Resilienz im Cyber-Raum

Autor(en): **Thomann-Baur, Irène**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **184 (2018)**

Heft 6

PDF erstellt am: **03.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-772543

Resilienz im Cyber-Raum

Auf Störungen, Manipulationen und gezielte Angriffe via elektronische Netzwerke ist unsere Informationsgesellschaft anfällig. Die Bedrohung ist wenig fassbar, am Handlungsbedarf zweifelt niemand.

Irène Thomann-Baur*

Der Resilienz im Cyber-Raum widmete CHANCE SCHWEIZ – Arbeitskreis für Sicherheitsfragen einen Anlass in Zürich. Mit ihren Auslegeordnungen schufen die drei Referenten aus drei Departementen, Peter Fischer, seit 2007 Delegierter für die Informatiksteuerung des Bundes (EFD), Gérald Vernez, Delegierter des VBS für Cyber Defense, und René Bühler, Stv. Direktor Fedpol (EJPD), beste Voraussetzungen für eine lebhafte Podiumsdiskussion, an der sich auch die Nationalräte Bea Heim (SP/SO) und Marcel Dobler (FDP/SG) beteiligten.

Das Cyber-Dispositiv

Die Liste der Cyber-Vorfälle ist lang, Tendenz steigend. Die Cyber-Technologie dient der Alltagskriminalität, der Spionage gegen Wirtschaft und staatliche Institutionen, sie ist Mittel der Sabotage und des Terrorismus. Cyber ist Teil der hybriden Kriegführung, taugt für Desinformation und Propaganda. Die Einsatzfelder sind nicht neu, aber die Informationstechnologie erweitert den Handlungsspielraum, nutzt Lücken und Schwachstellen. Es passiert mehr, als bekannt gegeben wird, einiges bleibt gänzlich verborgen.

Die Nationale Cyber-Strategie 2018–2022 (NCS II), vom Bundesrat am 18.04. 2018 verabschiedet und entstanden unter Mitarbeit zahlreicher Bundesstellen, der Privatwirtschaft, des Sicherheitsverbundes Schweiz und einer breiten Konsultation unterzogen, will neben der Prävention die Durchhaltefähigkeit gegenüber langanhaltenden und sektorübergreifenden Vorfällen steigern und die Resilienz kritischer Infrastrukturen stärken. Der Schutz der Schweiz vor Cyber-Risiken gilt als gemeinsame Aufgabe von Gesellschaft, Wirtschaft (es gibt 580 000 Firmen in der Schweiz) und Staat und bedarf der internationalen Zusammenarbeit. Ergänzend zur bisherigen Strategie soll die Melde- und Analysestelle Informationssicherung MELANI Produkte für KMU und die Bevölkerung entwickeln. Zudem soll es neu Minimalstandards für IT-Sicherheit geben, und zwar auch branchenbezogen. Geprüft wird eine Meldepflicht für Cyber-Vorfälle. Bis Ende 2018 organisiert der Bund seine Strukturen und die Zusammenarbeit in den drei Bereichen zivile Cyber-Sicherheit, Cyber Defense und Strafverfolgung von Cyber-Kriminalität. Mit der Schaffung eines Kompetenzzentrums für Cyber-Sicherheit erfüllt der Bundesrat die Motion von Ständerat Joachim Eder.

Resilienz
Die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, Störungen zu widerstehen und die Funktionsfähigkeit möglichst zu erhalten, respektive rasch wieder zu erlangen.
Definition im Glossar der NCS II

Cyberwar

Cyber ist eine Waffe. Unsichtbar, oft in unbekannter Hand – man ist mit Automaten konfrontiert – profitiert sie von der Verletzlichkeit und dem Leichtsinn der Gesellschaft. Bei der Cyber-Abwehr, einem Teil des Gesamtdispositivs, kann der Nachrichtendienst des Bundes (NDB) die Betreiber unterstützen und, sind die Voraussetzungen erfüllt, treten subsidiär Teile der Armee an. In der Verantwortung des VBS liegen der Schutz seines Informations- und Sicherheitsmanagement-Systems und die Abwehr der Angriffe auf die eigenen Informations- und Kommunikationssysteme und Infrastrukturen. Zur Cyber Defense gehören der Ausbau der Informationsbeschaffung und Gegenmassnahmen im Cyber-Raum.

Mit dem angestrebten Cyber-Defense-Campus schafft das VBS keine neue Universität, vielmehr soll ein Netzwerk entstehen, an dem Industriepartner, Hochschulen, Nachrichtendienst, die Armee und weitere relevante Stellen beteiligt sind. Wissenstransfer, Ausbildung, Führung, Forschung, Entwicklung und Übungen (wie «Locked Shields» der NATO, an der 22 Länder und auch ein Schweizer Team teilnahmen) sind entscheidend. Es braucht Fachleute. Solche will auch die Armee ausbilden. Wer eine abgeschlossene IT-Berufslehre vorweist und bereit ist, den Unteroffiziersgrad zu erwerben, erhält nach bestandener Prüfung ein eidgenössisches Fähigkeitszeugnis als «Cyber Security Spezialist».

Cyber-Kriminalität

Für Kriminelle ist die digitale Welt genauso attraktiv wie für uns. Sie wirken online von zuhause aus. Das ist die grosse Herausforderung der Strafverfolgung. Deshalb ist die Kriminalprävention so wichtig. Zuständig im Bereich Cyber-Kriminalität sind Polizei, Bundeskriminalpolizei, die Bundesanwaltschaft, die Staatsanwaltschaften, Europol und Interpol. Bekannte Fälle zeigen, wie leicht Cybercrime Landesgrenzen überwindet. Erst internationale Zusammenarbeit erlaubt den raschen Zugriff auf ausländische Server. Verdeckte Fahndung ist nötig, die Sichtung der Daten extrem aufwändig und damit ressourcenintensiv. Seit dem 1. Mai 2018 arbeiten die Kantone, der Bund, MELANI und der NDB im Verbund, womit das vorhandene Wissen besser vernetzt und ausgeschöpft wird.

Der Strategie müssen Taten folgen

Mit einer Flut von Vorstössen hat das Parlament den Bundesrat zum Handeln aufgefordert. Schnittstellen, Verantwortlichkeiten und Strukturen sind erkannt, jetzt geht's rasch ans Umsetzen. Darin waren sich alle Podiumsteilnehmer einig. Krisenmanagement ist gefragt, das Ziel: Sicherheit. Hinterher hinkt die Schweiz bei der digitalen Demokratie. Skeptische Aufmerksamkeit gebührt den überall eingesetzten Chips; wer überprüft deren Inhalt? Und wer ist im «Kriegsfall» für welche Infrastruktur zuständig? Umgesetzt wird dezentral mit einer klaren Aufgabenzuteilung. ■

* Journalistin, Hptm, zuletzt im Info Rgt 1, ehemals Generalsekretärin der SOG, Winterthur.