Bundesakademie
für Sicherheitspolitik

2/21

#BAKS Arbeitspapiere

Deutschlands Cybersicherheitsstrategie im nächsten Jahrzehnt

Sicherheitspolitische Selbstbehauptung in der amerikanisch-chinesischen Digitalweltordnung

von Jakob Kullik

Deutschlands Cybersicherheitsstrategie ist in vielerlei Hinsicht ein Abbild der konventionellen deutschen Sicherheitspolitik: zu risikoscheu, zu wenig strategisch, zu rechtsfixiert. In der digitalen Welt haben sich die Fähigkeiten und Machtpotenziale mittlerweile so verschoben, dass Deutschland nur noch ein teilsouveräner Akteur in einer von den USA und China dominierten Digitalweltordnung ist. Will Deutschland künftig eigene Handlungsräume bewahren und neue dazugewinnen, sollte die Bundesrepublik im Verbund mit der EU das strategische Ziel einer digitalen Selbstbehauptung verfolgen.

Drei grundlegende Probleme, die Deutschlands Cybersicherheit bestimmen

Deutschland hat die Digitalisierung verschlafen, so heißt es immer wieder. Das Problem ist jedoch größer und komplexer; es umfasst nicht nur versäumte politische Weichenstellungen, sondern drei grundlegende Probleme technologischer, ökonomischer und politisch-regulatorischer Art. Alle drei hängen miteinander zusammen und müssen angegangen werden, damit Deutschland als größte Volkswirtschaft in der EU wichtige Impulse gibt, um die Cybersicherheit im nächsten Jahrzehnt entscheidend voranzubringen.

Erstens: Deutschland und die EU sind aus digital-technologischer Sicht heute Teil des amerikanischen und zunehmend auch des chinesischen Datenraumes. Die wesentlichen Dienstleistungen und Infrastrukturen werden über außereuropäische Technologieunternehmen angeboten, die sich immer stärker zu integrierten Service-Plattformen entwickeln, um ihre Kunden langfristig an sich zu binden. Obwohl es nach wie vor bedeutende deutsche und europäische IT-Unternehmen gibt, die im Massensegment konkurrieren könn(t)en, sind die großen Marktsegmente derzeit unter Kontrolle eines kompetitiven amerikanisch-chinesischen Oligopols mit wenigen großen Namen: Amazon, Google, Facebook, Apple, Alibaba, Huawei und weitere.

Zweitens: Das größte ökonomische Problem der europäischen Wettbewerbsfähigkeit in der Digitalsphäre ist nicht das fehlende Potenzial an IT-(Spitzen-)Fachkräften oder innovativem Unternehmertum, sondern der unvollendete digitale Binnenmarkt. Unterschiedliche rechtliche und sprachliche Herausforderungen machen die EU zu einem Raum parzellierter mittelgroßer und kleinster Märkte, auf denen die notwendigen Skaleneffekte für datengestützte Innovationen nicht wie in den USA oder China gegeben sind.

Drittens: Die EU reagiert auf die globalen digitalen Herausforderungen bislang vor allem regulatorisch. Deutlich lässt sich das an der bislang stärksten Antwort in Form der Datenschutzgrundverordnung (DSGVO) zeigen, mit der ein weitreichendes, komplexes Regelwerk für den digitalen Verbraucherschutz geschaffen wurde. Zwar ist die zentrale Idee der DSGVO begrüßenswert, aber der Geist des Gesetzes ist im Grunde defensiv. Europas Antwort auf die Aufteilung der Welt durch fremde Unternehmen und zwei Weltmächte ist ein normativer Schutzzaun, dessen primäres Schutzgut – Daten – überwiegend nicht von europäischen Unternehmen erfasst, analysiert und zur Weiterentwicklung von Produkten und Dienstleistungen genutzt wird.

Obwohl es zu früh ist, um eine angemessene und differenzierte Bilanz der DSGVO und weiterer europäischer Regulierungsinitiativen zu ziehen, darf doch bezweifelt werden, ob durch diese Konzepte etwas Grundlegendes an den derzeitigen Markt- und Machtverhältnissen verändert wurde. Allein mit dem Instrument des Rechts wird den großen Datenmonopolisten – insbesondere den chinesischen – schwerlich Herr zu werden sein. Das Gegenteil könnte eintreten: Wenn es keine bedeutenden europäischen Player mehr gibt, werden in Zukunft die Regeln für das Datenzeitalter vorrangig durch Washington und Peking gesetzt. Europa spielt dann zwar noch bei der Rechtssetzung eine Rolle, nicht aber mehr auf den Märkten.

