Sicherheitspolitische Information

Juli 2018

Cyber Security Schweiz:

Risiken, Bedrohungen und Vorbereitungen – eine Auslegeordnung

Herausgeber: Verein Sicherheitspolitik und Wehrwissenschaft (VSWW)
Postfach 2407, 8021 Zürich 1
(Spenden bitte auf: Postkonto 80-500-4, Credit Suisse Zürich, Konto-Nr. 468809-0)
Präsident: Dr. Günter Heuberger, Vizepräsidenten: Jakob Baumann und Dr. Christoph Grossmann
www.vsww.ch
Autor: Daniel Heller, Dr. phil., Oberst i Gst, Armeestab, Geschäftsführer VSWW
Interview mit: Nicola Staub, RA LL.M., Staatsanwalt, Ambassador der Global Cyber Alliance
Redaktion: Luca Belci, BA

Inhalt

1 Cyberwar **4**

1.1 Bedrohungsanalyse 4

1.2 Vorkehrungen der Schweizer Sicherheitspolitik 5

1.3 Erkenntnisse und Beurteilung 7

2 Cybercrime **8**

2.1 Bedrohungsanalyse 8

2.2 Vorkehrungen von Staat und Wirtschaft 8

2.3 Fragen an Nicola Staub, Staatsanwalt des Kantons Schwyz und Experte für Cybercrime 9

2.4 Erkenntnisse und Beurteilung 11

3 Benchmarking **12**

3.1 Beispiele privater Initiativen 12

Die Global Cyber Alliance 12

WEF eröffnet in Genf ein Zentrum für globale Cyber Security 12

Technologiekonzerne unterzeichnen «Digital Geneva Convention» für mehr Sicherheit im Cyberspace 12

3.2 Israels Cyber-Security-Ansatz als Erfolgsmodell 13

Erfolgreiches Cyber-Security-Ökosystem 13

Sechs Erfolgsfaktoren 13

4 Fazit und Folgerungen **14**

Glossar **15**

Vorwort

Seit Längerem erachten Experten und Sicherheitspolitiker Computerwürmer als wirksamer gegenüber Bomben. Im Oktober 2012, vor rund sechs Jahren, fragten wir in einer Studie zu Cyber Defence: «Wie gut ist die Schweiz gerüstet?» Schliesslich hielt der damalige deutsche Innenminister Thomas de Maizière (CSU) im Frühjahr 2017 fest, dass er einen Computerangriff auf die deutsche Stromversorgung für wahrscheinlich erachte. Er bezeichnete die Folgen eines «langanhaltenden» Stromausfalls als katastrophal für Wirtschaft, Gesellschaft und Staat. Verteidigungsministerin Ursula von der Leyen (CDU) reagierte auf die neuen Herausforderungen, indem sie neben die klassischen Teilstreitkräfte Heer, Luftwaffe und Marine eine Abteilung Cyber- und Informationsraum aufstellte, deren Hauptaufgabe der Schutz der Truppe vor Angriffen von aussen ist. Die Cyberarmee weist einen Sollbestand von 13'500 Männern und Frauen auf und wird von einem Dreisterne-General geführt, der beinahe ebenso viele Soldatinnen und Soldaten befehligt, wie die komplette Marine zählt.

Die Gefahr durch Cyberattacken betrifft jedoch nicht nur die Landesverteidigung, sondern auch die Zivilbevölkerung: Gemäss den Angaben des Bundeskriminalamts hat die Polizei 2016 in Deutschland rund 83'000 Fälle von Cybercrime erfasst. Dabei sei ein Schaden von über 51 Millionen Euro entstanden. Um einen weiteren Anstieg zu verhindern, müssen die Ermittlungsbehörden der hochvernetzten Cyberkriminalität ebenfalls ein leistungsfähiges Netzwerk gegenüberstellen. Beratung, Prävention, Netzwerkarbeit und Kooperationen sind heute wichtige Bestandteile erfolgreicher Polizeiarbeit. Stellvertretend für eine verbesserte Zusammenarbeit steht in Deutschland etwa die neue Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Zitis) in München, die alle Sicherheitsbehörden berät und mit Werkzeugen unterstützt.

Was für Deutschland recht ist, sollte für die Schweiz billig sein. Der VSWW-Geschäftsführer Daniel Heller gibt in der aktuellen Ausgabe einen Überblick, was Bedrohungen und Vorkehrungen der Schweiz im Bereich Cyber Defence anbelangt, und der auf Cyber- und Wirtschaftskriminalität spezialisierte Staatsanwalt Nicola Staub beantwortet Fragen zur Wirksamkeit der Vorkehrungen in diesem Bereich.

Dr. Günter Heuberger, Präsident

1 Cyberwar

1.1 Bedrohungsanalyse

Die zunehmende Vernetzung der modernen Welt über das Internet und die neuen Formen der Informationsgesellschaft via Social Media führen zu laufend neuen Formen der Angriffsmöglichkeit, seien sie rein technologisch oder informationstechnisch. Deshalb ist die Resilienz, also die Widerstandsfähigkeit, gegenüber den Bedrohungen aus dem Cyber- und Informationsraum entscheidend für die Zukunft moderner Gesellschaften. Denn potenzielle Gegner nutzen schon heute das Cyberspace als Kommunikationsmittel und Angriffsfläche. In der sogenannten hybriden Kriegsführung haben IT-Attacken reale Folgen: Angriffe auf kritische Infrastruktur wie Stromversorgung oder Kommunikationsnetze können die Handlungsfähigkeit eines Staates empfindlich stören, die Wirtschaft beeinträchtigen oder die Gesellschaft schlimmstenfalls komplett lahmlegen.

Neben dem Angriff auf die vernetzten Technologien zielen Angriffe auch darauf ab, die neue Vernetzung für gezielte Desinformation zu nutzen. Bisher ist besonders Russland durch solche Aktivitäten aufgefallen. Der Vorsitzende des Militärausschusses der Nato, Petr Pavel, beurteilt die Intentionen Moskaus so, dass die Kremlführung aus Unzufriedenheit mit der jetzigen Weltlage eine Konfrontationspolitik betreibe und eine Desinformationskampagne gegen die Staaten der Nato führe. Der ehemalige tschechische Generalstabschef sieht für einen sogenannten hybriden Krieg seitens Russlands zahlreiche Beweise:

«Die russische Sicherheitsstrategie und die Militärdoktrin des Landes betrachten den Informationskrieg als Teil eines fortwährenden Konflikts. Russland nimmt die ganze Geschichte als einen solchen Konflikt wahr, nur dass die Intensität und die Mittel sich im Laufe der Zeit gewandelt haben. Russland sagt ganz offen, dass die Nato und der Westen seine Gegner seien, und führt eine Informationskampagne gegen das andere Lager.»[1]

