Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 182 (2016)

Heft: 5

Artikel: Cyber : wäre es nicht endlich Zeit, dass...?

Autor: Bölsterli, Andreas

DOI: https://doi.org/10.5169/seals-587051

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 27.11.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Cyber: Wäre es nicht endlich Zeit, dass...?

Cyber? Der Begriff ist in aller Munde. Zu Recht, denn jeden Tag werden neue Angriffsbeispiele bekannt. Jetzt geht es aber nicht mehr um einfache Informatiksicherheit, sondern um eine dringend gewordene sicherheitspolitische Herausforderung.

Andreas Bölsterli, Chefredaktor

Die Zeit, in der es sich bei obiger Frage einfach um einen *«Hype»* handelt, ist definitiv vorbei. Welches ist aber nun die richtige Marschrichtung, um dieser Herausforderung die Stirn bieten zu können?

Das Cyber-Risiko und seine Trends

Im Bericht *«The Global Risks Report 2016»* des World Economic Forums werden die Kosten der Cyber-Kriminalität im Jahr 2014 vorgestellt: 445 Milliarden US$, ... beinahe 1% des Bruttoinlandsproduktes (BIP) aller Nationen zusammen! Wenn diese Tatsache uns nicht wachrüttelt, was braucht es denn dann? Stellen wir uns drei Fragen:

- **Wer ist betroffen und wer bezahlt?** Wir alle! Dafür gibt es unzählige Beispiele: Missbrauch von Bankkonten, böswillige Verschlüsselung der Daten einer Firma mit einer sogenannten *Ransomware,* Veröffentlichung von gehackten Daten, etc.; Die Liste ist unendlich. Ihre Firma wurde noch nicht angegriffen? Wahrscheinlich wissen sie es ganz einfach noch nicht...!
- **Wieso ist es überhaupt möglich?** Weil es gemäss den Spezialisten rentabel, einfach und gefahrenlos für den Angreifer ist! Zudem sind heute fast alle Bereiche des täglichen Lebens mit nur schwach gesicherten IKT-Technologien durchdrungen. Und mit dem *«Internet of Things»* wird es nicht einfacher, wenn wir mit Milliarden leicht angreifbarer und vernetzter Objekte konfrontiert werden!
- **Kann es schlimmer werden?** Ja! Und der *«Point of no Return»* wurde längstens überschritten, weil es eine Gesellschaft ohne IKT nie mehr geben wird. Und der Cyber-Raum ist vom Strom abhängig, einer Ressource, welche selber auf viele Bedrohungsformen (inkl. Cyber) anfällig ist. Was würde ein verlängerter Stromausfall bedeuten?

In den Medien geht es mehrheitlich um Kriminalität, Vandalismus und Spionage. Die Entwicklung zeigt jedoch, dass der Cyber-Raum zusätzlich zu den oben geschilderten Problemen auch für terroristische und kriegerische Zwecke ein durchaus lohnendes Instrument geworden ist. Die jüngsten Vorfälle zeigen sogar, dass die Anwendungsbarrieren, diesen Raum als Mittel der Kriegführung zu verwenden, verschwinden. Die Frage eines wirklich schwerwiegenden Angriffs lautet daher nicht «ob», sondern «wann».

«Ihre Firma wurde noch nicht angegriffen? Wahrscheinlich wissen sie es ganz einfach noch nicht...!»

Die neue Bedeutung des Begriffs «Verteidigung»

