Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Schweizer Armee
Führungsunterstützungsbasis FUB

Verordnung über die militärische Cyberabwehr
Erläuterung der einzelnen Bestimmungen

Einführung

1. Gesetzliche Grundlagen

Im Rahmen der Weiterentwicklung der Armee wurde das Bundesgesetz über die Armee und die Militärverwaltung vom 3. Februar 1995 (MG) geändert.[1] Art. 100 MG regelt die militärische Sicherheit und ist mit Abs. 1 lit. c die Grundlage der vorliegenden Verordnung. Art. 100 Abs. 1 lit. c MG umschreibt die zu treffenden erforderlichen Massnahmen im Fall eines Angriffes auf militärische Informationssysteme und Informatiknetzwerke.

In Umsetzung der gesetzlichen Grundlagen bilden die Massnahmen zum Eigenschutz und zur Selbstverteidigung der Armee und der Militärverwaltung im Falle eines Angriffs auf ihre eigenen Informationssysteme oder Informatiknetzwerke, die die Auftragserfüllung der Armee beeinträchtigen können, den Kern dieser Verordnung. In Art. 100 Abs. 4 MG wird der Bundesrat zudem aufgefordert, die zuständigen Stellen im Einzelnen und deren Organisation zu regeln und so die entsprechenden Aufgaben und Kompetenzen innerhalb der Armee klar zuzuweisen. Die Verordnung regelt deshalb zusätzlich Aufgaben des Bundesrates sowie der Chefin oder des Chefs des VBS und enthält Ausführungsbestimmungen im Bereich Einsatz und Ausbildung sowie Forschung.

Nachrichtendienstliche Kompetenzen werden der Armee weder durch diese Verordnung noch durch das MG übertragen. Der Gesetzgeber hat mit Art. 99 MG, Nachrichtendienst, und Art. 100, militärische Sicherheit, die Unterscheidung dieser Tätigkeiten zum Ausdruck gebracht. Die Zuständigkeiten der Schweizer Armee werden durch die Verordnung nicht ergänzt.

2. Inhalt der vorliegenden Verordnung

Die Bedrohung durch Angriffe im Cyberraum hat sich verschärft.[2] Die Anzahl und die Arten der Angriffe haben sich vervielfacht, und es ist davon auszugehen, dass diese Entwicklung anhalten wird. Mit der vorliegenden Verordnung wird deshalb umgesetzt, was politisch bereits seit längerem gefordert wird: „Die Armee muss jederzeit, im Alltag wie in der Krise, ihre eigenen Informations- und Kommunikationssysteme und -infrastrukturen vor Angriffen schützen und Cyber-Angriffe abwehren können. Sie setzt die entsprechenden Mittel so ein, dass sie sich selber schützen und ihren Auftrag erfüllen kann.“[3]

Ziele von Cyberangriffen können zivile und militärische Informationssysteme und Informatiknetzwerke sein. Landesgrenzen und Distanzen spielen dabei kaum noch eine Rolle. Es ist

---

1 Änderung vom 18.03.2016 des Militärgesetzes vom 03.02.1995
2 Siehe dazu auch: Die Sicherheitspolitik der Schweiz Bericht des Bundesrates vom 24.08.2016 (SIPOL B), 7785.
3 Die Sicherheitspolitik der Schweiz Bericht des Bundesrates vom 24.08.2016 (SIPOL B 16), 7846.

staatlichen wie auch nichtstaatlichen Akteuren möglich, ohne vor Ort präsent zu sein, eine Wirkung zu erzielen und Schaden anzurichten. Dabei können Cyber-Angriffe verschiedene Zwecke verfolgen. Sie können für kriminelle Zwecke, für Spionage oder Sabotage genutzt werden. Sie können aber auch zur Unterstützung von militärischen Operationen durchgeführt werden. Wie Cyberangriffe eingesetzt werden und welche Rolle sie in aktuellen Konflikten spielen, wird ausführlich im sicherheitspolitischen Bericht des Bundesrates behandelt.[4]

