Widerstandsfähigkeit der VBS-Verwaltungseinheiten (mit Priorität auf Nachrichtendienst des Bundes und Armee) zu gewährleisten und ihnen, jederzeit und in jedem Fall, die Erfüllung ihrer Aufgaben zu ermöglichen. Umfasst die Überwachung der eigenen IKT-Infrastruktur und -Systeme, die Reaktion auf Vorfälle und das Management von Schwachstellen.
Abwehr und Aktion im Cyber-Raum (Rahmen: Nachrichtendienstgesetz für 5.1 und 5.2, Militärgesetz 5.3 und 5.4)	5.1 Cyber-Defence der zivilen kritischen Infrastrukturen	Gesamtheit der Interventionen (gemäss NDG) für Betreiber kritischer Infrastrukturen, die Cyber-Angriffe erleiden. Für Fähigkeiten kann sich der Nachrichtendienst des Bundes auf die Funktionen 5.2, 5.3 und 5.4 (nach vorheriger Leistungsvereinbarung oder subsidiär) abstützen.
	5.2 Nachrichtendienstliche Cyber-Aktionen	Gesamtheit aller Aktionen (gemäss NDG), um Cyber-Angriffe zu entdecken, zu qualifizieren oder zuzuweisen sowie laufende Aufgaben des Nachrichtendienstes zu unterstützen.
	5.3 Militärische Cyber-Aktionen	Gesamtheit der defensiven und offensiven Aktionen (gemäss MG), die von der Armee für eine militärische Operation oder den militärischen Nachrichtendienst erbracht werden. In Friedenszeiten unterstützt diese Funktion in erster Linie die militärische Cyber-Defence (Funktion 5.4) und den Nachrichtendienst des Bundes (Funktionen 5.1 und 5.2).
	5.4 Militärische Cyber-Defence	Gesamtheit der technischen und nicht-technischen Massnahmen (gem. Militärgesetz), um feindselige Aktionen gegen die IKT-Systeme und -Infrastrukturen der Armee zu verhindern, zu reduzieren und zu unterbinden und ihre Fähigkeit sicherzustellen, ihre originären Aufgaben zu erfüllen. Diese Funktion unterstützt die Funktionen 5.1 bis 5.3.
Unterstützung	6.1 Technologisches Monitoring Cyber	Verfolgung der technologischen Entwicklungen im Cyber-Bereich, um eine Gesamtschau zu erhalten und daraus Konsequenzen für die Entwicklung im VBS abzuleiten.
	6.2 Entwicklung und Anwendungen	Gemeinsame Plattform für VBS, Industrie, Betreiber kritischer Infrastrukturen und Hochschulen, um Tools für die Cyber-Sicherheit zu entwickeln, die in den Bereichen 4 und 5 eingesetzt werden können, und um über einen flexibel einsetzbaren Pool an Personen und Kompetenzen zu verfügen.
	6.3 Ausbildung und Training	Rekrutierung und Aufbereitung der verschiedenen Cyber-Berufe, die in den Bereichen 3, 4 und 5 erforderlich sind; erfolgt in enger Zusammenarbeit mit den Hochschulen; umfasst die Schaffung einer Reserve an technischem (6.2) und nicht technischem Personal.

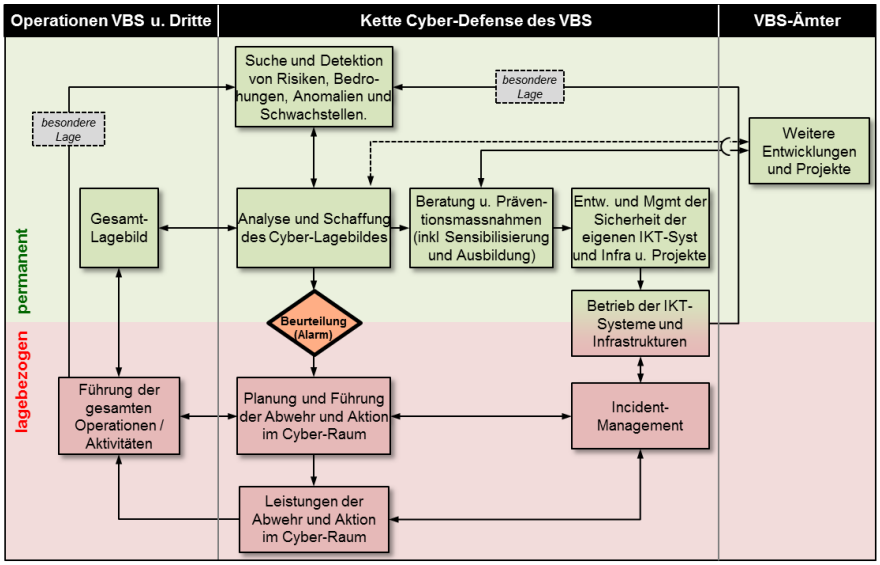
4 UMSETZUNG DES AKTIONSPLANS CYBER-DEFENCE