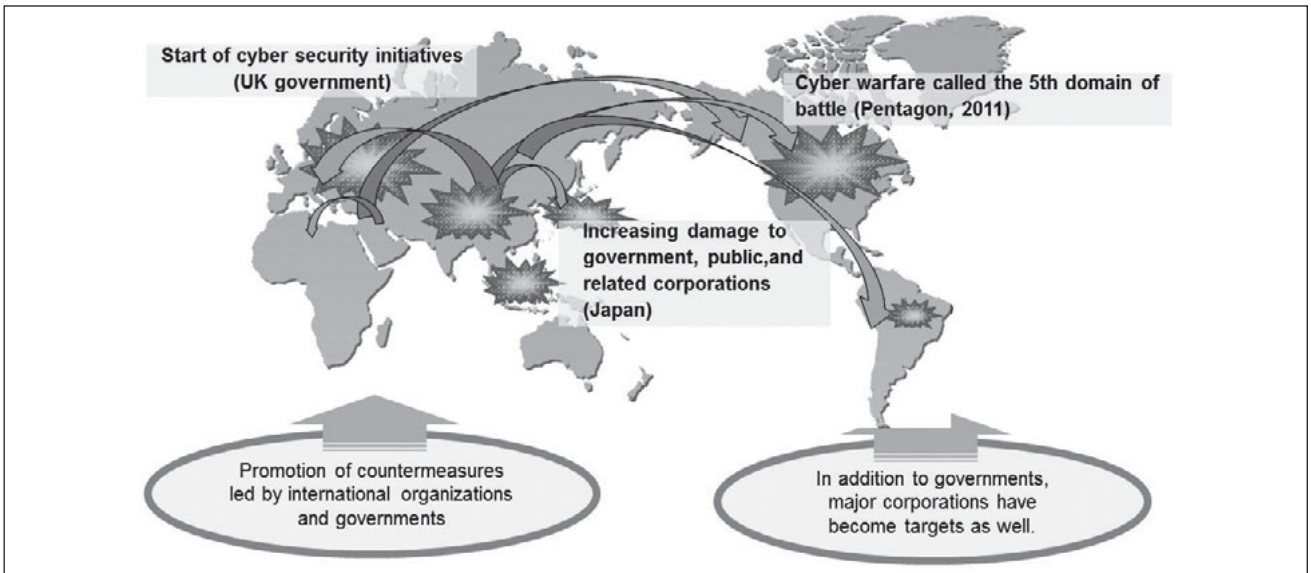
1 *Interview mit dem Tschechischem Rundfunk, 04.05.2018.*

Cyberwar – die fünfte Dimension des Krieges

Cyberangriffe können neben dem World Wide Web[2] auch andere Netze betreffen, darunter das Darknet (die «dunkle Seite des Internet»). Attacken auf Informationsinfrastrukturen sind in den letzten Jahren immer zahlreicher und komplexer geworden; gleichzeitig ist eine zunehmende Professionalisierung aufseiten der Kriminellen zu beobachten.

Der Virus «Petya» hatte 2017 Rechner in der Ukraine befallen, ehe er sich auf Geschäftspartner ukrainischer Firmen im europäischen, amerikanischen und asiatischen Ausland ausweitete. Der Virus verursachte in der Folge weltweite Schäden in Milliardenhöhe. Zu den Opfern gehörten unter anderem der Pharmariese Merck, die dänische Reederei Maersk und das Logistikunternehmen TNT. Die USA, Grossbritannien und Australien werfen dem russischen Militär vor, für die Cyberattacke «Petya» verantwortlich zu sein. «Petya» sei Teil der ständigen Versuche des Kremls, die Ukraine zu destabilisieren, so die Kritik aus dem Weissen Haus.

2 *Das **Internet** beschreibt einen weltweiten Verbund von Netzwerken und Servern, die über normierte Zugriffsprotokolle die Nutzung von zahlreichen Diensten wie dem World Wide Web, der E-Mail, Internettelefonie usw. ermöglicht. Das **World Wide Web** ist folglich ein über das Internet abrufbares System, bestehend aus Textdokumenten (sogenannten Webseiten, oft mit Bildern bestückt), die über Hyperlinks (z. B. www.vsww.ch) erreichbar sind.*



Viele Staaten und internationale Organisationen bemühen sich um die Abwehr von Cyberangriffen.

Auch die Schweiz war bereits Opfer von Attacken auf sicherheitsrelevante Infrastruktur: Beim Hackerangriff auf den Rüstungskonzern Ruag 2015/16 waren bis zur Entdeckung der Schadsoftware Anfang 2016 mehr als 20 Gigabyte Datenvolumen entwendet worden. Dies ging aus einem technischen Bericht im Auftrag des Bundesrats hervor. Die Publikationen in den Medien haben in der Folge das öffentliche Bewusstsein für Cyberrisiken gestärkt.

Es ist folglich denkbar, dass uns eines Tages ein Feind angreift und unsere kritischen Infrastrukturen lahmlegt, die Spitäler, die AKW, den Verkehr. Dass er unserer Bevölkerung schweren Schaden zufügt. Die zivilen Behörden sind darauf angewiesen, dass ihre Telekommunikations- und Alarmierungssysteme in allen Lagen funktionieren und dass die Bevölkerung über gesicherte Kanäle gewarnt und alarmiert werden kann sowie mit verlässlichen Informationen versorgt wird.

Aber auch die Streitkräfte im engeren Sinne sind bedroht: Mit stetig wachsenden Datenmengen, einer zunehmenden Vernetzung und dem «Internet der Dinge» steigt auch bei den Armeen das Risiko für Cyberangriffe. Schon jetzt fliegt ein Kampfjet der neusten Generation nur, weil an Bord gegen 100 Computer über 100 Kilometer Kabel vernetzt sind. Würde hier unentdeckt ein Virus eingeschleust, könnte dieser zu verheerenden Folgen führen – lahmgelegte Steuer- und Abwehrfunktionen oder gar ferngelenkte Bombardierungen der eigenen Truppen eingeschlossen. Dazu ein Beispiel: Die Bundeswehr verzeichnete Anfang 2017 innerhalb von neun Wochen 284'000 Cyberattacken gegen die Rechner der Streitkräfte.

1.2 Vorkehrungen der Schweizer Sicherheitspolitik

Als Grundlage für die Strategie und die Massnahmen des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) zum Schutz vor Cyberangriffen dient die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS). Sie hat zum Ziel, in Zusammenarbeit zwischen Behörden, Wirtschaft, Hochschulen und den Betreibern kritischer Infrastrukturen die Cyberrisiken zu minimieren. Als wesentlich für die Reduktion von Cyberrisiken bezeichnet diese Strategie:

- die Eigenverantwortung (der Staat soll nur eingreifen, wenn öffentliche Interessen auf dem Spiel stehen oder er im Sinne der Subsidiarität handelt),
- die Zusammenarbeit zwischen Wirtschaft, Hochschulen und Behörden,
- die Kooperation mit dem Ausland.

Die erste NCS 2012–2017 umfasste 16 Massnahmen. Das Urteil des VSWW lautete 2012: «Die vom Bundes-

rat vorgelegte Cyber-Defence-Strategie ist bezüglich Zielerreichung wie folgt zu beurteilen: Die Strukturen auf Stufe Bund zur Bewältigung von Cyberrisiken sind – wie in vielen anderen Fällen auch – bisher dezentral organisiert. Bereits heute werden viel zu geringe Mittel aufgewendet; allein schon aus diesem Grund ist die Ressourcensituation ungenügend für die Übernahme zusätzlicher Aufgaben. Die neu vorgesehenen Massnahmen und Strukturen beseitigen dieses Dilemma nicht wirklich. Es wird weiterhin über Departemente verzettelt gearbeitet: Was zur Sicherheit gehören sollte, wird guteidgenössisch statt im VBS oder in der Bundeskanzlei in irgendwelchen Departementen und Abteilungen verteilt angesiedelt nach dem Motto ‹Divide et impera›. Man kann auch für den virtuellen Raum nur hoffen, dass trotzdem nichts Ernstes passiert.»[3]

Im Herbst 2017 musste Bundesrat Guy Parmelin einräumen, dass der Bund den elektronischen Krieg unterschätzt hat. Zu diesem Zeitpunkt existierten im VBS ganze 50 Stellen für die Cyber Defence. Das Parlament beauftragte den Bundesrat im Winter 2017/18 in Zusammenhang mit der laufenden Überarbeitung der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken, ein Cyber-Security-Kompetenzzentrum auf Stufe Bund zu schaffen. Diese Organisationseinheit hat die Aufgabe, die zur Sicherstellung der Cyber Security notwendigen Kompetenzen zu verstärken und bundesweit zu koordinieren. Sie soll departementsübergreifend wirksam sein und im Bereich Cyber Security über Weisungsbefugnis gegenüber den Ämtern verfügen. Ausserdem soll das Kompetenzzentrum mit Vertretern der Wissenschaft (Hochschulen und Fachhochschulen), mit der IT-Industrie und mit den grösseren Infrastrukturbetreibern (insbesondere bei Energie und Verkehr) zusammenarbeiten. Der Ständerat überwies die Motion von Ständerat Joachim Eder (FDP, ZG) in der Herbstsession 2017, der Nationalrat folgte kurz darauf mit 177 zu 2 Stimmen. Analog verlangte das Parlament die Schaffung einer Cyber-Defence-Organisation innerhalb der Armee mit der Überweisung einer Motion Josef Dittli (FDP, UR).