Die vorliegende Verordnung befasst sich mit Cyberangriffen auf militärische Informationssysteme und Informatiknetzwerke unterhalb und oberhalb der Schwelle eines bewaffneten Angriffs und der Frage, wie die Armee darauf reagieren kann. Wie im sicherheitspolitischen Bericht des Bundesrates festgehalten, ist davon auszugehen, dass die Bedrohung durch solche Angriffe weiter zunehmen wird. Im Bericht steht dazu: „Es ist davon auszugehen, dass in künftigen Konflikten praktisch alle Parteien, grosse und kleine, staatliche und nichtstaatliche, im Cyber-Raum offensiv vorgehen werden. Die grössere Bedeutung des Cyber-Raums kann zur Folge haben, dass die Schweiz von bewaffneten Konflikten auch dadurch berührt wird, dass Informations- und Kommunikationsinfrastrukturen in der Schweiz von ausländischen Akteuren in Konflikten missbraucht oder beschädigt wird. “[5]

Angriffe auf militärische Informationssysteme und Informatiknetzwerke stellen deshalb eine wichtige Bedrohung dar, selbst wenn diese Angriffe unterhalb der Schwelle eines bewaffneten Konflikts bleiben. Als bewaffneter Angriff gilt ein Angriff von grösster Dimension mit gravierenden Auswirkungen auf die territoriale Integrität, die gesamte Bevölkerung oder die Ausübung der Staatsgewalt.[6] Die vorliegende Verordnung regelt die Zuständigkeiten und Entscheidabläufe für den Fall, dass die Armee ihre eigenen Informationssysteme oder Informatiknetzwerke schützen muss. Jede Aktion wird unter Berücksichtigung des nationalen und internationalen Rechtsrahmens sowie aussenpolitischen Aspekten im Einzelfall beurteilt, um das geeignete Mittel zur Anwendung zu bringen. Entscheidungen werden, sofern ein Eindringen in fremde Computersysteme oder –netzwerke erforderlich ist, dem Gesamtbundesrat vorgelegt.

Die nachfolgenden Erläuterungen beschränken sich zur besseren Lesbarkeit auf inhaltlich zu klärende Artikel und Absätze.

3. Erläuterungen der einzelnen Bestimmungen

Art. 1
Abs. 1
Die Verordnung kommt im Fall eines Angriffs auf die Informationssysteme und Informatiknetzwerke der Armee und der Militärverwaltung zur Anwendung. Die Verordnung regelt also die Massnahmen, die dem Eigenschutz und der Selbstverteidigung der Armee dienen. Die Armee hat keine Gesamtverantwortung im Bereich Cyber für die Schweiz und erhält mit dieser Verordnung keine über den Eigenschutz und die Selbstverteidigung hinausgehenden Zuständigkeiten.

---

4 Siehe dazu auch: Die Sicherheitspolitik der Schweiz Bericht des Bundesrates vom 24.08.2016 (SIPOL B 16), 7783-7784; 7853-7856.
5 Die Sicherheitspolitik der Schweiz Bericht des Bundesrates vom 24.08.2016 (SIPOL B), 7785.
6 Die Sicherheitspolitik der Schweiz Bericht des Bundesrates vom 24.08.2016 (SIPOL B 16), 7854.

Abs. 2
Die militärische Cyberabwehr ist als Teil der Cyberkriegführung zu verstehen und ist in drei Teile unterteilt: Cyberverteidigung, Cyberaufklärung und Cyberangriff. Das eigentliche Ziel der militärischen Cyberabwehr ist der Eigenschutz und die Selbstverteidigung der militärischen Informationssysteme und Informatiknetzwerke. Dieses Ziel wird mit Aktionen im Cyberraum auf militärstrategischer und operativer Führungsstufe zu erreichen versucht.