4.1 Prozesse

Dank der gesammelten Erfahrungen, insbesondere jenen aus der Übung *Cyber Pakt* 2016, konnten auf VBS-Ebene die Praxis vereinheitlicht und die operativen Schlüsselprozesse (***Wie läuft das ab***?) strukturiert werden. Es konnte auch Klarheit darüber geschaffen werden, wie die Armee ihre Leistungen erbringt, namentlich mit subsidiärer Unterstützung in Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken. Einer dieser Prozesse bezieht sich spezifisch auf die Verteidigung von kritischen Infrastrukturen im Falle eines Cyber-Angriffs. Der angegriffene Betreiber richtet sein Ersuchen an die zuständige zivile Behörde. MELANI OIC bearbeitet dieses anschliessend, führt eine Basisanalyse durch und leitet den Fall jenen weiter, welche die erforderlichen Leistungen erbringen, zum Beispiel an die Armee, sofern die Kriterien erfüllt sind (siehe Ziffer 3.3).

Diese Prozesse (siehe untenstehende Abbildung) werden vertikal (das "*wer*") und horizontal (das "*wann*") unterteilt und können wie folgt gelesen werden:

[15] Schutz der Vertraulichkeit, der Integrität und der Verfügbarkeit der Systeme und Dienste.



Permanent*:* Die *Cyber-Defence-Kette* des VBS sucht über ihr Netzwerk und mit ihren Sensoren im Cyber-Raum nach Bedro-hungen und Angriffen jeglicher Art gegen ihre IKT-Systeme und -Infrastrukturen. Darauf basierend wird ein Lagebild erstellt, das Folgendes ermöglicht:

- die für den Betrieb der eigenen IKT-Infrastrukturen und für Projekte zuständigen Stellen (einschliesslich nötigenfalls Projeke bei Dritten oder Partnern) zu alarmieren und/oder zu beraten, damit diese die nötigen Schutzmassnahmen ergreifen;
- bei Cyber-Ereignissen, die ihre Aktivitäten gefährden könnten, die Operations-führung zu alarmieren und wenn sinnvoll andere zuständige Behörden zu informieren;
- zum Cyber-Lagebild der Nachbarn beizutragen;
- rechtzeitig die ständige Weiterentwicklung der eigenen Cyber-Kapazitäten und die Schulung des Personals sicherzustellen.

Im Bedarfsfall, bei Ereignissen oder wenn von höherer Ebene angeordnet:

- die Planungs- und Führungsaktivitäten unterstützen und die Operationssphäre Cyber mit den anderen Bereichen abstimmen;
- den Empfängern die zugelassenen Produkte für Cyber-Verteidigung zur Verfü-gung stellen.

4.2 Erforderliche Ressourcen

Berufspersonal

Vorgesehen sind insgesamt 166 Stellen, davon 21 für den Teil *Unterstützung*. Mit Ausnahme der Funktionen 6.1–6.3 sind alle Funktionen der Architektur bereits mit Grundmitteln ausgestattet. Ende 2017 werden ca. 65 Stellen besetzt sein; diese werden durch rund 100 Stellen neu zugeteilte Stellen verstärkt, ohne Änderung der VBS-Strukturen.

