picture alliance

Wer stoppt die Cyberkrieger?

von Henning Wegener

Die Welt ist vernetzter und damit verletzlicher geworden. Cyberangriffe auf unsere Kommunikationssysteme nehmen zu und offenbaren: Regierungen bereiten sich auf den Cyberwar vor. Ein Plädoyer für Friedfertigkeit im digitalen Raum.

Ohne den Computerwurm Stuxnet würde die breite Öffentlichkeit vielleicht auch heute noch glauben, Cyberwar sei eine Erfindung verrückter Science-Fiction-Freaks. Der spektakuläre Virenangriff auf die Kontrollsysteme von Irans Urananlagen im vergangenen September hat aber auf eindrucksvolle Weise gezeigt, dass es längst keiner Star-Wars-Fantasien bedarf, um einen Gegner gezielt und subtil zu sabotieren. Ein ausgeklügelter Computerwurm kann ebenso wirkungsvoll, wenn nicht gar erfolgreicher sein als Spione oder ganze Armeen.

Die Welt ist vernetzter und damit auch verletzlicher und angreifbarer geworden. Längst ist unser Leben ohne Informations- und Kommunikationstechnologien (IKT) nicht mehr vorstellbar. Die gleichen Technologien aber, die uns befähigen zu lernen, Werte und Reichtum zu schaffen und Armut zu bekämpfen, stehen auch denen zur Verfügung, die angreifen und zerstören wollen. Trotz dieser offensichtlichen Gefährdung werden die Risiken im digitalen Raum nur unzureichend als Bedrohung wahrgenommen. Kaum jemand weiß, dass Angriffstechniken sich heute vornehmlich in der Hand großer, anonymer krimineller Konsortien befinden („organized crime"), dass aber auch immer mehr Staaten mit Cyberwaffen aufrüsten. Sie alle agieren, wenn überhaupt, in einem rechtlich unzureichend geordneten Raum.

Cyberangriffe gefährden längst nicht mehr nur die Privatheit der Nutzer, die Integrität der Information und das wirtschaftlich unerlässliche Vertrauen in die modernen Kommunikationsmittel, sondern insbesondere auch die großen Infrastrukturen unserer Gesellschaften: Energiesysteme, das Finanzwesen, den Flug- und Transportsektor, das Gesundheitssystem, die öffentliche Verwaltung – und nicht zuletzt die nationale und internationale Sicherheit. Informationssicherheit ist heute eine Grundvoraussetzung für das Funktionieren unserer Zivilisation; ihre Gefährdung ist eine der größten Bedrohungen unserer Gemeinwesen.

Die wirtschaftliche Bedrohung, die von Cyberangriffen ausgeht, dürfte inzwischen den meisten Computernutzern bewusst sein. Virenattacken, die die Funktionsfähigkeit von Computern stören; Versklavung von Armeen von Computern in „Botnets" durch unerkanntes Einpflanzen von „Malware" (Schadprogrammen) in Form von sogenannten Trojanern, die Computer in „Zombies" verwandeln; Eindringen in Firmencomputer mit Diebstahl oder Verfälschung sensibler technischer und kommerzieller Informationen; massiver Beschuss von Computern bis zur Blockierung oder Zerstörung der Systeme („distributed denial of service" – DDoS); systematisches Ausspähen von Individuen bis zum „identity theft" und der Plünderung von Bankkonten: All das geschieht täglich millionenfach. Aber nicht nur die geschätzten 1,8 Milliarden Computer weltweit bieten Angriffsflächen. Alle digitalen Systeme (Mikroprozessoren, eingebettete Systeme, RFIDs, mobile Geräte) sind verwundbar und werden auch massiv angegriffen.

Heute gehen Experten von einem weltweiten jährlichen Schaden von einer Billion, also 1000 Milliarden US-Dollar aus. Die IT-Sicherheitsfirma Symantec gibt an, drei Millionen Viren identifiziert zu haben und mit ihren Sicherheitssystemen 100 Cyberangriffe pro Sekunde zu blockieren. Die Sicherheitsexperten von McAfee, einem Hersteller von Antivirus- und Computersicherheitssoftware, haben erklärt, dass ihr automatisiertes elektronisches Prüfsystem für verdächtige digitale Kontakte im Jahr 2010 monatlich etwa 100 Milliarden Mal angesprochen wurde; McAfee schätzt, dass die Zahl der „Zombiecomputer" monatlich um mindestens fünf Millionen wächst und die erkannten Malwarevarianten sich derzeit jährlich verfünffachen. Das lässt das Ausmaß der organisierten Attacken und auch die Zahl der nicht abgewehrten Angriffe erahnen; das zeigt aber auch, welche Möglichkeiten in einem Cyberwar zur Verfügung stehen.