Verlockende, aber (derzeit) unrealistische Zielbegriffe in der Cybersicherheitsdebatte

Diese drei Hauptprobleme wirken auf unterschiedliche Weise. Hiervon Kenntnis zu nehmen ist ein erster Schritt, um sich mehr Klarheit über den realistischen Umsetzungsgehalt einiger populärer Begrifflichkeiten in der aktuellen Cybersicherheitsdebatte zu verschaffen. Nicht selten wird mit Blick auf Deutschlands und Europas defizitäre Cybersicherheitsfähigkeiten von mehr digitaler „Autonomie“ oder „Souveränität“ gesprochen. Bisher ist jedoch das Verständnis über die Tragweite dieser Zielbegriffe noch unzureichend. Auch existiert kein tragfähiges Politikkonzept, das aufzeigt, was größere Digital-Autonomie beziehungsweise Cyber-Souveränität in technischer, ökonomischer und politisch-regulatorischer Hinsicht bedeuten würden. Essenzielle Fragen, die damit im Zusammenhang stehen, sind zum Beispiel: Über welche (defensiven und offensiven) Cyberfähigkeiten sollten die Nationalstaaten oder die EU künftig verfügen? Wer kontrolliert und finanziert die europäischen Datennetze der nächsten Generation? Die Antworten auf diese und weitere strategische Fragen stehen noch aus. Sie sollten jedoch intensiver und konkreter diskutiert werden.

Digitale Selbstbehauptung als Zielvektor

Da die Diskussion um die ambitionierten Großziele von digitaler Souveränität und Autonomie noch am Anfang steht und diese – wenn überhaupt – wohl nur langfristig und mit großem Mitteleinsatz zu realisieren wären, sollte der mittelfristige Fokus bescheidener und realistischer sein. Ein realistisches Ziel wäre die digitale sicherheitspolitische Selbstbehauptung. Aus staatlicher Sicht hieße das, die vorhandenen technischen (Infra-)Strukturen und Möglichkeiten selbstbewusst-strategisch zu nutzen und eigene Fähigkeiten im Cyberraum kontinuierlich fortzuentwickeln. Das Ziel hierbei ist, bestehende ökonomische, technische und sicherheitspolitische Abhängigkeiten zu reduzieren.

Entscheidend ist, dass dabei der Zielfokus mehr auf politisch-strategische Beurteilungen und langfristige Interessen gelegt wird und weniger auf rechtliche Grundsatzbedenken. Gleichwohl rechtliche Vorgaben unbedingt zu beachten sind, gilt es doch, Spielräume auszuschöpfen, um die staatliche Kernfähigkeit in der Cybersicherheit, insbesondere bei der immer wichtiger werdenden weltweiten nachrichtendienstlichen Aufklärung und den offensiven (militärischen) Computernetzwerkoperationen, auf Dauer gewährleisten zu können. Nationalstaatliche beziehungsweise europäische digitale Selbstbehauptung heißt *nicht*, sich vom globalen Internet zu entkoppeln oder einer neoprotektionistischen Digital- und Technologiepolitik das Wort zu reden, sondern die gegebenen technischen, ökonomischen und politisch-regulatorischen Möglichkeiten und Potenziale, die Deutschland (und die EU) haben, stärker als bisher für die eigenen Interessen einzusetzen. Maßnahmen, die auf diesem Weg ergriffen werden könnten, müssen nicht unbedingt nur auf europäischer Ebene ansetzen. Auch wenn es wünschenswert wäre, die großen Probleme EU-gemeinschaftlich anzugehen,

sollten die Erwartungen diesbezüglich nicht allzu hoch gesteckt werden. Dass künftig alle Politikfelder mit Digitalbezug auf EU-Ebene bearbeitet werden, ist nicht in Sicht und würde zudem auf nationalstaatliche Vorbehalte stoßen. Es empfiehlt sich daher ein kleinschrittiges, realistischeres Vorgehen, das die richtigen Stellschrauben und Weichen sowohl auf deutscher als auch europäischer Ebene in den Blick nimmt. Letztlich ist die deutsche Cybersicherheitspolitik insgesamt handlungsfähiger, effektiver und durchsetzungsstärker auszugestalten und sind handlungseinschränkende Strukturen abzubauen.