Die Bestimmung einer genauen Zielgrösse ist angesichts der Natur der Cyber-Bedrohungen und -Ereignisse nicht möglich. Der angestrebte Bestand wurde des-halb auf der Grundlage folgender Kriterien bestimmt:

- eine stabile Struktur erreichen, in der alle benötigten Disziplinen vertreten sind; jeder Verzicht würde zu Fähigkeitslücken und damit zu langanhaltenden und schwierig zu bewältigenden Risiken führen;
- auf simultane Ereignisse, Grossereignisse und/oder komplexe Ereignisse rea-gieren können;

- über genügend Mittel verfügen, um bestehende Verwundbarkeiten rasch zu beseitigen und zu verhindern, dass aus der omnipräsenten Digitalisierung neue entstehen;
- über die Fähigkeit verfügen, die nächsten grossen Beschaffungen zu begleiten und so zu vermeiden, dass neue Cyber-Lücken entstehen;
- die rasche Entwicklung der Herausforderungen im Cyber-Raum antizipieren und nicht mehr nur erleiden;
- über eine kritische Grösse verfügen, um dem angestellten Personal innerhalb des Bereichs Karriereperspektiven bieten zu können.

Dieser Personalbestand wird einzig zur täglichen Schaffung von Sicherheit für das VBS und die Betreiber kritischer Infrastrukturen eingesetzt. Darin sind keine Unterstützungsfunktionen (z. B. Personal, Finanz, Sicherheit, Logistik) inbegriffen; diese Aufgaben werden durch die bereits bestehenden Organisationen erfüllt.

Milizpersonal

Das Berufspersonal wird, mit Ausnahme des Nachrichtendienstes des Bundes, durch Milizangehörige verstärkt. Die Detailplanung erfolgt im Rahmen des Konzeptes für den CYD-Campus. Wie in Ziffer 1.5 erwähnt, werden differenzierte Einsatzmodelle bevorzugt, und diese Angehörigen der Armee dürften zu attraktiven Spezialisten auch für die Privatwirtschaft werden.

Finanzen

Beim aktuellen Arbeitsstand kann keine detaillierte Planung aufgestellt werden. Jede Organisationseinheit muss ihren Bedarf bestimmen und diesen in die normalen Prozesse eingeben. Es wird kein spezieller Cyber-Prozess definiert. Auf Basis der Erfahrungswerte anderer Länder können die Kosten für Cyber-Defence, einschliesslich Personal, bei Erreichen der operativen Kapazität auf ca. 2 Prozent des Jahresbudgets des VBS geschätzt werden.

4.3 Massnahmen zur Umsetzung des Aktionsplans Cyber-Defence

Der Aktionsplan Cyber-Defence umfasst 11 Teilprojekte, und seine Umsetzung dauert bis 2020. Die Geschwindigkeit der Umsetzung hängt vor allem von der Fähigkeit des VBS ab, die nötigen Stellen[16] in das Projekt umzuteilen.

Teilprojekte	Ziele	Verantw.	Termin (Stand)[17]
1) Informationssicherheit	Die Funktion *Planung und Steuerung* (3.2) der Architektur verwirklichen. Die Entwicklung des Informationsschutzgesetzes (ISG) und die Implementierung des Integralen Sicherheits-Management-Systems VBS berücksichtigen.	GS VBS IOS	Ende 2017 (Optimierung läuft)
2) Zelle Cyber-Defence VBS (CYD VBS)	Die Funktionen *Strategische Steuerung* (3.1) und *Strategische Analyse* (3.3) der Architektur verwirklichen. Die Empfehlungen der Internen Revision VBS berücksichtigen. Das Kontinuum zwischen Cyber-Schutz und Cyber-Verteidigung durch enge Zusammenarbeit mit IOS sicherstellen. Die Kohärenz zwischen CYD-VBS, Beirat CYD VBS und CYD-Campus sicherstellen.	GS VBS Del CYD	Mitte 2017 (operativ nach aktuellem Stand, Del CYD VBS ernannt, erste Mitarbeiter angestellt)

[16] Die im Dezember 2016 vom Parlament beschlossene Plafonierung bedeutet eine Reduktion um ca. 300 Stellen im VBS. Nimmt man die Stellen für die Cyber-Verteidigung hinzu, sind es insgesamt 400 Stellen.