Cyberwar gewinnt aufgrund der dramatischen Aufrüstung für einen digital organisierten Konflikt und angesichts der technischen Möglichkeiten täglich an Bedeutung.

Dabei werden größere Kreativität und umfassendere finanzielle Ressourcen auf Angriffstechniken verwendet als für deren Abwehr (Cyberdefence).

Das Militär ist in unserem Informationszeitalter digital und hochtechnisiert. Planung, Kontrolle und Organisation des Gefechtsfelds basieren auf einer weitgehenden Computerisierung, Elektronisierung und Vernetzung fast aller militärischer Bereiche („network centric warfare"). Kaum ein Waffensystem wird ohne digitale Steuerung eingesetzt. Rechnergestützte Verbindungen sind die Essenz der häufig als „Revolution of Military Affairs" (RAM) bezeichneten modernen Entwicklung. Ihre Bedeutung, aber auch ihre Verwundbarkeit sind Ausgangspunkt für offensive und defensive Cyberwar-Überlegungen. Während die Digitalisierung und Beschleunigung militärischer Aktionen sich noch als „force multiplier" und als Betriebssysteme eines „kinetischen" Krieges mit dem Rechtsrahmen des Kriegs- und Konfliktvölkerrechts fassen lassen und auch das neuartige Informationsvolumen sowie die modernen Steuerungsinstrumente grundsätzlich unter den völkerrechtlichen Begrenzungen der Genfer Konventionen und der UN-Charta stehen, ist völlig unklar, wie es sich in Fällen des systematischen Eindringens in „feindliche" Systeme und Netze – einer Kriegsführung, die sich als „virtuale" grundsätzlich von „kinetischen" (konventionellen) Angriffen unterscheidet – verhält.

Vier Szenarien sind hierfür archetypisch. Gemeinsam ist ihnen das Fehlen eines verbindlichen internationalen Rechtsrahmens sowie die schwierige Identifizierung des Urhebers eines Angriffs und die Zurechnung des Angriffs – beides versucht ein aggressiver Urheber mit Kriegs- oder Angriffsabsichten zusätzlich zu verbergen.

Das erste Szenario ist das der massiven Cyberintelligence: Eine nicht überschaubare Zahl von Staaten und nichtstaatlichen Akteuren dringt permanent in die Informationssysteme des „Gegners" ein, erlangt damit Informationen über militärische Planungen und Kapazitäten in Realzeit und schafft so einen permanenten Spannungszustand. Diese digitale Invasion kann Gefechtsfeldinformationen verfälschen, das Funktionieren von Waffensystemen stören und ein militärisches Chaos mit weitreichenden Folgen bis in die Zivilgesellschaft hinein verursachen. Auch der jüngste, massive WikiLeaks-Datendiebstahl aus dem diplomatischen und sicherheitspolitischen Bereich der USA, teils offenbar von Insidern, großenteils aber von Hackern begangen, zeigt – auch wenn nicht in einem direkten Konfliktzusammenhang – die möglichen Dimensionen von Cyberintelligence.

Das zweite Szenario orientiert sich am massiven Angriff auf staatliche und private Netze. Die blitzartige paralysierende Wirkung von digitalen Angriffen auf ein ganzes Staatswesen und seine Infrastruktur war 2007 in Estland zu beobachten. Wochenlang waren Websites der Regierung, von Parteien, Firmen, Banken, Handynetzbetreibern und Zeitungen solchen Denial-of-Service-Attacken ausgesetzt. Von mancher Seite wurde zwar Russland verdächtigt, aber letztendlich blieben sowohl die tatsächlichen Täter im Dunkeln als auch die Frage unbeantwortet, inwieweit die mutmaßlichen Urheber in einem Nachbarstaat auch die käuflichen, internationalen kriminellen Konsortien mit ihrem Botnetpotenzial („Cybersöldner") rekrutiert haben.

Der Angriff auf Estland gilt als Weckruf für die internationale Debatte über das Potenzial von Cyberwar. Freilich blieb diese massive Attacke virtual. Beim Konflikt Russlands mit Georgien (und seinen unruhigen Randprovinzen) im Jahre 2008 – drittes Szenario – dienten die gravierenden virtualen Attacken auf die Regierungsinfrastruktur Georgiens auch der Erleichterung gleichzeitig geführter „kinetischer" Angriffe. Die Regierungskommunikation Georgiens wurde durch Sequenzen von DDoS-Angriffen lahmgelegt. Befreundete Regierungen kamen Georgien, wie bereits im Falle Estlands, mit technischer Unterstützung zu Hilfe, was schwerwiegende Fragen des Völkerrechts und der Neutralität aufwirft.

