Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 177 (2011)

Heft: 3

Artikel: Cyberwar : Krieg der Neuzeit

Autor: Arcioni, Sandro

DOI: https://doi.org/10.5169/seals-154223

Cyberwar: Krieg der Neuzeit

Der Begriff «Cyberwar» stammt leider nicht aus Videospielen oder einer anderen virtuellen Welt. Er bezeichnet eine neue Kriegführung und ist real, seit einigen Jahren sogar existent.

Sandro Arcioni

Aus ökonomischer Sicht sind Unternehmen seit zwanzig Jahren Zielscheibe von «Terroristen» oder korrupten Personen: Ob böswillige Konkurrenten, ob Studenten auf der Suche nach «einem Titel» oder durch die Presse, durch Operationen von Regierungen oder durch die Mafia. Angriffe durch Viren oder «Trojanische Pferde» entstanden bereits zu Beginn der 90er Jahre. Das IT-Management entwickelte die Möglichkeit, mit solchen Angriffen umzugehen.

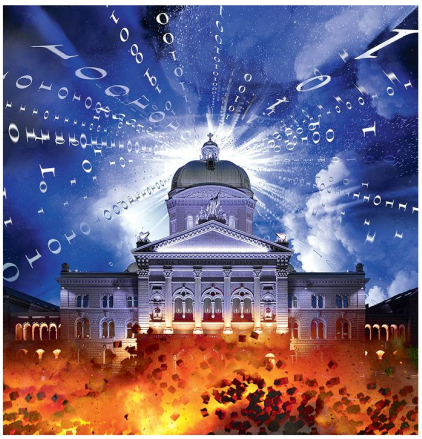
Unterdessen haben sich auch militärische Kreise mit den notwendigen Mitteln ausgestattet, ihre Informationssysteme wie CERT (Computer Emergency Response Team) unter den Schutz der NATO zu stellen, zumal sie selbst Anwender von zivilen Computersystemen sind, diese aber zu militärischen Zwecken nutzen.

Im Gegensatz zur Wirtschaftwelt gehört die Armee teilweise zum politischen Umfeld einer Nation. Um die gewünschten Effekte durch Cyber-Attacken zu verstehen, müssen zur Erklärung des Cyberwars die asymmetrische Bedrohung (nachstehend definiert), der Cyberterrorismus und die Einfluss-Faktoren (IO in der US Army) betrachtet werden.

Was bedeutet Cyberwar?

Der Cyberwar (cyberwarfare) oder Informatik-Krieg gebrauchen Computer und Internet, um einen Krieg im Cyberspace zu führen. Der Cyberspace, bestehend aus einem Netzwerk von Vernetzungen, unterscheidet sich vom physischen Raum durch folgende Faktoren: grenzenlos, ausdehnbar, anonym; die korrekte Identifikation des Angreifers ist heikel. Der Einsatz von Cyberwar betrifft Bereiche von Politik, Zivilbevölkerung, Militär und Ökonomie. Der Cyberwar stellt Herausforderungen in vier Bereichen dar: technisch, juristisch, kulturell und geopolitisch.

Einige Überlegungen sind zu berücksichtigen. Cybernetische Waffen sind allen zugänglich und verbreiten sich unkontrollierbar. Keine technologische Barriere, finanztechnischer oder juristischer Natur, kann deren Vervielfältigung verhindern. Der Konflikt im Cyberspace ist asymmetrisch zugunsten des Angreifers. Dieser kann die neuesten technologischen Entwicklungen leicht beschädigen, während der Angegriffene dauerhaft, alle ihm zur Verfügung stehenden Sicherheitsvorkehrungen, in Bezug auf die bestehende Bedrohung, aufrechterhalten muss.



Asymmetrische Kriegführung besteht hauptsächlich aus Terrorismus und ist von der Kriegführung zwischen Staaten zu unterscheiden.

Die asymmetrische Bedrohung dieses Krieges, welche der amtlichen Armeeführung eines Staates unbedeutende materielle Kriegsteilnehmer entgegenstellt, besteht darin, die Schwachpunkte des Gegners zu nutzen, um eigene Ziele zu erreichen. Letztere sind meist politischen oder religiösen Inhaltes. Asymmetrische Kriegführung besteht hauptsächlich aus Terrorismus und ist von der Kriegführung zwischen Staaten zu unterscheiden. Im Cyberwar kann der Cyberterrorismus auch als der vorsätzliche Gebrauch von störenden Aktivitäten oder die Bedrohung durch dieselben, gegen Computer und/oder Netzwerke, definiert werden. Stets in der Absicht, einen Schaden zu verursachen, sei dies nun sozial, ideologisch, religiös, politisch oder andere Gesichtspunkte betreffend. Der Cyberwar beinhaltet aber auch Einschüchterungsmanöver jeglicher Personen, die solche Gesichtspunkte vertreten.