[17] Es handelt sich um den Termin der Detailplanung, nicht um die Fertigstellung des Aufbaus, der bis 2020 vorgesehen ist. Die Schwierigkeit, die notwendigen Positionen durch interne Umteilungen zu generieren, sowie der Cyber-Angriff vom Sommer 2016 (http://www.vbs.admin.ch/content/vbs-internet/fr/die-schweizer-armee/schutz-vor-cyber-angriffen.detail.nsb.html/68135.html) verursachten eine Verzögerung von 4-5 Monaten auf den ursprünglichen Zeitplan.

Teilprojekte	Ziele	Verantw.	Termin (Stand)[17]
3) Cyber-Mittel des NDB	Die Funktionen *Cyber-Defence der zivilen kritischen Infrastrukturen* (5.1) und *Nachrichtendienstliche Cyber-Aktionen* (5.2) der Architektur konkretisieren.	NDB	Ende 2017 (operativ nach aktuellem Stand)
4) Cyber-Mittel der Armee	Die Funktionen *Militärische Cyber-Aktion* (5.3) und *Militärische Cyber-Defence* (5.4) der Architektur konkretisieren.	Armee FUB	Ende 2017 (operativ nach aktuellem Stand)
5) CYD-Campus	Die Funktionen *Technologisches Monitoring* Cyber (6.1), *Entwicklung und Anwendungen* (6.2) und *Ausbildung und Training* (6.3) der Architektur konkretisieren; armasuisse W+T integrieren; den Zeitraum 2018-2019 vorrangig abdecken und so rasch wie möglich operativ werden.	GS VBS Del CYD	Ende 11.2017 (Grundkonzept)
6) Entwicklung und Management des Berufspersonals	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 ziehen, ohne die Weiterentwicklung der Armee oder laufende Beschaffungen zu gefährden; - gleichzeitig die von Parlament angeordnete Reduktion der Personalbestände umsetzen; - einen regelmässigen und geordneten Personalaufbau bevorzugen um den Aufwand für Rekrutierung, Integration, Schulung und Organisation zu minimieren.	GS VBS Ressourcen	Ende 2017 (Planung läuft; Aufbau bis 2020; die Teilprojekte passen ihre Entwicklung an den Rhythmus der Beschaffung der Stellen)
7) Entwicklung und Management des Milizpersonals	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 Projekt 5 synchronisieren; die Bedürfnisse in die Armeeorganisation 2019 aufnehmen.	Armee FUB	Ende 2017 (operativ nach aktuellem Stand)
8) Ausbildung und Sensibilisierung des Personals	Die Aus- und Weiterbildung der verschiedenen Personalkategorien des VBS sicherstellen (ausser beim NDB, der seine Mitarbeiter selbst ausbildet); mit den Projekten 5, 6, und 7 synchronisieren.	Armee FUB	Ende 2017 (teilweise operativ)
9) Infrastrukturen CYD	Die Mittel des VBS örtlich zusammenlegen (ausser NDB); mit dem Projekt 5 synchronisieren.	Armee FUB	Ende 2017
10) Militärischer reglementarischer Rahmen	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 fertigstellen und in einem Cyber-Reglement der Armee umzusetzen; - die neue Organisation in die Geschäftsordnung der Führungsunterstützungsbasis umzusetzen; - eine Cyber-Richtlinie des Chefs der Armee ausarbeiten, um das Funktionieren der Cybersphäre in der Armee zu regeln.	Armee FUB	Ende 2017
11) Kontinuierliche Verbesserung	Es geht darum, die kontinuierliche Verbesserung des Dispositivs des VBS für Cyber-Defence mit einem geeigneten Verfahren zur Messung der Fortschritte sicherzustellen.	GS VBS Del CYD	Ende 2017