Nach vielen Jahren, in denen Ausserdienststellungen von Einheiten und Verbänden gewohnter Alltag waren, geht es in den nächsten Jahren darum, neue Kapazitäten bereitzustellen. Das VBS strebt 100 zusätzliche Stellen bis 2020 an. Zudem soll die EKF Schule 64 in Jassbach, dem Ausbildungszentrum für den elektronischen Krieg, jedes Jahr 50 Spezialisten ausbilden. Das VBS hofft, dass sich viele von ihnen anschliessend für eine Anstellung entscheiden werden. Gleichzeitig vertieft das Departement die Kooperation mit den Hochschulen. Die Rekrutierung dürfte allerdings nicht einfach sein, suchen doch die Unternehmen, die Verwaltung und die Armee alle dieselben IT-Spezialisten. Aktuell bildet die ETH jährlich rund 250 IT-Spezialisten aus, 200 von ihnen gehen nach dem Studium direkt zu Google. Und der Internetriese möchte in der Schweiz wachsen, von aktuell 2500 auf 6000 Mitarbeiter. Das VBS steht also vor einer schwierigen Aufgabe.

Ab diesem Sommer will die Schweizer Armee Cybersoldaten ausbilden.

Am 18. April 2018 verabschiedete der Bundesrat die NCS für 2018–2022. Diese überarbeitete Strategie baut auf den Arbeiten der ersten NCS auf, weitet diese aus und ergänzt sie mit neuen Massnahmen. Auch die revidierte Strategie zum Schutz der Schweiz vor Cyberrisiken soll dezentral umgesetzt werden. Sie umfasst folgende Kernpunkte:

- **Melde- und Analysestelle:** Eine wichtige Rolle spielt die Melde- und Analysestelle Informationssicherung (MELANI), die vom Informatiksteuerorgan des Bundes (ISB) im Finanzdepartement und dem Nachrichtendienst des Bundes (NDB) im VBS gemeinsam betrieben wird. MELANI dient vor allem

3 *Heller/Heizmann: Cyber Defence: Wie gut ist die Schweiz gerüstet? VSWW, Oktober 2012.*

dazu, Cyberrisiken frühzeitig zu erkennen und die Betreiber kritischer Infrastrukturen (z. B. Energieversorger, Telekommunikationsunternehmen, Banken) zu unterstützen, solche Risiken vorzubeugen und zu bewältigen.

- **Armee:** Die Armee spielt in den Vorkehrungen zum Schutz vor Cyberrisiken eine wesentliche Rolle. Sie stützt sich, wie die gesamte Gesellschaft, stark auf Informations- und Kommunikationstechnologien ab und kann das Ziel von Cyberangriffen sein. Deshalb muss sie zunächst ihre eigenen Infrastrukturen und Mittel schützen. Sie investiert in Netze, die gegenüber Angriffen und Gefahren aller Art geschützt sind. Dazu zählen die Projekte zum Neubau von Rechenzentren, Telekommunikation der Armee und Führungsnetz Schweiz. Soweit die Armee ihre eigenen Schutzbedürfnisse erfüllt hat, kann sie bei Bedarf ihre Kapazitäten zum Schutz vor Cyberangriffen subsidiär zivilen Behörden zur Verfügung stellen und damit einen Beitrag zur Aufrechterhaltung der Funktionsfähigkeit der kritischen Infrastruktur leisten. Die Armee will ab Sommer 2018 Cybersoldaten ausbilden. Vorerst ist der IT-Lehrgang für Milizsoldaten ein Pilotprojekt. Neben dem IT-Lehrgang für Rekruten geht es laut dem VBS auch um weitere Elemente innerhalb einer längeren Ausbildung, insbesondere um die Entwicklung einer Offizierslaufbahn sowie von vordienstlichen Aktivitäten. Das Pilotprojekt für einen Cyberlehrgang ist also erst der Anfang einer Cyber-Defence-Organisation von einigen Hundert Milizsoldaten. Auf Stufe Armee ist die Cyber Defence eine Fähigkeit der Führungsunterstützungsbasis (FUB). Sie ist im Bereich Verteidigung für Aktionsplanung, Lageverfolgung, Ereignisbewältigung und Ausbildung der Mitarbeitenden und AdA im Cyberraum auf operativer Stufe verantwortlich.
- **Bundesamt für Bevölkerungsschutz (BABS):** Aufgabe des Bevölkerungsschutzes ist es, die Bevölkerung und ihre Lebensgrundlagen bei Katastrophen und in Notlagen sowie im Falle bewaffneter Konflikte zu schützen und so wesentlich zur Begrenzung und Bewältigung von Schadenereignissen beizutragen. Das BABS führt im Rahmen der NCS Risiko- und Verwundbarkeitsanalysen für kritische Infrastrukturen durch. Basierend auf diesen Analysen erarbeitet das Bundesamt zusammen mit den Regulierungsbehörden, Verbänden und Betreibern kritischer Infrastrukturen (Spitäler usw.) Massnahmen zur Risikoreduktion.

In den Jahren 2016/17 erarbeitete das VBS zudem einen internen Aktionsplan für Cyber Defence. Der Prozess begann im Juli 2016 mit einer Standortbestimmung, aufgrund derer eine Strategie festgelegt wurde. Nach deren Genehmigung im Oktober 2016 folgte ein Umsetzungsplan, der wiederum im Juni 2017 verabschiedet wurde.

1.3 Erkenntnisse und Beurteilung

Der Bund hat viele Jahre benötigt, um die Bedrohung durch Cyberwar zu erkennen. Viel zu lange wurde der Schutz von militärischen und zivilen Netzwerken und kritischer Infrastruktur dezentral und mit ungenügenden Mitteln organisiert. Spätestens im Nachgang zum Hackerangriff auf die Ruag ist eine öffentliche Diskussion entbrannt, wer für den Schutz von privaten Geschäftsinteressen die Verantwortung trägt. Der Bund hat diese – korrekterweise – stets von sich gewiesen. Spätestens seit der NCS 2018–2022 existiert eine sinnvolle Arbeitsteilung: Der Staat muss primär die Verwundbarkeit der eigenen Systeme erkennen und wirkungsvolle Schutzmassnahmen treffen. Dabei gilt es jedoch eine sinnvolle Lösung zu finden, welche die Kantone und Gemeinden einbindet und ebenfalls schützt. Ebenso wichtig ist eine angemessene Unterstützung beim Schutz von kritischer Infrastruktur. Hierfür hat der Bund mit MELANI die passende Richtung eingeschlagen und ein Kompetenzzentrum für Informationssicherheit geschaffen.