Drei Handlungsempfehlungen für eine selbstbehauptungsorientierte Cybersicherheitsstrategie Deutschlands

I. Weniger (Cybersicherheits-)Behörden, dafür mehr Exekutivkompetenzen

Die föderale Struktur Deutschlands bringt es mit sich, dass eine Vielzahl staatlicher Stellen mit den Themen der Digitalisierung und Cybersicherheit betraut sind. Auch im originären Bereich der digitalen Sicherheitspolitik sind mehrere Ministerien und Sicherheitsbehörden verantwortlich. Allein fünf Bundesministerien (Inneres, Wirtschaft, Verkehr, Äußeres, Verteidigung), das Bundeskanzleramt und diverse Ministerien in den Bundesländern bearbeiten Cybersicherheitsthemen. Insgesamt sind auf Bundes- und Länderebene knapp 40 Sicherheitsbehörden beteiligt. Über den seit langem vorgebrachten Vorschlag, ein Bundes-Digitalministerium einzurichten, in dem mehrere Verantwortlichkeiten gebündelt werden könnten, hat die (nächste) Bundesregierung zu entscheiden.

Es muss jedoch nicht gleich der „große Wurf“ gewagt werden, da größere institutionelle Veränderungsprozesse bekanntermaßen lange dauern und oft auf interne Widerstände stoßen. Auch kleinere institutionelle Neuzuschnitte bei den für Cybersicherheit zuständigen Sicherheitsbehörden sind denkbar. Möglich wäre etwa, den Verantwortungsbereich für die digitale Spionageabwehr und den Wirtschaftsschutz aus der Zuständigkeit des Bundesamts für Verfassungsschutz (BfV) herauszulösen und künftig beim Bundesnachrichtendienst (BND) zu konzentrieren. Drei Überlegungen liegen diesem Vorschlag zugrunde. Erstens könnten dadurch das Bundesamt und auch die ebenfalls in diesem Feld tätigen 16 Landesverfassungsschutzämter entlastet werden, um sich ausschließlich mit ihrem eigentlichen Kernarbeitsfeld, der politischen Extremismus-Beobachtung zu befassen, gerade da deren Bedeutung gegenwärtig zunimmt. Da Cyberspionage in der Regel eine internationale Dimension hat, wäre ihre Bekämpfung auf Bundesebene grundsätzlich besser aufgehoben als in den personell und technisch höchst unterschiedlich ausgestatteten Landesämtern.

Zweitens gelten der BND, aber auch das Bundeskriminalamt (BKA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) bei der Analyse und Detektion von Cyber-Phänomenen als technisch versierter als der Verfassungsschutz. Der BND könnte mit der Hauptzuständigkeit für digitale Spionageabwehr und Wirtschaftsschutz seine bereits erworbene Cyber-Expertise ausbauen und neben seinen außen- und sicherheitspolitischen Hauptbeobachtungsfeldern auch die wirtschaftliche Dimension stärker in den Blick nehmen. Drittens wären damit künftig die vier Säulen der Cybersicherheitsarchitektur auf Bundesebene beim BND (Auslandsnachrichtendienst), dem BKA (Polizei), dem BSI (Technik) und der Bundeswehr (Militär) etwas stärker konzentriert. Die operative Effektivität aller Stellen wird freilich in entscheidendem Maße von den ihnen zur Verfügung stehenden technischen Wirkmitteln und rechtlichen Möglichkeiten abhängen.

II. Offensive Cyberoperationen gehören zum notwendigen Fähigkeitsspektrum

Die bisherige deutsche Debatte um offensive Computernetzwerk- beziehungsweise Cyberoperationen ist von dem Bestreben gekennzeichnet, für die vielen unterschiedlichen Einsatzszenarien und Phänomene im digitalen Ernstfall möglichst eindeutige, rechtsklare und objektive Begrifflichkeiten zu definieren, an denen sich die zuständigen staatlichen Stellen ausrichten können. Typische Termini bei Cybervorfällen sind zum Beispiel „offensiv“, „defensiv“, „militärisch“ und „Schadens(aus)maß“. Empirisch betrachtet verschwimmen jedoch die Phänomene, denen sich Deutschland und Europa ausgesetzt sehen, mit Blick auf die Akteure und eingesetzten Mittel. Cyberangreifer können einen politisch-aktivistischen, kriminell(kommerziell-)en, nachrichtendienstlichen und/oder militärischen Hintergrund haben.