Das vierte und vergleichsweise gravierendste Szenario sieht folgendermaßen aus: Ein Staat oder auch eine Kombination von Botnetbeherrschern und Regierungen greifen in Sekundenschnelle gleichzeitig Schlüsselkomponenten des Wirtschaftssystems, wesentliche nationale Infrastrukturen und die Verteidigungsstruktur an. Bei solch einem Angriff kann der totale Kollaps eines Staates drohen, ein Pearl Harbour in Potenz – dabei spielt es nicht einmal eine Rolle, ob diese Angriffe mit einem traditionellen „kinetischen" Angriff gekoppelt werden. Ein solcher digitaler Generalangriff kann enorme Zerstörungen verursachen und eine nicht kalkulierbare Zahl von Menschenleben kosten.

Für einen Angreifer bietet eine Cyberwar-Attacke zahlreiche Vorteile: Da im Wesentlichen vorhandene, duale Techniken eingesetzt werden, ist ihre Verwendung kostengünstig, effektiv, in Sekundenschnelle bereitstellbar, wegen der Entbehrlichkeit sichtbarer Vorbereitungen (Aufmärsche, Logistik) kaum erkennbar, ohne menschliche Eigenverluste kalkulierbar und durch Söldnerwerbung potenzierbar. Die Zurechnung ist nach dem gegenwärtigen Technikstand überaus schwierig und unzuverlässig – vor allem, wenn der Gegner seine Attacke zusätzlich verschleiert. Cyberwar ist asymmetrisch und setzt kein Kräftegleichgewicht voraus. Massive Cyberangriffe sind schwer dosierbar, ihre Folgen können unberechenbar sein. Sie können Machtgleichungen und die Geostabilität unserer digital abhängigen Welt entscheidend verändern.

Umso unverständlicher ist es, dass es der Staatengemeinschaft bisher nicht gelungen ist, dafür einen Rechtsrahmen zu entwickeln. Weder die sanktionsauslösenden Bestimmungen der UN-Charta noch die Normen des Nato-Vertrags bieten dafür geeignete Maßstäbe. Was ist Cyberwar? Was sind angesichts der Ununterscheidbarkeit der digitalen Technologien Cyberweapons? Kann man speziell für militärische Applikationen entwickelte Software definieren und verbieten? Ist eine Verifikation überhaupt möglich? Macht das im nuklearen Zusammenhang entwickelte Konzept der Abschreckung einen Sinn? Was ist ein „bewaffneter Angriff", was eine Verletzung der „territorialen Integrität" oder „nationalen Souveränität" – die Schlüsselkonzepte des Sicherheitssystems der UN-Charta und der Nato – im digitalen, grenzenlosen Raum? Wie kann der Angreifer identifiziert und eine Selbstverteidigung oder ein Gegenschlag inszeniert werden?

Die World Federation of Scientists fordert seit 2001 einen umfassenden Verhaltenskodex für den digitalen Raum und ein „Universal Law of Cyberspace". Der Generalsekretär der „International Telecommunications Union", Hamadoun Touré, verlangt einen „Global Cyber Treaty", der die militärische Nutzung des digitalen Raums völkerrechtlich begrenzt und sanktioniert. Vornehmlich Russland, das Protagonist einer Information Security Convention ist, hat diese Fragen auch in den Vereinten Nationen thematisiert. An der Umsetzung dieser Vorschläge fehlt es aber immer noch.

Heute rüsten sich schätzungsweise 150 Staaten mit offensiver Cyberstrategie und können zusätzlich mit der käuflichen Unterstützung der Botnetbeherrscher rechnen – schon allein deshalb muss diese Herausforderung konzeptionell angenommen werden. Entscheidend ist: Die offensive militärische Nutzung des digitalen Raumes muss negativ besetzt werden, sie muss als unvereinbar mit den Funktionsbedingungen einer weltweiten digitalen Ordnung, der Geostabilität und des Cyberpeace erkannt werden. Alle internationalen Akteure müssen an der Aufrechterhaltung transnationaler Netze und Informationsinfrastrukturen – der Essenz globaler Cyberstabilität – interessiert sein. Sie sind ein wichtiges öffentliches Gut.