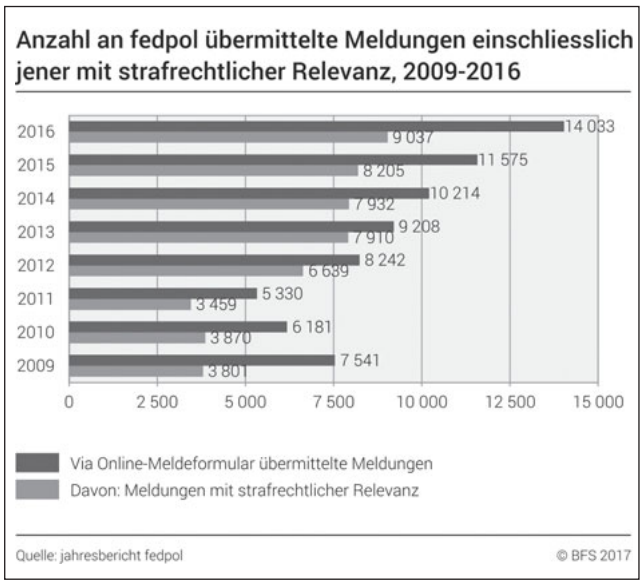
Es gehört jedoch nicht zu den Kernaufgaben des Bundes, jegliche Angriffe gegen Infrastrukturen im Inland zu schützen. Der Schutz von individuellen Geschäftsgeheimnissen und -interessen muss Aufgabe der Unternehmen sein. Mit MELANI bietet der Bund sein Wissen zur Unterstützung an.

Die Bedeutung von Cyber Security scheint nun definitiv im Bundesrat und Parlament angekommen zu sein. Ein effektiver Schutz benötigt jedoch genügend Mittel, um Fachleute rekrutieren und wirkungsvolle Massnahmen umsetzen zu können.

2 Cybercrime

2.1 Bedrohungsanalyse

Die Internetkriminalität kostet Unternehmen jährlich fast 600 Milliarden Dollar, was 0,8 Prozent des weltweiten BIP entspricht. Zu diesem Ergebnis kommt eine Studie, die vom IT-Security-Anbieter McAfee in Zusammenarbeit mit dem amerikanischen «Center for Strategic and International Studies» (CSIS) durchgeführt und im Report «Economic Impact of Cybercrime – No Slowing Down» veröffentlicht wurde. In der Schweiz wurden im Jahr 2016 ganze 14'033 Verdachtsfälle von Cyberkriminalität gemeldet. Dies geht aus dem Jahresbericht des Bundesamts für Polizei fedpol hervor. Damit stieg die Zahl der Meldungen um mehr als 20 Prozent gegenüber dem Vorjahr (11'570 Fälle). Zwar handelt es sich hierbei nicht um rechtskräftig abgeschlossene Straffälle; zudem sind Veränderungen auch auf die Wahrnehmung von Cyberkriminalität in der Gesellschaft sowie die Bereitschaft, diese aktiv an die Behörden weiterzuleiten, zurückzuführen. Dennoch zeigt der deutliche Anstieg der letzten Jahre auch eine zunehmende Gefährdung durch kriminelle Aktivitäten im Internet.



Über 20 unterschiedliche Cybercrime-Formen listet ein Katalog des fedpol derzeit auf – vom inzwischen klassischen Phishing[4] über die Infizierung eines Computers mit Spionageprogrammen («Spyware») bis zur Bildung sogenannter Botnets: Dabei übernehmen kriminelle Banden die Kontrolle über ein ganzes Netz von Computern, ohne dass die Besitzer etwas davon ahnen. Neben technischen Aspekten rückt der Benutzer immer weiter in den Fokus: Durch «Social Engineering» versuchen die Angreifer, die Betroffenen so zu manipulieren, dass sie anschliessend persönliche Informationen preisgeben, Geld überweisen oder gefälschte Produkte kaufen. Kurz: Der Mensch wird zur Schwachstelle.

Cyberkriminalität nimmt in der Schweiz rasch zu. Die Täter attackieren in kurzer Zeit eine hohe Zahl von Opfern im ganzen Land. Doch die Polizeistrukturen in der Schweiz stammen aus dem letzten Jahrhundert. Eine effektive Bekämpfung von Cyberkriminalität bedingt heute eine effiziente Koordination der Ermittlungen. Um sich den Tätern an die Fersen zu heften, sind technisches Know-how und Ressourcen nötig, die vor allem in kleinen Kantonen oft zu wenig vorhanden sind. Zudem befinden sich viele der Handelsplattformen, deren Daten die Polizei für ihre Arbeit braucht, im Ausland. Spuren führen die Ermittler rasch über die Grenze, was Rechtshilfe und damit oft die Einbindung des Bundes erfordert und die Aufklärung stark erschwert.

2.2 Vorkehrungen von Staat und Wirtschaft

Der Bund und die Kantone betreiben gemeinsam die nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK), die beim fedpol angesiedelt ist. Sie ist einerseits die nationale Anlaufstelle für Personen, die verdächtige Internetinhalte melden möchten. Diese Meldungen werden nach Überprüfung durch die KOBIK an die zuständigen Strafverfolgungsbehörden im In- und Ausland weitergeleitet. Andererseits sucht die KOBIK auch aktiv im Internet nach strafrechtlich relevanten Inhalten. Weiter betreibt sie eine vertief-

4 ***Phishing*** *bezeichnet Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Informationen eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen.*

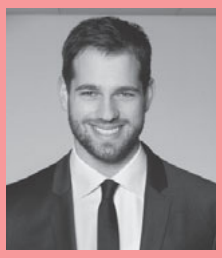
te Analyse im Bereich der Internetkriminalität und steht der Öffentlichkeit, Behörden und Internetservice-Providern als Kompetenzzentrum zur Verfügung.

Die KOBIK entstand 2003 als typisches Konstrukt der föderalen Schweiz: Mit wenigen Ausnahmen wurden seither Internetverbrecher von Ermittlern des Bundes verfolgt und aufgespürt und zur Anklage an kantonale Stellen weitergeleitet. Die Mittel stammen jedoch zu zwei Dritteln von den Kantonen. Die Bundesanwaltschaft (BA), das fedpol und kantonale Partner starteten im Jahr 2018 eine neue Initiative, wie Bundesanwalt Michael Lauber anlässlich der Präsentation des Tätigkeitsberichts 2017 der BA vor den Medien bekannt gab. Neue Kompetenzzentren sollen die Ermittler in Zukunft schneller und schlagkräftiger machen. Bund und Kantone planen mehrere Cybercrime-Kompetenzzentren. Sie sollen verhindern, dass die Schweizer Behörden in der komplexen, technisch anspruchsvollen, koordinationsintensiven und häufig grenzüberschreitenden Verbrechensbekämpfung im Netz gegenüber den Tätern ins Hintertreffen geraten. In die Arbeiten involviert sind die Bundesanwaltschaft, das fedpol, die Schweizerische Staatsanwälte-Konferenz (SSK) sowie die Konferenz der kantonalen Polizeikommandanten (KKPKS). Die neuen Kompetenzzentren sollen nicht nur die regionale Kooperation stärken und zusätzliche Ressourcen erhalten, sondern auch die Zusammenarbeit zwischen der Polizei und den Staatsanwälten und einen effizienten Wissenstransfer zwischen ihnen fördern. Im Frühsommer hat als Koordinationsorgan ein Schweizer «Cyberboard» die Arbeit aufgenommen. Bis heute ist nicht klar geregelt, wer im Cyber-Bereich was bekämpfen soll. Die BA ist für Phishing zuständig, also für das Aufspüren und Anklagen von Kriminellen, die zum Beispiel versuchen, mit gefälschten E-Mails Passwörter von Bankkontoinhabern zu erbeuten. Aber das ist die Ausnahme: Die meisten Formen von Cybercrime fallen in den Aufgabenbereich der Kantone. Das soll möglicherweise bald geändert werden, denn vor allem in kleinen Kantonen fehlt Spezialwissen.

