„Cyberkrieg“

Eine sicherheitspolitische Aufgabe ersten Ranges

PATRICK KELLER
Geboren 1978 in Bonn, Koordinator für Außen- und Sicherheitspolitik der Konrad-Adenauer-Stiftung, Lehrbeauftragter für Internationale Sicherheitspolitik an der Zeppelin Universität in Friedrichshafen.

Sowohl in sicherheitspolitischen Expertenzirkeln als auch in der breiten Öffentlichkeit hat das Thema „Cyber“ derzeit Konjunktur, weil es mit viel Angst und Ungewissheit verbunden ist. Das liegt zum einen an der offensichtlichen Verwundbarkeit unserer vernetzten Lebenswelt und den katastrophalen Folgen, die ein umfassender Angriff auf dieses digitale System haben könnte. Zum anderen liegt es an der Neuartigkeit des Cyberspace und der weitverbreiteten Ahnungslosigkeit über seine technischen Voraussetzungen, Funktionsweisen und wahrscheinlichen nächsten Entwicklungsschritte. Ganze Generationen von Entscheidungsträgern und einfachen Bürgern, die sich soeben erst mühsam mit ihrem E-Mail-Account vertraut gemacht haben, meinen sich nun für den Cyberkrieg rüsten zu müssen. Welche Bedeutung kommt „Cyber“ aber tatsächlich in der Sicherheitspolitik zu?

Zunächst einmal gilt, dass Bedrohungen im Cyberspace vielgestaltig sind. Das Spektrum reicht von Kriminalität über Spionage, Sabotage und Terrorismus bis hin zum Krieg. In der öffentlichen Debatte über Cybersicherheit ist eine besondere Fokussierung auf das extreme Ende dieser Skala, den Cyberkrieg, zu beobachten. Die Vokabel „Krieg" erzeugt besondere Aufmerksamkeit und Furcht, was oftmals auch privaten Gewinninteressen dienlich ist. Allerdings führt dieser einseitige Fokus zu einer Schieflage, denn die bislang bei Weitem häufigsten und schädlichsten Cyberangriffe bewegen sich im Bereich der Kriminalität: Betrug und Diebstahl machen den Großteil der Schadensfälle aus. Aus technischer Sicht ist die Unterscheidung zwischen einem Cyberangriff zum Zweck des Diebstahls oder der Spionage von einem Cyberangriff zum Zweck der Sabotage oder der Beschädigung kritischer Infrastrukturen zwar nicht zu unterscheiden, aber aus politischer und strategischer Sicht verlangen diese unterschiedlichen Motivationen unterschiedliche Schutzmaßnahmen und Reaktionen.

NEUE DIMENSION DER KRIEGSFÜHRUNG?

Im Ringen um die angemessenen Maßnahmen bedienen sich die Strategen bestimmter Analogien, um die Neuartigkeit des Cyberspace entlang bekannter Muster handhabbar zu machen. Oft entstehen dabei aber falsche Analogien, die nur scheinbar zutreffen und daher zu nutzlosen oder sogar gefährlichen Empfehlungen führen. Zum Beispiel ist immer wieder vom Cyberspace als „fünfter Dimension der Konfliktaustragung" die Rede. Demnach wäre der Cyberspace neben Land, Wasser, Luft und All eine weitere, originäre Sphäre militärischer Aktion. Richtig ist jedoch, dass Cyber integrativer Bestandteil aller vier gängigen Sphären ist – ohne computergestützte, vernetzte Operationsführung und Datenerhebung sind heute Heer, Marine und Luftwaffe nicht mehr denkbar. Gerade das macht sie verwundbar für Cyberangriffe. Spätestens bei der praktischen Frage des Aufgabenzuschnitts der Teilstreitkräfte erweist sich daher die Dimensionen-Analogie als irreführend.

