Digitale Grundrechte!

Die Konsequenz des NSA-Skandals sollte ein Cybersicherheitsabkommen sein

Oliver Rolofs | **Die Enthüllungen von Edward Snowden haben transatlantisches Vertrauen zerstört und dürften auch in Washington zu einem Umdenken führen. Benötigt wird jetzt ein internationales Rahmenwerk zur Cybersicherheit. Europa sollte hierbei die Standards setzen; ein EU-weites „No-Spy"-Abkommen wäre ein guter erster Schritt.**

Nach der Veröffentlichung Hunderttausender teils hochsensibler Depeschen des amerikanischen Außenministeriums durch WikiLeaks Ende November 2010 herrschte in Washington das Gefühl, dass neun Jahre nach „9/11" ein digitaler Angriff nun von innen erfolgt sei. Gut drei Jahre später, nach den Enthüllungen von Edward Snowden zu den amerikanisch-britischen Massenüberwachungsprogrammen, muss man sich allerdings fragen, ob die Vereinigten Staaten daraus gelernt haben.

Der Tsunami, der über sich ahnungslos gebende Europäer hinwegraste, hat schweren politischen Schaden angerichtet und Debatten über die Grenzen dessen angestoßen, was man unter Freunden tun darf und was nicht. Beteuerten Politiker hierzulande zunächst, dass auch ausländische Dienste in Deutschland stets Recht und Gesetz einhielten, begriffen langsam auch breitere Gesellschaftsschichten, dass die amerikanischen und britischen Spionageaktivitäten nicht nur dem Schutz vor Terror dienten.

Dabei hätte man annehmen können, dass im Zuge des gigantischen WikiLeaks-Datenlecks sowohl der Umgang mit als auch der Zugang zu vertraulichen Informationen überdacht worden sei. In Europa führte WikiLeaks noch nicht mal zu einer ernsthaften Diskussion über einen besseren institutionellen Datenschutz; vielmehr vertraute man auf das Sankt-Florians-Prinzip: Heiliger Sankt Florian, verschon' mein Haus, zünd' and're an.

Digitaler Wilder Westen

Die NSA-Affäre hat nicht nur Mythen von Freiheit und Freundschaft zerstört. Sie hat auch offengelegt, dass ein zum digitalen Wilden Westen degenerierter Cyberraum, als Vehikel staatlicher Massenüberwachungsprogramme missbraucht, eine solche Entwicklung erst möglich gemacht hat. Dabei ist Spionage

im Cyberraum an sich nichts Neues; neu ist die Dimension. Quantität und Qualität der digitalen Angriffe und Operationsmöglichkeiten haben ungeahnte Ausmaße erreicht. Die meisten Europäer fühlen sich verletzt, weil sie – wie Bundeskanzlerin Angela Merkel – glaubten, dass dies unter Freunden „nicht gehe"; eine Haltung, für die NSA-Direktor Keith Alexander kein Verständnis zeigte: Schließlich spionierten Verbündete die USA und deren Spitzenpolitiker ebenfalls aus.

Immerhin reifte auf amerikanischer Seite die Einsicht, dass das Risikomanagement versagt habe und eine bessere Überwachung der Geheimdienste erforderlich sei. Der republikanische Kongressabgeordnete Jim Sensenbrenner, der nach den Anschlägen vom 11. September 2001 maßgeblich den „Patriot Act" mitverfasst hatte, ging sogar noch weiter und kündigte an: „Der Kongress wird der NSA die Flügel stutzen!" Die US-Behörden hätten das Gesetz falsch ausgelegt. Sensenbrenner hat nun einen „Freedom Act" eingebracht, der die Massensammlung von Daten in Amerika verbietet. Das mögen erste Schritte zur Normalisierung sein. Doch bringen sie auch mehr Sicherheit im Cyberraum und stellen verlorengegangenes Vertrauen wieder her?

Keine „Fortsetzung der Politik mit digitalen Mitteln" um jeden Preis

Ein Rahmenwerk für Cybersicherheit

Spätestens seit der NSA-Affäre gehören Cyber- und Datensicherheit zu den wichtigsten Themen der internationalen sicherheitspolitischen Debatte. Ein kürzlich von Brasilien und Deutschland gemeinsam eingebrachter Resolutionsentwurf gegen Datenspionage wurde im Menschenrechtsausschuss der UN-Vollversammlung einstimmig angenommen. Es scheint überhaupt einen breiten Konsens zu geben, dass es so nicht weitergehen kann. Selbst Präsident Barack Obama überlegte öffentlich, dass man „vielleicht nicht alles tun sollte, was man technisch tun könnte".

Die Affäre dürfte also auch in den USA zu der Einsicht führen, dass gute Beziehungen nicht durch solche Maßnahmen aufs Spiel gesetzt werden sollten. Dabei wird man auch nach der Verlässlichkeit des größten Auslandsgeheimdiensts der USA zu fragen haben, der bis vor kurzem offenbar so leichtfertig mit seinen geheimsten Dokumenten umging, dass externe Mitarbeiter wie Edward Snowden einen ungehinderten Zugriff hatten.

Ein vertrauensvolles und störungsfreies transatlantisches Partnerschaftsverhältnis ist notwendig, um die Grundlage für ein globales Cybersicherheits-Rahmenwerk zu legen. Darüber müssen in Europa und in den USA ernsthafte Debatten geführt werden – nicht nur regierungsintern und unter Fachleuten, sondern transparent in den Parlamenten. Ziel sollten eine gesunde Balance von Freiheit und Sicherheit sein und eine Abkehr von der „Fortsetzung der Politik mit digitalen Mitteln" um jeden Preis.

