CSS Analysen zur Sicherheitspolitik

CSS ETH Zurich

Nr. 71 • April 2010

CYBERWAR: KONZEPT, STAND UND GRENZEN

Politische, wirtschaftliche und militärische Konflikte werden immer mehr auch im Cyberspace ausgetragen. Cyberwar umfasst konzeptionell allerdings nur einen engen Teilbereich aller Cyberkonflikte. Auf der operativen Ebene sind Cyberwar-Fähigkeiten von zunehmender Bedeutung. Strategische IT-Kriege, die sich nur noch im virtuellen Raum abspielen, bleiben jedoch unwahrscheinlich. Für Staaten wie die Schweiz besteht vor allem im Bereich der Cyberverteidigung Handlungsbedarf.

Istock.com

Die Bedeutung des Informationsraums als Ort der Konfliktaustragung hat in den letzten Jahren zugenommen. Ein Teil jedes politischen, wirtschaftlichen und militärischen Konflikts findet heute im Internet statt. In diesem Zusammenhang ist «Cyberwar» zu einem viel benutzen Schlagwort geworden. Oft wird damit jede Auseinandersetzung im Cyberspace mit internationaler Dimension bezeichnet. Eine solch breite Verwendung des Begriffs ist jedoch wenig sinnvoll. Stattdessen ist eine konzeptionelle Kategorisierung verschiedener Konfliktformen im Cyberspace nötig. Erst auf dieser Basis lassen sich die konkrete Gefahr und deren Tragweite einschätzen, Verantwortlichkeiten zuweisen, präventive und reaktive Gegenmassnahmen implementieren und allfällige strafrechtliche Untersuchungen einleiten.

Cyberwar deckt demnach nur einen engen Teilbereich aller Cyber-Attacken ab. Aus militärischem Blickwinkel ist er als Teil der Informationskriegsführung zu verstehen. Um den Gehalt und die Relevanz des Konzepts «Cyberwar» bestimmen zu können, ist neben der inhaltlichen Abgrenzung auch eine Differenzierung zwischen der operativen und der strategischen Dimension von Cyberwar angebracht. Zudem ist zwischen offensiven und defensiven Cyberwar-Massnahmen zu unterscheiden, wobei die Rolle des Militärs in der Cyberverteidigung begrenzt ist.

Cyberwar als Teilkonzept

Eine Kategorisierung von Cyber-Attacken primär nach Urhebern ist in der Praxis zunehmend schwierig. Da sich Angreifer immer besser zu verstecken wissen, ist eine zeitnahe klare Zuordnung oft unmöglich. Dennoch ist, soweit eruierbar, die Intention hinter einer Attacke von konzeptioneller Bedeutung, ist doch längst nicht jeder Cyberangriff militärisch motiviert und Teil eines Cyberwar. Ein weiteres wichtiges Unterscheidungsmerkmal ist das potentielle Schadenausmass eines Vorfalls. Damit verbunden ist das Bild einer Cyber-Leiter: Je weiter oben auf der Leiter man sich befindet, desto grösser ist der mögliche Schaden.

Auf Sprosse eins dieser Leiter befindet sich der Cyberhacktivismus bzw. Cybervandalismus. Dabei geht es um virtuelle Veränderung oder Zerstörung von Inhalten, wie dem Hacken von Webseiten oder dem Ausschalten eines Servers durch Datenüberflutung. Cybervandalismus ist die häufigste Form von Cyberkonflikt und erhält grosse öffentliche Aufmerksamkeit. Die Effekte solcher Taten sind jedoch zeitlich begrenzt und relativ harmlos, zumal sie nicht politisch oder wirtschaftlich motiviert sind.

