Deutscher Bundestag **Drucksache 20/13810**

20. Wahlperiode 14.11.2024

Antrag

der Abgeordneten Volker Münz, Nicole Höchst, Dr. Götz Frömming, Dr. Michael Kaufmann, Barbara Benkstein, Matthias Moosdorf, Norbert Kleinwächter, Martin Reichardt, Tobias Matthias Peterka, Jan Wenzel Schmidt und der Fraktion der AfD

Den 360-Grad-Blick bei der Wissenschaftsspionage jetzt umsetzen – Deutsche Wissenschaft schützen

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Neben nichtwestlichen Staaten wie der Russischen Föderation oder der Volksrepublik China, deren Wissenschaftsspionageaktivitäten gegen Deutschland zurecht Objekt der Spionageabwehr sind, müssen auch die USA als Ausgangspunkt von gegen Deutschland gerichteter Wissenschaftsspionage und deren entsprechende Aktivitäten als Gefahr für die Leistungsfähigkeit, die Datensicherheit, das geistige Eigentum und die Wissenschaftsfreiheit des deutschen Wissenschaftssystems, seiner wissenschaftlichen Einrichtungen und seiner Wissenschaftler anerkannt werden. Die Erfahrungen aus der Globalen Überwachungs- und Spionageaffäre (NSA-Affäre), die hohe Zahl von Cyber-Angriffen auf Forschung und Entwicklung (F&E), die beträchtlichen kapazitären Voraussetzungen, US-rechtlichen Befugnisse sowie strategischen Motive zur Durchführung von Wissenschaftsspionage geben dazu hinreichenden Anlass. Neben vergleichbaren rechtlichen Sicherheitsrisiken im Falle Russlands und Chinas lässt sich laut Forschungsergebnissen der Universität Kassel die US-rechtliche Lage wie folgt zusammenfassen: US-Unternehmen und Staatsangehörige sind verpflichtet, mit den US-Geheimdiensten zusammenzuarbeiten. Die Geheimdienste können eigene (Tarn-)Unternehmen gründen oder Mitarbeiter in bestehende Unternehmen einschleusen. Dies gilt nicht nur für Unternehmen, die in den USA tätig sind, sondern auch für weltweit tätige Unternehmen und deren Tochterorganisationen in anderen Staaten. Von diesem System werden auch ausländische Töchter deutscher Organisationen erfasst, die in den USA tätig sind. Die verpflichteten Unternehmen wirken in Deutschland oder in der Kommunikation mit deutschen Stellen wie „Trojanische Pferde“. Ihnen ist ihre Funktion für die nachrichtendienstliche Tätigkeit nicht anzusehen. Die US-Geheimdienste haben potenziell Zugriff auf alle in den USA gespeicherten Daten. Dies gilt auch für alle Daten, die Organisationen aus den USA und ihren Tochterorganisationen anvertraut werden – insbesondere, wenn diese eine gewisse Bedeutung für nachrichtendienstliche Zwecke haben wie z. B. Forschungsdaten. Mit Blick auf die Erfahrungen aus der NSA-Affäre und ihre politischen Folgen kann festgehalten werden, dass die NSA und andere amerikanische Geheimdienste in ihren Programmen kein Eigenleben außerhalb politisch gesetzter Rahmenbedingungen geführt, sondern auf eindeutige und belegbare politische Initiative im Rahmen einer klaren sicherheits-

politischen Strategie und einer eindeutig festgelegten strategischen Rolle hin gehandelt haben. Nach Einschätzung von Experten verfolgen die USA bei der Zusammenfassung globaler Informationen, die in dieser Art vermutlich einzigartig ist, eine allumfassende Strategie von Informationsbeschaffung, deren Ziel sich im Kern als globale Informationsdominanz durch Technologieüberlegenheit zusammenfassen lässt. Während das Kompetenzzentrum Internationale Wissenschaftskooperationen (KIWi) des Deutschen Akademischen Austauschdienstes (DAAD) für den Fall einer Kooperation mit chinesischen Hochschulen und Wissenschaftseinrichtungen das Risiko betont, dass China das Ziel eines technologischen Großmachtstatus verfolge, scheint kein entsprechendes Gefahrenbewusstsein mit Blick auf die strategischen Ziele der USA zu bestehen.

Auch die Rolle der USA ist daher für eine Lageanalyse in den Blick zu nehmen, um aus den gesammelten Erkenntnissen Schlussfolgerungen für Schutzmaßnahmen und zukünftige Prävention zu ziehen. Die Tatsache, dass jeder Staat, der über die entsprechenden technischen und humanen Ressourcen verfügt, Cyberspionage betreibt, führt nach Einschätzung von Experten zu einer Aufhebung der herkömmlichen Kategorien „Bündnispartner“ oder „Alliierter“ und macht Deutschland zu einem „Verbündeten 3. Klasse“ und einem strategischen Spionageziel auch der USA.[1] Dabei zählt es in den Worten von Datenschutzexperten zu den Erfahrungen aus der NSA-Affäre, dass es im Falle größerer Angriffe auf Daten „auch die angeblichen Verbündeten sein könnten – die sich der Tarnung halber eines Servers in China bedienen“. So geht nach Meinung von Cyberspionage-Experten aus den „Vault 7-Leaks“ hervor, dass es sich bei den Maßnahmen der NSA und CIA zur Verschleierung ihrer Spionageaktivitäten um die fortgeschrittensten weltweit handelt.

Angesichts der mangelhaften und durch den Europäischen Gerichtshof (EuGH) daher für ungültig erklärten „Safe-Harbor-Abkommen“ aus dem Jahre 2000 sowie „EU-US-Datenschutzschild“ aus dem Jahre 2016 besteht auch auf EU-Ebene bereits rein rechtlich betrachtet seit Jahrzehnten kein ausreichender Datenschutz vor Zugriffen durch US-Behörden wie die NSA. Der im Juli 2023 in Kraft getretene Datenschutzrahmen EU-USA begründet bereits durch seine Fundierung durch die Durchführungsverordnung „Enhancing Safeguards for United States Signals Intelligence Activities“ des Präsidenten der Vereinigten Staaten Joe Biden vom 7. Oktober 2022 keine Aussicht auf Besserung. Die Durchführungsverordnung berechtigt US-Behörden zum Einsatz von Spionage und Überwachung, sobald dadurch auch nur eines unter einer Vielzahl von Zielen erreicht werden könnte, wie z. B. die Fähigkeiten, Intentionen oder Aktivitäten ausländischer Regierungen, Militärs, Fraktionen oder politischer Organisationen fremder Staaten sowie politischer Organisationen oder Einzelpersonen, die im Auftrag oder unter der Kontrolle einer dieser ausländischen Entitäten agieren, zu verstehen oder auch um den Klima- oder anderen ökologischen Wandel, Risiken für die öffentliche Gesundheit, humanitäre Bedrohungen, politische Instabilität oder geographische Rivalitäten zu verstehen. Die breite Auswahl an möglichen Zielen, die gemäß der Durchführungsverordnung den Einsatz geheimdienstlicher Mittel legitimieren, sowie die explizit darin aufgeführte Möglichkeit des US-Präsidenten, diese Ziele ohne Verpflichtung, dies öffentlich mitzuteilen, zu erweitern, berechtigt die US-Geheimdienste aus US-Perspektive potenziell jederzeit dazu, umfassende Spionageaktivitäten auszuüben. Nicht zuletzt gilt dies für den Bereich der Wissenschaftsspionage, da eine Vielzahl der Themen, deren potenziell besseres Verständnis gemäß der Durchführungsverordnung Spionageaktivitäten der US-Behörden rechtfertigt, Gegenstand ressourcenintensiver Forschung ist.

Zudem kritisiert der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg an der Durchführungsverordnung u. a., dass der hierin vorgesehene „Data Protection Review Court“, an den sich Bürger beim Verdacht auf Spionageak-

[1] Für Belege vgl. Begründungsteil.

tivität der US-Behörden gegen sie richten können sollen, im Ressort des US-Justizministers eingerichtet wird, somit der Exekutive zuzuordnen wäre und damit nicht richterlich unabhängig sein kann. Weiterhin bleibt unklar, wie sich die Verordnung zu anderen bestehenden US-Regulierungen wie dem „CLOUD Act“ verhält und wann aus Sicht der USA ein Zugriff auf die Daten von Bürgern von EU-Mitgliedstaaten zulässig bleibt sowie dass die Einhaltung einer solchen Verordnung für eben jene Bürger nicht einklagbar ist und auch das „Aussieben“ unerwünschter Beschwerden der Bürger möglich bleibt. Zudem werden Beschwerdeführer ausdrücklich nicht darüber informiert, ob sie Gegenstand von nachrichtendienstlichen Aktivitäten der US-Behörden waren, sondern erhalten lediglich eine standardisierte Mitteilung, die besagt, dass die Überprüfung ihrer Beschwerde abgeschlossen ist und dass derselbe Wortlaut auch für eine nachfolgende Entscheidungen des Data Protection Review Court vorgegeben ist. Laut Auskunft der Bundesregierung wird in regelmäßigen Abständen intervallartig geprüft, ob ein Beschwerdeführer das seinen Fall betreffende Urteil des Data Protection Review Courts und somit eine Antwort auf die Frage, ob er Ziel von Überwachung durch die US-Geheimdienste geworden ist, erhalten kann, was jedoch keinesfalls garantiert wird. Auf Nachfrage bzgl. der unklaren Auslegung des Rechtsbegriffs der Verhältnismäßigkeit durch die US-Behörden, bestätigte die Bundesregierung die Auffassung, „einigermaßen überzeugt“ davon zu sein, dass die US-Sicherheitsbehörden „den Zugriff auf Daten auf das notwendige und erforderliche Maß beschränken können“. Die Bundesregierung konnte die genannten Kritiken, soweit sie sie überhaupt adressiert hat, somit nicht entkräften und hat sie in Teilen sogar bestätigt. Während die Bundesregierung das Gefahrenpotenzial nichtwestlicher Staaten wie Russland oder China zumindest anerkennt, muss das von der Bundesregierung in die US-Behörden gesetzte Vertrauen, angesichts der bereits genannten Fälle von US-Spionageangriffen und der technisch sowie rechtlich mangelhaften Schutzvorkehrungen von deutscher und unionaler Seite, als unbegründet und naiv beurteilt werden.

