www.jusletter-it.eu

Balthasar Glättli

Sicherheitspolitik im Informationszeitalter

Cyberkrieg und Cybersecurity: vom Bedrohungs-Mythos zur angemessenen Reaktion

In the security policy discussion, cyber threats as a new challenge are emphasized increasingly from the politically left as well as the right wing. But how does the threat situation really change in the information age? What are the right strategies? And what is the army's role in this? (ah)

Category: Essay
Region: Switzerland
Field of law: E-Government; E-Democracy; Data Protection

Citation: Balthasar Glättli, Sicherheitspolitik im Informationszeitalter, in: Jusletter IT 25 May 2016

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

1. Zwischen Naivität und Übertreibung

[Rz 1] Wer sich mit Sicherheitspolitik im Informationszeitalter beschäftigt, begegnet oft zwei gegensätzlichen Extremhaltungen.

[Rz 2] Auf der einen Seite herrscht vielerorts noch vollkommene Ahnungslosigkeit und Naivität. So schliessen nicht nur Private ihre Haustechnik ohne adäquate Sicherheitsmassnahmen ans Internet an. Auch die Steuerung industrieller Prozesse oder relevanter Infrastrukturanlagen ist oft nicht einmal auf die banalste Weise gesichert.

[Rz 3] Ende 2013 deckte die Sonntagszeigung auf, dass 2742 Steuerungen von Anlagen wie Kleinkraftwerken, Kläranlagen oder Produktionsbetrieben ohne besonderen Schutz online zugänglich waren, oft mit gar keinem oder nur mit einem Standartpasswort gesichert.[1]

[Rz 4] Dass solche Schwächen durchaus auch genutzt werden, illustrierte das Blatt ein gutes Jahr später mit einem simulierten Wasserkraftwerk, das als sogenannter Honeypot online ging. Innert nur dreier Wochen kam es zu 31 Ereignissen, vier davon dienten nicht nur der Erkundung, sondern hätten ein tatsächliches Kraftwerk konkret angegriffen. «Es braucht gutes Insiderwissen, um ein System zu hacken und Kraftwerke zu steuern», kommentierte damals Max Klaus von der Melde- und Analysestelle Informationssicherung des Bundes (MELANI) gegenüber der Zeitung, «doch viele kleinere Kraftwerke scheinen nur ungenügend geschützt.»[2]

2. «Cyberkatastrophe» als Mythos hat problematische Folgen

[Rz 5] Andererseits kann die Bedrohung einer Cyberkatastrophe oder eines Cyberkriegs zum eigentlichen Mythos werden. Sie wird dann unhinterfragt herangezogen zur Rechtfertigung für die digitale Aufrüstung von Armee und Nachrichtendienst und für die Errichtung einer Präventions- und Überwachungs-Infrastruktur. Myriam Dunn Cavelty verweist darauf, dass «in der Cyber-Narration zwei zentrale menschliche Ängste verknüpft [werden]: die Angst vor der Technik und die Angst vor dem Terrorismus.»[3] und die damit verbundene Problematik des unspezifischen Nichtwissens[4].

---

1 Florian Imbach / Alexandre Haederli, *Fahrlässig durchlässig*, SonntagsZeitung 30. November 2013, abrufbar unter: http://info.sonntagszeitung.ch/archiv/detail/?newsid=268454 (alle Internetadressen wurden zuletzt besucht am 25. April 2016), S. 13.

2 Barnaby Skinner, *Angriff auf die Stromversorgung*, SonntagsZeitung 8. Februar 2015, abrufbar unter http://www.sonntagszeitung.ch/read/sz_08_02_2015/nachrichten/Angriff-auf-die-Stromversorgung-27051, S. 10.

3 Myriam Dunn Cavelty, *Der Cyber-Krieg, der (so) nicht kommt – Erzählte Katastrophen als (Nicht)Wissenspraxis*, in: Leon Hempel / Marie Bartels (Hrsg.), Aufbruch ins Unversicherbare – Zum Katastrophendiskurs der Gegenwart, Bielefeld, S. 222.