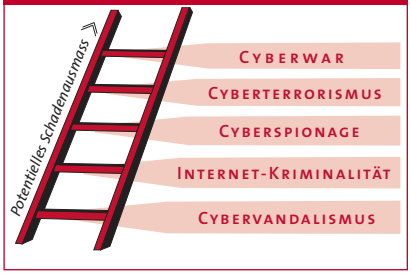
Auf den Stufen zwei und drei befinden sich die Internet-Kriminalität und die Cyberspionage. Beide finden laufend und unabhängig von Konflikten statt. Hauptleidtragende ist die Wirtschaft: Auch wenn die Datenerhebung ausserordentlich schwierig ist, werden die globalen Kosten dieser Phänomene auf rund eine Billion Dollar jährlich geschätzt. Regierungsnetzwerke mit klassifizierten Informationen sind ebenfalls betroffen, stellen jedoch ein vergleichsweise selteneres Angriffsziel dar.

Unter Cyberterrorismus auf Sprosse vier werden rechtswidrige Angriffe nichtstaatlicher Akteure gegen Computer, Netzwerke und die darin gespeicherten Informationen verstanden, mit dem Ziel, eine Regierung (und/oder die Bevölkerung) einzuschüchtern oder zu spezifischen Handlungen zu zwingen. Ein Cyber-Angriff wird also nur dann als Cyberterror bezeichnet, wenn er

in physische Gewalt gegen Personen oder Sachen mündet oder zumindest so viel Schaden anrichtet, dass beträchtliche Angst entsteht. Das potentielle Schadenausmass ist als sehr gross einzustufen, wobei in der Praxis bisher keine Fälle von Cyberterrorismus zu verzeichnen sind.

Auf der obersten Sprosse befindet sich der Cyberwar. Damit ist die kriegerische Auseinandersetzung im virtuellen Raum vorwiegend mit Mitteln aus dem Bereich der Informationstechnik gemeint. Cyberwar umschreibt einen Teilbereich des Informationskriegs. Innerhalb dieses breiteren Konzepts, das auf der Ebene von Information und Informationssystemen darauf abzielt, den Willen und die Entscheidungsfähigkeit der politischen Führung und der Streitkräfte eines Gegners und/oder die Einstellung der Zivilbevölkerung in Einsatzgebieten zu beeinflussen (siehe CSS Analyse Nr. 34), umfasst Cyberwar die Aktivitäten im Cyberspace. Konzeptionell spiegelt Cyberwar damit die zunehmend hochtechnisierte Form des Krieges im Informationszeitalter wider, die auf der Computerisierung, Elektronisierung und Vernetzung fast aller militärischer Bereiche und Belange basiert.

Konfliktformen im Cyberspace



Im Rahmen von Cyberwar ist auf doktrinaler Ebene zwischen drei Formen von *Computer Network Operations* zu unterscheiden (CNO): Die dezidierte Lahmlegung oder Zerstörung gegnerischer Netzkapazitäten wird als *Computer Network Attack* (CNA) bezeichnet. Unterstützend zielt die *Computer Network Exploitation* (CNE) darauf, mit Hilfe von Computern im nachrichtendienstlichen Sinne Informationen auf gegnerischen Rechnern zu ermitteln. Schliesslich umfasst die *Computer Network Defense* (CND) die Massnahmen zum Schutz der eigenen Computer und Computersysteme vor gegnerischen CNA und CNE.

Operative Realität

Das Schadenspotential eines Cyberwar für die Sicherheit und Wohlfahrt eines Staates ist enorm. Allerdings sind CNA-Fähigkeiten heute vor allem als *ein* operatives Mittel im Rahmen militärischer Einsätze zu verstehen. Die Bedeutung dieses Mittels wird in den nächsten Jahren weltweit zweifellos zunehmen. Hingegen erscheinen Szenarien eines strategischen Cyberwar, d.h. eines nur noch im Informationsraum ausgetragenen Konflikts, zum heutigen Zeitpunkt wenig realistisch.

In Bezug auf den heutigen Entwicklungsstand offensiver Cyberwar-Fähigkeiten mangelt es an gesicherten Erkenntnissen. Anders als bei den unteren Stufen der Cyber-Leiter ist die Debatte über Cyberwar deshalb stark von Spekulationen geprägt. Klar ist, dass CNE bereits heute eine nicht mehr wegzudenkende Realität ist. Die Unsicherheit betrifft denn auch vor allem das Ausmass der bereits verfügbaren CNA-Fähigkeiten. Hier wirken manche Schätzungen übertrieben respektive wenig fundiert.