Die Digitalisierung von Informationen und Kommunikationsmedien erzeugt überdies Angriffspunkte für Wissenschaftsspionage, was bei der Förderung digitaler Infrastruktur und digitaler Lernmedien gerade in Hinblick auf wissenschaftliche Institutionen wie Hochschulen konzeptionell eingepreist werden muss, um eine Wissensabschöpfung durch ausländische Konkurrenten zu vermeiden. Die meisten der betreffenden Unternehmen unterfallen dem US-Recht, sodass US-Behörden auf Basis des CLOUD Act per Herausgabeverlangen bezüglich elektronischer Beweismittel in Strafverfahren Zugriff auf die Server der Unternehmen erlangen können, ohne auf die Entscheidung über die Herausgabe durch die jeweils zuständige ausländische (also bspw. deutsche) Behörde angewiesen zu sein. Die Unternehmen und ihre Tochterfirmen sind demnach nicht nur zur Herausgabe ihrer eigenen Daten verpflichtet, sondern auch der ihrer Kunden und das auch dann, wenn diese Daten in europäischen Rechenzentren der US-Anbieter gespeichert sind. Eine entsprechende Herausgabeanordnung kann auch Daten europäischer Unternehmen betreffen, sofern diese Cloud-Reserven an einem europäischen Rechenzentrumsstandort eines US-Anbieters nutzen. Der Zugriff von US-Behörden auf die gespeicherten Daten lässt sich damit von deutscher Seite zeitlich und örtlich nicht begrenzen, was eine nicht tragbare Gefährdung der Datensicherheit und des Datenschutzes der Nutzer und gerade im Falle von wissenschaftlichen Institutionen wie Hochschulen ein Einfallstor für Wissenschaftsspionage und Wissensabschöpfung darstellt. Die Zugriffsmöglichkeit von US-Behörden, über ihre marktdominierenden IT-Unternehmen und unter Verweis auf legale Ermittlungsvorgänge deutsche Forschungsergebnisse und Wissensbestände auszuforschen und abzuschöpfen, weist nach Auffassung der Antragsteller gravierende Ähnlichkeit mit dem Vorgehen von US-Behörden und -Unternehmen im Rahmen der NSA-Affäre auf, wie es bereits 2014 im NSA-Untersuchungsausschuss im deutschen Bundestag von sachverständiger Seite herausgestellt worden ist. Zum Zweck einer digitalen und technologischen Souveränität Deutschlands müssen hier Sicherheitskonzepte entwickelt und konsequent umge-

setzt werden, zumal es sich bei der IT-Sicherheit um das „digitale Herz“ jeder Institution handelt. Gehemmt wird der Ausbau der Cybersicherheit an Hochschulen zudem durch die geltende Rechtslage, gemäß der auch das wohlmeinende Identifizieren, Melden und Schließen von Sicherheitslücken potenziell einen Strafbefehl zur Folge haben kann. Die Bundesregierung hat im Koalitionsvertrag zwar angekündigt, das „Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z. B. in der IT-Sicherheitsforschung, soll legal durchführbar sein“. Umgesetzt hat sie dies bislang jedoch nicht, einen entsprechenden Gesetzentwurf hat sie laut ihrer Antwort auf eine Schriftliche Frage für das erste Halbjahr 2024 angekündigt. Hier besteht dringender Handlungsbedarf, um Rechtssicherheit für die IT-Sicherheitsforschung zu schaffen und so den dringend erforderlichen Ausbau der Cybersicherheit an und mithilfe von Hochschulen und wissenschaftlichen Einrichtungen besser unterstützen zu können.

Eine mangelnde Diversifizierung der Anbieter bei der Ausstattung von Bildungseinrichtungen birgt überdies insbesondere mit Blick auf die quasimonopolistischen Marktführer mehrheitlich US-amerikanischer Provenienz die Gefahren einseitiger Abhängigkeiten und des Datenmissbrauchs. Diese Abhängigkeit äußert sich nicht zuletzt in der Anpassung von Curricula und Lehrmethoden an Lernziele und Werbestrategien der IT-Anbieter, wie sie an deutschen Schulen bereits stattfindet und vor allem mit Blick auf die Situation in den USA auch für die Hochschulen droht. Während diese Gefahren durch ehemalige Präsidenten der Nachrichtendienste klar benannt werden, lassen die für Spionage- und Cyberabwehr zuständigen Behörden Bundesamt für Verfassungsschutz (BfV), Bundesamt für den Militärischen Abschirmdienst (BAMAD) und Bundesnachrichtendienst (BND) in ihren Publikationen kein hinreichendes Gefahrenbewusstsein erkennen. Die Nachrichtendienste beschränken sich bei der Benennung von Gefahrenquellen auf Akteure von außerhalb westlicher Kooperations- und Bündnisstrukturen wie China und Russland, was der realen Situation nicht gerecht wird. Anders als es gemäß Presseberichten zur BSI-Affäre von der Spitze des Bundesministeriums des Innern und für Heimat (BMI) vertreten wird, ist ein restriktives Vorgehen im Umgang Sicherheitsrisiken wie digitalen Hintertüren in IT-Produkten für Zugriffe von Ermittlungsbehörden oder Geheimdiensten im Sinne der Cybersicherheit nicht zuletzt an wissenschaftlichen Einrichtungen wie den Hochschulen dringend geboten.

Der auch vom Wissenschaftsrat betonten geopolitischen Dimension digitaler und technologischer Souveränität muss durch eine Förderung inländischer Sicherheitslösungen begegnet werden, um eine größere Unabhängigkeit von insbesondere chinesischen und US-amerikanischen Technologie- und Dienstanbietern und damit letztlich Selbstbestimmung im internationalen Rahmen zu erreichen. Andernfalls sieht sich Deutschland nach Einschätzung von Experten der Gefahr ausgesetzt, in einem „neuen kalten IT-Krieg“ von den USA oder China dominiert zu werden oder sich in Abhängigkeiten von ausländischen Unternehmen im Sinne eines „Überwachungskapitalismus“ zu begeben. Die sicherheitspolitische Abhängigkeit von den USA wird durch einen fortwährenden Verlust eigener Hoheitsgewalt und eine dauerhafte Einschränkung eigener autonomer Handlungsmacht immer wieder hervorgerufen. Der eigene Handlungsspielraum ist angesichts der asymmetrisch verteilten Fähigkeiten extrem begrenzt. Was Deutschland wissen darf, bleibt unter den gegebenen Umständen außerhalb seines eigenen Gestaltungsvermögens.

Die Ausbildung von deutschen Entscheidungsträgern und Praktikern der Cybersicherheit unter der Aufsicht des Verteidigungsministeriums der Vereinigten Staaten, wie sie bislang im Rahmen des Master-Studiengangs „International Security Studies“ an der Universität der Bundeswehr München durch das „Program on Cyber Security Studies“ des deutsch-amerikanischen George C. Marshall European Center for Security Studies erfolgt, kann vor diesem Hintergrund nicht ohne Weiteres als verlässliche Bildungsmaßnahme zum Schutz deutscher wissenschaftlicher Informationen vor dem Zugriff

durch US-amerikanische Behörden und IT-Unternehmen betrachtet werden. Die entsprechende Bildungskooperation zwischen dem BMVg und dem Verteidigungsministerium der Vereinigten Staaten muss daher umgehend überprüft werden. Eine vergleichbare Bildungskooperation zwischen Deutschland und Staaten wie Russland oder China besteht aus nachvollziehbaren Gründen nicht.

