Herrscht Cyberwar?

Herrscht Cyberwar?

Nach den Angriffen von WikiLeaks-Sympathisanten auf die PostFinance und andere Finanzdienstleister war der Cyberwar einmal mehr in aller Munde. Aber herrscht denn nun wirklich Krieg im Cyberspace?

Bruno Blumenthal

Die Waffen dieses Krieges sind Exploits (Software-Sicherheitslücken), Viren oder Bot-Netzwerke, um nur einige zu nennen. Es ist unbestritten, dass genau solche Waffen im Cyberspace ständig für Angriffe auf Firmen und Behörden verwendet werden. Von einem Krieg im Sinne eines bewaffneten Konflikts zwischen zwei Staaten kann jedoch kaum die Rede sein.

Um die Frage nach Krieg im Cyberspace zu klären, muss man diese Angriffe also etwas differenzierter betrachten. Für die Einordnung eines Angriffs sind stets die Motivation der Täter und der verursachte Schaden mit einzubeziehen. Demnach handelt es sich beispielsweise bei den Aktionen von Anonymus gegen PostFinance als Reaktion auf die Schliessung des WikiLeaks-Spendenkontos eher um die virtuelle Form einer Sitzblockade von Demonstranten vor einer Postfiliale und sicher nicht um eine kriegerische Handlung. Was das Ganze so bedrohlich erscheinen lässt, ist die Tatsache, dass die Demonstranten dazu nicht vor die Haustüre gehen mussten. Ausserdem waren dabei erst noch alle Kunden betroffen und nicht nur diejenigen einzelner Filialen, wie dies bei einer realen Sitzblockade der Fall wäre.

Vom digitalen Vandalismus zum Krieg im Netz

Vandalismus und Protestaktionen im Cyberspace sind keine neuen Phänomene. Website Defacements, bei denen der Internetauftritt einer Firma oder Organisation durch eine Parole ersetzt wird, gibt es schon fast so lange wie das Internet selber. Durch die Kommerzialisierung des Internets hat zwar deren Bedeutung zugenommen, die grössten Probleme und Schäden im Internet entstehen aber durch die organisierte Kriminalität. Mit Erpressung, Identitätsdiebstahl und Betrug werden riesige Summen erwirtschaftet. Einige Schätzungen gehen davon aus, dass dabei mehr Geld umgesetzt wird als im gesamten Drogenhandel weltweit. Verwundbare Webseiten werden mit Malware verseucht und greifen so die Besucher der Seite an. Diese Angriffe werden immer gezielter und technisch raffinierter. Denn solange sich damit Geld verdienen lässt, schrecken Kriminelle auch nicht vor gros-

sem technischem und logistischem Aufwand zurück.

Die organisierte Kriminalität ist jedoch bei weitem nicht die einzige Bedrohung im Cyberspace. Für die Nachrichtendienste ist dieser schon seit langem eine wichtige Informationsquelle für die passive Ermittlung im Kampf gegen Terrorismus und andere Bedrohungen gegen den Staat. Einige Nachrichtendienste nutzen aber auch die Möglichkeiten des Netzes, um sich aktiv unerlaubten Zugang zu Informationen zu verschaffen. Auch das ist keinesfalls ein neues Phänomen. Bereits Mitte der 80er-Jahre wurde ein spektakulärer Fall aufgedeckt, bei dem deutsche Hacker gegen Bezahlung für den KGB massenhaft in amerikanische Rechner eingedrungen waren, um sensible Daten zu entwenden. Seither wurden immer wieder Angriffe entdeckt, welche mehr oder weniger eindeutig als Tat staatlicher Akteure identifiziert werden konnten. Auch die Schweiz wurde schon Opfer solcher Angriffe. Diese Attacken werden in den Medien oft als Zeichen für den Cyberwar gewertet; allerdings handelt es sich dabei wohl eher um unerlaubten Nachrichtendienst denn um einen bewaffneten Angriff, was völkerrechtlich eindeutig unter der Kriegsschwelle liegt.

«Diese Angriffe werden immer gezielter und technisch raffinierter.»

