# Krieg im Cyberspace – ganz real

Die Regierungen wollen das Internet zivil-militärisch wieder in den Griff bekommen. **Von Matthias Monroy und Andrej Hunko**

Im Internet herrscht Krieg – Krieg zwischen engagierten Hackern auf der einen, Regierungen und von ihnen beeinflußten Unternehmen auf der anderen Seite. Im Zentrum des Schlachtfeldes steht Wikileaks, die von dem Australier Julian Paul Assange betriebene Enthüllungsplattform. Die stellt ungeniert Hunderttausende Informationen ins Netz, die für Bürgerinnen und Bürger wichtig, diversen Regierungen aber höchst peinlich sind. Sie arbeiten daher fieberhaft daran, das Internet in den Griff zu bekommen.

US-Politiker rücken Assange in die Nähe des Terrorismus, während der Cyberspace auch von Aktivisten sprachlich militarisiert wird: »Der erste ernsthafte Infowar läuft«, hatte John Perry Barlow, Netzaktivist und Gründer der Bürgerrechtsorganisation Electronic Frontier Foundation, letzte Woche ausgerufen. »Das Schlachtfeld ist Wikileaks. Ihr seid die Truppen«.

Die Bezahldienste Visa, PayPal und Mastercard, der Schweizer Bankkonzern PostFinance sowie das Versandhaus Amazon hatten ihre Geschäftsbeziehungen mit der Whistleblower-Plattform zuvor gekündigt. Die Dienste wurden daraufhin – wie die Website der US-Politiker Sarah Palin oder Joe Liebermann – massenhaft mit sogenannten »Distributed-Denial-of-Service-Attacken« (DDoS) bedacht. Auch die DDoS-Proteste wurden von Politik und Medien als »Cyberkrieg« kommentiert, obgleich es sich – im Vergleich zu einer Wortschöpfung aus der analogen Welt – eher um einen »Online-Riot« oder – da hinterher keine Sachschäden aufzuräumen waren – wenigstens einen »Cyber-Flashmob« gehandelt hat: Tausende Aktivisten schließen sich bzw. ihre Rechner zusammen, einigen sich auf Zeitpunkt und Ziel des Protestes und sind nur im Kollektiv erfolgreich.

## Die »@-Bombe«

Erst vor kurzem hatte eine andere digitale Bedrohung die Sorglosigkeit im Cyberspace nachhaltig durcheinandergebracht. Das von immer noch unbekannter Seite lancierte Computervirus »Stuxnet« wurde vielerorts als Protagonist eines Paradigmenwechsels angesehen. Mit den Angriffen auf die Rechner von größtenteils iranischen Atomanlagen scheint eingetreten, was Regierungen, Geheimdienste und ominöse »Sicherheitsberater« seit Jahrzehnten orakeln und der *Spiegel* 2001 als »@-Bombe« betitelte: ein »digitaler Erstschlag«. So hatte der Sprecher des Chaos Computer Club, Frank Rieger, das Auftauchen von »Stuxnet« in der *Frankfurter Allgemeinen Zeitung* kommentiert. Der Gründer der gleichnamigen Firma für Antivirus-Software, Eugene Kaspersky, sieht sogar ein neues »Zeitalter des Cyberterrorismus, der Cyberwaffen und -kriege« heraufziehen.

»Cyberangriffe haben eine neue Dimension der Gefährdung erreicht – und zwar in Quantität und Qualität«, tönt Michael Hange, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Kein Wunder also, daß der Bundesinnenminister das BSI in die von ihm geplante Superpolizeibehörde integrieren will. Längst haben auch die Verfolgungsbehörden eine Reihe von Maßnahmen gegen Ungehorsam im Cyberspace auf den Weg gebracht. Die Konferenz der Innenminister (IMK) wolle mit einer Internet-Zentralstelle aufwarten, kündigt der IMK-Vorsitzende und Hamburger Innensenator, Christoph Ahlhaus (CDU), an: »Die rasant wachsende Bedrohung durch Kriminelle im Netz ist eine der zentralen Herausforderungen. Es braucht jetzt einen großen Wurf, um die Entwicklung aufzuhalten.« Die IMK setzt sich für eine Meldepflicht auf EU-Ebene für Hackerangriffe ein.

## Grenzüberschreitend

Dabei ist die Europäische Union diesbezüglich alles andere als untätig. Pünktlich zum Auftauchen von »Stuxnet« überraschte die EU-Kommission mit der Fertigstellung neuer Maßnahmen, um die »Verteidigungsfähigkeit gegen Angriffe auf wichtige Informationssysteme« sicherzustellen. Weil Cyberkriminalität »ihrem Wesen nach grenzüberschreitend« sei, mache ihre Bekämpfung auch »angemessene grenzüberschreitende Vorkehrungen« erforderlich. Die EU-Mitgliedstaaten werden aufgerufen, umgehend das Übereinkommen des Europarates über Computerkriminalität aus dem Jahr 2001 zu ratifizieren. Indes soll die Kommission »Partnerschaften zwischen dem öffentlichen und dem privaten Sektor« verbessern und hierfür ein EU-Musterabkommen ausarbeiten.