Der Cyberraum ist ein virtueller Raum, in welchem digitale Daten erfasst, gespeichert, verarbeitet und übermittelt werden. Es ist in diesem Sinne eine virtuelle Welt, welche das ganze Internet umfasst. In diesem Raum können, wie in der realen Welt, Verbrechen verübt oder im konkreten Fall die Armee in der Wahrnehmung ihrer Aufgaben eingeschränkt oder gehindert werden.

lit. a
Als Cyberverteidigung wird eine Aktion im Cyberraum verstanden, die das Ziel hat, die eigenen Ressourcen zu schützen (vgl. Art. 2 Abs. 1 und 2). Damit soll Angriffen und fremder Cyberaufklärung entgegengewirkt und eigene Informationssysteme und Informatiknetzwerke geschützt werden, damit die Integrität, die Vertraulichkeit oder die Verfügbarkeit von Informationen und Daten nicht beeinträchtigt wird.

lit. b
Die Cyberaufklärung ist vergleichbar mit der herkömmlichen militärischen Aufklärung, jedoch im Cyberraum. Es sollen gezielt Aktionen durchgeführt werden, um einen Angriff auf Informationssysteme und Informatiknetzwerke der Armee oder der Militärverwaltung zu erkennen und zu lokalisieren. Nachrichtendienstliche Kompetenzen gemäss Art. 99 MG sind dabei dem Nachrichtendienst der Armee vorbehalten.

lit. c
Ein Cyberangriff hat das Ziel, gegnerische Ressourcen und Aktionen im oder durch den Cyberraum zu stören, zu verhindern oder zu verlangsamen. Hier kann eine Durchlässigkeit des Cyberraums in die reale Welt erkannt werden: Mit einem Cyberangriff kann direkt auf die Funktionen von militärischer Ausrüstung eingewirkt werden. Bei einem Cyberangriff handelt eine Person oder eine Gruppierung im Cyber-Raum, um die Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen und Daten zu beeinträchtigen; dies kann je nach Art des Angriffs auch zu physischen Auswirkungen führen.

Ein Cyberangriff ist dann oberhalb der Schwelle des bewaffneten Angriffs einzustufen, wenn es sich um einen Angriff von grösster Dimension mit gravierenden Auswirkungen auf die territoriale Integrität, die gesamte Bevölkerung oder die Ausübung der Staatsgewalt handelt.[7] Wenn Aktionen im Cyberraum in Verbindung mit einem bewaffneten Konflikt durchgeführt werden oder einen solchen Konflikt auslösen, müssen diese mit dem humanitären Völkerrecht vereinbar sein.

Es ist jedoch davon auszugehen, dass Cyberangriffe oft im Verbund mit anderen Mitteln zur Störung und Einflussnahme eingesetzt werden und – auch bewusst – unter der Schwelle eines bewaffneten Angriffs oder bewaffneten Konflikts gehalten werden.

---

[7] Die Sicherheitspolitik der Schweiz Bericht des Bundesrates vom 24.08.2016 (SIPOL B 16), 7854.

Die obigen Begrifflichkeiten ermöglichen es den betroffenen Stellen, die Aktion rund um die Cyberabwehr einzuordnen, damit die Zuständigkeiten innerhalb der Armee klar sind.

Art. 2
Abs. 1
Bewilligungspflichtige Massnahmen sind solche, die das Eindringen in andere, fremde Computersysteme und/oder Computernetzwerke im Rahmen einer Aktion im Cyberraum erfordern. Diese bedürfen der Genehmigung des Bundesrates.

Beispielsweise wird ein speziell für den konkreten Anwendungsfall erstelltes (Computer-)Programm auf jenen Computer implementiert, welcher als Urheber eines Angriffes auf Systeme der Armee identifiziert worden ist. Dieses Programm hat zum Zweck, Angriffe von diesem Computer zu unterbinden. Solche Massnahmen bedürfen wie bereits ausgeführt der Genehmigung des Bundesrates.[8]

Abs. 2
Nicht bewilligungspflichtige Massnahmen sind solche, die kein Eindringen in andere Computersysteme und/oder Computernetzwerke erfordern.

