Cybercrime und Cyberwar : vom Aufbau einer schlagkräftigen Cyber-Truppe

Cybercrime und Cyberwar – vom Aufbau einer schlagkräftigen Cyber-Truppe

Das Schlagwort Cyber ist zurzeit in aller Munde. Ist das eine Gefahr für den Einzelnen? Die Armee? Unser Staatswesen? Vereinfacht kann in Cybercrime und Cyberwar unterschieden werden: Kriminelle Tätigkeiten bei denen Private Opfer sind und in Aktionen, welche dem Staat schaden.

Ariel Wyler

Ein klassisches Beispiel für Cybercrime ist der Diebstahl von Kreditkartendaten, für Cyberwar steht der Angriff auf Speicher der RUAG, bei welcher nicht öffentliche Daten kopiert wurden.

Hybride Kriegführung auch im Cyber-Bereich

Lange Zeit herrschte die Meinung vor, bei Krieg handle es sich um eine bewaffnete Auseinandersetzung zwischen Armeen von verfeindeten Staaten. Die Erfahrungen zeigen jedoch, dass es sich bei Krieg um ein Ereignis handelt, das weiter gefasst werden muss: Wie bereits von Clausewitz definiert, als die Weiterführung der Politik mit anderen Mitteln. Somit erhält auch der Bund nach Art. 2 der BV mit dem Ziel, die Freiheit und die Rechte des Volkes zu schützen und die Unabhängigkeit und die Sicherheit des Landes zu wahren und die Armee im Speziellen nach Art. 58 der BV mit der Aufgabe zur Kriegsverhinderung und zur Landesverteidigung ein weiteres Aufgabenspektrum.

In den letzten Jahren hat sich die Einsicht durchgesetzt, dass sich auch im Cyber-Raum die Grenzen zwischen organisierter Kriminalität und staatlicher Konfliktführung verwischen, der hybride Krieg also schon heute im Cyber-Raum stattfindet. Dabei gibt es zum Beispiel verschieden Mischformen:

- Ein fremder Staat attackiert Private, spioniert zum Beispiel Bankkundendaten aus, um einen Staat an den Pranger zu stellen, bzw. den Finanzplatz und so die Wirtschaft eines Landes zu schwächen;
- Private attackieren staatliche Netzwerke oder Institutionen, um von ihnen Geld zu erpressen;
- Private Akteure werden von staatlichen Organen beauftragt, die öffentliche Meinung auf sozialen Netzwerken zu beeinflussen oder Computer von staatstragenden politischen Parteien zu attackieren.

Gefährdung im Cyber-Raum: Der Bund ist zuständig

Die vom Bundesrat verabschiedete Botschaft zur Revision des Fernmeldegesetzes verstärkt die Pflicht der Anbieter und Betreiber von Netzwerken zum Schutz vor Cybercrime. Dies genügt jedoch angesichts möglicher katastrophaler Folgen kaum. Als Analogie: Auch wenn es Vorschriften zum Brandschutz und Betriebsfeuerwehren gibt, entbindet dies den Staat dennoch nicht vom Aufstellen von Feuerwehren und Katastrophenschutzeinheiten. Genauso braucht es eine staatliche Kompetenz im Cyber-Bereich.

«In den letzten Jahren hat sich die Einsicht durchgesetzt, dass sich auch im Cyberraum die Grenzen zwischen organisierter Kriminalität und staatlicher Konfliktführung verwischen.»

Auch wenn die innere Sicherheit im Allgemeinen Aufgabe der Kantone ist, so gibt es doch Bereiche, in denen der Bund grundsätzlich in der ganzen Schweiz zuständig ist und die Armee immer eingesetzt wird, nämlich im Luftraum. Dieser wird vom BAZL verwaltet, für die Sicherheit im Luftraum ist auch in Friedenszeiten die Luftwaffe verantwortlich.

Gerade weil die Übergänge von Cybercrime zu Cyberwar fliessend sind und der Cyber-Krieg, wenn auch hybrid und nicht als erklärter Krieg, bereits heute stattfindet, ist die Armee auch heute schon gefordert.

Armee(ausbildungs)organisation nicht vorbereitet

Die Schweizer Armee verfügt nur über kleine Mittel im Bereich des subsidiären Cyber-Schutzes und Cyberwars. Die gegenwärtige Ausbildungsorganisation der Armee ist nicht auf die Cyber-Kriegführung ausgerichtet. Zwar gilt es, die Ziele der WEA umzusetzen, gleichzeitig ist es aber nötig, sich neuen Herausforderungen zu stellen. Der politische Konsens für allfällige Ressourcenallokationen zur Verstärkung der Cyber-Abwehr ist vorhanden. Mit der ETH verfügt die Eidgenossenschaft auch über einen weltweit anerkannten Ausbildungsstandort im Bereich der Informatik.

Eine der grössten Herausforderungen ist es, für die Cyber-Kriegführung die genügende Anzahl motivierter und qualifizierter Personen zu finden, welche auch noch eine genug lange Dienstzeit vor sich haben. Für einen effektiven Einsatz im Bereich Cyber sind vertiefte Kenntnisse der Informatik nötig.

