Datum: 14.04.2022

Neue Zürcher Zeitung

Neue Zürcher Zeitung
8021 Zürich
044/ 258 11 11
https://www.nzz.ch/

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 87'908
Erscheinungsweise: 6x wöchentlich

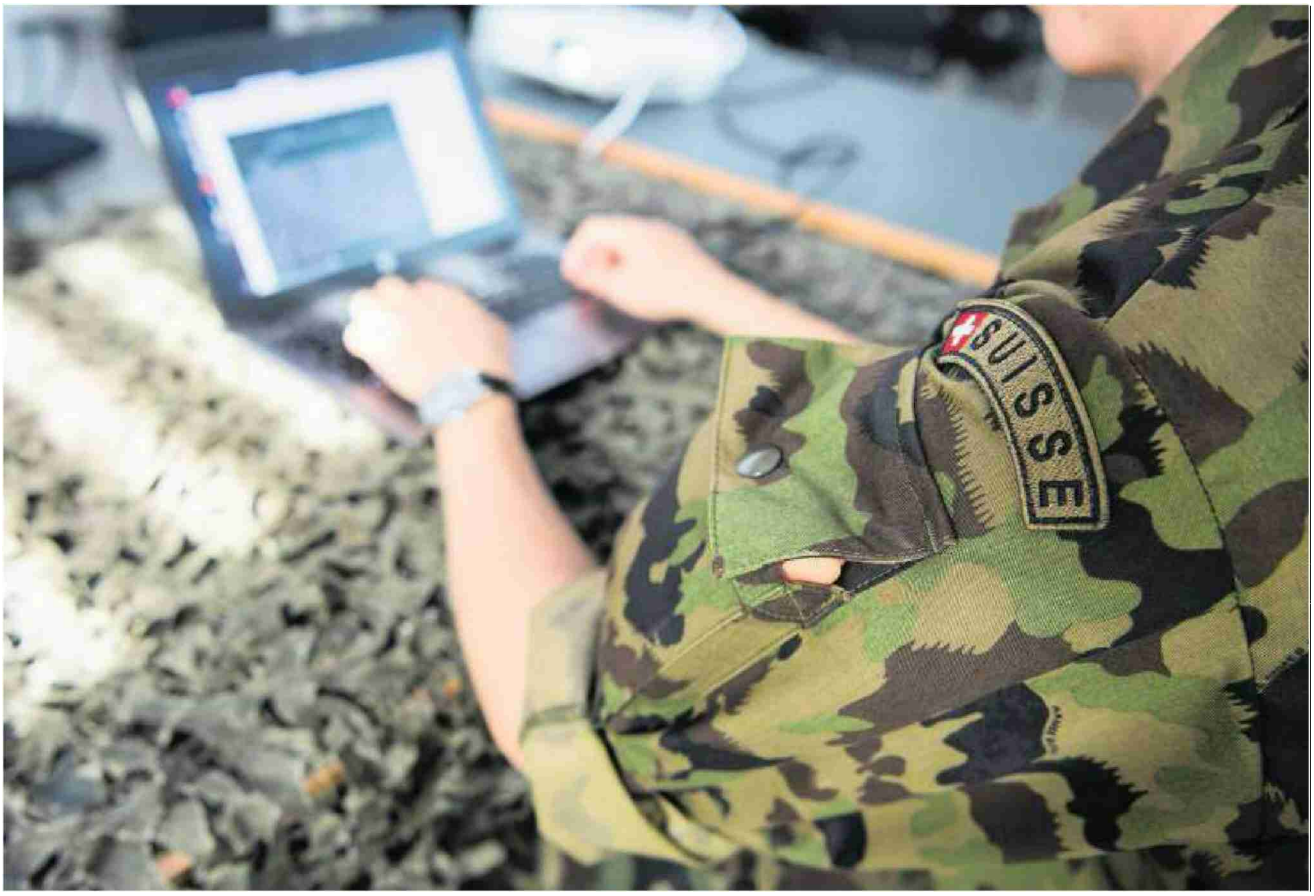
Seite: 7
Fläche: 88'804 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 83998659
Ausschnitt Seite: 1/3