Eine andere beliebte, aber falsche Analogie ist die zwischen Cyberstrategie und Nuklearstrategie. Die zwei wichtigsten Säulen der Nuklearstrategie sind Abschreckung einerseits und internationale Abkommen zur Reglementierung (Transparenz, Abrüstung) der nuklearen Bestände andererseits. Aufgrund des apokalyptischen Potenzials der Atombombe ist die Nuklearstrategie zur „strategischen Königsdisziplin" aufgestiegen, wird dadurch aber nicht zum Passepartout. Denn die Voraussetzung für eine glaubwürdige Abschreckung ist – neben ausreichenden eigenen Kapazitäten für einen Zweitschlag –, dass der Urheber (oder wenigstens Ausgangspunkt) des Erstschlags eindeutig zu bestimmen ist. Solche Rückverfolgung („Attribution") ist aber im Cyberspace nicht zuverlässig möglich. Digitale Informationen sind flüchtig, Daten-

spuren lassen sich leicht als falsche Fährten legen und die finale Lücke zwischen Mensch und Maschine – zwischen dem auslösenden Finger und der Tastatur – kann meist nicht mit Bestimmtheit geschlossen werden. Angesichts solch löchriger Beweisketten kann Abschreckung nicht funktionieren, *mutual assured destruction* ist im Cyberspace hinfällig.

Außerdem sind „Waffen" im Cyberspace sehr viel erschwinglicher und leichter zugänglich als nukleare Waffen, woraus sich eine große Zahl relevanter nicht-staatlicher Akteure ergibt. Das erschwert nicht nur die inter-staatliche Abschreckung, sondern offenbart auch die Schwächen internationaler Abkommen zum Cyberspace. „No first use"-Erklärungen nach dem Vorbild der nuklearen Friedensbewegung oder Selbstbeschränkungen im Geiste des Atomteststoppabkommens werden den Cyberspace unsicherer machen, weil sie nicht-staatliche Akteure wie terroristische Gruppierungen nicht binden und somit – relativ zu staatlicher Macht – aufwerten. Ohnehin wären solche Abkommen nicht überprüfbar und würden daher nur diejenigen Staaten begünstigen, die skrupellos nach ihrem strategischen Vorteil greifen.

WETTRÜSTEN IM CYBERSPACE

Eine Folge dieser Überlegungen ist der gegenwärtig noch camoufliert und geheim stattfindende internationale Wettlauf um Fähigkeiten im Cyberspace: Das amerikanische Militär hat das U.S. Army Cyber Command eingerichtet, die NATO ein Cyber Defence Center of Excellence in Tallinn. Russland wird verdächtigt, 2007 kritische Internetstrukturen in Estland lahmgelegt und auch im Krieg gegen Georgien 2008 Cyberangriffe durchgeführt zu haben. China hat im Oktober 2011 seine erste große Cyberkriegsübung abgehalten. Was genau in diesen Übungen, Kommandos und Einsätzen geschieht, weiß man nicht. Auch ist unbekannt, an welchen Kapazitäten die Staaten derzeit forschen. Unstrittig ist jedoch, dass immer neue Entwicklungen einsatzfähig werden. Das illustrierte zuletzt der Stuxnet-Virus, der 2010 Industrieanlagen der Firma Siemens sabotierte – vor allem in den Werkstätten des iranischen Atomprogramms.

Für die deutsche Sicherheitspolitik ergeben sich aus dieser Situationsanalyse vier zentrale Aufgaben. *Erstens* muss die strategische Kommunikation zwischen Informatik- und Cyberexperten auf der einen und militärischen und politischen Experten auf der anderen Seite verbessert werden. Das sind traditionell sehr verschiedene Gemeinschaften, mit eigenen Codes, Verhaltensweisen und impliziten Annahmen. Jedes Forum, das diese Gräben zu überwinden und eine gemeinsame Sprache zu finden hilft, verdient Unterstützung. Zu beachten ist dabei allerdings, dass viele Konferenzen und Strategieworkshops, die sich mit dem Thema Cyber beschäftigen, ihre Aufmerksamkeit auf die technischen Fragen richten, aber die Einbettung in den sicherheitspoliti-

schen Gesamtzusammenhang vernachlässigen. Dem durchaus faszinierenden Technik-Fetischismus dürfen die genuin politischen und strategischen Fragen nicht untergeordnet werden – im Kalten Krieg wurden schließlich auch keine Strategieworkshops zur AK-47 (sowjetisches Sturmgewehr „Kalaschnikow“) durchgeführt.