Cyberkriminalität beschäftigt auch die Wirtschaft zunehmend. Nach wiederkehrenden Medienberichten über Angriffe gegen Unternehmen, teilweise verbunden mit Erpressungsversuchen, hat das Risikobewusstsein stark zugenommen. Jedoch hat es vielerorts relativ lange gedauert, bis konkrete Massnahmen umgesetzt wurden. Heute befindet sich der Cyber-Defence-Markt stark im Wachstum: Firmen investieren in ihre IT-Infrastruktur, bauen Firewalls aus oder schliessen Ausfallversicherungen ab.

Cyberangriffe können jederzeit erfolgen und bleiben oft lange unbemerkt.

2.3 Fragen an Nicola Staub, Staatsanwalt des Kantons Schwyz und Experte für Cybercrime



Nicola Staub ist Staatsanwalt bei der Staatsanwaltschaft des Kantons Schwyz. Er führt Strafuntersuchungen im spezialisierten Bereich Wirtschafts- und Cyberkriminalität und ist zusammen mit der Kantonspolizei für das Thema Cyberkriminalität im Kanton Schwyz verantwortlich. Er engagiert sich zudem für die internationale Organisation Global Cyber Alliance.

Herr Staub, was ist Ihre Rolle bei der Global Cyber Alliance?

Nicola Staub: «Die Global Cyber Alliance wurde von der Staatsanwaltschaft Manhattan und der Londoner Polizei – also von Strafverfolgungsbehörden –

mitbegründet. Als unabhängige, internationale und nicht gewinnorientierte Organisation entwickelt und fördert sie ‹Cyber Security›, also konkrete Initiativen zur besseren Prävention vor Cyberkriminalität. Bessere Cyber Security heisst weniger Cyberkriminalität, also weniger Fälle auf den Tischen der Strafverfolgungsbehörden. Für mich war deshalb sofort klar, ehrenamtlich Unterstützung zu leisten – seit Mai in Form eines ‹Ambassador›. Mein Ziel ist es, die Arbeit der Organisation in der Schweiz besser bekannt zu machen. Von deren Initiativen, wie z. B. DMARC, können vor allem KMU auch in der Schweiz stark profitieren und sich ohne zusätzliche Kosten besser vor Cyberangriffen schützen.»

Wo orten Sie die grössten Defizite im Bereiche der staatlichen Prävention gegen Cybercrime?
«Cyber Security ist eine Verbundsaufgabe. Die Schweiz hat zwar mit der NCS eine nationale Strategie. In der Umsetzung erfordert dies Investitionen, eine starke Koordination, schnelles und zukunftsorientiertes Handeln mit klaren Zuständigkeiten und einem rigorosen Zeitplan. Hier stehen der Bund und die Kantone in der Pflicht: Sie müssen die notwendigen Mittel zur Verfügung stellen. In Grossbritannien beispielsweise hat der Staat für die Umsetzung einer Fünfjahresstrategie umgerechnet rund 2,5 Milliarden Franken investiert. Das gleiche Vorgehen gilt übrigens auch für die Strafverfolgung. Es ist höchste Zeit, dass wir uns koordinieren und die Cyberkriminalität in effizienter Weise gemeinsam bekämpfen. Die kürzliche Lancierung des nationalen Cyberboards – mit genau diesem Ziel – finde ich deshalb sehr begrüssenswert.»

Wie schätzen Sie die Anfälligkeit neuer Technologien wie Blockchain für Betrügereien ein?
«Wo viele Menschen einen Nutzen sehen, wird sich eine neue Technologie durchsetzen. Doch die sind nie perfekt. Es wird immer Lücken und Schwachstellen geben – meist ungewollt, teilweise aber auch sehr bewusst. Diese Schwachstellen werden von Kriminellen ausgenutzt. Deshalb ist es sehr wichtig, die Präventionsmassnahmen jeweils auf dem aktuellsten Stand zu halten. Ich hoffe, dass es den Staaten und Organisationen, wie z. B. der GCA, gelingt, möglichst viele Schwachstellen für Unternehmen und Privatpersonen zu eliminieren. Dies kann mittels konkreter Initiativen oder aber – wo notwendig – durch gesetzliche Massnahmen bzw. zusätzliche Regulierung geschehen. Zudem muss es unser Ziel bei der Strafverfolgung sein, bei der Cyberkriminalität durchzugreifen und involvierte Personen unabhängig von Kantons- und Landesgrenzen zur Rechenschaft zu ziehen.»

Viele Start-ups finanzieren sich heute über Initial Coin Offerings (ICO). Erachten Sie die heutige Regulierung im Bereich der ICOs als genügend?
«Diese Finanzierungsart ist tatsächlich ein neuartiges Phänomen, die Finma hat mit ihrer Wegleitung zu ICOs nun einen ersten Schritt gemacht. Aus Sicht der Strafverfolgung wäre es meiner Meinung nach notwendig, die Bevölkerung noch besser und breiter über die hohen Risiken bei solchen Investitionen zu informieren. Der aktuelle Hype führt teilweise zu leichtsinnigen Investments; davon profitieren auch Wirtschaftskriminelle. Anlagebetrügereien gibt es zwar schon lange, die ICOs und die damit verbundene ‹Goldgräberstimmung› scheinen aber momentan ein idealer Vorwand zu sein, um einfach an Geld zu gelangen. Ich bin deshalb überzeugt, dass ICOs unsere Strafverfolgungsbehörden leider noch einiges an Arbeit bescheren werden.»

Was sind in der föderalistischen Schweiz die grössten Hindernisse für eine erfolgreiche Verbrechensbekämpfung im Bereich Cyberkriminalität?
«Bei Cyberkriminalität gibt es keine Landesgrenzen und schon gar keine Kantonsgrenzen. Den föderalistischen Ansatz mit all seinen unbestrittenen Vorteilen gilt es deshalb hier neu zu denken. Das heisst natürlich nicht, dass die einzelnen Kantone ihre Verantwortung nicht wahrnehmen müssen. Im Kanton

Schwyz wurde ein Grobkonzept erarbeitet, die Arbeiten sind in vollem Gange. Es braucht aber klar eine enge Koordination auf nationaler Ebene aller in der Strafverfolgung involvierten Behörden. Ich bin zuversichtlich, dass mit dem Cyberboard nun ein erster Schritt in diese Richtung erfolgt.»

Welche zusätzlichen Mittel wünschen Sie sich, um effizienter gegen Cyberkriminalität vorgehen zu können?
«Wir können die Verbrechensbekämpfung grundsätzlich auf zwei Ebenen verbessern: Einerseits brauchen wir mehr Effizienz bei der internationalen Rechtshilfe. In den meisten Fällen dauert es Monate, bis wir Beweismittel aus dem Ausland erhalten. Bei Cyberkriminalität ist das besonders stossend, denn der Tatort ist schwer auszumachen und die Beweismittel meistens über diverse Länder verteilt. Ohne Beweise sind wir aber machtlos – die Strafverfolgung blockiert. Ich mache mir dennoch keine Illusionen; das Problem ist international anzugehen und teilweise sehr politisch. Zudem leisten gewisse Länder gar keine Rechtshilfe, was Cyberkriminelle zu ihren Gunsten nutzen. Auch die Schweiz ist international in Sachen Effizienz bei Rechtshilfe keine Musterschülerin. Das Ausland wartet regelmässig monatelang. Das ist nicht zeitgemäss, und da ist meines Erachtens der Gesetzgeber gefordert.
Andererseits erhoffe ich mir natürlich auch in der Schweiz genügend Mittel durch den Bund und die Kantone, um unsere Aufgabe im Inland sauber und effizient bewältigen zu können.»