4 Cavelty (Fn. 3), S. 224 ff.

[Rz 6] Sie warnt davor, dass das damit verbundene Gefühl eines umfassenden Kontrollverlusts zu missbrauchen: «Nichtwissen sollte jedoch nie als Katalysator und Beweis für die Notwendigkeit von zusätzlichen Sicherheitsanstrengungen verstanden und eingesetzt werden».[5]

[Rz 7] Genau diese Problematik ist allerdings in der aktuellen politischen Debatte nicht von der Hand zu weisen. So wird im Art. 37 des neuen Nachrichtendienstgesetzes (NDG), zu dem im Herbst 2016 noch eine Referendumsabstimmung stattfinden wird, der Nachrichtendienst des Bundes (NDB) ermächtigt, bei Cyberangriffen in ausländische Netzwerke und Computer einzudringen. Damit könnte der Bundesrat – ohne gesetzliche Informationspflicht gegenüber dem Parlament – auch Handlungen, welche völkerrechtlich als kriegerischer (Gegen-)angriff gewertet werden können, bewilligen.

3. Acht Thesen für eine realistische Cyber-Sicherheitspolitik

[Rz 8] Vor diesem Hintergrund ist es nötig, eine realistische Cyber-Sicherheitspolitik zu formulieren. Diese muss nötige und angemessene Sicherheitsmassnahmen vornehmen ohne gleichzeitig eine unbestimmte «Cyber-Gefahr» politisch zur militärischen Aufrüstung oder zur Delegation schwerwiegender Kompetenzen an den Nachrichtendienst zu missbrauchen.

[Rz 9] Voraussetzung dafür ist es, dass man die Besonderheit des Cyber-Raums beachtet:

- Im Cyber-Raum kann nicht einfach eine physische Landesgrenze verteidigt werden.
- Vielmehr ist einerseits ein Netzwerk zu schützen, welches heute von vielen verschiedenen meist privaten Anbietern erstellt und unterhalten wird.
- Andererseits sind die Angriffspunkte die an dieses Netzwerk angeschlossenen Systeme, welche wiederum meist von Privaten betrieben sind.

[Rz 10] Daraus ergeben sich bereits wichtige Schlüsse, welche ich thesenartig wie folgt zusammenfassen kann:

1. Die Aufgabe, Sicherheit im Cyber-Raum zu schaffen, kann nur als klassische Verbundsaufgabe angegangen werden, die sich Bund, Kantone, Gemeinden, vor allem aber auch Private miteinander teilen. Dabei ist zu beachten, dass wirtschaftliche Akteure über völlig unterschiedliche eigene Ressourcen verfügen. Während grosse Konzerne wie beispielsweise Banken und Versicherungen über eigene IT-Abteilungen verfügen und der Aufbau und Erhalt der notwendigen Kompetenzen zum Schutz der eigenen IT-Infrastrukturen mit zu ihren Kernkompetenzen zählen, sind mittlere und vor allem kleine Unternehmen mit dieser Aufgabe oft überfordert. Allerdings wäre es falsch, daraus den Schluss zu ziehen, dass der Staat ihnen diese Aufgabe abnehmen könnte oder gar müsste.
2. Eine vertrauliche Koordination der Informationen über aktuelle Angriffsvektoren und angemessene Reaktionen, wie sie die Melde- und Analysestelle Informationssicherung (MELANI) in einer geschlossenen Benutzergruppe von grossen Unternehmen anbietet, hat sich bewährt. Sinnvollerweise wäre allerdings die vollkommene Loslösung von MELANI vom Nachrichtendienst des Bundes (NDB) zu prüfen. Die Tatsache, dass der NDB auch im Informations-Austausch mit ausländischen Diensten steht, könnte sonst einzelne Akteure davon abhalten, ihre Kenntnisse offen auszutauschen.