In Frankreich hat sich mit der „École de guerre économique“ (EGE) eine ökonomische Schule zur Ausbildung von Führungskräften im Wirtschaftskrieg etabliert, die aus den strategischen, operativen und taktischen Konzepten des Militärs Erkenntnisse für einen Wirtschaftskrieg ableitet, während in Deutschland nichts Vergleichbares existiert. Das Denken in geopolitischen und geostrategischen Kategorien ist für Großmächte wie die USA, China und Russland und sowie für Atommächte wie Frankreich, Großbritannien, Indien oder Israel eine Normalität. Deutschland wird sich diesem Kalkül nicht länger entziehen können. Die Bundesregierung ist deshalb aufgefordert, entsprechende Maßnahmen zum Schutz der Leistungsfähigkeit, der Datensicherheit, des geistigen Eigentums und der Wissenschaftsfreiheit des deutschen Wissenschaftssystems, seiner wissenschaftlichen Einrichtungen und seiner Wissenschaftler zu ergreifen.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. tragfähige Konzepte zum Schutz digitalisierter wissenschaftlicher Informationen an den Hochschulen und Forschungseinrichtungen des Bundes sowie an den vom Bund finanzierten Wissenschaftsorganisationen vor auf Grundlage des US-amerikanischen CLOUD Acts oder der Durchführungsverordnung „Enhancing Safeguards for United States Signals Intelligence Activities“ erfolgender Wissensausforschung und Wissensabschöpfung zu entwickeln;
2. Förderungen im Bereich digitaler Infrastruktur und digitaler Lernmittel an Hochschulen nur unter der Maßgabe zu gewähren, dass die betreffenden Hochschulen tragfähige Konzepte zum Schutz der damit zu digitalisierenden wissenschaftlichen Informationen vor Wissenschaftsspionage und Cyberangriffen vorweisen;
3. Förderungen im Bereich digitaler Infrastruktur und digitaler Lernmittel an Hochschulen nur unter der Maßgabe zu gewähren, dass die betreffenden Hochschulen sich dazu verpflichten, keine Kooperationen mit IT-Anbietern einzugehen, die Werbung für die oder eine überwiegende oder ausschließliche Verwendung der Produkte des jeweiligen Anbieters voraussetzen;
4. umgehend die Bildungskooperation zwischen dem BMVg und dem Verteidigungsministerium der Vereinigten Staaten, in deren Rahmen bislang im Master-Studiengang „International Security Studies“ an der Universität der Bundeswehr München durch das „Program on Cyber Security Studies“ des deutsch-amerikanischen George C. Marshall European Center for Security Studies deutsche Entscheidungsträger und Praktiker der Cybersicherheit ausgebildet werden, durch eine unabhängige Kommission auf ihre möglichen Risiken für den Schutz wissenschaftlicher Daten vor Cyberangriffen aus den USA hin überprüfen zu lassen;
5. dem von der Fraktion der AfD geforderten Forschungsinstitut für geopolitische Studien an der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg einen geoökonomischen Forschungszweig anzugliedern, in dessen Rahmen analog zur französischen EGE Wissenschaftsspionage und Cyberkriegführung um F&E als Bestandteil der Ausbildung von Führungskräften im Wirtschaftskrieg gelehrt und aus den strategischen, operativen und taktischen Konzepten des Militärs Erkenntnisse für den Wirtschaftskrieg abgeleitet werden;
6. umgehend eine Studie in Auftrag zu geben, in der die Risiken und Herausforderungen der akademischen und forschenden Zusammenarbeit mit US-amerikanischen Partnern vor dem Hintergrund des strategischen Ziels der USA einer glo-

balen Informationsdominanz durch Technologieüberlegenheit untersucht werden, um analog der vom DAAD angebotenen „Checklist for Collaboration with Chinese Universities and Other Research Institutions“ eine Handreichung zu entwickeln, die Entscheidungsträger bei der potenziellen oder tatsächlichen Zusammenarbeit mit US-amerikanischen Universitäten und anderen Forschungseinrichtungen bei der Einschätzung der Risiken und potenziellen Einschränkungen unterstützen soll;

7. die Analyse des Versagens des von der deutschen Spionageabwehr beanspruchten 360-Grad-Blicks insbesondere in Hinblick auf Angriffe aus den USA auf wissenschaftliche Daten sowie die Formulierung von Lehren für zukünftige Schutzmaßnahmen als Thema für die nächste Wissenschaftskonferenz des Zentrums für Analyse und Forschung (ZAF) aufzusetzen;
8. umgehend ihre Ankündigung aus dem Koalitionsvertrag, das Identifizieren, Melden und Schließen von Sicherheitslücken im Rahmen der IT-Sicherheitsforschung legal zu ermöglichen, dergestalt umzusetzen, dass die Durchführung von in gutem Glauben durchgeführten IT-Sicherheitstests keine Strafverfolgung oder Ermittlung durch die Staatsanwaltschaft begründen kann und auf diesem Weg Rechtssicherheit für die IT-Sicherheitsforschung zu schaffen, um so den dringend erforderlichen Ausbau der Cybersicherheit an und mithilfe von Hochschulen und wissenschaftlichen Einrichtungen besser unterstützen zu können.

Berlin, den 26. Juni 2024

Dr. Alice Weidel, Tino Chrupalla und Fraktion

Begründung

In Ermangelung einer einheitlichen Verwendung im Sprachgebrauch oder einer Legaldefinition des Begriffs „Wissenschaftsspionage“ möchten die Antragsteller in Anlehnung an die Begriffsverwendung Sabine Carls, ehemalige Senoir Researcher in der Abteilung Kriminologie am Max-Planck-Institut für ausländisches Strafrecht, unter Wissenschaftsspionage die Ausforschung und Wissensabschöpfung von Wissenschaftseinrichtungen durch fremde staatliche Akteure, Unternehmen oder wissenschaftliche Konkurrenten verstanden wissen.[2] Während sich Wissenschaftsorganisationen in einem beständigen Zielkonflikt zwischen dem auf Austausch ausgerichteten Wissenschaftsbetrieb und dem Bedürfnis, selbst generierte Daten zu schützen, befinden und Spionage für sie daher eine anders gelagerte Herausforderung darstellt als für Wirtschaftsunternehmen, werden die nachfolgenden Referenzen zu Fragen der Wirtschaftsspionage und des Wirtschaftskrieges insoweit für die Fragen der Wissenschaftsspionage als relevant erachtet, dass Investitionsausgaben des Bundes ihren volkswirtschaftlichen Nutzen im Fall der fremden Abschöpfung neuer Erkenntnisse verfehlen, zumal die Publikationen der Spionageabwehr die Wissenschaftsspionage im Verbund mit der Wirtschaftsspionage behandeln.[3]

In einem Positionspapier „zur Forschungssicherheit im Lichte der Zeitenwende“ vom März 2024 führt das Bundesministeriums für Bildung und Forschung (BMBF) „Multipolarität, Cyberbedrohungen und systemische Rivalität“ als maßgebliche Faktoren eines weltweiten Umbruchs an.[4] Das BMBF habe „als Reaktion auf den russischen Überfall auf die Ukraine alle laufenden und geplanten Maßnahmen mit Russland eingefroren“ und zugleich „den kritischen Blick auf Staaten wie China oder Iran geschärft“.[5] Vor diesem Hintergrund definiert das BMBF u.a. das Ziel, „im Wissenschaftssystem ein breiteres Bewusstsein und Wissen für die Risiken und Bedrohungen, denen Forschung zunehmend ausgesetzt ist“ zu schaffen.[6] Zu den Risiken zählten insbesondere „Missbrauch von Forschung, ausländische Einflussnahme, Ausspähen von Mitarbeitenden und vor allem der Abfluss von Know-how und Technologie ins Ausland“.[7] Angesichts dieses Ziels erscheint der Blickwinkel des BMBF auf jene Staaten, von denen solche Risiken für das deutsche Wissenschaftssystem ausgehen, einseitig verengt. In einem Input Papier für den Gesprächskreis Nachrichtendienste in Deutschland e. V. (GKND) bezeichnete es der wissenschaftliche Mitarbeiter für Forschungsinformation und Qualitätssicherung in der sozialwissenschaftlichen Forschung an der Humboldt-Universität zu Berlin Tim Flink 2020 als „womöglich immens unterschätztes Problem“, dass die von Wissenschaftlern und Institutionen erbrachten Forschungsergebnisse sowie ihr Prozesswissen durch ausländische Akteure in strukturierter Weise abgeschöpft werden und der Innovationsstandort hierdurch insgesamt geschwächt wird.[8] Das Bundesamt für Verfassungsschutz (BfV) behandle den Tatbestand der Wissenschaftsspionage in seinen Jahresberichten nur „en passant“, berichte dabei hauptsächlich über Cyberangriffe aus den Staaten Volksrepublik China, Russland und der Türkei.[9] Das BfV berücksichtige dabei lediglich ein rein technisch orientiertes Verständnis von wissenschaftlicher Forschung nahe an der wirtschaftlichen Wertschöpfung, anstatt auch strategisches und forschungspolitisches Prozesswissen in den Blick zu nehmen, obwohl international betrachtet ausländisches Abschöpfen von Forschungsdaten in nahezu allen wissenschaftlichen Bereichen beklagt werde.[10] Wer unmittelbar und mittelbar relevantes technologisches Wissen abschöpfen wolle, werde in Deutsch-

---

2 Sabine Carl: Wissenschaftsspionage – Risiken für den deutschen Forschungsstandort?, in: Elisa Wallwaey, Esther Bollhöfer, Susanne Knickmeier (Hrsg.): Wirtschaftsspionage und Konkurrenzausspähung. Phänomenologie, Strafverfolgung und Prävention in ausgewählten europäischen Ländern, Berlin 2019, S. 138 f.