2.4 Erkenntnisse und Beurteilung

Seit mehreren Jahren lässt sich eine starke Bewusstseinszunahme im Bereich der Cyber Security feststellen. Der Bund hat seine Aktivitäten intensiviert und arbeitet aktuell an Kompetenzzentren, um die relevanten Partner bei der Aufklärung von Cyberkriminalität einzubinden und ihre Ressourcen zu bündeln. Das neue Cyberboard soll vorderhand keine Zusatzkosten verursachen und auch keine Anpassungen der Gesetze erfordern. Spätestens aber, wenn regionale Cybercrime-Zentren den Betrieb aufnehmen, stellt sich die Frage: Wer bezahlt die neuen Strukturen, und damit verbunden, wie lautet die künftige Kompetenzordnung? Zusätzliche Mittel werden nötig sein, und wenn nicht analog zum Gesundheitswesen eine teure und ineffiziente Kompetenzverflechtung resultieren soll, muss der Föderalismus in diesem Bereich neu erfunden werden.
Die Wirtschaft hat erst spät damit begonnen, ihre Sicherheitsinfrastruktur auszubauen. Insbesondere KMU kämpfen hierbei mit den kostenintensiven Massnahmen. In einer Umfrage der Zurich Insurance Group von 2016 unter 200 KMU glaubten nur 2,5 Prozent der Teilnehmer, dass sie ausreichend vor Hackerangriffen geschützt waren. Sowohl beim Bund als auch in der Wirtschaft hat sich mittlerweile die Erkenntnis durchgesetzt, dass es für Cyberkriminelle einfacher ist, Menschen zu täuschen als in Computersysteme einzudringen.
Verschiedene Experten, darunter das Deutsche Bundeskriminalamt und das Kompetenzzentrum Cybercrime des Kantons Zürich, empfehlen deshalb drei übergeordnete Massnahmen:

- Technische Präventionsmassnahmen: Sowohl Firmen als auch Verwaltungen sollen wirkungsvolle Firewalls einrichten, geeignete Passwortrichtlinien erlassen und ihre Betriebssysteme jeweils auf dem aktuellen Sicherheitsstandard halten.
- Sensibilisierung der Mitarbeiter: Um Phishing, Social Engineering und ähnliche Risiken zu minimieren, müssen Mitarbeiter zurückhaltend mit vertraulichen und persönlichen Informationen umgehen. Zudem sollen sie bei ungewöhnlichen Vorgängen, E-Mails unbekannter Absender oder verdächtigen Links misstrauisch reagieren.
- Krisenplanung: Um bei einem IT-Sicherheitsvorfall zeitnah und passend reagieren zu können, helfen vorbereitete Abläufe und Szenarien. Diese helfen auch, den Reputationsschaden zu minimieren. Dabei ist es wichtig, dass wichtige Stellen, darunter Compliance-, Datenschutzverantwortliche, Rechts- und Kommunikationsabteilungen sowie die Geschäftsleitung, in die Planung eingebunden werden.

3 Benchmarking

3.1 Beispiele privater Initiativen

Die Global Cyber Alliance

Die Global Cyber Alliance (GCA) ist eine internationale, branchenübergreifende Initiative, die sich der Bekämpfung von Cyberrisiken widmet. Um ihr Ziel zu erreichen, setzt sie folgende Schwerpunkte:

- Branchenübergreifende Vereinigung der globalen Gemeinschaften gegen Cyberrisiken,
- Kreation konkreter Lösungen, welche kostenlos von Organisationen, Gesellschaften und Privatpersonen genutzt werden können, um systembedingte Cyberrisiken zu minimieren und schliesslich zu beseitigen sowie
- Messung und transparente Mitteilung des Effekts der eigenen Arbeit.

Im Bewusstsein über das Potenzial einer Organisation wie der GCA, hat die New Yorker Staatsanwaltschaft 25 Millionen US-Dollar über einen Zeitraum von fünf Jahren zur Finanzierung der Arbeiten bereitgestellt. Das Center for Internet Security und die Londoner Polizei leisteten ebenfalls wichtige Beiträge zur Organisation, u. a. zur Bereitstellung von Räumen, finanziellen Mitteln, Personal und beim Aufbau strategischer Partnerschaften. Durch diese Beiträge und den regen Austausch gelang es der GCA bereits, ein eindrückliches globales Partnernetzwerk aufzubauen und erste Initiativen umzusetzen.

Mehr Informationen und Angebote zum Schutz vor Cyberrisiken unter www.globalcyberalliance.org

www.globalcyberalliance.org

WEF eröffnet in Genf ein Zentrum für globale Cyber Security

Im WEF-Bericht 2017 «Global Risks Report» tauchen Cyberattacken auf Rang drei der grössten Bedrohungen auf. Internetangriffe könnten die Weltwirtschaft jährlich bis zu 500 Milliarden Dollar kosten, so das WEF in einer Mitteilung. Nun hat das Weltwirtschaftsforum eine Massnahme gegen die Gefahr angekündigt: In Genf wurde im Frühjahr 2018 ein globales Zentrum für Cybersicherheit eröffnet.

Das Center soll unter der Federführung des WEF als unabhängige Institution dabei helfen, ein sicheres globales Cyberspace zu etablieren. Es soll als globale Plattform für Regierungen, Unternehmen, Experten und Strafverfolgungsbehörden dienen, auf welcher sie zusammenarbeiten, Informationen sammeln und sich austauschen sowie Standards entwickeln können.

Das Zentrum soll 30 bis 40 Stellen umfassen und ein jährliches Budget im zweistelligen Millionen-Franken-Betrag umfassen. Finanzieren wird es sich durch Mitgliederbeiträge aus dem Privatsektor, zu Beginn sollen rund 50 Unternehmen dabei sein. Zur Präsentation des Zentrums sassen bereits Unterstützer von Comcast, Interpol und der Moskauer Sperbank auf dem Podium. Zudem hat die britische BT Group ihre Beteiligung zugesichert.

Weitere Informationen: www.weforum.org

Technologiekonzerne unterzeichnen «Digital Geneva Convention» für mehr Sicherheit im Cyberspace

Mehr als 30 Technologiefirmen, angeführt von Microsoft und Facebook, kündigten im April 2018 eine Reihe von Prinzipien zum Schutz gegen Cyberwars an. Darunter war eine Erklärung, dass sie keiner Regierung – einschliesslich derjenigen der Vereinigten Staaten – helfen würden, Cyberangriffe gegen «unschuldige Zivilisten und Unternehmen» auf der ganzen Welt zu verüben. Damit widerspiegelten sie die Bemühungen des Silicon Valleys, sich von der staatlichen Cyberkriegsführung zu distanzieren.