5 Cavelty (Fn. 3), S. 228.

3. Zum Schutze mittlerer und kleiner Unternehmen und von Privatpersonen ist ein anderer Ansatz zielführender. Hier sollte der Bund für alle einfach einzusetzende Sicherheits-Technologien identifizieren oder – wo diese fehlen – ihre Entwicklung fördern. Ich denke dabei ein Projekte wie Pretty Easy Privacy (PEP), welches bewährte Verschlüsselungstechnologien durch Automatisierung des Schlüsselhandlings und eine benutzerfreundliche und einfach Oberfläche für KMU und Privatpersonen zugänglich macht. Mit einer leider aus Fristgründen abgeschriebenen Motion (13.4086) habe ich in diesem Sinne angeregt, ein Nationales Forschungsprogramm «Alltagstauglicher Datenschutz in der Informationsgesellschaft» zu lancieren – eine Neuauflage könnte auch weitere Aspekte der Cyber-Sicherheit miteinschliessen.
4. Auch gesetzliche Rahmenbedingungen können für bessere Sicherheit sorgen. Eine Möglichkeit, die sich gerade im Infrastrukturbereich aufdrängt, ist das Festschreiben von IT-Sicherheitsstandards. Deren Überprüfung kann Aufsichtsorganen übertragen werden, wo bereits solche existieren. So ist konkret nicht einzusehen, weshalb im Bereich der Stromversorgung zwar Regeln zur physischen Sicherheit von Anlagen bestehen, welche vom eidgenössischen Starkstrominspektorat überprüft werden, nicht aber Grundlagen für die Informationssicherheit. Auch Regelungen im Haftungsbereich können einen Teil der Verantwortung für Informatik-Sicherheit vom Anwender oder Betreiber auf den Anbieter verlagern. Wären Hersteller von Industriesteuerungsanlagen haftbar für allfällige Schäden, welche durch eine ungenügende Sicherung der Online-Zugänge entstehen, dann wären unverschlüsselte Webzugänge und simple Standardpassworte schnell verschwunden.
5. Die Militarisierung der Cybersicherheit ist nicht zielführend. Allerdings ist es sinnvoll und wichtig, dass die Armee ihrer eigenen Cybersicherheit die notwendige Beachtung schenkt und gegebenenfalls auch für die anderen Organisationen im Sicherheitsverbund ausfallsichere, vom Internet unabhängige und gehärtete Netzwerke anbietet.
6. Die Schweiz sollte sich weiterhin auf dem internationalen Parkett aktiv für gute Standards im Bereich Cybersecurity, vor allem aber auch für Grundrechte im Cyberraum einsetzen. Sie sollte energisch darauf hinarbeiten, dass ein völkerrechtlicher Rahmen für die Verurteilung, Aufklärung und Verhinderung von Cyberkriegs-Handlungen geschaffen wird.
7. Ebenso notwendig ist es auch, dass gewisse Software und Hardware, welche auch missbräuchlich zur Überwachung beispielsweise von Oppositionellen eingesetzt werden kann, gleich wie Kriegsmaterial resp. Dual-Use-Güter behandelt wird, damit ihr Export aus der Schweiz notfalls unterbunden werden kann.
8. Last but not least stellt sich die Frage des Umgangs mit unveröffentlichen Sicherheitslücken von IT-Systemen wie den sogenannten Zero-Day Exploits. Der Staat, vorab Polizei und Nachrichtendienste tragen mit dem Kauf oder der eigenen Herstellung von Staatstrojanern und anderen Mitteln zur Umgehung von Sicherheitsmassnahmen dazu bei, den Schwarzhandel mit solchen Sicherheitslücken zu fördern. Das ist falsch und sicherheitstechnisch höchst problematisch. Der Staat müsste vielmehr darauf dringen, dass Sicherheitslücken rasch geschlossen werden.

[Rz 11] Die grösste gesellschaftliche Verantwortung der politischen Akteure im Bereich der Sicherheit im Informationszeitalter liegt aber wohl darin, weder populistisch Ängste zu schüren noch umfassende militärische oder nachrichtendienstliche Kompetenzen im Cyberraum aufzubauen, welche doch nur eine vermeintliche Sicherheit garantieren können. Vielmehr gilt es, pragmatisch, die Sensibilität von wirklich handlungsfähigen Akteuren gegenüber Cyberrisiken ange-

messen zu erhöhen, bestehende Risiken zu minimieren und auch der Resilienz, also der Fähigkeit, mit Risiken umzugehen, die nötige Beachtung zu schenken.

Balthasar Glättli ist Nationalrat und Fraktionspräsident der Grünen, Mitglied der Sicherheitspolitischen Kommission (SiK-N) und der Staatspolitischen Kommission (SPK-N).