3 Sabine Carl: Wissenschaftsspionage – Risiken für den deutschen Forschungsstandort?, in: Elisa Wallwaey, Esther Bollhöfer, Susanne Knickmeier (Hrsg.): Wirtschaftsspionage und Konkurrenzausspähung. Phänomenologie, Strafverfolgung und Prävention in ausgewählten europäischen Ländern, Berlin 2019, S. 138; www.academia.edu/69482637/Zum_Dilemma_internationaler_Wissenschaft_Wissenschaftsspionage_als_untersch%C3%A4tzte_Gefahr; abgerufen am 12. April 2023, S. 2; www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2023-03-23-spoc-magazin.pdf?__blob=publicationFile&v=4; abgerufen am 13. April 2023.

4 www.bmbf.de/SharedDocs/Downloads/de/2024/positionspapier-forschungssicherheit.pdf?__blob=publicationFile&v=1; abgerufen am 27. März 2024, S. 1.

5 www.bmbf.de/SharedDocs/Downloads/de/2024/positionspapier-forschungssicherheit.pdf?__blob=publicationFile&v=1; abgerufen am 27. März 2024, S. 1.

6 www.bmbf.de/SharedDocs/Downloads/de/2024/positionspapier-forschungssicherheit.pdf?__blob=publicationFile&v=1; abgerufen am 27. März 2024, S. 1.

7 www.bmbf.de/SharedDocs/Downloads/de/2024/positionspapier-forschungssicherheit.pdf?__blob=publicationFile&v=1; abgerufen am 27. März 2024, S. 1.

8 www.academia.edu/69482637/Zum_Dilemma_internationaler_Wissenschaft_Wissenschaftsspionage_als_untersch%C3%A4tzte_Gefahr; abgerufen am 12. April 2023, S. 2.

9 www.academia.edu/69482637/Zum_Dilemma_internationaler_Wissenschaft_Wissenschaftsspionage_als_untersch%C3%A4tzte_Gefahr; abgerufen am 12. April 2023, S. 2.

10 www.academia.edu/69482637/Zum_Dilemma_internationaler_Wissenschaft_Wissenschaftsspionage_als_untersch%C3%A4tzte_Gefahr; abgerufen am 12. April 2023, S. 2 f.

land zudem bereits an Universitäten, Fachhochschulen und außeruniversitären Forschungseinrichtungen fündig, da Innovationen oft unmittelbar am Ort der Wissensproduktion (mit)realisiert würden und jenseits der Ergebnisse von F&E das implizite Handlungswissen („tacit knowledge“) in F&E-Prozessen aufgrund seiner Bedeutung für den eigentlichen Aufbau von Kapazitäten und wegen seiner Übertragbarkeit auf andere komplexe Prozesse relevant geworden sei.[11] Flink formuliert dabei folgendes Dilemma: Offenheit der Wissenschaft sei für diese funktional und normativ notwendig, jedoch werde die Wissenschaft, je offener und grenzüberschreitender sie kooperiere, desto anfälliger für ausländische Abschöpfungs-, Einfluss- und Störversuche.[12]

Unter Berufung auf die Ergebnisse des vom BMBF geförderten und abgeschlossenen Forschungsprojekts „Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa – WISKOS“ erklärte Flink, dass es aus Erfahrung im Nachrichtendienstwesen „geradezu wahrscheinlich“ sei, dass sich der Täterkreis hybrider Akteure aus dem Ausland nicht auf einige wenige Staaten beschränken ließe und mit Sicherheit nicht auf diejenigen, die „zurzeit ohnehin öffentlich am Pranger des Westens“ stünden.[13] Auch der Cyberspionage-Experte Dr. Timo Steffens stellt fest, dass im Unterschied zu den regelmäßig veröffentlichten Berichten von Sicherheitsfirmen zu den genannten Staaten Analysen von Angriffen mit vermutlich westlichem Ursprung äußerst selten seien.[14] Dabei würden zum einen wirtschaftliche Interessen unterstellt – etwa, dass eine Firma keine Operation einer Behörde aufdecke, die zu ihren Kunden gehöre. Zum anderen würden aber auch ideologische oder politische Gründe für möglich gehalten. Es sei zwar nicht davon auszugehen, dass ein Unternehmen es sich leisten könnte, seine Detektionsprodukte bewusst so zu konfigurieren, dass bestimmte Samples nicht erkannt werden.[15] Bei Attributions-Veröffentlichungen hingegen handele es sich um Zusatzaufwände und niemand erwarte von Sicherheitsunternehmen, alle von ihnen entdeckten Schadprogramm-Familien mit gleicher Intensität auf ihren Ursprung hin zu untersuchen. Daher sei es deutlich einfacher, Berichte zu vermeiden, die bspw. westliche Staaten oder Organisationen behandeln würden.[16]

Flink argumentiert, die kapazitären Voraussetzungen hochentwickelter Staaten zur Abschöpfung des Potentials in F&E sowie des forschungspolitischen Organisationswissens aus Deutschland seien schließlich weitaus höher als diejenigen von wissenschaftlich-technologisch aufstrebenden Autokratien. Dies korrespondiert nach Ansicht der Antragsteller den Enthüllungen der ehemaligen NSA-Mitarbeiter Edward Snowden und William Binney zum sogenannten „Black Budget“ (Congressional Budget Justification/National Intelligence Program), den jährlichen finanziellen Zuweisungen aus dem Haushalt der Vereinigten Staaten für die US-Geheimdienste.[17] Snowdens Enthüllungen hatten für das Jahr 2013 eine Summe von über 50 Milliarden US-Dollar ausgewiesen, während Binney 2014 als ehemaliger technischer Direktor der NSA und unter Verweis auf die Verteilung der Zuweisungen auf die Haushalte verschiedener US-Ministerien angab, die Summe belaufe sich auf annähernd 100 Milliarden US-Dollar.[18] Selbst die offiziellen Zahlen hatten für die US-Geheimdienste bereits 2010 einen Etat von 80,1 Milliarden US-Dollar ausgewiesen.[19] 2020 bezeichnete Dr. Gerhard Conrad, ehemaliger Leiter des präsidialen Leitungsstabs des BND, ehemaliger Direktor des „EU Intelligence Analysis Centre“ des Europäischen Auswärtigen Dienstes der Europäischen Union, Gastprofessor am Department of War Studies des King’s College London und Dozent an der Hochschule des Bundes für öffentliche Verwaltung, die „bestürzend“ deutliche Diskrepanz zwischen dem Etatvolumen europäischer Länder wie Deutschland von 1,5 Milliarden Euro auf Bundesebene für Nachrichten- und Sicherheitsdienste einerseits und dem der USA, das „hohe jährliche zwei-, wenn nicht dreistellige Milliardenbeträge in US-Dollar“ umfasse, andererseits als „Reflex der traditionellen machtpolitischen Anlehnung Europas“ an die USA.[20] Die gebündelten Budgets aller europäischen Geheimdienste beliefen

---

[11] www.academia.edu/69482637/Zum_Dilemma_internationaler_Wissenschaft_Wissenschaftsspionage_als_untersch%C3%A4tzte_Gefahr; abgerufen am 13. April 2023, S. 4.

[12] www.academia.edu/69482637/Zum_Dilemma_internationaler_Wissenschaft_Wissenschaftsspionage_als_untersch%C3%A4tzte_Gefahr; abgerufen am 13. April 2023, S. 7.

[13] www.academia.edu/69482637/Zum_Dilemma_internationaler_Wissenschaft_Wissenschaftsspionage_als_untersch%C3%A4tzte_Gefahr; abgerufen am 12. April 2023, S. 3.

[14] Timo Steffens: Auf der Spur der Hacker. Wie man die Täter hinter der Computer-Spionage enttarnt, Berlin 2018, S. 151.

[15] Timo Steffens: Auf der Spur der Hacker. Wie man die Täter hinter der Computer-Spionage enttarnt, Berlin 2018, S. 152.

[16] Timo Steffens: Auf der Spur der Hacker. Wie man die Täter hinter der Computer-Spionage enttarnt, Berlin 2018, S. 151f.

[17] Constanze Kurz u. Frank Rieger: Cyberwar – Die Gefahr aus dem Netz, München 2018, S. 135f.

[18] Constanze Kurz u. Frank Rieger: Cyberwar – Die Gefahr aus dem Netz, München 2018, S. 136; www.opendemocracy.net/en/we-had-to-wait-for-snowden-for-proof-exchange-with-william-binney/; abgerufen am 17. November 2023.

[19] Thomas Jäger, Verena Diersch, Stephan Liedtke: Was Europa wissen darf. Die Geheimdienste der USA und die europäische Politik, Zürich 2020, S. 81.