So werden zwar immer wieder Verwendungsbeispiele von CNA ins Feld geführt. Die USA etwa sollen im Irakkrieg die lokalen Mobilfunk- und Computernetzwerke mit CNA ausgeschaltet haben, um Aufständische an der Planung von Bombenattentaten zu hindern. Im Kontext des israelischen Luftangriffs auf eine syrische Atomanlage im September 2007 wurde ebenfalls spekuliert, ob israelische Flugzeuge dank eines Cyberangriffs auf das syrische Flugabwehrsystem in den syrischen Luftraum eindringen konnten. Solche Berichte sind jedoch stets interpretationsbedürftig, zumal sie Cyberwar häufig synonym mit Informationskriegsführung verwenden und unklar bleibt, ob wirklich CNA-Fähigkeiten eingesetzt wurden.

Die von Geheimdiensten verwendeten Indikatoren zur Bestimmung von CNA-Fähigkeiten wie Doktrin, Training, Simulation oder Industriekooperation sind nur bedingt aussagekräftig. Unbestritten ist allerdings, dass offensive Cyberwar-Fähigkeiten in den USA ein grosses Thema sind. Ein Infowar-Team im Pentagon ist seit 1999 mit dem Aufbau solcher Mittel befasst. 2002 ordnete der damalige US-Präsident George W. Bush die Ausarbeitung einer Strategie an, in der Richtlinien und Kriterien für die Führung eines Cyberwars festgelegt werden sollten. Wie weit diese Bemühungen gediehen sind, ist aber unklar. Offensive Kapazitäten werden auch Frankreich, Israel, Russland und China nachgesagt. In der deutschen Bundeswehr befindet sich Medienberichten zufolge eine Abteilung «Informations- und Computernetzwerkoperationen» im Aufbau, die über CNA-Mittel verfügen soll. In manchen anderen Staaten wird über eine entsprechende Fähigkeitsentwicklung diskutiert. Die Debatten stehen aber häufig erst am Anfang.

Strategischer Cyberwar?

Cyberwar wird oft als fundamental andere Art des Krieges dargestellt, die billiger, «sauberer» (ohne Blutvergiessen) und für einen Angreifer weniger riskant sei als andere Formen des bewaffneten Konflikts. Mit solch positiven Einschätzungen ist bisweilen die Erwartung verbunden, dass wir in Zukunft nicht nur ein Wettrüsten im Cyberspace, sondern auch strategische Cyberkriege erleben werden. Diesbezüglich sind allerdings einige Fragezeichen angebracht.

So bestehen nach wie vor erhebliche Zweifel bezüglich der Realisierbarkeit eines strategischen Cyberwar. Experten gemäss ist es heute etwa nach wie vor nicht möglich, cyberbasierte Angriffe gezielt durchzuführen. Dies wiederum stellt die Logik des strategischen Cyberwar in Frage. Unkontrollierbare Rückkoppelungseffekte im stark vernetzten virtuellen Raum bergen beträchtliche Risiken auch für einen angreifenden Staat. Dieser Faktor ist umso wichtiger, als diejenigen Staaten, die das technologische Know-how für strategischen Cyberwar am ehesten besitzen oder entwickeln können, besonders abhängig von ihren Informationsinfrastrukturen und damit im IT-Krieg sehr verletzlich sind. Aufgrund unkontrollierbarer Nebeneffekte wäre ein Cyberwar auch mit einer langfristigen Unterminierung des Vertrauens in den Cyberspace verbunden, was negative Folgen für die Weltwirtschaft und damit ebenfalls für alle Beteiligten nach sich ziehen könnte. Hinzu kommt, dass die Entwicklung solcher Cyberwar-Fähigkeiten wohl weit kostenintensiver ist, als bisweilen behauptet wird.