Kosovo, Estland, Georgien, Iran

Die Frage, was ein bewaffneter Angriff im Sinne des Völkerrechts und damit eine kriegerische Handlung im Cyberspace ist, ist nicht abschliessend beantwortet. In der jungen Geschichte des Cyberspace wurden schon verschiedenste Ereignisse als erster Cyberwar betitelt. Als populärstes Beispiel gelten sicherlich die Attacken gegen Estland im Sommer 2007. Bereits 1999 war aber im Zusammenhang mit den NATO-Angriffen im Kosovo auch schon vom ersten Cyberwar gesprochen worden. Der damalige NATO-Kommandant General Wesley Clark war allerdings der Meinung, dass man in diesem Bereich noch mehr hätte tun können. Wegen der rechtlich unsicheren Situation und den schwer abzuschätzenden Folgen solcher Angriffe wurde jedoch davon abgesehen. So waren es am Ende primär die Amerikaner, die im Internet unter Angriffen zu leiden hatten. Nach dem versehentlichen Beschuss der chinesischen Botschaft wurden amerikanische Webseiten – unter anderem die des Weissen Hauses – von chinesischen Hackern angegriffen. Der angerichtete Schaden war zwar deutlich geringer als derjenige in Estland 2007, die Ereignisse sind aber durchaus vergleichbar. In beiden Fällen ist davon auszugehen, dass die jeweiligen Regierungen von China bzw. Russland wohl nicht direkt an den Angriffen beteiligt waren, diese aber zumindest geduldet haben.

Im Konflikt um Ostossetien, zwischen Russland und Georgien, kam es begleitend zum Einmarsch der russischen Truppen zu Attacken im Cyberspace. Das Timing der Angriffe deutet darauf hin, dass die Angriffe vom Kreml zumindest indirekt koordiniert wurden, auch wenn dies offiziell dementiert wird.

Bei all den genannten Angriffen normalisierte sich die Lage relativ schnell

wieder und es entstand kein nachhaltiger Schaden.

Im Falle von Stuxnet ist die Situation etwas anders. Erstmals wurde ein Fall bekannt, bei dem durch einen Angriff in der virtuellen Welt offenbar ein konkreter Schaden in der physischen Welt entstand. Auch wenn viele Details zum angerichteten Schaden und der Motivation des Angriffs nach wie vor spekulativ sind, deutet vieles darauf hin, dass diese Malware gezielt für einen Angriff auf die iranischen Atomanlagen in Natanz und Bushehr entwickelt wurde. Ein solcher Fall von Sabotage hat eine ganz neue Qualität und kann mit einem gezielten Militärschlag verglichen werden. Die grosse Komplexität des Angriffs und die Tatsache, dass kein direkter finanzieller Gewinn für den Angreifer ersichtlich ist, machen einen Einzeltäter oder eine kriminelle Organisation als Urheber äusserst unwahrscheinlich. Man muss daher davon ausgehen, dass es sich dabei tatsächlich um einen staatlich geführten Militärschlag mit Mitteln des Cyberwar handelt.

Cyberwar als Bedrohung für die Schweiz?

Der Chef der Armee, André Blattmann, und Verteidigungsminister Ueli Maurer bezeichneten den Cyberwar in den letzten Monaten als die grösste Bedrohung für unser Land. Damit haben sie sicher recht, leben wir doch in einer stark von Technologie abhängigen Gesellschaft. Auch wenn es unwahrscheinlich ist, dass ein anderer Staat den offenen Krieg mit der Schweiz sucht, so sind Angriffe im Cyberspace sicher wahrscheinlicher als ein bewaffneter Konflikt im klassischen Sinn.

Es ist daher absolut richtig, dass man sich im Rahmen der Sicherheitspolitik mit dem Thema Cyberwar intensiv auseinandersetzt. Wie der Bundesrat bereits deutlich gemacht hat, ist die Schweiz heute nicht in allen Bereichen ausreichend gegen Bedrohungen aus dem Cyberspace gewappnet.

Auch wenn also im Cyberspace noch kein Krieg herrscht, ist der Aufbau der entsprechenden militärischen Fähigkeiten, um im Cyberspace zu operieren, für eine zeitgemässe Armee zwingend notwendig. Erste Schritte wurden in den letzten Jahren auch in der Schweiz eingeleitet. Im Vergleich zu anderen Nationen besteht aber noch einiger Nachholbedarf. Zudem ist die Diskussion zu führen, in welcher Form die Schweiz dabei auch aktive Fähigkeiten zur Aufklärung oder gar zum Angriff im Cyberspace entwickeln sollte. Anhand der Diskussion müssen dann die entsprechenden gesetzlichen Grundlagen geschaffen werden, um Operationen im Cyberspace zu regeln. Im Parlament wurden in dieser Richtung auch schon verschiedentlich Vorstösse gemacht und der Bundesrat befasst sich entsprechend auch schon seit einiger Zeit mit dem Thema.