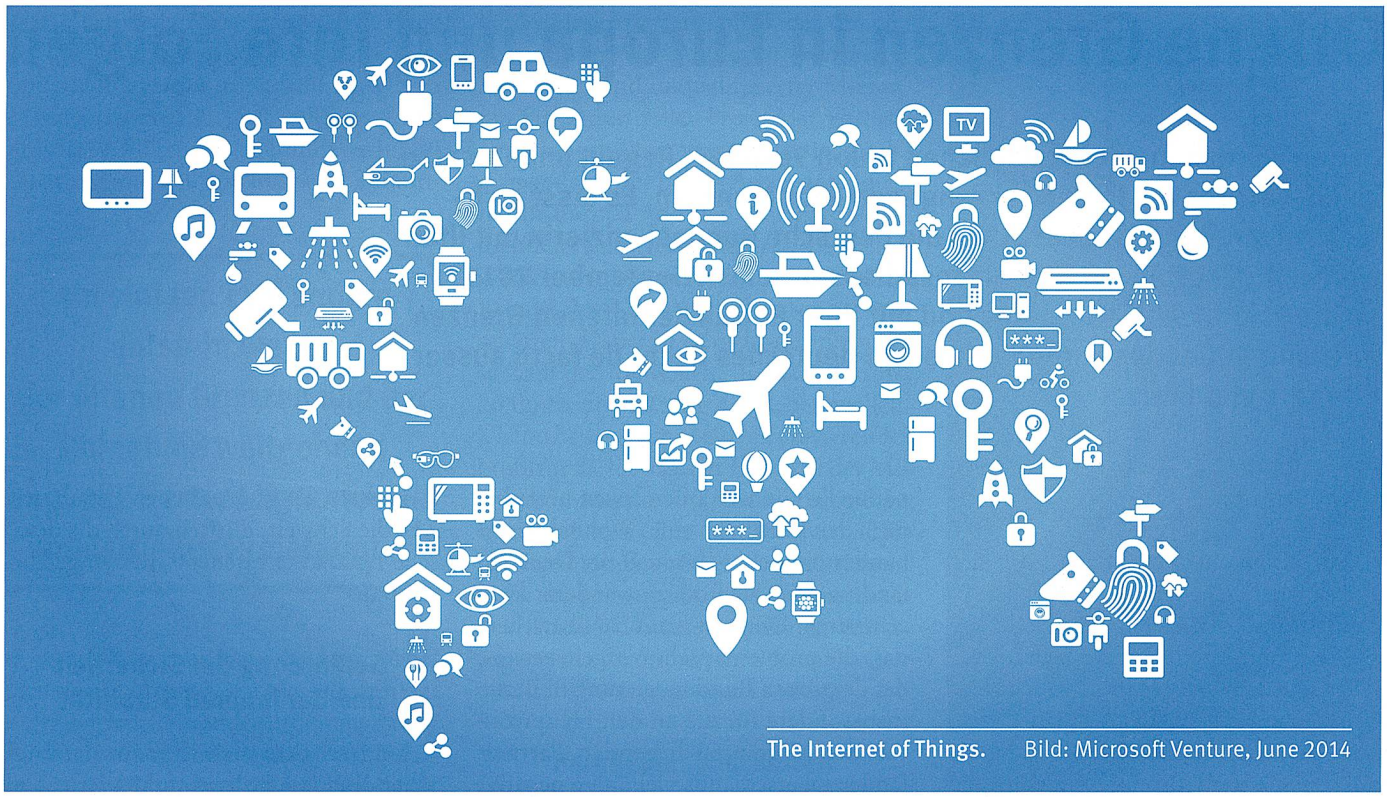
Wie die letzten Jahre weltweit gezeigt haben, ist der Krieg – leider – weder im Mai 1945 noch nach dem Zerfall der Berliner Mauer ausgestorben! Ganz im Gegenteil; Neben den bisherigen Mitteln wie Panzern und Kampfflugzeugen haben die neuesten technologischen und taktischen Entwicklungen weitere Elemente ins Spiel gebracht. Wörter wie «hybrid» oder «cyber» zeugen davon. So können zum Beispiel Angriffe gegen den Cyber-Raum[1] und somit gegen die damit verbundenen Prozesse in Wirtschaft und Gesellschaft enormen Schaden verursachen.

Sollen wir hier auch von einem Verteidigungsfall sprechen? Ja, wegen der neuen Definition des Begriffes «Verteidigung» des Bundesrates: Ein «Verteidigungsfall» ist dann gegeben, wenn die folgenden Argumente kumuliert zutreffen: a) konkrete Bedrohung der territorialen Integrität, der gesamten Bevölkerung oder der Ausübung der Staatsgewalt; b) zeitlich anhaltende Bedrohung, die über eine punktuelle zeitliche Bedrohung hinausgeht; c) landesweite Bedrohung, die über eine örtliche oder regionale Bedrohungslage hinausgeht; d) Bedrohung, die eine solche Intensität erreicht, dass sie nur mit militärischen Mitteln bekämpft werden kann. Somit ist klar, dass ein grossangelegter Cyber-Angriff gegen die Schweiz rasch zu einer «verteidigungsrelevanten Lage» eskalieren könnte.

Welche strategische Ausrichtung ist für die Schweiz angebracht?

Unsere Gesellschaft profitiert sehr von den Fortschritten des Cyber-Raumes. Eine Option *«zurück ins Mittelalter»* wäre, rein aus wirtschaftlicher Sicht, ein Suizid! Damit aber unsere Gesellschaft und Wirtschaft nicht handlungsunfähig gemacht wird, sind wir gezwungen, eine sichere, vertrauenswürdige und resiliente Cyber-Plattform zu etablieren. Denn ohne sichere Nutzungsmöglichkeit des Cyber-Raumes würde es keine Schweiz mehr geben.

Eine cyber-sichere Nation zu sein, wie es die Nationale Cyber-Strategie (NCS) fordert, ist zwar ein Muss, doch zuerst ist der gesellschaftliche Endzustand zu definieren. Dass heisst, vor der Erarbeitung der NCS braucht es Antworten auf die zwei Fragen, wie die strategische Ausrichtung des Landes in den Bereichen Industrie und Wirtschaft und wie eine dazugehörende Bildungs-, Forschungs- und Innovationsstrategie aussehen sollen. Denn ohne Köpfe, deren Ideen und Prozesse kommen wir nicht weiter – es geht hier um die Souveränität und Zukunft des Landes.



