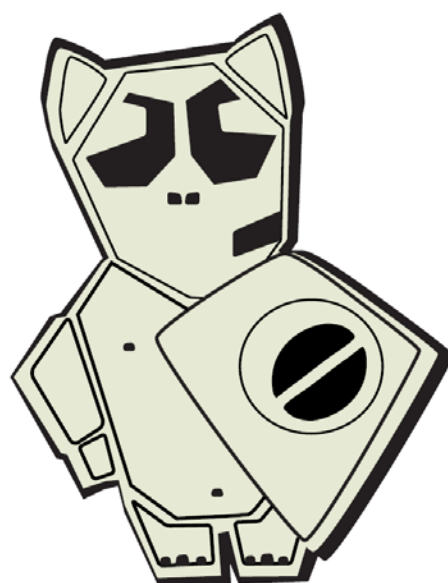


Schutz vor Cyberwar



Verabschiedet vom Präsidium am 12. November 2010

Die Art der Kriegsführung hat sich seit dem Ende des Kalten Krieges enorm gewandelt. Kriege finden heute nicht mehr nur zwischen Staaten statt. Spätestens der „Krieg gegen den Terrorismus“ hat gezeigt, dass auch zwischen Gruppen von Privaten und Staaten Kriege geführt werden. Obwohl heute enorme Ressourcenunterschiede zwischen Staaten und erst recht zwischen Privaten und Staaten bestehen, können sie doch gegeneinander (asymmetrische) Kriege führen. Militärische Operationen finden nicht mehr notwendigerweise auf dem offenen Schlachtfeld oder im Rahmen einer Guerilla-Aktion statt. ICT-Netzwerke spielen dabei eine wichtige Rolle. Für die Schweiz sind die aktuellsten Bedrohungen nicht mehr traditionelle Panzerdivisionen oder Luftangriffe, sondern Angriffe auf die digitale Infrastruktur unseres Landes. Unsere digitalen Netze sind unserer verwundbarste Stelle. Die Schweizerische Volkswirtschaft, unsere Infrastruktur ja gar unser Lebensraum kann durch einen Cyber-Angriff massiv beschädigt werden. Unser Verkehrswesen, die Stromversorgung, das Sozialversicherungssystem, die Banken – alles hängt am Netz und ist potentiell manipulierbar. Unser Land könnte von einem Tag auf dem anderen sprichwörtlich ins Mittelalter zurückgeworfen werden. Wir fordern deshalb:

- **Schutz der Kommunikationsnetzwerke und Daten als Staatsaufgabe:** Tagtäglich finden tausende kriminell motivierte Angriffe auf die Kommunikationsnetze und Daten der Schweiz statt. Unsere Wirtschaft sowie staatliche Behörden erleiden dadurch massive Schäden. Wissen wird gestohlen (Produktpiraterie), betrügerische Machenschaften ermöglicht, die Arbeit von unzähligen Mitarbeitern für Stunden verlangsamt oder gar unterbrochen. Der Schutz der Kommunikationsnetze und Daten der Schweiz und ihrer Wirtschaft muss deshalb zu einer Staatsaufgabe auf Verfassungsebene werden.
- **Kapitel zu Cyberwar im Sicherheitspolitischen Bericht:** Als erstes ist nachzuholen, was der Bundesrat im sicherheitspolitischen Bericht versäumt hat: Das Thema Cyberwar ist gründlich zu analysieren, einschliesslich der fließenden Übergänge von Cybercrime und Cyberwar. Ebenfalls müssen Massnahmen zur Prävention und Bekämpfung bestehender und zukünftiger Bedrohungen von cyberterroristischen Organisationen und Gruppen formuliert und ein konkreter Plan zu deren Umsetzung vorgelegt werden.
- **Konzept zum Schutz der digitalen Infrastruktur der Schweiz:** Es soll ein Konzept vorgelegt werden, wie die vereinigten Sicherheitskräfte unseres Landes – einschliesslich der Armee – befähigt werden, im Verbund mit Wirtschaft und Forschung die Fähigkeit zum Schutz der gesamten digitalen Infrastruktur der Schweiz zu erlangen. Der stetige Kampf im Internet ist eine Kernaufgabe der Sicherheitskräfte im 21. Jahrhundert. Welche Aufgaben die Armee in welcher Organisationsform

im Verbund wahrnehmen wird, muss das Konzept zeigen. Sicher aber ist der Auftrag „die Armee schützt sich selbst“ auch im Zusammenhang mit Cyberwar ungenügend.

Definitionen

Um ein besseres Verständnis der Thematik zu ermöglichen, hier wenige grundlegende Definitionen:

Cyber-Angriff, Cyber-Attacken: Es sind viele Formen solche Angriffe möglich - das Spektrum reicht vom reinen Bemühen, Rechner funktionsuntauglich zu machen bis hin zum Ziel der Spionage.

Cybercrime, Netzwerkkriminalität, Internetkriminalität, kriminelle Machenschaften im Internet: Verschiedene Begriffe für kriminelle Handlungen, die ausschliesslich oder teilweise mit Hilfe der Informations- und Kommunikationstechnologie begangen werden. Kriminelle Handlungen, die im und um das Cyberspace von Privaten mit Mitteln aus der Informationstechnologie verübt werden und „strafrechtlich“ relevant sind.

Cybespace / Virtuelle Welt: Als virtuell bezeichnet man eine Entität (etwas), die (das) zwar physisch nicht existiert, aber dennoch Wirkung entfaltet. Diese virtuelle Welt heisst auch *Cyberspace*. Computer verbinden Menschen, Maschinen etc. in unzähligen sehr schnellen und vor allem unsichtbaren Formen.

Cyberwar: Cyberwar ist Kriegführung im virtuellen Raum (s.d.), vorstellbar als reine eine Ballung von computergestützten Angriffshandlungen auf verschiedene kritische Infrastrukturen der Schweiz, oder als Teil eines umfassenderen Angriffskonzepts, das beispielsweise auch rechtliche, wirtschaftliche oder gar klassisch militärische Sanktionen & Drohkulissen einschliesst. Es werden alle Tätigkeiten zusammengefasst, die sich gegen den Staat, seine Institutionen, seine Integrität, gegen die Bevölkerung oder Teile davon richten und diese existentiell bedrohen können. Cyberwar wird von Staaten, parastaatlichen oder terroristischen Organisationen geführt.