Herkömmliche Modelle versagen

Reines Milizmodell

Die normale «Laufbahn» mit einer Grundausbildung in der RS und dem WK-Modell, aber auch das Durchdienermodell sind wenig geeignet, da die Kenntnisse in Informatik fehlen und die Dienstzeit zu kurz ist. Bei einer späteren Umteilung von AdA anderer Truppen, einem abgeschlossenen Bachelor oder Master, verbleiben im Allgemeinen nur noch wenige Diensttage.

In Frankfurt hat die Bahn Tafel und Kreide rausgeholt. Bild: Deutsche Bahn

Profis vom Markt

Bei der Gewinnung von ausgebildeten Kandidaten als Profis steht der Staat in Konkurrenz zur High-Tech-Branche, welche einerseits gute Arbeitsbedingungen und andererseits interessante Tätigkeitsfelder anbietet, mit welchen der Staat insbesondere lohnmässig nicht mithalten kann.

Wie machen es andere

Israel hat mit der Schweiz einige Ähnlichkeiten: Hochtechnologisiert, vergleichbare Bevölkerungsgrösse, offene Märkte und vor allem ein Milizmodell, das sich an das der Schweiz anlehnt. Israel ist bekannt für seine zivile High-Tech-Branche, aber auch für seine Cyber-Einheiten.

Während der Inhalt der cyber-bezogenen Ausbildung grosser Geheimhaltung unterliegt, ist doch einiges über diverse Ausbildungslehrgänge bekannt. Diese sind durch folgende Eckpunkte gekennzeichnet: Junge Vollprofis, (ergänzt durch semiprofessionelle Miliz).

Vollprofis:

1. Früherkennung und Vorauswahl der Kandidaten: Diese beginnt schon auf der Gymnasialstufe;
2. Grundausbildung durch besonderes Studium an ziviler Eliteuniversität zum Beispiel Doppel BA in drei Jahren für das härteste Programm: Havatzelet;
3. Fachausbildung im Rahmen der Einheit;
4. Verpflichtung als Berufsoffizier für einen Zeitraum von 4–6 Jahren.

Die Absolventen dieser Laufbahnen haben beste Karriereaussichten, da sie über einen Erfahrungshintergrund verfügen, den ein ziviler Mitbewerber nicht haben kann. Dementsprechend gibt es genügend Anwärter und die Konkurrenz zum Privatsektor wird umgangen, indem nicht nur bessere Jobaussichten als wie nach einer Berufserfahrung bei einem High-Tech-Unternehmen angeboten werden, sondern der Markt bearbeitet wird, bevor die Konkurrenz überhaupt erwächst. Durch die guten Jobaussichten wird auch sichergestellt, dass nach einer gewissen Verweilzeit die Absolventen in den Privatsektor übertreten.

«Eine der grössten Herausforderungen ist es, für die Cyber-Kriegführung die genügende Anzahl motivierter und qualifizierter Personen zu finden, welche auch noch eine genug lange Dienstzeit vor sich haben.»

Umgemünzt auf Schweizer Verhältnisse

CYBER-SPHAIR

Analoge Ausbildung wie Militärberufspiloten.

1. Früherkennung: Besonders talentierte Gymnasiasten werden direkt zum Screening eingeladen. Daneben können sich andere Schüler zu den Eignungstests melden;
2. Aufnahme ins Grundprogramm: Vorgängige Verpflichtung als Cyber-Offizier, beschleunigtes/erweitertes BA-Programm an der ETH (Studiengebühren und Studentenlohn vom Bund übernommen, rückzahlbar im Falle, dass der Anwärter das Programm verlässt);
3. Interner Lehrgang im Bereich Cyberwar;
4. Dienst während mindestens fünf Jahren als Cyber-Berufsoffizier und Ausbildner im Cyberwar-Lehrgang.

Bei 30 Absolventen pro Jahr und einer Verweildauer von sechs Jahren ergibt sich, unter Berücksichtigung unvermeidlicher Abgänge, eine Cyber-Truppe von ca. 150 Aktiven. Dies entspricht ungefähr dem ausgewiesenen Bedarf. Der durchschnittliche Abgänger ist unter 30 Jahre alt und hat fünf Jahre Berufserfahrung in einem höchst sensiblen Bereich, was beste Jobaussichten eröffnet.

In Erfüllung der Motion Dittli könnte dieses Modell folgendermassen ergänzt werden: Milizspezialisten können ihre RS bis nach dem Abschluss des BA- oder HF-Abschlusses verschieben und sich für eine Milizoffizierlaufbahn verpflichten. Dabei werden sie jedoch nicht zu Zugführern ausgebildet, sondern durchlaufen eine spezielle Cyber-Schule und leisten anschliessende WK.

Gewiss könnte der Bund für ein solches anforderungsreiches Programm Kandidaten gewinnen, die heute aus verschiedenen Gründen als Zivi's den Militärdienst vermeiden.

Dadurch sollte es möglich sein, mit vertretbaren Kosten (ca. 40 Mio. CHF oder < 1% des Militärbudgets) die Besten und Fähigsten zu gewinnen und die Eidgenossenschaft mit einer hochqualifizierten und motivierten Cyberforce möglichst gut zu schützen. ■

Oberst
Ariel Wyler
Dr. sc. tech.
Ökonom
8002 Zürich