GEOPOLITIK

Die nächste Eskalationsstufe

Sandro Gaycken

China und die USA bekämpfen sich jetzt schon verbissen über Hackerangriffe im Internet. Eine Eskalation dieser Auseinandersetzung könnte fatale Folgen für die Weltwirtschaft haben.

Einen Krieg zwischen Großmächten mag man sich nicht vorstellen. Zum Glück muss man es auch nicht. Aber der Weltfriede kann auch ganz anders ins Wanken geraten. Es gibt eine kaum bemerkte, sich aber stetig aufbauende Eskalation zwischen China und den USA – im Cyberspace.

Ursache ist die digitale Industriespionage, die die USA in den meisten Fällen in China verorten. Seit fast einer Dekade verschwinden massenhaft Daten aus Forschung, Entwicklung, Verwaltung, aus Wirtschaft und dem Staat in Richtung chinesischer Server. Bis vor einigen Jahren wurde kein großes Aufhebens gemacht, da China für quasi alle ein wichtiger Partner ist. Ein mächtiges Land obendrein. Der Umstand, dass die Empfängeradresse der gestohlenen Daten chinesisch war, sagt in einem globalen Internet, in dem sich jeder Hacker jede beliebige Empfängeradresse besorgen kann, außerdem letztlich nicht viel aus. Aber in den letzten Jahren überschlugen sich derartige Spionagevorfälle. Heute gehören sie zur Tagesordnung. Weltweit.

Viele Länder gehen nach wie vor tolerant damit um. Die besonders betroffenen USA nicht mehr. Aufgrund der immensen Zahl an Vorfällen aus China ist man nicht mehr willens, an die immer wieder beteuerte Unschuld zu glauben. Jetzt reagiert man.

Die erste Stufe dieser Eskalation begann in den letzten beiden Jahren: Die Industrie prangerte Vorfälle öffentlich an, die Regierung begann einen kritischen Dialog mit China, der durch diplomatische Manöver und Druck gestützt wurde. Anfang 2012 hat die US-Regierung Peking das erste Mal öffentlich der Cyber-Spionage beschuldigt – ein aggressiver Schritt gegen ein Land, das Beschuldigungen schnell als beleidigend empfindet.

Doch die Bemühungen verliefen im Sand. China gibt sich unbeeindruckt von den US-Beschwerden, provokativ desinteressiert, wie US Defence Secretary Leon Panetta bei seinen Gesprächen erfahren musste.

Die USA sehen sich so zu weiterem Handeln genötigt. Sofern China nicht doch einlenkt, wird wohl bald eine härtere diplomatische Gangart folgen. Einen bewaffneten Konflikt zwischen den Ländern wird es deshalb nicht geben. Auch im Cyberspace wirkt das Gleichgewicht des Schreckens.

Doch unterhalb dieser Schwelle gibt es genug Spielraum. Beide Staaten könnten versuchen, das Gleichgewicht der Abschreckung über professionelles und verdecktes militärisches Hacking herbeizuführen. Als Werkzeug einer Eskalation hätte diese neue Waffe einiges für sich. Professionelle, von Staaten ausgeführte Hacks sind flexibel und präzise, gut steuerbar. Viele Angriffe sind reversibel. Strom etwa ließe sich ab-, aber auch wieder anschalten.

Vor allem aber sind Cybermaßnahmen nicht tödlich und haben nur geringes Potenzial, die Bevölkerungen aufzuschrecken. Das hat man im Fall „Stuxnet“, beim Cyberangriff auf die iranischen Atomanlagen, bereits beobachtet. Cyberangriffe werden lange nicht als so bedrohlich oder brutal wahrgenommen wie Raketenschläge. Es gibt eben keine Bilder von Blut und Zerstörung, nur ausrastende Computer – auch wenn die Zweit- oder Drittfolgen verheerend sein können.

Für cyberbasierte Eskalationsstufen gibt es bereits konkrete Überlegungen, wie unlängst etwa von James Dobbins vorgestellt, dem Forschungsdirektor des International Security and Defense Policy Centers bei RAND. Beide Seiten erwägen Angriffe auf Satelliten. China könnte gezielt amerikanische Spionagesysteme oder Kontrollinfrastrukturen der Pazifikflotte angreifen. Ein proportionaler Rückschlag wäre den USA dann nicht möglich, da die chinesischen Spionagesysteme kaum zu durchbrechen sind. Die Amerikaner müssten daher zivile Logistik angreifen und Schäden in Wirtschaft und Infrastruktur anrichten.

So könnte sich eine Phase wechselseitiger militärischer Eskalation entwickeln, die sich letztlich auf zivile Systeme, vor allem auf die Märkte, ausweiten und kaum absehbare Schäden in der Weltwirtschaft auslösen könnte.

Das alles hat Konsequenzen für die Bundesrepublik. Eine unter Umständen innerhalb weniger Tage stattfindende Eskalation muss schnell verstanden und kompetent beurteilt werden, und es müssen diplomatische und technische Werkzeuge zur Eindämmung möglicher globaler Folgen und zur Intervention bereit stehen.

Von solcher Diplomatie und Sicherheitstechnik sind wir weit entfernt. Bemühungen und Investitionen der Bundesregierung sind nach wie vor höchstens moderat. Technische Ansätze zu Hochsicherheit werden von der deutschen Industrie nicht produziert, da keine Anreize gesetzt werden. International ausgerichtete Bemühungen der eher technisch orientierten Sicherheitsbehörden sind deshalb weiterhin eher an Marketing für im Binnenmarkt absatzschwache IT-Sicherheitsprodukte interessiert.

Der Autor lehrt an der FU Berlin.
Sie erreichen ihn unter:
gastautor@handelsblatt.com