Nicht bewilligungspflichtige Massnahmen umfassen beispielsweise die stetige Aktualisierung der Informationssysteme und Informatiknetzwerke der Armee und der Militärverwaltung. Dazu gehört die Sicherung von geheimen und funktionsrelevanten Daten sowie die Updates von Systemen und Programmen (bspw. Antivirus).

Art. 3
Falls die Chefin oder der Chef der Armee der zuständigen Stelle (Führungsunterstützungsbasis FUB) einen Auftrag für eine bewilligungspflichtige Massnahme erteilen will, muss dies vorgängig der Chefin oder dem Chef des VBS beantragt werden. Dieser Antrag muss schriftlich verfasst sein, eine Begründung und folgende Angaben enthalten:

- den Zweck der Aktion im Cyberraum;
- den Zeitraum, in dem die Aktion im Cyberraum erfolgen soll;
- die betroffenen Computersysteme und Computernetzwerke;
- die maximale Anzahl Eindringen in die betroffenen Computersysteme und Computernetzwerke und
- den Nachweis der Rechtmässigkeit insbesondere der Verhältnismässigkeit und die Beurteilung der politischen Risiken der Aktion im Cyberraum.

lit. e
Bewilligungspflichtige Massnahmen müssen unter rechtlichen und politischen Gesichtspunkten beurteilt werden. Die Prüfung umfasst internationale Verpflichtungen und nationales Recht sowie die Beurteilung der politischen Risiken und Auswirkungen einer Aktion im Cyberraum. Aktionen im Cyberraum müssen stets verhältnismässig (Eignung, Erforderlichkeit und Zumutbarkeit der Aktion) und mit der Neutralität der Schweiz sowie, in bewaffneten Konflikten, mit dem humanitären Völkerrecht vereinbar sein. Die Überprüfung erfolgt in Konsultation mit den zuständigen Stellen innerhalb der Verwaltung.

---

[8] Geschäftsordnung Führungsunterstützungsbasis (GO-FUB), 3.1.

Massnahmen im Ausland müssen nebst den Voraussetzungen im nationalen Recht immer auch völkerrechtlich zulässig sein.
Gegenmassnahmen gegen ausländische Computersysteme sind völkerrechtlich erlaubt, wenn der Cyberangriff, welcher von diesen Computersystemen ausgeht, einem Staat zurechenbar ist und eine völkerrechtswidrige Handlung darstellt. Handlungen im Cyberraum unterhalb der Schwelle eines bewaffneten Angriffs verletzten in der Regel die Souveränität oder territoriale Integrität des benachteiligten Staates. Sie können auch eine unzulässige politische oder wirtschaftliche Einmischung eines Staates in die inneren und äusseren Angelegenheiten eines anderen Staates darstellen und damit gegen das völkerrechtliche Interventionsverbot verstossen.

Gegenmassnahmen gegen solche Verletzungen zielen gemäss den anwendbaren Kriterien der Staatenverantwortlichkeit darauf ab, mittels Zufügung von (Rechts-) Nachteilen den betreffenden Staat zur Einstellung seines völkerrechtswidrigen Verhaltens und/oder zu einer Wiedergutmachung zu bewegen. Sie können ergriffen werden, wenn der verantwortliche Staat vorgängig zur Einstellung des Völkerrechtsbruchs aufgefordert und die Gegenmassnahme angekündigt worden ist, die Gegenmassnahme verhältnismässig ist und darauf abzielt, den verantwortlichen Staat zur Einhaltung seiner völkerrechtlichen Pflichten zu bewegen. Gegenmassnahmen, die eine Botschaft oder eine konsularische Vertretung betreffen, müssen die Voraussetzungen des Wiener Übereinkommen über diplomatische Beziehungen[9] bzw. des Wiener Übereinkommens über konsularische Beziehungen[10] einhalten.

Erfolgt ein Cyberangriff durch nichtstaatliche Akteure, so sind Gegenmassnahmen gegen einen anderen Staat nur dann zulässig, wenn das Handeln der nichtstaatlichen Akteure einem Staat zugerechnet werden kann. Fehlt die notwendige zwischenstaatliche Dimension, so sind Gegenmassnahmen gegen einen anderen Staat grundsätzlich völkerrechtlich unzulässig. Die Schweiz müsste in diesem Fall dann die Kooperation mit demjenigen Staat suchen, von dessen Territorium der Cyber-Angriff auf die Schweiz ausgeht. Eine abschliessende völkerrechtliche Beurteilung ist erst im Lichte der konkreten Umstände des Einzelfalls möglich.

