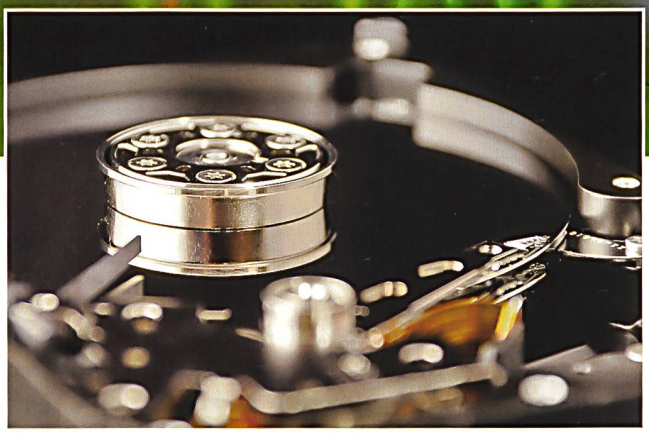
Wir verlieren den Cyber-Krieg

Wir verlieren den Cyber-Krieg

Wir verlieren den Cyber-Krieg. Dies wurde mir spätestens dann bewusst, als ein höherer Stabsoffizier mir gegenüber behauptet hat: «Ein Krieg wird nicht mit Cyber entschieden.» Eine fatale Fehleinschätzung, die auf lange Zeit hinaus direkte Konsequenzen haben wird.



Speicher.

Marc Ruef

Es ist Pflicht unserer Gesellschaft, ihre Werte zu verteidigen. Um diesem Ziel gerecht werden zu können, muss militärische Souveränität gewährleistet sein. Und diese lässt sich im Jahr 2018 effektiv nur aufrecht erhalten, indem das Thema «Cyberwar» ernst genommen wird. Nicht umsonst hat die NATO vor zwei Jahren die klassischen Räume Luft, Land und Wasser um «Cyber» erweitert. Man weiss, wie wichtig diese Domäne in einer technokratischen Zeit wie der unseren ist.

Führt man sich den «Lagebericht 2017 des Nachrichtendienstes des Bundes» zu Gemüte, findet man auf den 88 Seiten insgesamt 76 Mal das Wort «Cyber» (das Jahr zuvor nur 19 Mal). Schliesslich wird das Thema gar explizit als «Schwerpunkt» geführt (ab Seite 25).

Papier ist geduldig. Und tatsächlich mutet der Schwerpunkt des Berichts an, als sei er aus der Zukunft. Aus einer Zukunft, in der sich die Schweiz systematisch und aktiv mit dem Thema Cyberwar auseinandersetzt. Und man müsse halt nun geduldig sein, bis die Realität den Schwerpunkt des Berichts abzubilden beginnt. Wann das passieren wird? Vielleicht im Jahr 2030. Doch dann ist es etwa 30 Jahre zu spät. Denn das Reglement «Taktische Führung XXI» erwähnt zwar in Kap. 4.3 den elektromagnetischen Raum und die Informationssphäre. «Cyber» wird aber nicht als Effektor wahrgenommen.

Heute ist nicht mehr der Staat derjenige, der mit seinen breit abgestützten Mitteln die technologische Kultur diktieren kann. Vielmehr sind es die multinationalen Unternehmen, die mittels revolutionärer Technologien und disruptiver Ideen die dynamischen Märkte formen. Der Staat wirkt dem gegenüber längst träge und unflexibel. Hört man sich um, wird schnell klar: Ungestüm werden Grossprojekte angerissen und halbherzig verfolgt. Und wenn sie mal ein Ende finden, dann in einer Qualität, die nicht zeitgemäss ist und es auch niemals gewesen wäre. Hauptsache der teure Partner, der vorgängig mit seinem grossen Namen und mit bunten Präsentationsfolien punkten konnte, hat sich eine goldene Nase verdient. Auf Kosten der Steuerzahler. Auf Kosten der Souveränität der Schweiz.