[20] www.kas.de/documents/258927/10554422/DPM+565_Gesamtausgabe_WEB.pdf/6ce0974e-61aa-1888-99e8-d2c367a1478b?t=1605528699991; abgerufen am 13. Februar 2024, S. 66f.

sich laut Conrad demgegenüber selbst bei optimistischer Schätzung auf „allenfalls zwanzig Milliarden Euro“.[21] Die Cybersicherheitsexperten Constanze Kurz und Frank Rieger erklärten 2018, man könne „mit Recht hoher Wahrscheinlichkeit davon ausgehen, dass die US-Geheimdienste die bestfinanzierten der Welt sind und dadurch über eine hohe Angriffspotenz verfügen“.[22] Prof. Dr. Thomas Jäger, Inhaber des Lehrstuhls für Internationale Politik und Außenpolitik an der Universität zu Köln, sowie die wissenschaftlichen Mitarbeiter am Lehrstuhl Dr. Verena Diersch und Dr. Stephan Liedtke beurteilen den Diebstahl geistigen Eigentums und die Sicherheit von Forschungsergebnissen für US-Wirtschaftsinteressen als so wichtiges Handlungsmotiv des US-Auslandsgeheimdienstes CIA, dass dieser immer wieder als Instrument der amerikanischen Außenwirtschaftspolitik agiere.[23] Zugleich verfolge die CIA „eine aggressive Humint-Strategie, nach der die CIA sich auf den gesamten Globus ausdehnen, risikofreudiger und weniger abhängig von den Partnerdiensten werden“ solle.[24] Unter HUMINT werden Informationen von menschlichen Quellen verstanden, wobei der Cyberspionage-Experte Dr. Timo Steffens die Anwerbung von Mitarbeitern von Fachbehörden wie Handels-, Außen- oder Forschungsministerien als besonders erfolgversprechend einschätzt.[25] Flink bringt die Diskrepanz zwischen potenzieller westlicher Bedrohung und der auf die oben genannten nichtwestlichen Staaten reduzierten Darstellung der Bedrohungslage durch die Behörden mit der Frage auf den Punkt: „Sind wir auf dem westlichen Auge blind“?[26]

Zu Forderung 1

Die Kooperation und Verflechtung US-amerikanischer Geheimdienste mit US-IT-Unternehmen ist in diesem Kontext nach Ansicht der Antragsteller von besonderer Bedeutung. Die meisten der marktbeherrschenden IT-Unternehmen unterfallen US-Recht, sodass US-Behörden die Unternehmen verpflichten können, Daten und Informationen, auf die sie rechtlich und tatsächlich zugreifen können, unabhängig von ihrem Standort bzw. dem Standort des Servers, herauszugeben.[27] Die Unternehmen und ihre Tochterfirmen sind demnach nicht nur zur Herausgabe ihrer eigenen Daten verpflichtet, sondern auch der ihrer Kunden und das auch dann, wenn diese Daten in europäischen Rechenzentren der US-Anbieter gespeichert sind.[28] Eine entsprechende Herausgabeanordnung kann auch Daten europäischer Unternehmen betreffen, sofern diese Cloud-Reserven an einem europäischen Rechenzentrumsstandort eines US-Anbieters nutzen.[29] So warnt auch der Medienberater und Datenschutzbeauftragte für Schulen im Kreis Olpe in Nordrheinwestfalen, dass eine Ausstattung von Bildungsstätten mit Geräten und Software von US-Unternehmen besonders kritisch sei, da US-Ermittlungsbehörden „jederzeit“ Zugang zu den Servern ihrer heimischen Unternehmen hätten – „egal wo in der Welt“.[30] Dies korrespondiert nach Ansicht der Antragsteller den Ergebnissen der im Rahmen der Wissenschaftlichen Arbeitsgruppe des Nationalen Cybersicherheitsrats (NCSR) angestellten Analyse der „Projektgruppe verfassungsverträgliche Technikgestaltung“ (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel. Neben vergleichbaren rechtlichen Sicherheitsrisiken im Falle Russlands und Chinas sind demnach auch US-Unternehmen und Staatsangehörige verpflichtet, mit ihren Geheimdiensten zusammenzuarbeiten.[31] Die Geheimdienste könnten außerdem eigene (Tarn-)Unternehmen gründen oder Mitarbeiter in bestehende Unternehmen einschleusen. Dies gelte nicht nur für Unternehmen, die in den USA tätig sind, sondern auch für weltweit tätige Unternehmen und deren Tochterorganisationen in anderen Staaten. Von diesem System würden auch ausländische Töchter deutscher Organisationen erfasst, die in den USA tätig sind. Die verpflichteten Unternehmen wirkten in Deutschland oder in der Kommunikation mit deutschen Stellen wie „Trojanische Pferde“. Ihnen sei ihre Funktion für die nachrichtendienstliche Tätigkeit nicht anzusehen. Die US-Geheimdienste hätten potenziell Zu-

---

21 www.kas.de/documents/258927/10554422/DPM+565_Gesamtausgabe_WEB.pdf/6ce0974e-61aa-1888-99e8-d2c367a1478b?t=1605528699991; abgerufen am 13. Februar 2024, S. 66.

22 Constanze Kurz u. Frank Rieger: Cyberwar – Die Gefahr aus dem Netz, München 2018, S. 139 f.

23 Thomas Jäger, Verena Diersch, Stephan Liedtke: Was Europa wissen darf. Die Geheimdienste der USA und die europäische Politik, Zürich 2020, S. 81.

24 Thomas Jäger, Verena Diersch, Stephan Liedtke: Was Europa wissen darf. Die Geheimdienste der USA und die europäische Politik, Zürich 2020, S. 197.

25 Timo Steffens: Auf der Spur der Hacker. Wie man die Täter hinter der Computer-Spionage enttarnt, Berlin 2018, S. 113.

26 www.academia.edu/69482637/Zum_Dilemma_internationaler_Wissenschaft_Wissenschaftsspionage_als_untersch%C3%A4tzte_Gefahr; abgerufen am 12. April 2023, S. 8.

27 www.bundestag.de/resource/blob/990440/baf5c0d018ff7cdbfc08edf0f4ce6e64/WD-3-105-23-pdf.pdf; abgerufen am 10. Mai 2024, S. 16; www.bundestag.de/resource/blob/796102/ea53ffe8e08a9ab11e270719263d8c53/WD-3-181-20-pdf-data.pdf; abgerufen am 14. April 2023, S. 8; www.sueddeutsche.de/bildung/apple-bildung-schule-einfluss-1.4787334; abgerufen am 14. April 2023.

28 www.it-business.de/was-ist-der-cloud-act-a-1072997/; abgerufen am 14. April 2023.

29 www.it-business.de/was-ist-der-cloud-act-a-1072997/; abgerufen am 14. April 2023.

30 www.sueddeutsche.de/bildung/apple-bildung-schule-einfluss-1.4787334; abgerufen am 14. April 2023.

31 Auswirkungen ausländischer Gesetzgebung auf die deutsche Cybersicherheit, S. 157 ff., 163, in: Datenschutz und Datensicherheit 3 | 2022, S. 156-163.

griff auf alle in den USA gespeicherten Daten. Dies gelte auch für alle die Daten, die Organisationen aus den USA und ihren Tochterorganisationen anvertraut werden – insbesondere, wenn diese eine gewisse Bedeutung für nachrichtendienstliche Zwecke haben wie z. B. Forschungsdaten. Der ehemalige Präsident des BND Gerhard Schindler bemerkte zur fehlenden Durchsetzung von Datensicherheit und Datenschutz gegen die betreffenden US-Unternehmen und US-Behörden 2020: „Es liegt aber auch daran, dass es Mut erfordert, sich mit diesen Giganten anzulegen. Wie wäre es mit einer gesetzlichen Verpflichtung, dass zum Beispiel Google seine Server so dezentral und gegebenenfalls gar national konfigurieren muss, damit sie für deutsche oder europäische Rechtsvorgaben zugänglich sind? Diesen Konflikt, nicht nur mit Google, sondern auch mit den USA, scheuen viele“.[32]