Ein kürzlich von der Kommission vorgelegter Vorschlag einer Richtlinie zu Angriffen auf Informationssysteme soll den hierzu gültigen EU-Rahmenbeschluß von 2005 schnellstmöglich ablösen. Das neue Papier will »inadäquate Strafverfolgungsverfahren« ersetzen und kritisiert, Angriffe würden oft nicht bemerkt oder – aus Furcht vor Rufschädigung – zu selten angezeigt. Regierungen sollen verpflichtet werden, im Falle von Cyberangriffen schnell auf dringende Hilfeersuchen von EU-Mitgliedstaaten zu reagieren und etwa entsprechende Informationen bereitzustellen. Im FoKus stehen Rechnersysteme, die von außen unbemerkt manipuliert und zu sogenannten Botnetzen zusammengefaßt werden, die wiederum zu Angriffen genutzt werden können.

Mit einer neuen Verordnung soll indes die seit 2004 bestehende Europäische Agentur für Netz- und Informationssicherheit (ENISA) einer »Stärkung und Modernisierung« unterzogen werden. Das Mandat der ENISA soll hierfür ab 2012 um fünf Jahre verlängert werden, nicht ohne finanzielle und personelle Mittel aufzustocken. Für vertrauensbildende Maßnahmen soll ENISA Mitgliedstaaten und »Akteure des Privatsektors« in gemeinsame Aktionen einbinden. Auf dem Programm stehen »Cybersicherheitsübungen, Public-Private-Partnerschaften für Netzwerkstabilität, Wirtschaftsanalysen und Risikobewertung sowie Sensibilisierungskampagnen«. Die Informationsinfrastrukturen der Mitgliedsstaaten werden von ENISA mittels einer »digitalen Feuerwehr« unterstützt: Nationale, staatliche Computer-Notfallteams sollen in jedem Mitgliedstaat patrouillieren und über ENISA grenzüberschreitend vernetzt werden. Auch in Bezug auf gemeinsame »Cyber-Sicherheitsübungen« ist ENISA längst aktiv. Mit »CYBER EUROPE 2010« ist im November erstmals eine übergreifende Simulation digitaler Angriffe auf »Kritische Infrastrukturen« unter Einbezug aller EU-Mitgliedstaaten sowie Islands, Norwegens und der Schweiz abgehalten worden.

## »Umfassender Ansatz«

Alle EU-Maßnahmen rund um Cyberterrorismus und -kriminalität münden in neuen Kompetenzen für die Polizeiagentur Europol. Bereits jetzt existiert dort eine »Strategische Gruppe der Leiter der nationalen, auf Hightech-Kriminalität spezialisierten Fahndungsdienste«. Im Juli wurde eine »Cyber Crime Task Force« gegründet, die Europol-Datensammlung »Cyborg« bevorratet bei Ermittlungen anfallende Personen- und Sachdaten. Die von der deutschen IMK erwähnte Stelle zur Meldung von Straftaten im Internet ist längst im Aufbau und wird auch von deutschen Verfolgungsbehörden mit Informationen beliefert. Europol soll überdies »verstärkt strategische Analysen zur Cyberkriminalität« durchführen und »Tätererkenntnisse« oder Lagebilder zu »Verletzung der Privatsphäre, Cyberfinanzstraftaten, unerlaubten Zugang zu Sabotagezwecken, Verletzung der Rechte des geistigen Eigentums, Angriffe auf Netzwerke und Informationssysteme, Online-Betrug, Kinderpornografie und Spam sowie Handel mit verbotenen Stoffen« liefern. Vor allem die Zusammenarbeit mit Interpol soll intensiviert werden. Die internationale Polizeiorganisation war im Herbst mit Häme bedacht worden, nachdem unbekannte Aktivisten auf das Facebook-Profil von Direktor Ronald K. Noble zugriffen und von ihm dort brisante Informationen erfragten. »Cybercrime ist die gefährlichste Bedrohung«, blies Noble zerknirscht zum Gegenangriff.

Wie üblich obliegt es dem sogenannten »EU-Antiterrorismus-Koordinator« Gilles de Kerchové, die zivil-militärische Kombination von EU-Maßnahmen und Institutionen voranzubringen: In einem kürzlich vorgelegten Papier droht Kerchové, ein »umfassenderes Konzept für das Vorgehen gegen Cyberterrorismus, Cyberkriminalität, Cyberangriffe und Cyberkriege« zu entwickeln. Zudem verweist er auf die USA, die seit diesem Jahr mit Keith Alexander einen Vier-Sterne-General zur Abwehr und Ausführung von Cyberangriffen eingesetzt haben.

Kerchovés Statement klingt nach dem »umfassenden Ansatz«, wie er gemeinhin für die Durchsetzung einer zunehmenden Zusammenarbeit von Polizei, Militär und Geheimdiensten verwendet wird. Damit wird die militärische Beantwortung eines Cyberangriffs salonfähig gemacht, obwohl Zwangsmittel im wirklichen Leben immer noch durch das Ziel, den Ausführenden, das Tatmittel oder die Schwere der Tat bestimmt werden. Im November hat auch die NATO darüber beraten, ob Störungen des Cyberspace eines Mitgliedstaates als Angriff auf das Kriegsbündnis gewertet werden können. Vorsichtshalber wurde beschlossen, im Falle eines Cyberangriffs zumindest Artikel 4 des NATO-Vertrags in Kraft zu setzen, wonach die Mitglieder »einander konsultieren, wenn nach Auffassung eines von ihnen die Unversehrtheit des Gebiets, die politische Unabhängigkeit oder die Sicherheit einer der Parteien bedroht sind«.

**Andrej Hunko ist Bundestagsabgeordneter der Linkspartei, Matthias Monroy sein Mitarbeiter**


**Solidaritäts-Demonstration für den in London inhaftierte Wikileaks-Begründer Julian Assange**