4.4 CYD-Campus

Dreh- und Angelpunkt des Aktionsplans Cyber-Defence sind die Kompetenzen und der Informationsaustausch mit a) nationalen und internationalen operativen Partnern, b) der technologischen Industriebasis und c) den Hochschulen. Für einen solchen Austausch braucht es allerdings mehr als eine Absichtserklärung. Die verschiedenen Akteure müssen sich kennen und im Alltag gemeinschaftlich handeln. Dafür müssen Distanzen verkürzt und ein *Sammelpunkt* für die Cyber-Defence eingerichtet werden, mit dem Namen *CYD-Campus* und den folgenden Zielen:

- eine **Antizipationsplattform** aufbauen, die sämtlichen Akteuren der Cyber-Verteidigung in der Schweiz dient;
- im Rahmen einer Public-Private-Partnership die **technisch-operativen Kompetenzen und Kapazitäten** des VBS stärken, um es zu befähigen, die Betreiber kritischer Infrastrukturen dauerhaft, agil und mit den erforderlichen Kompetenzen zu unterstützen;
- die Fähigkeit der Schweizer Akteure der Cyber-Defence zum vernetzten Handeln stärken, durch die Sicherstellung ihrer **Interoperabilität**;
- **Talente** für den Bereich Cyber-Defence anziehen und halten, und hierfür eine dynamische Gemeinschaft aufbauen.

Verschiedene Interessenkonflikte werden die Schaffung des *CYD-Campus* erschweren. Unterschiedliche Vertraulichkeitsstufen sowie operative und akademische Themen mit unterschiedlichen Bedürfnissen und Zielen werden nebeneinander existieren müssen. Ausserdem wird darauf zu achten sein, keine Doppelspurigkeiten zu schaffen. Das Projekt muss ab 2018 erste Wirkungen zeitigen, bis Mitte 2019 eine operativen Grundkapazität und bis Ende 2020 die vollen Kapazitäten erreichen. Das VBS muss dabei jederzeit die Kompetenzen und Kapazitäten nutzen können, um Betreiber kritischer Infrastrukturen zu unterstützen.

Die Ausbildung des Personals wird ein besonders wichtiger Aspekt sein, um die Exponierung des VBS und der Armee zu den Cyber-Risiken zu verringern. Das Berufs- und das Milizpersonal muss also ab Einsatzbeginn während der ganzen Karriere kontinuierlich für die Herausforderungen und Bedrohungen des Cyber-Raums geschult werden.

4.5 Führung der Umsetzung

Die Umsetzung des Aktionsplans Cyber-Defence besteht aus 3 Handlungsfelder:

- die **Mittel** zur Ausstattung der betroffenen Einheiten, damit sie ihre Aufgaben erfüllen können;
- die **Prozesse**, um jederzeit mit den verfügbaren Mitteln die grösstmögliche Wirksamkeit zu erreichen;
- die **Kompetenzen** durch die Ergänzung des Dispositivs mit den Bereichen Steuerung und Unterstützung zur Stärkung der Mittel und Sicherstellung einer einheitlichen Steuerung der Prozesse.

Die Umsetzung des Aktionsplans Cyber-Defence dauert bis Ende 2020, was – wegen der rasanten Entwicklung des Cyber-Raumes – eine permanente Überprüfung und Anpassung erforderlich macht. Die Projektleitung wird dem Delegierten des VBS für Cyber-Defence obliegen, die Überwachung dem Informatikrat VBS. Ausserdem werden die Elemente des Aktionsplans Cyber-Defence, welche die Gruppe Verteidigung betreffen, im Masterplan aufgenommen, das vom Armeestab geführt wird.

5 FAZIT

Das VBS muss als wichtiger Akteur der Sicherheitspolitik zusammen mit seinen Partnern die komplexen und zahlreichen Herausforderungen der digitalen Transformation der Gesellschaft angehen und sie zur Sicherstellung seiner Aufträge berücksichtigen. Aufgrund der rasanten Entwicklungen in diesem Bereich duldet die Stärkung der Fähigkeiten zur Cyber-Defence keinen Aufschub. Ein gutes Fundament ist bereits gelegt, es bleibt aber trotz der erreichten Fortschritte noch vieles zu tun.

Der Aktionsplan Cyber-Defence ist die erste Roadmap des VBS auf dem konkreten und pragmatischen Weg zu Antworten auf die vielfältigen Herausforderungen des Cyber-Raums für unsere Sicherheitspolitik.