Schweizer Armee rüstet sich für den Cyberkrieg

Verteidigungsministerin Viola Amherd will bis zu 2,4 Milliarden Franken in Störsender und mobile Rechenzentren investieren



Die Armee soll künftig besser ausgerüstet sein, um gegnerische Funksignale zu orten oder das Radar zu stören. PETER SCHNEIDER / KEYSTON

LUKAS MÄDER, GEORG HÄSLER

—

Welche Rolle spielen Cyberangriffe bei militärischen Konflikten der Zukunft? Der Krieg in der Ukraine liefert auf diese grosse Frage keine klaren Antworten – auch weil viele Details nicht öffentlich bekannt sind. Doch unbestritten ist, dass Cyberangriffe und Desinformationskampagnen eine wichtige Rolle spielen.

Wie die Schweizer Armee das künftig tun will, zeigt die Gesamtkonzeption Cyber. Es handelt sich um einen 120-seitigen Bericht, der grösstenteils noch vor Ausbruch des Kriegs in der Ukraine entstanden ist. Der Bundesrat hat das Grundlagendokument am Mittwoch zur Kenntnis genommen. Die Armeeführung legt darin dar, wo die Armee künftig digitale Fähigkeiten haben muss und wo Nachholbedarf besteht. Keine einfache Aufgabe angesichts der raschen technologischen Entwicklung.

In einem Punkt ist der Bericht klar – erstaunlich klar: Die Verteidigung gegen Angriffe im Cyberraum hat höchste Priorität. Im Vergleich dazu sollen die offensiven Fähigkeiten, also die Möglichkeit, selbst Cyberangriffe durchzuführen, nur gemässigt ausgebaut werden. Diese Priorisierung ist nicht selbstverständlich, denn immer wieder taucht die Idee auf, dass sich die Armee im Kampf gegen die Cyberkriminalität engagieren solle. In Deutschland wurde kürzlich gar über die Möglichkeit staatlicher Gegenschläge, sogenannter Hack-Backs, diskutiert.

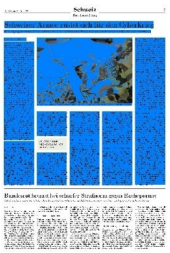
Der Bundesrat hat sich nun für den Mittelweg entschieden: Das Verteidigungsdepartement soll die militärischste der drei Optionen umsetzen, die finanziell in der Mitte liegt. Diese sieht Investitionen von 1,6 bis 2,4 Milliarden Franken bis etwa 2035 vor. Der Personalbestand bliebe unverändert. Das Kommando Cyber würde dereinst knapp 1000 Berufsmilitär und 6000 bis 7000 Milizangehörige umfassen. Der Bericht spricht vom «ausgewogensten Gesamtpaket» bezüglich Kosten und Technologierisiko.

Datum: 14.04.2022

Neue Zürcher Zeitung

Neue Zürcher Zeitung
8021 Zürich
044/ 258 11 11
https://www.nzz.ch/

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 87'908
Erscheinungsweise: 6x wöchentlich



Seite: 7
Fläche: 88'804 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 83998659
Ausschnitt Seite: 2/3

Selbstschutz an erster Stelle

Im Zentrum der Weiterentwicklung in den nächsten rund 15 Jahren steht der Eigenschutz. Die Armee muss ihre IT-Systeme auch im Cyberraum selbständig gegen Angriffe schützen können. Das klingt selbstverständlich und banal, ist aber angesichts der komplexen Informatik, die auch unterschiedliche vernetzte Waffensysteme umfasst, eine Herausforderung. Zudem müssen die Systeme jederzeit geschützt und funktionstüchtig sein, also auch im Katastrophen- oder Kriegsfall. Dies soll zum Beispiel mit kleinen, mobilen Rechenzentren bei den Bataillonen sichergestellt werden.