Die neuen Prinzipien, die nun seit mehreren Wochen unter den Führungskräften der Technologiebranche im

Umlauf sind, verpflichten die Unternehmen auch dazu, jedem von Cyberangriffen betroffenen Staat Hilfe zu leisten, unabhängig davon, ob das Motiv für den Angriff «kriminell oder geopolitisch» ist. Obwohl die Liste der unterzeichnenden Unternehmen lang ist, haben mehrere Konzerne das Abkommen – zumindest bis jetzt – nicht unterschrieben, darunter Google, Apple und Amazon.
Ebenso wichtig ist vermutlich, dass keiner der Unterzeichner aus den Ländern stammt, die für das verantwortlich gemacht werden, was Brad Smith, der Präsident von Microsoft, in einem Interview als die «verheerenden Angriffe des vergangenen Jahres» bezeichnet hatte. Konkret sind dies hauptsächlich Russland, Nordkorea, der Iran und in geringerem Ausmass auch China.
Im April 2018 gaben die amerikanischen und britischen Behörden zudem erstmals eine gemeinsame Warnung über die jahrelangen Cyberattacken von Seiten Russlands heraus. Sie sollen sich nicht nur gegen Unternehmen und öffentliche Institutionen gerichtet haben, sondern in einigen Fällen auch gegen Einzelpersonen und Kleinbetriebe. Die Warnung war nur die letzte in einer Serie zur russischen Bedrohung von Wahlen und Wahlsystemen.
Weitere Informationen: www.microsoft.com

3.2 Israels Cyber-Security-Ansatz als Erfolgsmodell

Erfolgreiches Cyber-Security-Ökosystem
In den vergangenen Jahren wurde Israel zu einem erfolgreichen Zentrum im Bereich Cyber Security, was Erforschung, Entwicklung und Angebot von Lösungen betrifft. Mit Dienstleistungen und Produkten werden dort mittlerweile 82 Milliarden US-Dollar umgesetzt (ohne Ausgaben für «internal security staff and processes»).
Neben der Zusammenarbeit mit Hegemonialmächten unterstützt Israel auch kleinere Nationen (z. B. Singapur) und hat die israelische Wirtschaft über 300 Cyber-Security-Start-ups hervorgebracht. Bis jetzt haben über 30 multinationale Konzerne in Israel lokale Forschungs- und Entwicklungszentren eröffnet und ausländische Investoren angelockt. Im Jahr 2016 erfolgten ungefähr 20 Prozent der weltweiten Investitionen in Cyber Security in Israel.

Das Zentrum des israelischen Cyber-Defence-Biotops befindet sich im Advanced Technologies Park an der Ben-Gurion University in der Stadt Beer-Sheva. Der Park hat nicht nur zahlreiche grössere multinationale Konzerne und ihre Forschungs- und Entwicklungszentren angelockt (darunter Deutsche Telekom, Dell EMC, IBM, und Oracle), auch Venture-Capital-Firmen, angewandte Forschungslabore, das israelische National Cyber Research Institute und die israelische Cyber Emergency Response Teams haben ihren Sitz dort. Momentan verlegt auch das Verteidigungsministerium seine strategischen Technologieeinheiten in diesen Campus.

Sechs Erfolgsfaktoren
Folgende sechs Erfolgsfaktoren waren dafür verantwortlich:

1. **Koordination durch die Behörden:** Statt auf Mehrjahrespläne, die durch sich rasch ablösende Technologiegenerationen obsolet werden, setzt Israel in seiner National Cyber Initiative auf die Entwicklung eines responsiven Ökosystems, das auf unvorhersehbare Bedrohungen reagieren kann. Das System setzt auf eine kontinuierliche Kooperation von Behörden, Streitkräften, Wirtschaft und Forschung. Den Behörden kommt dabei eine leitende und beratende Funktion zu.
2. **Behörden als Katalysator:** Das 2011 gegründete nationale National Cyber Bureau hatte von Beginn weg den Auftrag, Israel innert weniger Jahre unter den fünf führenden Nationen für Cyber Security zu positionieren. Das Thema wurde als Wachstumstreiber identifiziert, weil Israel über eine konkurrenzfähige Forschungs- und Anwendungserfahrung verfügte.
3. **Streitkräfte als Start-up-Förderer:** Die permanente Existenzbedrohung Israels seit 1948 führte zu einer überproportionalen Ressourcenallokation zur Entwicklung und Aufrechterhaltung überlegener Militärtechnologie. Mit dem Einzug von Computern und Digitalisierung in Krieg und Gesellschaft wurde Cyber Defence zu einer Schlüsselkompetenz des Verteidigungsministeriums. «Früher wurde der Militärdienst als Zeitverschwendung empfunden, heute ist es anders. Denn mittlerweile sind die israelischen Streitkräfte ein wichtiger Katalysa-

tor für die israelische Wirtschaft.» Die israelischen Cyber-Defence-Einheiten agieren wie Start-ups: Teamwork-Erfahrung, Führungserfahrung, Verantwortung übernehmen und entscheiden.

4. **Aufbau von Humankapital:** Menschen mit ihren Fähigkeiten, Erfahrungen und Ambitionen bilden die Ingredienz für erfolgreiche Cyber Defence. Die Ausbildung fördert das zusätzlich: Cyber Security ist bereits auf Stufe Maturität ein Schulfach, Universitäten offerieren von IT-Lehrgängen bis zum PhD in Cyber Security.
5. **Interdisziplinarität und Vielfalt:** Cyber Security umfasst das Verständnis von verschiedenen Disziplinen: Es stellen sich juristische, psychologische, soziologische, wirtschaftliche und andere Fragen. Unterschiedliche Sichtweisen helfen Barrieren zu überwinden. Die im Militär gesammelten Erfahrungen werden durch akademisches Know-how ergänzt und später in der Wirtschaft erfolgreich angewendet. Ergänzt wird das durch die grosse Diversität der israelischen Gesellschaft: 2014 waren 25 Prozent der jüdischen Bevölkerung immigriert, weitere 35 Prozent waren Kinder von Immigranten.
6. **Fähigkeitsbasierter Ansatz:** Der typische Approach zur Cyber Security war auf den Gegner fokussiert. Viele Staaten neigen dazu, jeder Art des Gegners eine bestimmte Behörde zuzuweisen. Das macht die Abwehrstrategien ineffizient, fragmentiert und kaum koordinierbar. Israel hat nach Jahren des «trial and error»-Prinzips heute einen anderen Ansatz gefunden: proaktiv, kohärent, die Disziplinen vereinigend und langfristig ausgerichtet. Die Strategie fokussiert nicht auf potentzielle Gegner resp. Angreifer, sondern auf die Fähigkeiten, Attacken jeder Art jederzeit wirksam zu bekämpfen. Dazu baut Israel auf Einheiten als «first line of defence».

4 Fazit und Folgerungen

Eine erfolgreiche an die Erfahrungen Israels angelehnte Cyberstrategie muss auf drei Ebenen ansetzen:

1. Robustheit: Immunisierung der Infrastruktur und Netze gegen Attacken. Der Staat berät, gibt Anweisung und Führung. Die betroffenen Organisationen und Unternehmen handeln eigenverantwortlich.
2. Resilienz: Schutz vor neuen Risiken dank Erforschung, Aufklärung und Entschärfung von Attacken. Hier braucht es das aktive Engagement des Staates und seiner Experten.
3. Verteidigung: Die erfolgreiche Abwehr von Attacken erfordert Ressourcen und Kapazitäten, die nur Staaten und ihre Behörden aufbringen.

Richtig verstandene Robustheit und Resilienz machen 95 Prozent des Abwehrerfolges aus. Israels Cyber-Security-Philosophie ist ein praktisch erprobtes Beispiel einer erfolgreichen Herstellung von Interdisziplinarität, gegenseitiger Befruchtung und Konsolidierung öffentlicher und privater Interessen.

Darüber hinaus braucht es in der Schweiz

- neben vielen guten Konzepten nun konkrete Umsetzungsschritte,
- mehr Mittel und Ressourcen in diesem Bereich,
- eine bewährte Arbeitsteilung Staat/Wirtschaft nach den Prinzipien des Public Private Partnership,
- eine optimierte Aufgabenteilung zwischen Bund und Kantonen nach den Prinzipien der Subsidiarität und der Wirksamkeit.