Ist der Cyber-Angriff als bewaffneter Angriff zu qualifizieren, so kann die Schweiz gestützt auf das Selbstverteidigungsrecht gemäss Art. 51 UNO-Charta11 und den darin enthaltenen Rahmenbedingungen unilateral Gegenmassnahmen ergreifen. Die Schweiz würde sich dann im Kriegszustand mit dem Staat befinden, von dem der Cyber-Angriff ausgeht.

Auf Gegenmassnahmen, die in Verbindung mit einem internationalen oder nicht-internationalen bewaffneten Konflikt durchgeführt werden oder einen solchen Konflikt auslösen ist insbesondere das humanitäre Völkerrecht anwendbar. Solche Gegenmassnahmen müssen insbesondere die humanitären Grundprinzipien der Menschlichkeit, Notwendigkeit, Verhältnismässigkeit, Unterscheidung und das Vorsichtsprinzip erfüllen.

Für die Informationsbeschaffung in Computersystemen und Computernetzwerken im Ausland über die Urheber einer Cyber Operation in der Schweiz bestehen keine spezifischen Regeln im Völkerrecht. Die Informationsbeschaffung erfolgt grundsätzlich zu einem Zeitpunkt, in dem über die Zurechenbarkeit der Operation zu einem Staat noch nicht entschieden werden kann.

---

9 SR **0.191.01**
10 SR **0.191.02**
11 SR **0.120**

Erst die Informationsbeschaffung wird die für die Beurteilung erforderlichen Informationen generieren. Es bietet sich deshalb die Analogie zu den völkerrechtlichen Regeln der Spionage an. Spionage ist völkerrechtlich grundsätzlich nicht verboten, es müssen dabei jedoch gewisse Rahmenbedingungen beachtet werden. Beschränkungen von Spionagetätigkeiten finden sich namentlich in verschiedenen Instrumenten zum Schutz der Menschenrechte (bspw. dem UNO-Pakt II[12]). Im selben Sinne untersagen das Wiener Übereinkommen über diplomatische Beziehungen und das Wiener Übereinkommen über konsularische Beziehungen die Einmischung in interne Angelegenheiten des Empfangstaates.

Art. 4
Abs. 1
Für die militärische Cyberabwehr ist die Führungsunterstützungsbasis (FUB) zuständig. Die FUB nimmt die Cyberabwehr mit eigenen Ressourcen wahr. Jedoch können der FUB Ressourcen auch unterstellt oder zugewiesen werden. Dabei handelt es sich bspw. um spezifisches Material und Personal aus anderen Bereichen der Armee und der Militärverwaltung zur Auftragserfüllung. Diese Ressourcen werden der FUB beschränkt für die Dauer eines Auftrages unterstellt oder zugewiesen.
Für die Ausführung sämtlicher Aktionen im Cyberraum werden nur zivile Angestellte der FUB eingesetzt. Milizangehörige unterstützen die FUB nur indirekt, wenn gewisse Fähigkeiten oder personelle Ressourcen fehlen oder die Durchhaltefähigkeit sichergestellt werden muss.