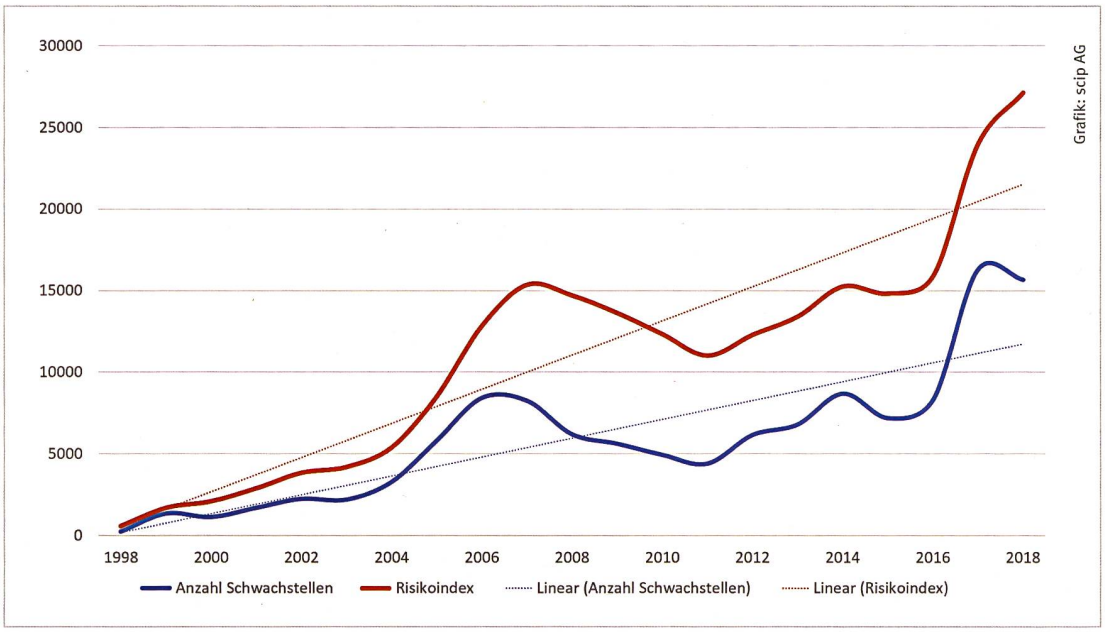
Befehl von Oben

Wird das Thema «Cyber» nicht durch die Führung vorgegeben, vorgelebt und unterstützt, kann es niemals vollumfänglich und nachhaltig etabliert werden. Dies gilt in der Privatwirtschaft als auch im Rahmen der politischen Führung oder der Armee. Der Bundesrat redet zwar gern davon, wie wichtig «Cyber» doch sei – dann aber im selben Atemzug zugeben, dass man seinen eigenen Laptop nicht schützen würde, mutet an wie blanker Hohn. Eine solche flappsige Bemerkung wirft die Diskussion um Jahre zurück. Geopolitische Partner und Gegner werden sich darüber amüsieren, das ist sicher.

Die Cybersecurity-Industrie sieht sich bisweilen gerechtfertigter Kritik ausgesetzt: Manche Leute machen Geld ausschliesslich mit der Angst der anderen. Aber scheinbar muss auch hier zuerst etwas passieren, bis man die Zeichen der Zeit erkennt. Vielleicht muss zuerst im grossen Stil das Parlament durch fremde Akteure ausgehorcht werden, so wie es im Netzwerk der Bundesregierung Deutschland vor Wochen passiert ist. Oder es muss mal zwei Tage der Trambetrieb in Zürich oder Bern aufgrund einer gezielten Störung

durch Erpresser ausfallen. Erst dann wird man merken, dass «Cyber» wichtig ist, dass man professionell damit umgehen muss. Und zwar hier. Und zwar jetzt.

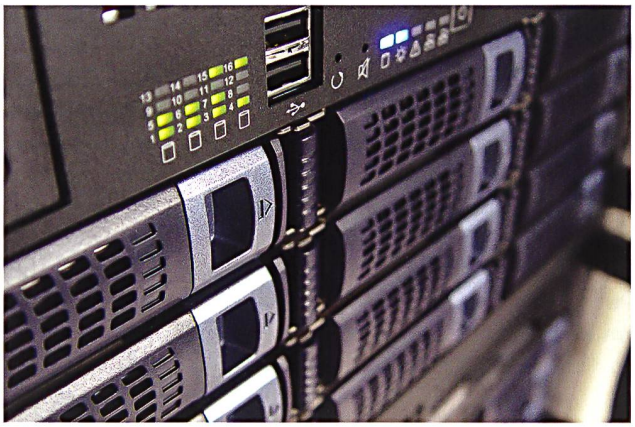
Sowohl Armee als auch Nachrichtendienst haben die Aufgabe, sich auf solche Krisen vorzubereiten. Die einen wollen nichts davon wissen, da sie während Friedenszeiten nicht zuständig sind bzw. nur für rein militärische Angelegenheiten. Und die anderen sind durch eine politisch konservative Führung gehemmt. Da hilft auch eine Gesetzesänderung nur wenig, um eine zeitgemässe Entwicklung voranzutreiben.