Umso dringender bedarf es einer Cyberpeace-Strategie – einer Friedensordnung im digitalen Raum. Sie kann an traditionelle Friedensdefinitionen einer „culture of peace" anknüpfen. Wenn weit über 100 Staaten militärische Optionen haben, neigen Instinkt und Erfahrung dazu, sie auch zu nutzen, wenn Gegensignale

fehlen. Daher muss ein restriktiver Rechtsrahmen etabliert werden, der nicht von militärischen Überlegungen gesteuert wird. Grundidee muss sein, den digitalen Raum von Konflikten möglichst freizuhalten, und wenn dieser nicht zu verhindern ist, Selbstschutz und Cyberdefence den Vorrang vor Angriff zu geben. Diskutiert wird bereits über verstärkte kollektive Definitionsanstrengungen für Cyberwar und Cyberterrorismus und eine Aktualisierung der einschlägigen Völkerrechtsbegriffe; Staatenverpflichtungen, keinen Ersteinsatz von Cyberweapons zu praktizieren oder auf deren Einsatz ganz zu verzichten; bilaterale oder multilaterale digitale Nichtangriffsvereinbarungen und Hilfszusagen; Erarbeitung einer Definition und Liste (weit über den Minimalschutz der Genfer Konventionen hinaus) von essenziellen Infrastrukturen – besonders solchen mit hohem technischem und humanem Schadenspotenzial im Falle der Zerstörung – und von transnationalen Informationsnetzen sowie einer Feststellung derer Unverletzbarkeit; eine Absage an den Einsatz von „Cybersöldnern". Ein weitreichender Schritt wäre die grundsätzliche Delegitimierung digitaler offensiver Strategien in der Militärplanung von Staaten.

Nicht weniger schwierig ist die Frage, wie auf einen Angriff – wenn er denn stattfindet und folgenreich ist – reagiert werden soll.

Hier zwingen die Unterschiede zwischen traditionellem („kinetischem") und digitalem Angriff in erster Linie zur Erhaltung oder Wiederherstellung einer friedlichen Situation, der Cyberstabilität. Dass man Angriffe abwehren darf und bei einem „bewaffneten Angriff" das Selbstverteidigungsrecht der Charta gelten würde, ist unbestritten. Vorrang müssen aber Selbstschutz, Zurückhaltung und Cyberdefence haben. Präventiver Selbstschutz, die gemeinsame Verantwortung aller digitalen Akteure, sich mit angriffssicheren, im Angriffsfall selbstheilenden Systemen und Netzen auszurüsten und ein robustes Sicherheitsmanagement einzuführen, sowie Allianzen zur gegenseitigien Unterstützung komplettieren dieses Konzept friedenskonformer Antworten.

In Fällen, in denen dieser defensive Ansatz nicht ausreicht und aktive Selbstverteidigung notwendig wird, sind aus der Cyberpeace-Perspektive einfache militärische Analogien trügerisch. Auch die Anwendung kriegsvölkerrechtlich etablierter Einsatzregeln („Rules of Engagement") führen zu militärischen Denkschemen, in denen zu leicht die Zerstörung des Feindes und seiner Waffen im Vordergrund steht.

Die Einsatzregeln müssen eng mit dem Ziel der raschen Wiederherstellung der Cyberstabilität ausgelegt werden. Sie erfordern eine ständige Risikoanalyse und Gewissheit über den tatsächlichen Urheber des Angriffs. Auch hier muss defensives Denken im Vordergrund stehen; unter den Prämissen des Cyberpeace ist meist Verteidigung die beste Offensive. Diese Einsicht erfordert ein Umdenken bei vielen militärischen Planern.

Aber die Sache ist nicht verloren, bezeichnet doch sogar die National Security Strategy der USA vom Mai 2010 verstärkte internationale Partnerschaft im digitalen Raum als strategisches Ziel. Und die Nato, die sich seit geraumer Zeit intensiv mit der neuen Konfliktdimension im digitalen Raum beschäftigt, hat in ihrem neuen strategischen Konzept vom 19. November 2010 weise die Frage offengelassen, ob und wann ein „bewaffneter Angriff" mit möglicherweise auch militärischen Folgen vorliegt. In diesem Konzept wird der Akzent auf den Ausbau kollektiver, integrierter Fähigkeiten zur Verhinderung, zum Schutz und zur Abwehr eines Cyberangriffs sowie zur Wiederherstellung der Systeme gelegt. Dieser Ansatz stellt wichtige Weichen für einen Cyberpeace.

Henning Wegener

ist Botschafter a.D. und Vorsitzender des Permanent Monitoring Panel on Information Security der World Federation of Scientists.