Nach Ansicht der Antragsteller weisen diese Gefahren gravierende Ähnlichkeit mit dem Vorgehen US-amerikanischer Behörden und IT-Unternehmen auf, wie es Frank Rieger bereits 2014 als Sachverständiger im Rahmen des NSA-Untersuchungsausschusses im Deutschen Bundestag beschrieben hatte: „Die Kooperation der Firmen mit den Diensten, also sagen wir mal Facebook und ähnliche. Sie haben die Struktur - gezielte Anfragen, strukturelle Zusammenarbeit und am Ende Angriffe gegen diese Unternehmen - richtig zusammengefasst. Was ich weiß, ist, dass zumindest bei Google die Aufregung da groß war, als die verstanden haben, dass die NSA sie auch direkt angegriffen hat und nicht nur über Kooperation gearbeitet hat, sondern eben auch die Leitungen zwischen den Data Centers angegriffen hat und ähnliche Dinge. Das hat denen so gar nicht gefallen. Diese Unternehmen haben alle den Anspruch, Kontrolle über ihre Daten zu haben. Das Prinzip heißt: „no one but us“, also: niemand außer uns. Das verfolgt auch Facebook. Das heißt, die wollen die vollständige Kontrolle über diese Daten haben und versuchen da auch irgendwie, was zu tun. Die haben allerdings das strukturelle Problem, dass gerade in den Boards und den Managementetagen, insbesondere in amerikanischen Firmen, viele Ex-Mitarbeiter von Geheimdiensten sitzen, die noch für ihre alten Kumpels arbeiten. Dieses Prinzip ist eben auch genau bei der Wirtschaftsspionage zu finden. Also, die Amerikaner - aus dem, was wir aus den Dokumenten wissen oder sonst beobachten können - versuchen, ihre Wirtschaftsspionage immer rechtlich zu legitimieren, indem sie sagen: „Okay, wir machen keine Wirtschaftsspionage zum Vorteil von einzelnen Unternehmen, sondern wir sorgen für Ausschreibungsgerechtigkeit“, oder: „Wir verfolgen Steuerhinterziehung“, oder: „Wir suchen nach Firmen, die halt Embargobrüche begangen haben“, und erheben diese Daten über Unternehmen, zum Beispiel auch in Deutschland, unter diesem Vorwand“.[33] Auf die Aktualität entsprechender politisch verursachter Sicherheitsmängel deuten nach Ansicht der Antragsteller auch Vorgänge im Vorfeld der BSI-Affäre hin, in deren Rahmen der damalige Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) Arne Schönbohm durch die Bundesministerin des Innern und für Heimat Nancy Faeser aufgrund haltloser Vorwurfe einer Nähe zu russischen Geheimdiensten und fehlerhafter Amtsführung geschasst worden war.[34] Schönbohm hatte sich unter anderem in sicherheitsstrategischen Fragen mehrfach gegen die Spitze des BMI positioniert und in der Frage, ob Hard- und Softwareentwickler in ihre Produkte digitale Hintertüren, etwa für Zugriffe von Ermittlungsbehörden oder Geheimdiensten, einbauen sollten, eine deutlich restriktivere Haltung als das BMI vertreten.[35] Dieser Vorgang ist nach Auffassung der Antragsteller insbesondere deshalb relevant für die Cybersicherheit der Hochschulen, da der Verein der „Zentren für Kommunikationsverarbeitung in Forschung und Lehre“ (ZKI e.V.) als Zusammenschluss aller Rechenzentren an Hochschulen in Deutschland methodisch auf der Grundlage des IT-Grundschutzes des BSI agiert und mit Unterstützung des BSI das IT-Grundschutzprofil für Hochschulen entwickelt hat.[36] Somit ist nach Ansicht der Antragsteller ein Zusammenhang zwischen der Frage nach dem Restriktionsgrad im Umgang mit digitalen Hintertüren in IT-Produkten für Zugriffe von Ermittlungsbehörden oder Geheimdiensten seitens des BSI und der Cybersicherheit an Hochschulen anzunehmen. Die NSA weist zudem offen darauf hin, dass sie für die Überwachung von Internet- und Telekommunikation auf ihre „Strategic Partnership“ mit Telekommunikations- und Netzwerk-Service Providern, Betreibern von Netzwerkinfrastruktur, Herstellern von Hardware, Computerbetriebssystemen, Applications Software, Programmierern von Sicherheitssoftware und -hardware so-

---

[32] Gerhard Schindler: Wer hat Angst vorm BND? Warum wir mehr Mut beim Kampf gegen die Bedrohungen unseres Landes brauchen. Eine Streitschrift, Berlin 2020, S. 154.

[33] www.bundestag.de/resource/blob/372418/97c666605f875474927dfcf5b42c4fcb/09-waidner_gaycken_rieger_endgueltig-data.pdf; abgerufen am 14. April 2023, S. 47 f.

[34] www.businessinsider.de/politik/deutschland/faeser-an-vorwuerfen-gegen-ex-bsi-chef-schonbohm-war-nichts-dran/; abgerufen am 12. September 2023.

[35] www.wiwo.de/technologie/digitale-welt/neue-bsi-chefin-startet-auf-schleudersitz-jetzt-ist-die-willkuer-an-der-spitze-der-deutschen-cyberabwehr-amtlich/29229880.html; abgerufen am 12. September 2023.

[36] Brandel, B.; Porombka, S.; Oevel, G. (2020): IT-Schutz ist kein Projekt, sondern ein Prozess. Cybersicherheit ist für Forschungseinrichtungen essenziell. Ein Überblick über die besonderen Herausforderungen für Hochschulen, S. 657, in: Forschung & Lehre 27 (2020) 8, S. 656–657.

wie Systemintegratoren wie H-P, Intel, Microsoft uvm. zurückgreift.[37] Die Daten deutscher und europäischer Nutzer werden dadurch für die NSA unmittelbar zugänglich und in intransparenter Weise nutzbar.

Nach Auffassung der Antragsteller stellt dies eine nicht tragbare Gefährdung der Datensicherheit und des Datenschutzes der Nutzer und gerade im Falle von Hochschulen ein Einfallstor auch für Wissenschaftsspionage dar. Dies gilt umso mehr, da die Digitalisierung von Informationen und Kommunikationsmedien an sich bereits Angriffspunkte für Ausforschungsaktivtäten und damit für Wissenschaftsspionage und Wissensabschöpfung bietet.[38] Dies korrespondiert nach Ansicht der Antragsteller auch den Feststellungen Prof. Dr. Dr. h.c. Ulrich Blums vom Lehrstuhl für Wirtschaftspolitik und -forschung der Martin-Luther-Universität Halle-Wittenberg, wonach die USA zu den drei Hauptherkunftsländern von Cyberangriffen auf Deutschland zählen und bspw. im Jahr 2014 mit über 8 Millionen Angriffen sogar das Land mit den meisten Cyberangriffen auf Deutschland waren, wobei sich der Großteil der Attacken gegen F&E richtet.[39] Laut Blum gelten neben Russland, China und Nordkorea die USA und Israel als die kompetentesten Länder im Cyberkrieg, was nach Ansicht der Antragsteller Flinks Annahme stützt, dass auch unter westlichen Staaten besonders hohe kapazitäre Voraussetzungen zur Wissensabschöpfung vorhanden sind.[40] Vergleichbar stellt der Politikwissenschaftler an der Technischen Universität Chemnitz Jakob Kullik in seiner Analyse der deutschen Cybersicherheitspolitik fest: Jeder Staat, der über die entsprechenden technischen und humanen Ressourcen verfügt, betreibt heutzutage Cyberspionage. Diese Tatsache und die veränderten Parameter der digitalen Operationsführung sorgen dafür, dass die althergebrachten Kategorien „Bündnispartner“ oder „Alliierter“ im Cyberspace de facto nicht mehr existent sind […] Die Bundesrepublik Deutschland ist demnach nur noch ein „Verbündeter 3. Klasse“ und ein strategisches Spionageziel der USA“.[41] Die Vorstellung, dass die USA IT-Spionage lediglich im weltweiten Antiterrorkampf und zur Militärspionage betreibe, müsse laut Kullick dahingehend ergänzt werden, dass die USA „in enger Zusammenarbeit mit Großbritannien“ nahezu den gesamten weltweiten Datenverkehr speichern und auswerten.[42] Kullik zitiert dazu Constanze Kurz: „Galt bisher bei jedem größeren Angriff auf die Daten von Unternehmen immer der Glaubenssatz ‚Die Chinesen waren's!‘, so ist nun unbestreitbar, dass es auch die angeblichen Verbündeten sein könnten – die sich der Tarnung halber eines Servers in China bedienen“.[43] Da Deutschland auch von offiziellen Partnerstaaten ausspioniert werde, so Kullik, böten kollektive Sicherheitsbündnisse wie die NATO keinen ausreichenden Schutz mehr vor Cyberspionage; Der souveräne Nationalstaat könne nur versuchen, sich selbst zu schützen.[44] Kurz stellte das umschriebene Problem der Attribution von Cyberangriffen gemeinsam mit Frank Rieger vertieft dar: die Suche nach einem Schuldigen sei oft „überformt von politischen Motiven“, die mit technischen Fakten nur am Rande zu tun hätten.[45] Hinzu komme das Legen falscher Fährten als Methode von Geheimdiensten. So sei durch die WikiLeaks-Publikation „Vault 7“ bekannt geworden, dass die CIA ein eigenes Team mit dem Namen „Umbrage“ beschäftige, dessen einzige Aufgabe darin bestünde, Komponenten fremder Schadsoftware zu extrahieren und für die Verwendung in eigenen Angriffswerkzeugen aufzubereiten, um eine Attribuierung von Cyberangriffen zur CIA unmöglich zu machen.[46] Laut dem Cyberspionage-Experten Dr. Timo Steffens zeigen die „Vault 7-Leaks“, dass es sich bei den Maßnahmen der NSA und CIA zur Verschleierung ihrer Spionageaktivitäten um die fortgeschrittensten weltweit handelt.[47]

Auch die Datenschutzrechtlichen Entwicklungen auf EU-Ebene geben nach Ansicht der Antragsteller keinen Anlass zur Entwarnung, sondern reihen sich in die bereits geschilderte Problemlage ein. Das im Jahr 2000 zwischen der EU und den USA geschaffene Safe-Harbor-Abkommen war bereits wegen mangelnder Datenschutzstandards und des Zugangs von US-Behörden wie der NSA zu den Daten der Bürger der EU-Mitgliedstaaten bemängelt und im Jahr 2015 durch das Urteil des Europäischen Gerichtshofs (EuGH) in der Rechtssache „Sch-

---

37 Thomas Jäger, Verena Diersch, Stephan Liedtke: Was Europa wissen darf. Die Geheimdienste der USA und die europäische Politik, Zürich 2020, S. 188.

38 www.uni-bielefeld.de/verwaltung/informationssicherheit/regelungen/Forschungsspionage_Research_Espionage_DE_EN.pdf; abgerufen am 14. April 2023, S. 1.

