STANDPUNKTE: BRAUCHT DIE BUNDESWEHR OFFENSIVE CYBERFÄHIGKEITEN?

PRO

VON DR. REINHARD BRANDL MdB,
MITGLIED DES VERTEIDIGUNGSAUSSCHUSSES

Dr. Reinhard Brandl MdB

Der Schutz der eigenen Kommunikation sowie das Aufklären und Stören von gegnerischer Kommunikation ist seit der Zeit ihrer Gründung fester Bestandteil des Fähigkeitsspektrums der Bundeswehr („Elektronische Kampfführung"). In den vergangenen 60 Jahren haben sich die technischen Rahmenbedingungen und die Bedeutung dieser Fähigkeiten grundlegend verändert. Elektronische Kommunikationsmittel werden nicht mehr nur zur Verständigung zwischen Truppenteilen und zur Steuerung von konventionellen Waffensystemen eingesetzt, sondern sind zum eigenständigen Instrument zwischenstaatlicher Konflikte geworden. Der Cyberraum hat sich zu einem militärischen Operationsraum analog zu Land, See, Luft und Weltraum entwickelt. Jeder bewaffnete Konflikt – heute und in Zukunft – wird zumindest in Teilen auch über das Internet geführt werden. Die Abwehr von Cyber-Angriffen ist eine gesamtstaatliche Aufgabe. Dafür und für mögliche Auslandseinsätze muss die Bundeswehr geeignete Kapazitäten vorhalten. Wie in jedem anderen Operationsraum gehören dazu sowohl defensive als auch offensive Mittel. Da auch mögliche Gegner von Fähigkeiten und Ressourcen im Cyberraum abhängig sind, kann die Bundeswehr in Auslandseinsätzen und im Verteidigungsfall offensive Mittel einsetzen, um sie an der Nutzung dieser Fähigkeiten und Ressourcen zu hindern. Ein solcher Einsatz der Bundeswehr unterliegt dabei denselben rechtlichen Voraussetzungen wie jeder andere Einsatz deutscher Streitkräfte.

In Friedenszeiten ist es die vorrangige Aufgabe der Bundeswehr, sich selbst vor Cyber-Angriffen zu schützen. Als mittlerweile voll digitalisierte Großorganisation bietet sie zahllose mögliche Angriffspunkte und ist täglich mehr oder weniger professionellen Attacken ausgesetzt. Bereits eine kleine unentdeckte Schwachstelle kann es einem Angreifer ermöglichen, maximalen Schaden anzurichten. Für eine wirkungsvolle Cyberabwehr benötigt die Bundeswehr deshalb auch Personal, das sich aus der Perspektive von Angreifern intensiv mit Schwachstellen, Angriffsmethoden und -instrumenten beschäftigt.

Unsere zunehmend vernetzte Gesellschaft ist in hohem Maße auf die Verfügbarkeit, Integrität und Vertraulichkeit ihrer Informations- und Kommunikationsinfrastruktur angewiesen. Es liegt nicht in unserem Interesse, dass der Cyberraum sich mehr und mehr zu einem Feld entwickelt, auf dem zwischenstaatliche Konflikte ausgetragen werden. Die deutsche Außen- und Sicherheitspolitik ist auf allen Feldern dem Frieden verpflichtet. Das entbindet uns aber nicht von der Verantwortung, die Bundeswehr für den Ernstfall auszurüsten und die politische sowie militärische Handlungsfähigkeit in jeder Situation sicherzustellen.

CONTRA

VON DR. MARCEL DICKOW,
LEITER FORSCHUNGSGRUPPE SICHERHEITSPOLITIK, SWP

Dr. Marcel Dickow

Ist der Cyberspace die neue, fünfte Dimension des Krieges? Nicht nur das neue deutsche Weißbuch zur Sicherheitspolitik formuliert das so. Tatsächlich zeigen die millionenfachen und geradezu sekündlichen Angriffe im Netz, dass viele Akteure diese Einschätzung teilen. Müssen Deutschland und die Bundeswehr deswegen auch im Cyberspace aufrüsten? Es bestehen in meinen Augen erhebliche Zweifel.

Unzweifelhaft ist, dass die zivilen und militärischen Netze der Bundesrepublik geschützt und im Ernstfall auch verteidigt werden müssen. Doch sind dafür auch offensive Fähigkeiten nötig? Und sollten Cyberangriffe zu einem Bestandteil der regulären Kriegsführung werden, nicht nur im Bereich der Landes- und Bündnisverteidigung, sondern auch bei Auslandseinsätzen? Drei Beobachtungen aus jüngster Vergangenheit legen nahe, Zurückhaltung zu üben. Erstens, die Angriffe im Cyberspace funktionieren weitestgehend über das Ausnutzen von offenen Sicherheitslücken in Hard- und Software, sogenannte 0-day-Exploits. Wer angreifen will, muss diese Schwachstellen suchen oder das Wissen bei dubiosen Firmen einkaufen. Um im Ernstfall einen gezielten digitalen Angriff durchzuführen, muss das Zielsystem schon im Vorfeld infiltriert und ausgespäht werden, wozu der Vorrat an Exploits teilweise eingesetzt wird. Da wir hier in der Regel über Schwachstellen in Betriebssystemen und gängigen kommerziellen Anwendungen sprechen, werden diese nicht geschlossen sondern bleiben ein gefährliches Einfallstor für Dritte, und zwar auf allen Rechnern. Das Pflegen von Cyberangriffswaffen vergrößert also das Sicherheitsrisiko aller Computerbenutzer, weil Sicherheitslücken nicht geschlossen werden. Zweitens zeigt der Einsatz staatlicher Schadsoftware, dass Kriminelle, wie beim Fall Stuxnet, diesen hochentwickelten Code im Nachgang recyceln und dann millionenfach an private Benutzer verteilen. Selbst Nachrichtendienste können ihren digitalen Instrumentenkasten nicht garantiert geheim halten, wie die letzten Enthüllungen über die Spionagetools der NSA nahelegen. Drittens, kann Deutschland wohl kaum international glaubwürdig für Regulierung und Rüstungskontrolle im Cyberspace eintreten, wenn es selbst offensive Cyberfähigkeiten entwickelt. Die Stärke der normenbasierten Außenpolitik besteht eben gerade darin, gutes Verhalten vorzuleben und keine Doppelstandards aufzubauen.

Dies alles schließt nicht aus, dass ein guter Verteidiger die Techniken der Angreifer im Cyberraum studieren sollte. Die dabei entdeckten Sicherheitslücken sollten aber geschlossen werden, sonst gefährden wir weltweit die Sicherheit unserer Computer.

Impressum
Herausgeber: Arbeitskreis Außen- und Sicherheitspolitik (ASP) der CSU • **Konzept & Gestaltung:** IT'S LIVE! Advertising GmbH
Redaktion: ASP-Landesgeschäftsführer Peter Rief, M. A. • **Kontakt Redaktion:** asp@csu-bayern.de • **Stand:** November 2016
Hinweis: Die Beiträge in dieser Zeitschrift geben die Meinung des Verfassers, nicht aber die der Redaktion oder des ASP wieder.