Aufrüsten für den Krieg im Cyberspace

Jan Flückiger, NZZ, 6.2.2015

Das Stören fremder Netzwerke könnte vom Ausland als feindlicher Akt interpretiert werden. (Bild: Simon Dawson / Bloomberg)

Der Nachrichtendienst soll künftig in Computernetzwerke im Ausland eindringen und diese stören dürfen − auch zur Abwehr von Wirtschaftsspionage. Doch Angriffe auf digitale Infrastrukturen bergen stets auch das Risiko von Kollateralschäden.

Feindliche Übergriffe oder Spionagetätigkeiten im Cyberspace sind eine Realität. Darauf müssen sich auch der Bundesrat und der Nachrichtendienst des Bundes (NDB) einstellen. Im neuen Nachrichtendienstgesetz, das im Frühling im Nationalrat behandelt wird, ist denn auch vorgesehen, das der NDB künftig in Computersysteme und -netzwerke eindringen kann – auch im Ausland. Einerseits soll er dort Informationen beschaffen dürfen. Andererseits soll er den digitalen Informationsfluss aber auch «stören, verhindern oder verlangsamen» können, falls er den begründeten Verdacht hat, dass Systeme für Angriffe auf kritische Infrastrukturen in der Schweiz verwendet werden.

Die Informationsbeschaffung im Cyberspace gehört zum Einmaleins der internationalen Nachrichtendienste. Es ist deshalb eine Anpassung an

internationale Gepflogenheiten, dem NDB dies zu erlauben. In «politisch heiklen Fällen» muss der NDB zudem die Erlaubnis des Vorstehers des Verteidigungsdepartements (VBS) einholen.

«Kaskade von Wirkungen»

Heikler ist hingegen das Eindringen in ausländische Systeme und Netzwerke, um diese zu stören. Zwar soll das nur zur Verteidigung der eigenen Infrastrukturen erlaubt sein. Dennoch stellt sich die Frage, ob solches vom Ausland nicht als feindlicher Akt interpretiert werden könnte. Zumal Angriffe über Computernetzwerke etliche Schwierigkeiten bergen. So ist es gemäss einem Gutachten des Bundesamtes für Justiz und der Direktion für Völkerrecht «äusserst schwierig, einen Erstschlag zurückzuverfolgen», weshalb die Gefahr bestehe, dass der Gegenschlag auf das falsche Ziel gerichtet werde. Zudem könnten Angriffe über Computernetzwerke eine «Kaskade von Wirkungen verursachen», die sowohl militärische als auch zivile Objekte treffen könne und deren Ausmass «schwer voraussehbar» sei. Es besteht also stets das Risiko, ein falsches Ziel zu treffen oder Kollateralschäden zu verursachen.

Die Geschäftsprüfungsdelegation (GPDel) des Parlaments hat in einem Bericht explizit darauf hingewiesen, dass sich in diesem Zusammenhang «verschiedene völkerrechtliche Fragen» stellten, auf die der Bundesrat in seiner Botschaft nicht eingehe. Die GPDel hat der Sicherheitspolitischen Kommission (SiK) nahegelegt, dies im Rahmen ihrer Beratungen vertiefter abzuklären.

Nun hat die SiK des Nationalrats diesen Punkt Ende des vergangenen Jahres zwar ausführlich diskutiert. Doch faktisch hat sie einzig Hürden abgebaut. Während die Vorlage des Bundesrates vorsieht, dass das Eindringen in ausländische Computernetzwerke in jedem Fall vom Bundesrat genehmigt werden muss, will die SiK dies abschwächen: Der Entscheid soll an den VBS-Vorsteher oder – in «Fällen von untergeordneter Bedeutung» – gar an den Direktor des NDB delegiert werden können. Dies, obwohl der Bundesrat in seiner Botschaft schreibt, dass solche Aktionen «aussenpolitisch sensibel» seien und deshalb «nicht in der alleinigen Zuständigkeit des NDB liegen können».

Stellt sich die Frage, welche Angriffe auf kritische Infrastrukturen denn «untergeordnete Bedeutung» hätten. SiK-Mitglied Corina Eichenberger (fdp., Aargau) erklärt dies so: In einem ersten Schritt könne der NDB im Fall eines Angriffs schnell Gegenmassnahmen einleiten und zum Beispiel den Datenverkehr verlangsamen und erst danach den Bundesrat involvieren. SiK-Präsident Thomas Hurter spricht von einer «Präzisierung, nicht einer Abschwächung» der Bewilligungspraxis. In Fällen grösserer Tragweite müsse der Bundesrat selbstverständlich involviert sein.

Für Daniel Vischer (gp., Zürich) stehen hingegen taktische Gründe im Vordergrund: «Gerade weil solche Aktionen aussenpolitisch äusserst riskant sind, ist es in den Augen der Kommissionsmehrheit besser, wenn der Bundesrat nicht über alles Bescheid weiss.» Vischer selbst gehört zur Minderheit in der Kommission, die das Eindringen in Computernetzwerke aus der Vorlage streichen will. «Wir sprechen hier von Cyberkrieg. Solche Massnahmen sollten nicht im Rahmen des Nachrichtendienstgesetzes geregelt werden.»

Auch Eichenberger ist sich bewusst, dass sich der Gesetzgeber hier auf heiklem Terrain bewegt. «Es ist klar, dass solche Massnahmen neutralitätspolitische Implikationen haben können.» Deshalb müssten sie «äusserst zurückhaltend» und «mit grösster Vorsicht» angewendet werden.

Eine allzu grosse Zurückhaltung stünde allerdings im Widerspruch zu früheren Äusserungen von Bundesrat Ueli Maurer. So hatte dieser bereits im Vorfeld der Beratungen angekündigt, dass der Nachrichtendienst künftig auch zur Abwehr von Wirtschaftsspionage eingesetzt werden soll. Tatsächlich ist im Gesetz vorgesehen, dass der NDB auch «zum Schutz des Werk-, Wirtschafts- und Finanzplatzes Schweiz» tätig werden kann. Hurter weist darauf hin, dass der Dienst zu diesem Zweck nur «in besonderen Lagen» zum Einsatz käme. Angriffe auf einzelne Firmen reichten dazu seines Erachtens nicht aus.

Schwer kontrollierbar

Nicht nur politisch, auch juristisch ist das geplante Aufrüsten im Cyberspace umstritten. «Solche Aktionen haben Angriffscharakter – etwas, was im militärischen Bereich für ein neutrales Land bisher undenkbar war», sagt

Martin Steiger, Anwalt und Spezialist für Rechtsfragen im digitalen Raum. Zudem würden ziemlich sicher private Organisationen mit den Hackerangriffen betraut, weil das entsprechende Wissen beim Bund fehle. Umso schwieriger gestalte sich die Kontrolle darüber.

Der Nachrichtendienst selber gibt sich zugeknöpft. Die Ausgestaltung des betreffenden Artikels sei Gegenstand der «politischen Entscheidfindung durch das Parlament». Der NDB nehme dazu keine Stellung. Ebenfalls nichts sagen will der Dienst dazu, wie er beim Eindringen in ausländische Computersysteme Kollateralschäden vermeiden würde. Über Einzelheiten operativer Tätigkeit könne man keine Auskunft erteilen. Auch die Frage, gegen welche Akteure sich allfällige Hackerangriffe richten könnten, lässt der NDB unbeantwortet. Er hält jedoch fest, dass für das Vorgehen gegen nichtstaatliche Akteure in jedem Fall ein Bundesratsbeschluss nötig sei.