Die Frage ist allerdings: Sollten künftige Erkenntnisse des politischen Risikomanagements in die Entscheidungsprozesse geheimdienstlicher Aktivitäten einfließen und der teils pervertierte Anti-Terror-Kampf auf ein gesundes Maß

Bild nur in Printausgabe verfügbar

zurückgestutzt werden, um in Zukunft außenpolitische Schäden zu vermeiden? Wenn ja, wäre dies ein „Weiter so“ mit der Maßgabe, dass es nur keinen zweiten Snowden geben darf. Oder wie steht es, aus Sicht der Betroffenen, um die eigene Gefahrenabwehr und den Aufbau eigener technologischer Fähigkeiten?

Regelwerke müssen vereinbart und vertrauensbildende Maßnahmen geschaffen werden, nicht nur zwischen den transatlantischen Partnern, sondern weltweit. Ein wichtiger Schritt dahin könnte das transatlantische „No-Spy“-Abkommen sein, das einen wichtigen Mosaikstein in der Weiterentwicklung der transatlantischen Sicherheits- und Wertegemeinschaft bilden würde. Dabei darf nicht außer Acht gelassen werden, dass nicht nur die USA technische Spionagekapazitäten besitzen, sondern auch Staaten wie China, Russland und Nordkorea. Bei aller Enttäuschung über die transatlantischen Partner sollte man deshalb nicht vergessen, dass es mehr gemeinsame Gegner als Gegensätze gibt.

Gleiches gilt für die Cyberkriminalität. Binnen weniger Jahre ist sie zu einer globalen Bedrohung mit massiven wirtschaftlichen, politischen, rechtlichen und sozialen Implikationen geworden, deren Schaden durch Europol im vergangenen Jahr auf 750 Milliarden Euro beziffert wurde. Bislang haben Cyberangriffe verschiedenster Art in erster Linie finanzielle Schäden verursacht. Sie könnten aber auch immensen physischen Schaden anrichten, wenn sie sich zum Beispiel gegen kritische Infrastrukturen wie Energieversorgung oder Verkehrsleitsysteme richten und damit Katastrophen verursachen oder sogar Staaten existenzbedrohend destabilisieren.

Trotz der wachsenden Gefahren aus dem Cyberraum und der Verwundbarkeit der digitalen Gesellschaft einschließlich ihrer Ökonomien sind wir weit

von tragfähigen internationalen Cybersicherheitsabkommen entfernt. Gleichzeitig bewegen wir uns von „Government“ hin zu „Googlement“: Nicht nur die NSA, auch große Unternehmen sammeln „Big Data“. Aber nach welchen Schutzregeln und Kontrollmechanismen geschieht das?

Es mangelt also nicht nur an Vertrauen, sondern auch an einheitlichen Standards und Definitionen. Europa muss verbindlich definieren, welches Ausmaß an Datensammlung und Überwachung als notwendig und erträglich angesehen wird. Ein europäisches „No-Spy“-Abkommen wäre ein wichtiger Anfang: So würde die Privatsphäre jedes EU-Bürgers durch jedes einzelne EU-Mitglied respektiert, wie Ben Scott und Georg Mascolo in ihrer kürzlich beim Wilson Center veröffentlichten Studie „Lessons from the Summer of Snowden: The Hard Road Back to Trust“ konstatieren. Nur für zuvor präzise ausgehandelte Ziele – etwa den Kampf gegen Terrorismus, die Verhinderung der Proliferation von Massenvernichtungswaffen sowie besonders schwerer Straftaten – wären Datenspeicherung und Überwachung zulässig. Jede Form von politischer und Wirtschaftsspionage wäre verboten.

Wohlstand, Sicherheit und Freiheit stehen auf dem Spiel

US-Internetunternehmen als Verbündete

Ein EU-Standard könnte dann Ausgangsbasis für den Dialog mit Washington und anderen Partnern sein. Hier hätte Europa zudem möglicherweise in US-Firmen Verbündete, deren Geschäftsmodell auf dem Spiel steht, wenn Konsumenten weltweit Zweifel an der Sicherheit ihrer Daten haben. Weitere Impulse für mehr Cyber- und Datensicherheit könnten die 2001 in Budapest verabschiedete „Convention on Cybercrime“ des Europarats, das „Cybersecurity Toolkit“ der Internationalen Fernmeldeunion (ITU) oder die praktischen Vorschläge des EastWest Institute geben. Letzteres hat angeregt, die Genfer und Haager Konventionen auf den Cyberraum zu erweitern, was bereits eine gute Grundlage für ein internationales Regelwerk wäre. Schließlich ist ein sicherer Cyberraum eng mit Demokratie, Freiheit und offenen Gesellschaften verbunden. Der Anschluss an die digitale Welt mittels einer sicheren Internetarchitektur fördert soziales und wirtschaftliches Wachstum, kann Gesellschaften weiter entwickeln und Regierungsapparate transparenter machen. Hierfür müssen Datensicherheit und der Schutz der Privatsphäre im Cyberspace zu essenziellen Werten werden – zu digitalen Grundrechten! Denn letztlich stehen unser Wohlstand, unsere Sicherheit und am Ende die Freiheit des Individuums auf dem Spiel.

Oliver Rolofs
ist Pressesprecher der Münchner Sicherheitskonferenz.