Auch aus rechtlicher Sicht bleibt die offensive Dimension des Cyberwar kontrovers, wobei dies sowohl die strategische als auch die operative Ebene betrifft. Dies hängt damit zusammen, dass im Cyberwar keine Trennung zwischen zivilen und militärischen Zielen mehr möglich ist bzw. zivile Infrastrukturen bewusst angegriffen werden. Völkerrechtlich ungeklärt ist die Frage, ob der Einsatz von Computern als Waffe und als militärische Gewaltanwendung bezeichnet werden kann. Klärungsbedarf herrscht auch bei der Frage, inwieweit das blosse Eindringen in Computernetzwerke im Rahmen von CNE völkerrechtswidrig ist.

Verteidigung: Begrenzte Rolle des Militärs

Trotz der beträchtlichen Unwägbarkeiten bezüglich offensiver Cyberwar-Fähigkeiten sind bereits Rufe nach einer Cyber-Rüstungskontrolle laut geworden. Allerdings ist derzeit kaum vorstellbar, wie ein entsprechender Mechanismus etwa im Bereich der Verifikation wirksam umgesetzt werden könnte. Als Alternative wäre ein auf politischen Verzichtserklärungen basierender Prozess denkbar, doch dürften sich viele Staaten davor hüten, ihren Handlungsspielraum diesbezüglich einzuschränken.

So oder so ist davon auszugehen, dass sich die Mehrheit der Streitkräfte in den kommenden Jahren schwergewichtig mit Cyberverteidigung statt mit offensiven Mitteln auseinandersetzen wird. *Computer Network Defense* ist bereits heute von grosser Bedeutung. Angriffe auf die Informationstechnik, manipulierte Informationen oder erfolgreiche Spionage können die Leistungsfähigkeit der eigenen Armee massiv beeinträchtigen. Militärische Netzwerke müssen entsprechend gegen alle Formen von Cyberkonflikt gesichert werden.

Allerdings ist CND ein auf militärische Netzwerke limitiertes Konzept. Gegenmassnahmen auf allen Sprossen der Cyber-Leiter, seien sie präventiv oder reaktiv, werden dominiert von zivilen Massnahmen. Die Betonung der Bedeutung ziviler Akteure in diesem Bereich ist auch deshalb sinnvoll, weil gemessen an der Zahl der realen Vorfälle und dem geschätzten Schadenausmass die Internetkriminalität (verknüpft mit Cyberspionage) mit Abstand das schwerwiegendste Problem darstellt, dem sich die Staatenwelt heute gegenüber sieht.

Die Gegenmassnahmen für die Sprossen eins bis drei sind zum einen die Informationssicherung (*Information Assurance*), für die jeder einzelne Bürger und jede Firma selber zuständig ist, zum anderen privat- und strafrechtliche Handlungen. Der Staat sollte seine eigenen Netzwerke schützen und als Gesetzgeber dafür sorgen, dass allfällige Lücken im Internetrecht geschlossen werden. In diesem Zusammenhang kommt auch der internationalen Zusammenarbeit eine grosse Bedeutung zu. Spätestens ab Sprosse vier werden diese Aspekte ergänzt durch den Schutz kritischer Infrastrukturen (siehe CSS Analyse Nr. 16). Diese Schutzkonzepte erfordern primär eine enge zivile Partnerschaft zwischen Staat und Wirtschaft sowie intensive zwischenstaatliche Kooperation. Allerdings kann das Militär wichtige Beiträge etwa zur Erkennung feindlicher Desinformation oder zum Schutz von nationalen Führungsstrukturen erbringen.

Cyberwar in der Schweiz

In der Schweiz ist der Aufbau von Fähigkeiten zur Durchführung von Informationsoperationen in den letzten Jahren ins Stocken geraten (siehe CSS Analyse Nr. 34). Dies lässt sich u.a. auf rechtliche Unklarheiten, finanzielle und personelle Engpässe sowie politische Vorbehalte etwa gegenüber psychologischen Operationen zurückführen. In Bezug auf den Teilbereich Cyberwar sind auf Stufe Armee erste Schritte unternommen worden. Die Schweizer Armee ist nach eigenen Angaben heute aber nicht in der Lage, einen professionellen Hacker-Angriff auf der eigenen Infrastruktur zu detektieren und eine adäquate, zeitgerechte Reaktion darauf auszulösen. Wie verwundbar Schweizer Regierungsstellen gegenüber Cyber-Attacken sind, hat der massive Angriff auf das EDA im Oktober 2009 illustriert.