Sicherlich muss juristisch und politisch hinreichend geklärt werden, wann der sogenannte digitale Verteidigungsfall eintritt, der ein Aktivwerden der Bundeswehr im Cyberraum erforderlich machen würde. So schwierig dieser Fall vorab auch zu bestimmen sein mag, sollte die zentrale Schlussfolgerung daraus jedoch nicht sein, die Möglichkeit des digitalen Gegenschlags oder *Hack-Backs* grundsätzlich zu untersagen oder rechtlich so einzuschränken, dass er faktisch wirkungslos bleibt. Wer mittels Cyberangriffen staatliche Institutionen, kritische Infrastrukturen oder Wirtschaftsunternehmen in Deutschland angreift und dabei erhebliche Schäden verursacht, sollte auch mit spürbaren Konsequenzen rechnen müssen. Diese können dann nicht allein diplomatischer oder juristischer Art sein. Rein symbolische Verurteilungen oder das Bemühen, die Angreifer – insofern sie zweifelsfrei identifizierbar sind – vor ein deutsches Gericht zu stellen, sind selten erfolgreich und haben kaum abschreckende Wirkung.

Das digitale Pendant zu den analogen militärischen und nachrichtendienstlichen Reaktionsfähigkeiten sind offensive Cyberoperationen. Und diese sollten im Fähigkeitsspektrum des Staates grundsätzlich verfüg- und bei Bedarf einsetzbar sein. Ob Cyberoperationen durch die entsprechenden Einheiten der Bundeswehr oder des Bundesnachrichtendiensts durchgeführt werden, sollte vorrangig an den Parametern Interessen, Ziele und Möglichkeiten ausgerichtet werden. Gleichwohl gilt es auch bei dieser Art von Operationen, einen handlungsbefähigenden Rechtsrahmen zu haben – wie etwa bei Auslandseinsätzen der Bundeswehr. Denkbar wäre auch, eine neue Rechtsgrundlage zu schaffen, die die zusammenhängenden Operationsfelder Cyberspionage(abwehr) und Offensivoperationen gemeinsam adressiert. Diese sollte freilich mit den geltenden völkerrechtlichen Prinzipien (für den Cyberbereich) übereinstimmen.

Das Fähigkeitsspektrum von Cyberoperationen würde das Eindringen in und das Verändern von Computernetzwerken umfassen. Mögliche operative Wirkungen wären etwa der Datenabgriff, die Unterbrechung von Diensten, das Platzieren und Ausnutzen von Schwachstellen in gegnerischen Systemen sowie das Erzeugen einer temporären oder dauerhaften Schadenswirkung in den Zielsystemen. Es steht außer Frage, dass leitende operative Handlungsmaßstäbe die zielgenaue Verhältnismäßigkeit der Einsatzmittel und die Schadensminimierung, gerade mit Blick auf Unbeteiligte, sein müssen. Die Uneindeutigkeit des digitalen Gefechtsfeldes, die zeit- und ressourcenintensive Rückverfolgung von Angriffen und die Furcht vor Schadensfolgen (mögliche Kaskadeneffekte) dürfen jedoch nicht die grundsätzliche Bereitschaft zum offensiven Gebrauch von Cyberwirkmitteln in Frage stellen, da ansonsten Deutschland Gefahr läuft, in der digitalen Sicherheitspolitik nicht ernst genommen zu werden und potenzielle Angreifer womöglich noch animiert, Cyberattacken durchzuführen. Deswegen sollte eine effektive Cybersicherheitspolitik nie nur auf das defensive Sichern der eigenen Systeme und technischen Infrastrukturen beschränkt bleiben. Um im Ernstfall operative Alternativen zu haben, sollten immer auch offensive Fähigkeiten und Mittel dazugehören.

III. Eigene (europäische) Netz-Infrastrukturen aufbauen und relevante Unternehmen unterstützen

Das bisher nahezu uneingeschränkte Vertrauen auf die Kräfte des Marktes und die gleichzeitige strategische Missachtung der damit einhergehenden neuen Machtstrukturen auf den Digitalmärkten haben dazu geführt, dass Europa unter den führenden Wirtschaftsmächten bei der digitalen Wettbewerbsfähigkeit momentan am schlechtesten positioniert ist. Bei den Digitalplattformen, den Cloudanbietern und den führenden Softwareunternehmen gibt es mit wenigen Ausnahmen auf dem Weltmarkt keine bedeutenden europäischen Unternehmen mehr. Lediglich bei den Netzwerkausrüstern existieren mit Nokia und Ericsson noch alternative Anbieter zu den amerikanischen und chinesischen Marktführern. Dasselbe Versäumnis erleben wir momentan bei der Batterietechnologie, wo nicht nur Europa, sondern der gesamte Westen asiatischen Playern schon vor Jahren das Feld überlassen hat. Wäre vor Jahrzehnten nicht die Entscheidung getroffen worden, mit Airbus einen gemeinsamen europäischen Luftfahrtkonzern aufzubauen, würde Europa heutzutage auch im Flugverkehr vollkommen von außereuropäischen Anbietern abhängig sein.