Dass der Eigenschutz der Armee so wichtig ist, hängt auch mit einer zweiten Fähigkeit zusammen, die der Bericht herausstreicht. Dabei handelt es sich simpel ausgedrückt um die «Digitalisierung der Armee». Es geht um die operationellen Fähigkeiten zur Kommunikation und Datenverarbeitung, zur Darstellung der aktuellen Lage sowie zur Führung der Truppen über die digitalen Kanäle.

Wie wichtig eine funktionierende Datenverbindung ist, zeigt der Krieg in der Ukraine. Das Internet sei die Lebensader des ukrainischen Staates, sagt Divisionär Alain Vuitel, der das Projekt für das künftige Kommando Cyber der Armee leitet. «Präsident Selenski braucht den Zugang zum Internet, um seine Botschaft nach aussen tragen zu können.» Sonst wäre die Ukraine ein schwarzes Loch auf unseren Bildschirmen, sagt Vuitel im Gespräch mit der NZZ.

Obschon der Krieg des Kremls vor allem konventionell geführt wird, werden die Trends des 21. Jahrhunderts deutlich sichtbar. Nach einem mutmasslich russischen Cyberangriff auf die Satellitenkommunikation hat die Ukraine nun über das Starlink-Satellitensystem des Tech-Unternehmers Elon Musk flächendeckend Internetzugang. Die Verbindung mit der Welt bleibt bestehen.

Dieses Beispiel zeigt die zunehmende Dominanz grosser Technologiefirmen, wie es der Bericht nennt. Im Gegensatz zum 20. Jahrhundert wird der technologische Fortschritt nicht mehr von der militärischen, sondern von der zivilen Seite vorangetrieben. Diesem Paradigmenwechsel muss auch die Schweizer Armee Rechnung tragen. Sie darf den Anschluss an technologische Entwicklungen nicht verlieren und muss ihren Beschaffungsprozess schlanker gestalten.

Mängel erst 2029 behoben

Damit die Vernetzung der Armee funktioniert, braucht sie die nötige Infrastruktur. Dazu gehören sichere Kommunikationsverbindungen zur Übertragung und Rechenzentren zur Verarbeitung der Daten. Das entsprechende milliardenschwere Projekt Fitania hat die Armee bereits vor knapp zehn Jahren lanciert. Nach einigen Verzögerungen soll es nun bis 2029 fertig sein.

Dereinst sollen die Daten der Sensoren, die sich in einem Kampfjet oder einem Schützenpanzer befinden, in die Rechenzentren geschickt werden, wo sie mittels moderner Analysemethoden verarbeitet werden. Die Resultate werden für die Darstellung des aktuellen Lagebilds verwendet, auf dem aufbauend die Führung ihre Befehle wiederum an die Truppe im Feld übermitteln kann. Das Programm Fitania soll auch die teilweise eklatanten IT-Mängel beheben, die sich in der Armee aus einer Nachlässigkeit heraus über die letzten Jahrzehnte angesammelt haben. Der Cyber-Bericht weist an mehreren Stellen darauf hin. Der grösste Flop war die Beschaffung des Führungssystems für die Bodentruppen. Das FIS Heer funktioniert bis heute nur eingeschränkt.

Der grosse Modernisierungsschritt bringe nun aber Vorteile für die Sicherheit, sagt Vuitel: «Dass wir neue Rechenzentren mit einer einheitlichen Plattform aufbauen, ermöglicht uns, zeitgemässe Technologie mit den entsprechenden Schutzmechanismen einzusetzen.»

Gegenangriffe zur Verteidigung

Die Armee soll künftig auch besser imstande sein, selber Angriffe durchzuführen. Diesen Ausbau brauche es, zeigt sich Vuitel überzeugt: «Um sich effektiv verteidigen zu können, muss man auch in der Lage sein, falls nötig offensiv vorzugehen.» Die rechtlichen Grundlagen dafür seien vorhanden.