Abs. 2
lit. a
Die FUB nimmt die Aufträge der Chefin oder des Chefs der Armee entgegen, priorisiert und führt sie aus. Dabei obliegt ihr die Planung und Umsetzung der Aufträge der militärischen Cyberabwehr.

lit. b
Zur Vorbereitung und Sicherung von Massnahmen ergreift die FUB die notwendigen vorsorglichen Massnahmen. Diese Vorbereitungen werden unter Einhaltung von internationalen Verpflichtungen sowie nationalem Recht getroffen. Diese Massnahmen umfassen unter anderem die Vorbereitung der Soft- und der Hardware der militärischen Informationssysteme und Informatiknetzwerke. Nebst den technischen Massnahmen können Übungen mit den beteiligten Stellen durchgeführt werden, um die Abläufe zu prüfen und zu optimieren. Als vorsorgliche Massnahme gilt unter anderem die Trennung der Systeme als Eigenschutzmassnahme, um deren Verwundbarkeit zu reduzieren.

lit. c
Erhaltene Aufträge zur Ausführung einer Aktion im Cyberraum werden durch die FUB sowohl auf ihre technische Machbarkeit wie auch auf ihre rechtliche Zulässigkeit hin geprüft. Die grundsätzliche Klärung der Rechtmässigkeit durch die FUB stellt die erste Stufe einer zweistufigen Prüfung dar (die zweite Stufe wird durch das Generalsekretariat VBS sichergestellt). Laufende Massnahmen werden im Rahmen der militärischen Lageverfolgung stetig auf ihre Rechtmässigkeit und Machbarkeit hin überprüft.

---

12 SR **0.103.2**

lit. d
Die Unterbrechung stellt einen Spezialfall einer nicht-bewilligungspflichtigen Massnahme dar. Wenn ein Angriff entdeckt wird, kann es nötig sein, dass eine rasche Unterbrechung des Zugangs zu militärischen Informationssystemen und Informatiknetzwerken notwendig ist, um den Angriff einzudämmen und weiteren Schaden zu verhindern. Eine solche Unterbrechung wird von den für den Betrieb der militärischen Informationssysteme und Informatiknetzwerke zuständigen Stellte innerhalb der FUB beantragt. Die Chefin oder der Chef FUB genehmigt eine solche Unterbrechung.

lit. e
Die Armee hat die rechtliche Grundlage erhalten, den Eigenschutz und die Selbstverteidigung im Cyberraum sicherzustellen. Dazu muss die Armee unabhängig und in allen Lagen über die technischen Informationen verfügen, um eine Bedrohungsanalyse zu erstellen bzw. um sicherzustellen, dass ein Angriff auf militärische Informationssysteme und Informatiknetzwerke überhaupt antizipiert und erkannt werden kann.
Es handelt sich hierbei nicht um eine nachrichtendienstliche Tätigkeit. Ebenfalls werden keine besonders schützenswerten Personendaten erfasst. Abgespeichert werden lediglich jene Informationen, die auch zu einem späteren Zeitpunkt das Erkennen eines Angriffs ermöglichen.

lit. f
Die FUB wertet sichergestellte Computer aus. Sie stützt ihre Arbeit auf die einschlägigen Normen des Militärstrafprozessrechts.

lit. g
Die FUB pflegt nach Rücksprache mit den verantwortlichen Behörden des Bundes direkte Kontakte zu anderen Fachstellen. Eine Zusammenarbeit mit ausgewählten militärischen Stellen ist zwingend. Hierbei handelt es sich um den Dialog auf fachtechnischer Stufe. Weiter soll auf fachtechnischer Stufe ebenfalls der Dialog mit zivilen Partnern im In- und Ausland gepflegt werden. Jegliche nachrichtendienstlichen Kontakte müssen zuvor mit dem Nachrichtendienst des Bundes geklärt werden (vgl. Art. 6 V-NDA).

lit. h
Die FUB hat den Einsatz und die Ausbildung im Bereich der militärischen Cyberabwehr zu unterstützen. Hierbei handelt es sich um die Ausbildung von militärischem und zivilem Personal, welches Aufträge zu Aktionen im Cyberraum durchführt.

lit. i
Die Dokumentation gibt Aufschluss über die Durchführung, das Ergebnis und die Beendigung bewilligungspflichtiger Massnahmen im Cyberraum.

Abs. 3
Jegliche Massnahmen, welche eine Genehmigung durch den Bundesrat erfordern, werden ausschliesslich durch das ZEO ausgeführt.

Art. 5
Abs. 1
Die Chefin oder der Chef der Armee erteilt die Aufträge für Aktionen im Cyberraum.