Zunahme der Schwachstellen und des Risikoindexes in den letzten 20 Jahren.

Was es braucht

Es braucht eine ganzheitliche, langfristige Strategie, wie sich die Schweiz als Nation mit den Möglichkeiten, Aktivitäten und Gefahren im Cyber-Raum auseinandersetzen will. Diese muss zwingend in einem ersten Schritt Probleme und Konflikte unterhalb der Kriegsschwelle abdecken können. Sowohl Polizei als auch Nachrichtendienste müssen entsprechend befähigt werden. Eine solide Gesetzeslage konnte mit dem neuen Nachrichtendienstgesetz mittlerweile geschaffen werden, um mit der Dynamik zeitgenössischer Kriminalität, Cybercrime und Terrorismus umgehen zu können.



Server. Bilder: CCO

Die Armee muss sich aber ebenfalls vorgängig mit dem Thema auseinandersetzen. Und zwar während dem Aufbau und Betrieb der entsprechenden Systeme. Die Beschaffung von Führungs-, Kommunikations-, Sensor- und Effektorensystemen muss stets auch aus dem Blickwinkel «Cyber» angegangen werden. Autonomie und Zuverlässigkeit sind massgebliche Eigenschaften, die es für sich in Anspruch zu nehmen gilt. Die Evaluation von Material darf nicht auf die funktionalen Spezifikationen reduziert und über rein finanzielle Aspekte gesteuert werden. Eine umfangreiche konzeptionelle und technische Prüfung ist zur uneingeschränkten Schaffung von Transparenz erforderlich, um im Krisenfall «bösen Überraschungen» vorbeugen zu können. Ansonsten kann eine Operation nämlich entschieden sein, bevor die erste Taste gedrückt wurde.

Sämtliche Stellen müssen mit den entsprechenden finanziellen Mitteln unterstützt werden. Dies kann und muss kostenorientiert getan werden, denn nicht immer ist die teuerste Lösung auch die Beste. Punktuelle Massnahmen oder kurzsichtige Aktivitäten sind aber nicht nachhaltig und deshalb eine Verschwendung, die es dringendst zu vermeiden gilt. Sämtliche Aktivitäten müssen sich immer in die übergeordnete Gesamtstrategie eingliedern. In der Schweiz finden sich viele renommierte Firmen, die entsprechende Fähigkeiten mitbringen und im Sinn der Autonomie internationalen Verflechtungen vorzuziehen sind.

Besonders schwierig gestaltet sich das Anwerben und Schulen von Fachspezialisten, wie privatwirtschaftliche Kreise bestätigen können. Es müssen Kontakte und eine aktive Zusammenarbeit mit Partnern aufgebaut werden, um das Wissen und die Weitsicht verbessern zu können. Dazu gehören Universitäten, Hochschulen, Privatwirtschaft und Partnerdienste gleichermassen. Ein nationales Kompetenzzentrum sollte sich mit neuen und zukünftigen Entwicklungen auseinandersetzen, um einen Schritt voraus zu sein.

Am wichtigsten aber ist, dass endlich der Wille aufgebracht werden muss, sich mit einem hochgradig komplexen und dynamischen Thema auseinanderzusetzen, dem man nicht mit einer konventionellen Herangehensweise Herr werden kann. Hier muss ein Umdenken stattfinden. Es bleibt zu hoffen, dass nicht erst bis 2030 gewartet werden muss, bis man sich auf dieser Ebene professionalisieren konnte. Weil je nach politischer Lage ist es dann zu spät. Dann haben wir verloren. ■

Marc Ruef
Head of Research
scip AG, Zürich
5436 Würenlos