Welche Informations-Operationen gibt es?

Von Seiten der US Armee beinhalten diese Informations-Operationen (IO) den gesamten Gebrauch militärischer Waffen, militärische Unterstützungen sowie alle Aktionen und Einwirkungen, welche dem Schutz unserer eigenen Informationen dienen. Ziel bleibt die Beeinflussung, Störung, Vernichtung, widerrechtliche Aneignung, ja sogar Neutralisierung gegenteiliger humanistischer Ansichtspunkte. Letztendlich stellt auch die Automatisierung (elektronische Kriegsführung) eine Informations-Operation dar.

Der französische General, Marc Watin-Augouard, General-Inspektor von Armee und Polizei, soll gesagt haben: «Der Cyberspace ist grenzenlos. Die Geschwindigkeit, mit welcher eine Information verbreitet werden kann, komprimiert die Verhältnisse in Raum und Zeit. Die Herausgabe eines öffentlichen Befehls im Cyberspace folgt nach anderen Zeitverhältnissen, als ähnliche Vorgänge im physischen Raum.»

Die Sperrung und Blockade von Computer-Ressourcen, also Kommandozentralen oder Zentralen zur Informations-Übermittlung, ist eine Praxis, welche von all denen gefürchtet ist, welche sich mit der Computer-Sicherheit beschäftigen. Computer-Viren stellten die erste Armee dieses Typus dar.

Mit diesen Auswirkungen zielt der Cyberwar weder auf die Zerstörung von Menschen, noch auf solche von physikalischen Einrichtungen. Hingegen verursacht er eine Lähmung der Nervenzentren. Es ist daher notwendig, die Wirkung der nicht-tödlichen Handlungen auf das Verhalten des Gegners zu verstehen. Nichtkriegerische Elemente der Streitkraft werden somit an Bedeutung zunehmen und stellen die ersten Techniken, die eingesetzt werden, dar (z. B. Cyber-Kriegfüh-

rung, elektronische Kriegführung, Informations-Operationen, Einfluss-Operationen, usw.). Das Kommunikations-Management wird der entscheidende Faktor bezüglich der angestrebten Auswirkungen sein. Zu diesem Zweck wird das Kommunikations-Management nicht einer parallelen Einheit anvertraut, sondern im globalen Manöver integriert werden.

Gemäss Definition der amerikanischen Armee, aber auch nach vielen anderen Armeen, wie z. B. der Chinesischen (PLA «People's Liberation Army»), ist das globale Manöver der iterative Prozess der Zielerreichung einer gewünschten, endgültigen Auswirkung und ermöglicht dem Chef, die Auswirkung auf Gegner und Umwelt sowohl zu bestimmen, zu erhalten und zu bewerten. Dies wird durch die Umsetzung nicht-militärischer oder militärischer Fähigkeiten auf allen Ebenen eingesetzter Kräfte erreicht. Der Prozess impliziert alle Zellen eines Generalstabs oder Befehlsstandes einer grossen Einheit und zielt darauf ab, direkt oder indirekt, die Schwerkraftzentren oder Verwundbarkeitspunkte des Gegners durch nicht-physikalische oder physikalische Auswirkungen zu erreichen.

In diesem Sinne besteht die Armee der Computer-Eindringlinge des Cyberwars (definiert als Cyber-Attacke) aus:

- Boshaften Programmen (Virus, Wurm, Trojanisches Pferd, …);
- Technischen Angriffen durch Mitteilungen (Spams, Phishing, …);
- Netzangriffen (Sniffing, Bedienungsverweigerung, …);
- Angriffen auf Password (Crackage, Angriffe durch Wörterbücher, …);
- Netz-Kartierung (Ping, Port Abtastung, SNMP, Nessus, …);
- Technik der System-Aufschaltung (erhöhte Privilegien, Spurenverwischung);
- Anderen Angriffsmodi (Reversengineering, Cryptoanalyse, Snarfing, Cookies, …);
- Flucht-Technik (Poisoning, Spoofing, …).

Sich eines oder mehrerer Mittel bedienend wie Diebstahl, Unterschlagung von Geld, Blockade von neuralgischen Punkten, Verschmutzung von Kommunikationsnetzen, Telekommunikation und Energie, Schwächung oder Übernahme von gegnerischen Systemen, etc. … immer aber ein Endziel verfolgend, das der politischen/militärischen oder wirtschaftlichen Situation des Ziellandes angepasst ist.

Wie sieht die Vorbereitung aus?