Die Schweiz ist beraten, starre Strukturen zu beseitigen und gemeinsam mit allen relevanten Akteuren eine wirkungsvolle Verteidigungsstrategie zu schaffen. Diese ist entscheidend für den Schutz des Staates und seiner Institutionen und gleichzeitig eine wichtige Basis für einen langfristig erfolgreichen Innovations-, Crypto- und Digital-Wirtschaftsstandort Schweiz. Unser Land baut stark auf Eigenschaften wie Rechtssicherheit, Stabilität und ein hohes Bildungsniveau. Diese «analogen» Qualitäten gilt es nun für den digitalen Raum und kommende Generationen zu erhalten und zu adaptieren.

Glossar

Cyber (engl.) steht als Abkürzung für Cyberspace, zu Deutsch «kybernetischer Raum».

Cyberspace bezeichnet den virtuellen Raum aller auf Datenebene vernetzten IT-Systeme im globalen Massstab. Cyberspace bezeichnet die Gesamtheit der mittels Computern erzeugten räumlich anmutenden oder ausgestalteten Bedienungs-, Arbeits-, Kommunikations- und Erlebnisumgebungen. In der verallgemeinernden Bedeutung als Datenraum umfasst das Cyberspace das ganze Internet.

Cyber Risk umfasst die Gesamtheit der Risiken, die aus der Anwendung moderner internetbasierter (Computer-)Technologien entstehen und bezüglich Technologieanwendung, Schadenspotenzial und Zielsetzungen erheblich differieren können. Ihnen gemeinsam ist, dass sie einerseits auf das Funktionieren der vernetzten Wirtschaft und Gesellschaft grossen Einfluss haben und zumeist unterschätzt werden.

Cyber Security erweitert das Portfolio der klassischen IT-Sicherheit auf das gesamte Spektrum des Cyberraums und schliesst darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein, insbesondere auch mobile Kommunikation. Cyber Defence bezeichnet Massnahmen zur Erhöhung der Cyber Security.

Beim **Cyberwar** handelt es sich um eine kriegerische Auseinandersetzung im und um den virtuellen Raum, die mit Mitteln der Informationstechnologie geführt wird. Ein Cyberkrieg hat zum Ziel, Ländern, Institutionen oder der Gesellschaft auf elektronischem Weg Schaden zuzufügen und wichtige Infrastrukturen zu stören. Im völkerrechtlichen Sinn ist es schwierig, den Cyberkrieg offiziell als kriegerische Handlung zu deklarieren.

Information Warfare, resp. Informationskrieg (oft «infowar» abgekürzt), bezeichnet die gezielte Nutzung und Manipulation von gesteuerten Informationen, um in der Wirtschaft oder in der Politik Vorteile gegenüber Konkurrenten und Gegnern zu erzielen. Dazu gehört auch die Beeinflussung von Medien durch Falschinformationen («Fake News»), Teilinformationen oder Propaganda. In den öffentlich zugänglichen Medien ist der Informationskrieg eine Form des Cyberwars. In sozialen Netzwerken werden immer häufiger auch mithilfe von Algorithmen («Social Bots») Profile gefälscht, Informationen gesammelt oder auch gezielt gestreut.

Cybercrime umfasst die Straftaten, die sich im Internet gegen Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden. Aktuell verbreitete Erscheinungsformen von Internetkriminalität sind gekennzeichnet durch die Infektion und Manipulation von Computersystemen mit Schadsoftware, z. B. um persönliche Daten zu erhalten und missbrauchen, um Dateien zu verschlüsseln und «Lösegeld» zu erpressen oder um Computersysteme in kriminelle Netzwerke zusammenschliessen zu können.

Cyberterrorismus umfasst Angriffe auf Computersysteme mithilfe von Internettechnologien, die ein terroristisches Ziel verfolgen (vgl. Cybercrime). Möglich sind bspw. Schreckensszenarien mit Tausenden Toten durch falsch gesteuerte Schleusentore, veränderte Zusammensetzung von Medikamenten oder gar atomare Katastrophen durch Überlistung der Sicherheitssysteme. Die reale Bedrohungslage wird ganz unterschiedlich eingeschätzt, von einer akuten, permanenten Gefahr bis hin zur Negation des Risikos.

Digitalisierung meint im ursprünglichen Sinn die Umwandlung von analogen Informationen in digitale Formate. Erweitert bezeichnet Digitalisierung die digitale Revolution, auch digitaler Wandel oder digitale Transformation genannt. Der digitale Wandel beschreibt die durch die Digitalisierung ausgelösten Veränderungsprozesse in der Gesellschaft inklusive Wirtschaft, Kultur, Bildung und Politik.

VEREIN SICHERHEITSPOLITIK UND WEHRWISSENSCHAFT

Unsere Ziele

Der Verein Sicherheitspolitik und Wehrwissenschaft und seine Mitglieder wollen

- bekräftigen, dass die Schweiz auch in Zukunft ein militärisch ausreichend geschützter Raum bleiben soll,
- erklären, dass ein wirksamer Schweizer Beitrag an die Stabilisierung primär des europäischen Umfeldes eine glaubwürdige, kalkulierbare und umfassende Schweizer Sicherheitspolitik benötigt,
- herausarbeiten, dass die Schweiz nicht nur als Staat, sondern auch als Wirtschaftsstandort, Denk-, Werk- und Finanzplatz sicherheitspolitisch stabil bleiben muss, um weiterhin erfolgreich existieren zu können,
- darlegen, dass eine sichere Schweiz angemessene Mittel für ihre Sicherheitspolitik benötigt,
- aufzeigen, was für eine effiziente und glaubwürdige Armee im Rahmen des integralen Selbstbehauptungsapparates an Fähigkeiten, an Ausbildung, Ausrüstung und Organisation nötig ist,
- sich dafür einsetzen, dass künftige Reformen der Milizarmee und ihrer Einsatzdoktrin diesen Postulaten entsprechen.

Unsere Leistungen

Der Verein und seine Mitglieder verfolgen diese Ziele seit 1956 durch Informationsarbeit in Form von Studien, Fachbeiträgen, Publizität und Stellungnahmen (vgl. www.vsww.ch), Vorträgen, Interviews und Gesprächsbeiträgen.

So hat er wesentlich geholfen,

- gegen eine moderne Schweizer Sicherheitspolitik gerichtete Volksinitiativen und Referenden zu bekämpfen sowie
- Expertenbeiträge zu einer neuen Sicherheitspolitik und zu einer glaubwürdig ausgebildeten und ausgerüsteten Armee zu leisten.

Unsere Zukunftsvision

Wir wollen mit unserer Arbeit dazu beitragen,

- dass die Schaffung eines breit abgestützten inneren Konsenses im Bereich der militärischen Selbstbehauptung in der Schweiz gelingt und
- die gesellschaftliche, wirtschaftliche und politische Integration unserer Milizarmee auch in Zukunft intakt bleibt.

Unsere Mittel

Wir finanzieren unsere Publikationen durch Mitgliederbeiträge, Gönnerbeiträge, Spenden sowie Legate.

Unsere Publikationen

finden Sie unter: www.vsww.ch

Sie erreichen uns unter:
Verein Sicherheitspolitik und Wehrwissenschaft
Postfach 2407, 8021 Zürich 1
Internet: www.vsww.ch
Telefon: 044 266 67 67 oder Fax: 044 266 67 00

Spenden auf:

Credit-Suisse-Konto: CH36 0483 5046 8809 0100 0

Herzlichen Dank für Ihre Unterstützung!