«Auch wenn es unwahrscheinlich ist, dass ein anderer Staat den offenen Krieg mit der Schweiz sucht, so sind Angriffe im Cyberspace sicher wahrscheinlicher als ein bewaffneter Konflikt im klassischen Sinn.»

Die grösste Bedrohung für die Sicherheit der Schweiz ist zurzeit jedoch nicht ein militärischer Angriff im Cyberspace, sondern organisierte Kriminalität und die wirtschaftliche und politische Spionage. Diese Bedrohungen liegen nicht im Aufgabengebiet der Armee, sondern bei den Polizeibehörden respektive der Spionageabwehr des Nachrichtendienstes.

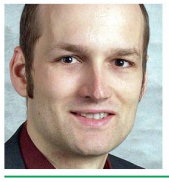
Da die Technologien und Methoden der Angreifer in all diesen Fällen zumindest ähnlich sind, ist hier eine Zusammenarbeit und ein Erfahrungs- und Informationsaustausch von zentraler Bedeutung. Diese Zusammenarbeit darf sich nicht nur auf staatliche Akteure beschränken, sondern muss auch mit privaten Unternehmen erfolgen. Schliesslich ist ein Grossteil der nationalen kritischen Informationsinfrastruktur, wie beispielsweise die Energieversorgung und die Finanzwirtschaft, in privater Hand. Der Bund hat mit MELANI (Melde- und Analysestelle für Informationssicherung) bereits 2004 eine Stelle geschaffen, welche heute im Rahmen einer Public Private Partnership in einem geschlossenen Kundenkreis mit Betreibern von nationalen kritischen Infrastrukturen zusammenarbeitet. MELANI unterstützt die privaten Firmen beim Schutz ihrer Infrastruktur mit Informationen und Mitteln, welche privaten Anbietern nicht direkt zur Verfügung stehen.

Fazit

Auch wenn im Cyberspace noch kein Krieg ausgebrochen ist, ist die Bedrohung aus dem Cyberspace für die öffentliche Sicherheit real und darf nicht unterschätzt werden. Es sind dringend entsprechende Massnahmen gegen diese Bedrohung einzuleiten und Kapazitäten für deren Abwehr zu schaffen. Obwohl noch einiges getan werden muss, ist die Schweiz bereits auf dem richtigen Weg, sich vor Angriffen aus dem Cyberspace, sowohl kriegerischer als auch krimineller Natur, effizient zu schützen. Das Bewusstsein gegenüber der Bedrohung ist allerdings noch nicht bei allen relevanten staatlichen und privaten Akteuren gleichermassen vorhanden. Es ist zu hoffen, dass sich dies in nächster Zeit ändert und die notwendigen Ressourcen für den Schutz der kritischen Informationsinfrastrukturen zur Verfügung gestellt werden. ■

Im Volksmund wird unter Cyberwar meist fälschlicherweise ein Krieg verstanden, der nur im Cyberspace – also in einem virtuellen Raum wie zum Beispiel dem Internet – stattfindet. Diese Vorstellung ist jedoch falsch. Schon früh wurde der Wert des virtuellen Raums als fünfte Domäne der Kriegsführung erkannt. Operationen im Cyberspace dienen dabei unterstützend zu den klassischen Domänen Land, Wasser, Luft und Weltraum.

Computer Network Operations (CNO) ist eine der fünf Kernaktivitäten im Rahmen von Information Operations. Die Schweizer Armee arbeitet im Rahmen von Computer Network Defense (CND), einem Teilgebiet von CNO, zusammen mit RUAG Defence an wegweisenden Methoden und Lösungsansätzen, um der zunehmenden Bedrohung aus dem Cyberspace entgegenzuwirken. Bei den Lösungen handelt es sich um neuartige Algorithmen und Methoden zum Schutz vor Malware, Bot-Netzen und anderen Bedrohungen aus dem Cyberspace. Die Erkennung von Bedrohungen in Hochgeschwindigkeitsnetzwerken in Echtzeit steht dabei im Zentrum.



Wm
Bruno Blumenthal
Dipl. Ing. FH Informatik
RUAG, IT Security Architect
3000 Bern 22