Zweitens wird beim Thema Cyber die in Deutschland stark ausgeprägte Bruchlinie zwischen sicherheitspolitischen Experten und der Öffentlichkeit besonders deutlich. Wer für eine Sicherheitspolitik eintritt, die Bedrohungen und Risiken klar benennt und darauf drängt, auch militärische Lasten zu tragen und Verantwortung für die Stabilität des internationalen Systems insgesamt zu übernehmen, hat in der deutschen Öffentlichkeit einen schweren Stand – ungeachtet der Tatsache, dass solch eine Haltung Deutschlands Werten und Interessen entspricht und auch von unseren Verbündeten erwartet wird. Der Vorwurf der „Militarisierung der Außenpolitik“ oder der zynischen Machtpolitik ist hierzulande schnell zur Hand. Es ist eine grundsätzliche und gesamtstaatliche Aufgabe, in Fragen der Sicherheits- und Militärpolitik zu einem sachlicheren und sachkundigeren gesellschaftlichen Diskurs zu gelangen.

Es ist jedoch zweifelhaft, ob Cyber dafür der richtige Ausgangspunkt ist. Schon die Unmöglichkeit einer zuverlässigen Trennung zwischen offensiven und defensiven Fähigkeiten im Cyberspace spricht nicht für einen glücklichen Beginn einer öffentlichen Debatte in Deutschland. Denn um im Cyberspace defensiv stabil zu sein, muss man seine Verteidigungslinien ständig neuen Angriffen aussetzen und entsprechend anpassen und optimieren. Eine Fernsehdebatte über „offensive Cyberkapazitäten der Bundeswehr“ zu führen, wäre allerdings mit Sicherheit eine undankbare Aufgabe für jeden Politiker. Möglicherweise wird man daher die sicherheitspolitische Debatte im Grundsatz vorantreiben, Cyberfähigkeiten aber vornehmlich ohne viel öffentlichen Aufhebens im Bündnis weiterentwickeln.

DEUTSCHLANDS VERWUNDBARKEIT

Drittens gilt es, angesichts der Mängel einer Abschreckungs- und Verhandlungsstrategie Deutschland auf eine Strategie der Verteidigung auszurichten. Vorsorge und Widerstandsfähigkeit sind dabei von zentraler Bedeutung. Die Fähigkeit, einen Cyberangriff zu verkraften („Resilienz“), wird zum entscheidenden Erfolgs- und Friedenskriterium potenzieller Cyberkonflikte. Vor allem mit Blick auf seine kritischen Infrastrukturen muss sich Deutschland auf denkbare Angriffe vorbereiten und seine Verwundbarkeit reduzieren. Dazu gehören Aufklärungskampagnen und Schutzmaßnahmen, die verschiedene Adressaten zum Handeln bewegen. So wie der private User seinen Computer gegen kapernde Bot-Netze absichern muss, so müssen Unternehmen ihre

Erfahrungen als Opfer von Cyberangriffen mit staatlichen Behörden vertraulich teilen, um optimale, koordinierte Gegenmaßnahmen zu ermöglichen. Die Cyber-Sicherheitsstrategie des Bundesinnenministeriums von 2011 wagt in diesem Sinne immerhin einige erste Schritte, aber es bleibt ein langer Weg zu gehen.

Viertens und nicht zuletzt sollte in der deutschen strategischen Community ein Bewusstsein für die Bedeutung des Themas geschaffen werden. Cybersicherheit ist kein Modethema, das vergehen wird. Aber es ist auch keine neue Welt, die mit den Regeln staatlicher Macht- und Interessenkonkurrenz und damit der Strategiebildung nicht zu fassen wäre. Allerdings verändert sich dieser Gegenstand der Strategiebildung fortlaufend und in rasantem Tempo. Der Cyberspace von 2014 ist nicht der Cyberspace von 1996, als Bill Clinton der erste amerikanische Präsident mit einer E-Mail-Adresse war, und er wird auch nicht der Cyberspace von 2020 sein. Diese Veränderungen im Blick zu behalten und adäquate Reaktionen darauf zu finden, ist eine sicherheitspolitische Aufgabe ersten Ranges.