Die Beispiele zeigen allesamt, dass es bei strategischen Sektoren und Zukunftstechnologien nicht genügt, auf kurz- und mittelfristige Renditeaussichten zu hoffen. Wer in den (künftigen) technologischen Massenmärkten relevant sein will, muss frühzeitig investieren und langfristig durchhalten. Wenn Europa seine Abhängigkeit von amerikanischen und chinesischen IT-Unternehmen reduzieren will, führt kein Weg daran vorbei, einige Schlüsselsektoren zu identifizieren, in die langfristig investiert werden muss, damit sie unter europäische Kontrolle gebracht werden. Hierzu gehören die technischen Infrastrukturen, insbesondere Rechenzentren und der Aufbau einer europäischen Cloud-Infrastruktur vorrangig für den öffentlichen Sektor.

Mit dem Projekt GAIA-X wurde bereits eine wichtige Initiative angeschoben. Der Erfolg der Initiative sollte jedoch nicht von den Hoffnungen der beteiligten Unternehmen abhängig gemacht werden. Die digitalen Pendants zu den analogen Bundesfernstraßen beziehungsweise Europastraßen sollten gemeinsame europäische digitale Datennetze und -zentren sein, die die Grundlage für die digitale Verwaltung in der gesamten EU bilden können. Wenn europäische Institutionen mithilfe europäischer IT-Unternehmen ihre eigene Infrastruktur kontrollieren würden, könnten die konkurrierenden Ziele von mehr digitaler Eigenständigkeit, strategischer Industriepolitik und Verbraucherschutz im (europäischen) Netz besser und womöglich gleichzeitig erreicht werden. Das von der EU-Kommission angestrebte Ziel einer Digital-Union kann dabei nur mit einem größeren Pool an eigenen Fähigkeiten und mehr Kontrolle über die eigenen Netzinfrastrukturen erreicht werden.

Politik und Wirtschaft können den strategischen Wettbewerb mit den USA und China nur gemeinsam bestreiten. Dabei sollte nicht außer Acht gelassen werden, dass trotz aller Bemühungen, Deutschland und die EU im Cyberbereich sicherheitspolitisch unabhängiger und handlungsfähiger zu machen, die enge transatlantische Bindung wichtigster Ankerpunkt bleiben sollte. Denn auch wenn die USA ein schwieriger Partner im Bereich Cybersicherheit sind, so sind sie doch in vielerlei Hinsicht auch im Digitalzeitalter verlässliche Schutzmacht und Wertepartner. Auch im Digitalen gilt daher für Deutschland und Europa, dass Selbstbehauptung nicht gegen, sondern mit den USA zu erreichen ist.

Deutschland als größte Volkswirtschaft in der EU kommt bei all diesen Überlegungen und Initiativen eine Schlüsselrolle als Impulsgeber und Motor zu. Ohne die politische Bereitschaft in Berlin, mit den europäischen Partnern industriepolitisch voranzugehen und sich für den Erhalt und die Unterstützung der verbliebenen europäischen Netzwerkausrüster einzusetzen, wird die nächste Debatte um den Mobilfunkstandard 6G womöglich nur noch darum geführt werden, wie die EU als digitale Kolonie der USA oder, weit schlimmer noch, Chinas ihre Standards – dann wohl nur noch auf dem Papier – erhalten kann. Europa wird dann keinen Einfluss mehr auf die relevanten Lieferketten haben, und der Aufbau der Netze wird zu den Bedingungen amerikanischer und chinesischer Unternehmen erfolgen. Ohne europäische Unternehmen, eigene Fähigkeiten und den politischen Willen, am Markt präsent zu sein, wird Europa in der digitalen Weltordnung von Morgen nur ein randständiger Akteur und machtpolitisch bedeutungslos sein. Die cybersicherheitspolitische Maxime für das nächste Jahrzehnt sollte daher lauten: digitale Selbstbehauptung.

Jakob Kullik ist Wissenschaftlicher Mitarbeiter und Doktorand an der Professur für Internationale Politik der Technischen Universität Chemnitz. Er ist Mitglied im Arbeitskreis „Junge Sicherheitspolitiker“ der BAKS. Der Autor gibt seine persönliche Meinung wieder.