39 Ulrich Blum: Wirtschaftskrieg. Rivalität ökonomisch zu Ende denken, Halle 2016, S. 569; Ulrich Blum: Wirtschaftskrieg. Rivalität ökonomisch zu Ende denken, Wiesbaden 2020, S. 840.

40 Ulrich Blum: Wirtschaftskrieg. Rivalität ökonomisch zu Ende denken, Wiesbaden 2020, S. 831.

41 Vernetze (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik, Hamburg 2014, S. 55.

42 Ebd. S. 55 f.

43 Ebd. S. 56.

44 Ebd. S. 59.

45 Constanze Kurz u. Frank Rieger: Cyberwar – Die Gefahr aus dem Netz, München 2018, S. 122.

46 Ebd. S. 127.

47 Timo Steffens: Auf der Spur der Hacker. Wie man die Täter hinter der Computer-Spionage enttarnt, Berlin 2018, S. 105.

rems I“ aufgrund mangelnden Schutzes personenbezogener Daten für ungültig erklärt worden.[48] Der im Jahr 2016 in Reaktion auf das Urteil „Schrems I“ des EuGH und als Nachfolger des Safe-Harbor-Abkommens eingeführte EU-US-Datenschutzschild wurde im Jahr 2020 durch das Urteil des EuGH in der Rechtssache „Schrems II“ ebenfalls für ungültig erklärt, da auch dieser US-Behörden wie der NSA den Zugang zu Daten der Bürger der EU-Mitgliedstaaten ermöglichte und den Bürgern keine wirksamen Rechtsbehelfe bot.[49] So wurde in der Urteilsbegründung des EuGH u.a. ausgeführt, dass hinsichtlich der für nachrichtendienstliche Tätigkeiten eingeführten Beschränkungen hervorzuheben sei, „dass Nicht-US-Personen nur von der PPD-28 erfasst würden, in der es lediglich heiße, dass nachrichtendienstliche Tätigkeiten „as tailored as feasible“ (so gezielt wie möglich) sein müssten. Auf der Grundlage dieser Feststellungen sei davon auszugehen, dass die Vereinigten Staaten eine massenhafte Datenverarbeitung durchführten, ohne einen Schutz zu gewährleisten, der dem durch die Art. 7 und 8 der Charta garantierten Schutz der Sache nach gleichwertig sei“.[50] In der Folge fanden Verhandlungen zwischen der EU und den USA statt, die am 25. März 2022 zu der gemeinsamen Erklärung der Präsidentin der Europäischen Kommission Ursula von der Leyen und des Präsidenten der Vereinigten Staaten Joe Biden führten, eine grundsätzliche Einigung unter dem Titel „EU-U.S. Data Privacy Framework“ erzielt zu haben.[51] Die rechtliche Umsetzung erfolgte von US-Seite am 7. Oktober 2022 in Form der Durchführungsverordnung „Enhancing Safeguards for United States Signals Intelligence Activities“ und auf dieser Grundlage trat im Juli 2023 der „Datenschutzrahmen EU-USA“ in Kraft.[52] Die Durchführungsverordnung des US-Präsidenten Biden erklärt US-Spionageaktivitäten dabei für explizit zulässig, sobald diese zur Verfolgung auch nur eines von zahlreichen Zielen dienlich erscheinen.[53] Hierzu zählen u. a.:

„(1) understanding or assessing the capabilities, intentions, or activities of a foreign government, a foreign military, a faction of a foreign nation, a foreign-based political organization, or an entity acting on behalf of or controlled by any such foreign government, military, faction, or political organization, in order to protect the national security of the United States and of its allies and partners;

(2) understanding or assessing the capabilities, intentions, or activities of foreign organizations, including international terrorist organizations, that pose a current or potential threat to the national security of the United States or of its allies or partners;

(3) understanding or assessing transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability, and geographic rivalry“. [54]

Nach Ansicht der Antragsteller berechtigt die breite Auswahl an möglichen Zielen sowie die explizit aufgeführte Möglichkeit des US-Präsidenten, diese Ziele ohne Verpflichtung, dies öffentlich mitzuteilen, zu erweitern, die US-Geheimdienste aus US-Perspektive potenziell jederzeit dazu, umfassende Spionageaktivitäten auszuüben. Nicht zuletzt gilt dies für den Bereich der Wissenschaftsspionage, da eine Vielzahl der Themen, deren potenziell besseres Verständnis gemäß der Durchführungsverordnung Spionageaktivitäten der US-Behörden rechtfertigt, Gegenstand ressourcenintensiver Forschung ist. Der für die Schrems-Urteile namengebende Jurist und Datenschutzaktivist Maximilian Schrems formuliert mit Blick auf die US-Durchführungsverordnung: „Auch Gesundheitskrisen und der Klimawandel können nun als Begründung für Massenüberwachung herhalten“[55]. Schrems stellt fest, dass der Datenschutzrahmen EU-USA genauso ungenügend wie seine Vorgänger sei und auch die DSGVO für den Datenschutz nicht zum Zuge komme, sobald die betreffenden Daten die EU verließen und in den USA oder auf den Servern von US-Unternehmen innerhalb der EU gespeichert oder verarbeitet würden, da auch in der EU aktive US-Unternehmen der US-Gesetzgebung unterlägen und der NSA gegenüber weisungsgebunden seien.[56] Zudem kritisierte auch der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg Dr. Stefan Brink an der oben genannten Durchführungsverordnung des US-Präsidenten u.a., dass der hierin vorgesehene „Data Protection Review Court“, an den sich Bürger beim Verdacht auf Spionageaktivität

---

48 www.sueddeutsche.de/digital/max-schrems-vs-facebook-was-das-bahnbrechende-urteil-des-eugh-bedeutet-1.2679115; abgerufen am 1. Juni 2023.

49 www.heise.de/news/EuGH-kippt-EU-US-Datenschutzvereinbarung-Privacy-Shield-4845204.html?seite=all; abgerufen am 1. Juni 2023.

50 https://curia.europa.eu/juris/document/document.jsf;jsessionid=10C0E77EEE258F53BE0DDECF981CD5C0?text=&docid=228677&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=17149305; abgerufen am 1. Juni 2023.

51 https://ec.europa.eu/commission/presscorner/detail/de/qanda_22_6045; abgerufen am 1. Juni 2023.

52 www.welt.de/wirtschaft/article246394034/Google-Facebook-Amazon-und-Co-Max-Schrems-kaempft-gegen-Europas-Daten-Deal.html; abgerufen am 4. April 2024.

53 www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf; abgerufen am 1. Juni 2023, S. 1f.

54 www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf; abgerufen am 1. Juni 2023, S. 1f.

55 https://osb-alliance.de/featured/der-transatlantische-datenschutz-bleibt-ein-problem-kommt-jetzt-schrems-iii; abgerufen am 10. Mai 2024.

56 https://osb-alliance.de/featured/der-transatlantische-datenschutz-bleibt-ein-problem-kommt-jetzt-schrems-iii; abgerufen am 10. Mai 2024.

der US-Behörden gegen sie richten können sollen, im Ressort des US-Justizministers eingerichtet wird, somit der Exekutive zuzuordnen wäre und damit nicht richterlich unabhängig sein könne.[57] Weiterhin kritisiert Brink, dass unklar bleibt, wie sich die Verordnung zu anderen bestehenden US-Regulierungen wie dem CLOUD Act verhält und wann aus Sicht der USA ein Zugriff auf die Daten von Bürgern von EU-Mitgliedstaaten zulässig bleibt sowie dass die Einhaltung einer solchen Verordnung für eben jene Bürger nicht einklagbar ist und auch das „Aussieben" unerwünschter Beschwerden der Bürger möglich bleibt.[58] Brink kritisiert zudem, dass Beschwerdeführer ausdrücklich nicht darüber informiert werden, ob sie Gegenstand von nachrichtendienstlichen Aktivitäten der US-Behörden waren, sondern lediglich eine standardisierte Mitteilung erhalten, die besagt, dass die Überprüfung ihrer Beschwerde abgeschlossen ist und dass derselbe Wortlaut auch für eine nachfolgende Entscheidungen des Data Protection Review Court vorgegeben ist.[59] Laut Auskunft der Bundesregierung wird in regelmäßigen Abständen intervallartig geprüft, ob ein Beschwerdeführer das seinen Fall betreffende Urteil des Data Protection Review Courts und somit eine Antwort auf die Frage, ob er Ziel von Überwachung durch die US-Geheimdienste geworden ist, erhalten kann, was jedoch keinesfalls garantiert wird.[60] Auf Nachfrage anlässlich der Kritik des Datenschutzbeauftragten Dr. Brink an der unklaren Auslegung des Rechtsbegriffs der Verhältnismäßigkeit durch die US-Behörden, bestätigte die Bundesregierung die Auffassung, „einigermaßen überzeugt" davon zu sein, dass die US-Sicherheitsbehörden „den Zugriff auf Daten auf das notwendige und erforderliche Maß beschränken können".[61] Angesichts der bereits genannten Fälle von US-Spionageangriffen und der nach Auffassung der Antragsteller technisch sowie rechtlich mangelhaften Schutzvorkehrungen von deutscher und unionaler Seite, erachten die Antragsteller dieses Vertrauen der Bundesregierung in die US-Behörden als unbegründet und naiv.