The Internet of Things. Bild: Microsoft Venture, June 2014

Welche «Instrumente» braucht die Schweiz?

- **Staatliche Governance:** Wer Anschluss zum Meer hat, braucht ein Marine-Ministerium! Wer versteht, dass der Cyber-Raum ein ähnliches Beispiel darstellt, sieht sofort, dass der Staat seine Souveränität mittels einer entsprechenden «Organisation für Digitale Affären» auf *strategischer Ebene* ausüben muss. Ob diese Organisation «Bundesamt für…» oder «Staatssekretariat für…» heissen soll, ist zum heutigen Zeitpunkt noch nebensächlich. Sicher ist, dass wir uns selber um unsere *Governance,* unsere Standards, usw. kümmern müssen. Darüber entscheiden heute Dritte und wir erleben im Bereich Cyber den massivsten Souveränitätsverlust unserer Geschichte;
- **Effektive Kompetenzen:** Wie viele Mittel braucht es, um die Gesellschaft auf die Cyber-Herausforderungen vorzubereiten? Um diese Frage zu beantworten, muss berücksichtigt werden, dass die Schweiz die 19. Wirtschaftsmacht der Welt ist, die über 580 000 Firmen «hostet», welche wiederum 5 Millionen Arbeitsplätze offerieren, dass unser Kleinparadies über eine sehr dichte Infrastruktur verfügt, welche fast vollständig von IKT abhängig ist. Der Bedarf an verantwortungsvollen Sicherheitsinvestitionen ist naheliegend. Der heutige Zustand dagegen, bei dem wenige Dutzende Spezialisten in mehreren kleinen Einheiten über die ganzen Bundesverwaltung verteilt sind, ist nicht zielführend. Jeder sorgt für die eigene Grundsicherheit und verriegelt seine Haustür, aber bei besonderen Ereignissen, die ausserhalb unsere Grund-Kompetenzen und -Kapazitäten liegen, kommt die Polizei, Feuerwehr, usw. Das Gleiche gilt für die Cyber-Sicherheit; die Grundversorgung obliegt jedem und jeder, aber darüber hinaus braucht es auf *taktischer und technischer Ebene* ein «Digitales-Sicherheitslabor» (D-Labor). Dieses D-Labor soll die Anstrengungen koordinieren und zu Händen der Schweiz eine Kompetenzplattform in der Form eines effizienten PPP *(Private Public Partnership)* aufbauen;
- **Wirksame Cyber-Verteidigung:** Die heutige zivile Organisation reicht kaum für die heutigen kleinen Vorfälle aus[2]. Für die gefährlichste Lageentwicklung ist sie überhaupt nicht gewappnet und somit für die Verteidigung des Landes völlig untauglich. Doch über die Kompetenzen und Fähigkeit zu verfügen, solche Aufgeben bewältigen zu können, ist zwingend. Denn wie die Diskussion zum Begriff «Verteidigung» zeigt, könnte sich die Schweiz extrem rasch in einer schwerwiegenden Lage befinden. Jetzt geht es einfach darum, der Armee klare Aufgaben und Mittel zuzuweisen und im Extremfall die Möglichkeit zu geben, die Mittel des D-Labors sowie ein starkes Milizsystem zu mobilisieren.

Wie weiter?

Die WEA, die Entwicklung der globalen Sicherheitslage im Allgemeinen und die des Cyber-Raumes im Speziellen, die wirtschaftlichen Bedürfnisse und Opportunitäten sowie die Überarbeitung der NCS und des SIPOL B 2016 stellen eine Reihe von guten Gelegenheiten dar, um das Thema Cyber endlich auf der richtigen Flughöhe zu behandeln.

Heute ist die Investition in die *Cyber-Verteidigung des Landes* zwingend. Das Argument der knappen Ressourcen, um damit die mangelnden materiellen und personellen Investitionen zu legitimieren (und sich so mit dem heutigen Dispositiv zufrieden zu erklären) ist unzulässig und nicht zu verantworten. Es ist zu hoffen, dass der neue Chef VBS die Cyber-Herausforderung ernst nimmt und die Bereitstellung der nötigen Instrumente möglichst rasch einleitet. ■

1 Solche Angriffe können nicht mit dem Radar entdeckt werden, erfolgen ohne Vorwarnzeit und in den meisten Fällen weiss man nicht einmal, wer die Täterschaft war.

2 Die Prozesse sind aber, beinahe vier Jahre nach der Veröffentlichung der NCS, noch nicht definiert und nicht trainiert.