Im Zentrum Elektronische Operationen (ZEO) der Führungsunterstützungsbasis der Armee sind derzeit zwei mit Cyberwar befasste Bereiche im Aufbau. Dabei handelt es sich einerseits um ein militärisches *Computer Emergency Response Team* (milCERT), das die Systeme und Netze der Armee überwachen und gegebenenfalls Alarm auslösen soll. Zu den zentralen Herausforderungen dieses Teams gehört neben dem personellen Ausbau vor allem die Koordination mit dem bestehenden *Government Computer Emergency Response Team* (GovCERT), das ein wichtiger Bestandteil der Melde- und Analysestelle Informationssicherung (MELANI) ist.

Andererseits wird im ZEO auch eine Zelle *Computer Network Operations* aufgebaut. Diesbezüglich hat ein Gutachten zuhanden des VBS im März 2009 ergeben, dass die heutigen Rechtsgrundlagen in der Schweiz für Cyberverteidigung (CND) genügen, offensive CNA und nachrichtendienstliche CNE nach derzeitigem Stand aber nur im Aktivdienst (d.h. v.a. im Verteidigungsfall) möglich wären.

Das VBS beabsichtigt gemäss eigenen Angaben (siehe Gutachten), sowohl CND- als auch CNE- und CNA-Fähigkeiten aufzubauen. Der Schwerpunkt der schweizerischen Cyberwar-Aktivitäten sollte zum heutigen Zeitpunkt jedoch bei den defensiven Massnahmen liegen. Hier drängen sich zusätzliche personelle Ressourcen auf. Dies gilt im Übrigen auch für MELANI, die wie das ZEO im internationalen Vergleich unterdotiert ist. Wichtig ist zudem eine enge zivil-militärische Kooperation in der Cyberabwehr, in die auch die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) einzuschliessen ist. Schliesslich erfordert eine wirksame Cyberverteidigung auch internationale Zusammenarbeit, wobei sich das 2008 gegründete *Cooperative Cyber Defence Centre of Excellence* in Estland zu einem wichtigen multilateralen Rahmen entwickeln dürfte.

Der Aufbau von CNE-Fähigkeiten für die Nachrichtenbeschaffungsorgane des Bundes für Aktivitäten ausserhalb des Aktivdiensts ist durchaus prüfenswert und würde dem internationalen Trend entsprechen. Die Schaffung der entsprechenden gesetzlichen Grundlagen dürfte allerdings politisch kontrovers sein. Sicherzustellen wäre etwa, dass CNE nicht für Wirtschaftsspionage zweckentfremdet werden könnte.

Im Fall von CNA stellt sich die Rechtsfrage nicht, da die Schweiz diese Fähigkeit nur im Aktivdienst als Reaktion auf einen Angriff auf ihre eigenen Systeme verwenden würde. Die zentrale Frage hier betrifft vielmehr die Machbarkeit und Notwendigkeit einer solchen Fähigkeit. Da es sich hierbei um eine Frage von strategischer Bedeutung handelt, sollten sich sowohl in der Armee als auch in der Politik die entsprechenden Stufen damit befassen.

Cyberwar in der Schweiz: Weiterführende Links

- Gutachten VBS (10.3.09)
- Interpellation Schlüer: Internet-Sicherheit (17.3.09)
- Interpellation Segmüller: Informationsoperationen (9.3.09)
- Interpellation Graber: Elektronischer Krieg (18.12.08)
- EDA Ziel einer Viren-Attacke
- Führungsunterstützungsbasis der Armee
- Melde- und Analysestelle Informationssicherung (MELANI)
- Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)
- Cooperative Cyber Defence Centre of Excellence

- Verantwortlicher Editor: Daniel Möckli
  analysen@sipo.gess.ethz.ch
- Bezug und kostenloses Abonnement:
  www.ssn.ethz.ch