«Cybersicherheit ist die Prävention der Sicherheits-Risiken gebunden an die Benutzung von Informations-Technologien. Somit ist sie ein Verschluss-Schieber zur Risiko-Intelligenz, selbst Anteil der Wirtschafts-Intelligenz», sagte Herr Bernard Besson, Animator des wirtschaftlichen Intelligenz-Zentrums von «MEDEF Ouest parisien». Militärisch gesehen stellt die Wirtschafts-Intelligenz die Durchführung von Informations-Operationen (InfoOps) dar.

Die Leitung der Operationsinformationen (Arcioni S., ASMZ 4/2010) besitzt sowohl Mittel zur defensiven, als auch zur offensiven Führung, wie :

- Sicherheitsinformations-Operationen: Massnahmen zum Schutz und zur Verteidigung von Information und Informationssystemen durch die Gewährleistung von Verfügbarkeit, Benutzung, Authentifizierung, Vertraulichkeit, Nachweisbarkeit und Datenintegrität. Sie berücksichtigt die Reaktionsfähigkeit und die Wiederherstellungsmöglichkeit von Informationssystemen.
- Der elektronische Krieg: Massnahmen zum Schutz von Informationssystemen (Verfügbarkeit der gesamten Informationssysteme, etc.).
- Die Operationen spezieller Informationen: Operationen, die auf nicht letalen Massnahmen basieren, z. B. auf ökonomischen Akteuren und finanziellen Gegnern.

Was sagt der Armeebericht 2010?

Der Armeebericht 2010 spricht ganz einfach gar nicht von «Cyberwar»! Er macht vage Aussagen über Angriffe auf IT-Infrastrukturen, konzentriert sich auch mehr auf elektromagnetische Angriffe! Und für den Rest rät die Armee zu «Leistungen», wie der Einrichtung einer temporären Infrastruktur. Nur in Punkt 4.2.3 dieses Berichts heisst es:

«Nötigung oder Erpressung ist eine sicherheitspolitische Bedrohung mit hoher Wahrscheinlichkeit. Sie kann ihren Ursprung im In- oder Ausland haben. Auch mit geringem Potenzial kann massiver Schaden bewirkt werden. Durch Aktionen gegen Personen, Informatikinfrastrukturen, Transportmittel wie Schiffe oder Schweizer Vertretungen im In- und Ausland, können die Sicherheit und weiterer Interessen der Schweiz gefährdet werden. Die Bewältigung solcher Ereignisse ist in einer Linie eine Sache der zivilen sicherheitspolitischen Instrumente, v. a. der Aussen- und Wirtschaftspolitik und der Polizei. Aber die Armee kann einen Beitrag leisten; sie kann z. B. Mittel zur Verfügung stellen, um Schutz- oder Transportaufgaben zu Land, Wasser und in der Luft zu übernehmen … und damit die zivilen Polizeikräfte unterstützen. Im Extremfall könnte sich eine solche Bedrohung bis zu einem indirekten Krieg gegen die Schweiz entwickeln, wenn etwa ein nicht staatlicher Akteur von einem anderen Staat unterstützt und dadurch in die Lage versetzt würde, vielfältige Mittel und moderne Waffen einzusetzen …».

Von diesem Paragraphen abgesehen, werden keinerlei konkrete Schritte vorgeschlagen. Die Schweizer Armee arbeitet in diesem Text nur reaktiv. Würden gegen die Schweiz Aktionen, die zum Cyberwar führen, gerichtet, wäre es leider zu spät, um zu reagieren!

Der französische General Vincent Desportes, ehemaliger Direktor der Schule für Verteidigungsstreitkräfte (CID) sagte: «Eine Armee, aus deren Gedankengut das kritische Denken verbannt ist, ist geschwächt und angreifbar». Nach diesen Worten von General Desportes liegt es an unseren Politikern, vom Militär eine umfassende und gründliche Analyse der Bedrohung zu verlangen. Aufgrund dieser Analyse hat der zuständige Departementschef einen Bericht zu verfassen, der die modernen Bedrohungen angemessen berücksichtigt und beispielsweise den Cyberwar, den Cyber-Terrorismus und die asymmetrischen Bedrohungen ausführlich behandelt. Dazu gehören auch konkrete Massnahmen, die geeignet sind, diesen Bedrohungen zu begegnen oder diese mindestens einzuschränken. Es sind diese letzteren, welche die Ressourcen und Budgets bestimmen, welche das VBS in den kommenden Jahren benötigt, nicht eine zufällig gewürfelte Zahl benötigter Truppen, um den einen besprochenen Punkt zu ermöglichen: die Entlastung des Budgets des VBS! ■

Oberstlt
Sandro Arcioni
Dr. ès sc.
Unternehmer
Experte der Info Ops
6715 Dongio TI