Der Schwerpunkt liegt beim Ausbau der elektromagnetischen Fähigkeiten, also zum Beispiel der Manipulation von Funk- oder Radarsignalen. Die Armee soll künftig bis auf die taktische Ebene der Truppen im Feld hinunter imstande sein, eigenständige Operationen durchzuführen. Im Idealfall sind die Kampfverbände zum Beispiel in der Lage, eigenständig den gegnerischen Funk aufzuklären, um die Standorte und Bewegungen des Gegners zu kennen. Oder sie verfügen auf ihren Fahrzeugen über Sender, um feindliches Radar oder die Steuerung einer gegnerischen Drohne zu stören.

Weniger hohe Priorität haben die Fähigkeiten für offensive Cyberaktionen, also die eigentlichen Cyberangriffe. Es sollen zwar gleichzeitig mehrere anspruchsvolle Angriffe gegen militärische Ziele möglich sein: mit Planung, Entwicklung der Software-Tools und der Durchführung. Aber auf der taktischen Ebene der Truppe sind keine Einheiten dafür vorgesehen. Dafür dauern Cyberangriffe zu lange und wären zu aufwendig. Hier besteht im Bericht der grösste Unterschied zur Maximalvariante, der für die Truppen umfassende Mittel für eigenständige Cyberangriffe vorgesehen hat.

Keine Erwähnung im Bericht findet der Informationskrieg. Wie das Beispiel der Ukraine zeigt, kann es im Kriegsfall für ein Land aber entscheidend sein, die öffentliche Wahrnehmung zu beeinflussen. Weil die Grenze zu Propaganda und Desinformation aber vage ist, sind solche Aktionen in einem freiheitlichen Staat heikel. Ganz unvorbereitet ist die Schweizer Armee allerdings nicht. Dem Vernehmen nach existieren im Kommando Operationen durchaus Überlegungen dazu, etwa zur Frage, wie unwahre Aussagen erkannt und gekontert werden können.

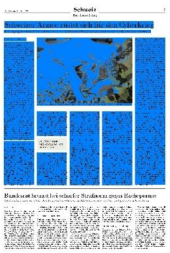
Nützlich für andere Behörden

Datum: 14.04.2022

Neue Zürcher Zeitung

Neue Zürcher Zeitung
8021 Zürich
044/ 258 11 11
https://www.nzz.ch/

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 87'908
Erscheinungsweise: 6x wöchentlich



Seite: 7
Fläche: 88'804 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 83998659
Ausschnitt Seite: 3/3

Die Politik bringt die Armee immer wieder als Mittel ins Spiel, wenn es um die Abwehr von Cyberangriffen geht. Solche Attacken können weitreichende Folgen haben, auch wenn Kriminelle dahinterstecken. Das war vor einem Jahr in den USA der Fall, als nach einem Ransomware-Angriff auf die Colonial-Pipeline an der Ostküste die Treibstoffversorgung für mehrere Tage ins Stocken kam.

Der Bericht ist in diesem Punkt klar: Damit die Armee subsidiär Hilfe leistet, müssen die Mittel der zivilen Behörden sowie kommerzieller Dienstleister ausgeschöpft sein. Selbst für diesen Fall nennt der Bericht eher eine Unterstützung im Hintergrund: etwa bei der Wiederherstellung infizierter Systeme oder bei der technischen Analyse des Vorfalls. Die Möglichkeit, dass Soldaten aktiv gegen Cyberkriminelle vorgehen, lässt der Bericht wohl bewusst weg.

Die Armee ist natürlich dennoch ein wichtiger Partner der zivilen Behörden, auch ausserhalb des Kriegsfalls. Bereits in der normalen Lage kann sie mit dem Lagebild rund um die Uhr einen wichtigen Beitrag zum Schutz vor Cyberangriffen leisten. Auch die sichere Infrastruktur für Kommunikation und Datenverarbeitung ist eine Fähigkeit, die für Behörden und kritische Infrastrukturen im Land auch in Friedenszeiten von grossem Nutzen sein kann.