Abs. 2
Von der FUB formulierte Anträge für bewilligungspflichtige Massnahmen werden von der Chefin oder dem Chef der Armee der Chefin oder dem Chef des VBS vorgelegt. Erst nach erfolgter Prüfung durch die Chefin oder den Chef des VBS und erfolgter Konsultation der betroffenen Ämter wird der Antrag dem Bundesrat zur Genehmigung unterbreitet.

Abs. 3
Aktivdienst bedeutet in der Schweiz den Einsatz der Schweizer Armee zur Abwehr von äusseren oder inneren Gefahren (Art. 76 Abs. 1 MG). Während des Aktivdienstes kann die Chefin oder der Chef der Armee und/oder auch die Oberbefehlshaberin oder der Oberbefehlshaber der Armee bewilligungspflichtige Massnahmen zum Eigenschutz und der Selbstverteidigung genehmigen. Die Delegation kann entweder an die Chefin oder den Chef Kommando Operationen oder an die Chefin oder den Chef der FUB erfolgen.

Art. 6
Der Chef oder die Chefin des VBS prüft Anträge der Chefin oder des Chefs der Armee für bewilligungspflichtige Massnahmen. Bei Zustimmung zur beantragten Massnahme unterbreitet die Chefin oder der Chef des VBS diesen Antrag dem Bundesrat zur Genehmigung.

Art. 7
Die bewilligungspflichtigen Massnahmen, welche ein Eindringen in andere Computersysteme und/oder Computernetzwerke erfordern, werden dem Bundesrat zur Genehmigung unterbreitet.

Art. 8
Die Aufsicht erfolgt über vier Stufen. Die FUB kontrolliert zuallererst sich selbst. Das bedeutet, dass sie mit dazu geeigneten Mitteln das Verhalten ihrer Mitarbeiterinnen und Mitarbeiter kontrolliert. Zudem trifft die FUB Massnahmen zur Verminderung von Risiken (beispielsweise mit Schulungen und Sensibilisierungen in kritischen Bereichen).

Die interne Kontrolltätigkeit der FUB wird nach dem Vier-Augen-Prinzip mit der Aufsicht der übergeordneten Stelle, Generalsekretariat VBS, abgesprochen und koordiniert. Die durch die Armee bezeichnete zweite Kontrollstelle muss der Chefin oder dem Chef der Armee zur personellen Genehmigung unterbreitet werden. Diese ist dem Armeestab (ASTAB) unterstellt und die FUB darf weder die Mehrheit noch den Vorsitz des Gremiums stellen.

Die Generalsekretärin oder der Generalsekretär regelt die Aufsicht über die militärische Cyberabwehr und somit die dritte Aufsichtsstufe auf Departementsebene. Die vierte Kontrollinstanz bildet die parlamentarische Oberaufsicht.

Abs. 1
Das VBS erstattet regelmässig dem Bundesrat über die militärische Cyberabwehr Bericht und informiert die parlamentarische Oberaufsicht (Geschäftsprüfungsdelegation) über die Tätigkeit in diesem Bereich.

Die departementsinterne Aufsicht über die militärische Cyberabwehr und die diesbezügliche Berichterstattung an den Bundesrat werden durch das Generalsekretariat VBS wahrgenommen.

Abs. 2
Den Vorsitz der armeeinternen Aufsicht über die militärische Cyberabwehr hat der Armeestab inne. Die Mitglieder der Aufsicht werden durch die Chefin oder den Chef der Armee bewilligt.

Art. 9
Zur Gewinnung, Pflege und Weitergabe von Fachwissen kann die FUB nach Absprache mit den zuständigen Verwaltungseinheiten des VBS Vereinbarungen zur Kooperation mit Forschungsinstituten und Hochschulen treffen. So kann die FUB bspw. Vereinbarungen mit schweizerischen Hochschulen mit naturwissenschaftlichem Schwerpunkt zur Entwicklung von Software eingehen.

Art. 11
Die Verordnung tritt am 1. März 2019 in Kraft.