Zu Forderung 2

Die nach Einschätzung der IT-Sicherheitsexperten Bernhard Brandel und Sebastian Porombka sowie der Leiterin des Zentrums für Informations- und Medientechnologien an der Universität Paderborn Prof. Dr. Gudrun Oevel für die Cybersicherheit an Hochschulen nötigen kontinuierlichen und proaktiven Maßnahmen binden Ressourcen, die der Forschung und Lehre dann nicht mehr direkt zur Verfügung stehen und schränken Flexibilität und Freiheiten ein, weshalb diese häufig „nicht mit Enthusiasmus begrüßt" würden.[62] Die Kanzlerin der Justus-Liebig-Universität Gießen (JLU) Susanne Kraus betonte 2023 mit Blick auf den bis dahin schwersten Cyberangriff auf eine deutsche Hochschule, der die JLU 2019 getroffen hatte: „Wenn der IT-Bereich nicht mehr funktioniert, steht die Hochschule still. Deshalb kann ich jeder Hochschule nur raten, an der IT-Sicherheit als elementarer Aufgabe nicht zu sparen. Es handelt sich eben nicht um eine Aufgabe von vielen, sondern ist das digitale Herz jeder Institution".[63] Entsprechende Konzepte der Hochschulen zum Schutz der damit zu digitalisierenden wissenschaftlichen Informationen müssen daher nach Ansicht der Antragsteller zur Maßgabe für eine Förderung im Bereich digitaler Infrastruktur und digitaler Lernmittel durch den Bund gemacht werden.

Zu Forderung 3

IT-Unternehmen wie Samsung, Microsoft, Google und Apple bieten heute bereits Fortbildungen für Lehrer an, verschenken Software und Geräte und zertifizieren ganze Schulen. So führt Microsoft aktuell vier Schulen in Deutschland als „Microsoft Showcase Schools", was u.a. voraussetzt, dass diese Schulen den Ansatz verfolgen, ihre Curricula und ihre Lehrmethoden auf den Einsatz von Microsoft-Produkten auszurichten und die Schüler dazu anzuhalten, diese auch im Rahmen selbstständigen Lernens und in Hinblick auf die Ausbildung „zukunftsreifer" Fähigkeiten zu verwenden.[64] Auch gibt es mittlerweile vierzehn, teils staatliche „Apple Distinguished Schools" in Deutschland, was u. a. bedeutet, dass alle Schüler und Lehrer Apple Geräte als primäre Lern- und Unterrichtsgeräte einsetzen, Apps aus dem App Store sowie Bücher von Apple Books und andere digitale Res-

---

57 www.baden-wuerttemberg.datenschutz.de/usa-eu-datentransfer-durchfuehrungsverordnung-us-praesident/; abgerufen am 1. Juni 2023.
58 www.baden-wuerttemberg.datenschutz.de/usa-eu-datentransfer-durchfuehrungsverordnung-us-praesident/; abgerufen am 1. Juni 2023.
59 www.baden-wuerttemberg.datenschutz.de/usa-eu-datentransfer-durchfuehrungsverordnung-us-praesident/; abgerufen am 1. Juni 2023.
60 www.bundestag.de/mediathek?videoid=7554214#url=L21lZGlhdGhla292ZXJsYXk/dmlkZW9pZD03NTU0MjE0&mod=mediathek; abgerufen am 1. Juni 2023, Zeitpunkt: 47:07.
61 www.bundestag.de/mediathek?videoid=7554214#url=L21lZGlhdGhla292ZXJsYXk/dmlkZW9pZD03NTU0MjE0&mod=mediathek; abgerufen am 1. Juni 2023, Zeitpunkt: 50:38.
62 Brandel, B.; Porombka, S.; Oevel, G. (2020): IT-Schutz ist kein Projekt, sondern ein Prozess. Cybersicherheit ist für Forschungseinrichtungen essenziell. Ein Überblick über die besonderen Herausforderungen für Hochschulen, S. 656, in: Forschung & Lehre 27 (2020) 8, S. 656–657.
63 Interview mit Susanne Kraus: Komplett offline. Rückblick auf den Cyberangriff an der Universität Gießen, S. 570, in: Forschung & Lehre 30 (2023), Nr. 8, S. 568–570.
64 Übersetzungen durch die Antragsteller; https://edudownloads.azureedge.net/msdownloads/Microsoft-Showcase-Schools-2022-2023.pdf; abgerufen am 14. April 2023, S. 70; https://edudownloads.azureedge.net/msdownloads/scs_rubric_V3.pdf; abgerufen am 14. April 2023.

sourcen in den Lehrplänen verwendet werden und mindestens 75 % des Führungsteams und der Lehrkräfte eine Fortbildung zum „Apple Teacher“ absolviert haben. In den USA werden bereits über 40 Hochschulen zu den Apple Distinguished Schools gezählt, in Europa gibt es sie bislang vereinzelt in Frankreich, Großbritannien und Irland.[65] Ein späterer Wechsel zu anderen Anbietern wird dabei dadurch erschwert, dass sich deutsche Schulen oft mit geschlossenen Systemen ausstatten, bei denen die Schnittstellen im Betriebssystem definiert sind und die Interoperabilität mit anderen Systemen vorgegeben ist; Lernapplikationen anderer Systeme sind damit weniger oder nicht kompatibel und entsprechend schwer oder unmöglich über die angeschafften Geräte als Lernmittel verwendbar.[66] Eine Verschärfung dieser Entwicklung droht nach Ansicht der Antragsteller durch die auch staatlich vorangetriebene Digitalisierung von Bildungs- und Wissenschaftseinrichtungen. Auf eine Kleine Anfrage der Bundestagsfraktion der AfD hin erklärte die Bundesregierung, das geplante Bundesprogramm Digitale Hochschule habe aufgrund der durch den Ukrainekrieg erheblich veränderten weltpolitischen und wirtschaftlichen Rahmenbedingungen noch nicht umgesetzt werden können.[67] Zum Beratungsstand zur Finanzierung und Ausgestaltung des Programms äußerte sie sich nicht. Zugleich fördert die Bundesregierung die Digitalisierung der Hochschulen bereits durch Mittel des „Zukunftsvertrags Studium und Lehre stärken“ sowie über die Förderung der Stiftung Innovation in der Hochschullehre, die den Ausbau digitaler Infrastruktur an den Hochschulen für Online-Lehre, Präsenzlehre und Formate des „Blended Learning“ fördert.[68] Prof. Blum betont, dass es besonders indirekt wirkende Instrumente in Gestalt von Regulierungen sind, die die Gefahr, Opfer eines Cyberangriffs zu werden, stetig erhöhen, indem sie Nutzer aus Gründen ökonomischer oder bürokratischer Effizienzsteigerung auf digitale Plattformen zwingen.[69] In seinen Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum vom Oktober 2023 stellt der Wissenschaftsrat (WR) ebenfalls fest, dass viele Hochschulen und teilweise auch Forschungseinrichtungen in Deutschland nicht ausreichend gegen Cyberangriffe sowie Sabotage- oder Spionageversuche geschützt sind.[70] Der WR verweist dabei auf die geopolitische Dimension digitaler und technologischer Souveränität und die Empfehlung von Cybersicherheitsexperten, die Sicherheit von IT-Infrastrukturen dadurch zu steigern, sich insbesondere von chinesischen und US-amerikanischen Technologie- und Dienstanbietern unabhängiger aufzustellen und durch die Förderung inländischer und europäischer Sicherheitslösungen Selbstbestimmung im internationalen Rahmen zu erreichen.[71] Entsprechend argumentiert auch Kullik, dass wir Gefahr laufen, künftig im Bereich Internet und anderen Technologien von den USA oder China dominiert zu werden: „Einige Analysten sprechen sogar schon von einem neuen kalten IT-Krieg. Zudem müssen wir aufpassen, inwieweit wir uns zu stark in die Abhängigkeit von Unternehmen begeben, Stichwort „Überwachungskapitalismus““.[72]

Zu Forderung 4

Zum bekannt gewordenen Satz der damaligen Bundeskanzlerin Angela Merkel, wonach „Ausspähen unter Freunden“ gar nicht gehe, mit dem sie am 24. Oktober 2013 öffentlich am Rande eines EU-Gipfels in Brüssel die NSA-Affäre kommentierte, bemerkt der ehemalige Präsident des BND Schindler: „Das Problem mit den »Freunden« war deshalb nicht so einfach, weil der Begriff »Freund« keine nachrichtendienstliche Kategorie ist – weder im Alltag noch im Gesetz. […] Abgesehen davon wussten wir mehr informell als offiziell, dass auch die allermeisten Partnerdienste die Kategorie »Freund« bei ihrer Auftragserfüllung nicht kannten“.[73]

Im Rahmen des Master-Studiengangs „International Security Studies“ an der Universität der Bundeswehr München sollen gleichwohl „key senior leaders“, „serving government officials“, „diplomats, legislators, ministerial staffs, policy-makers, military and law enforcement officers, and other officials involved in cyber security serving

---

65 www.apple.com/ca/education/k12/apple-distinguished-schools/docs/Directory-Apple-Distinguished-Schools-CAEN.pdf; abgerufen am 14. April 2023, S. 18f.

66 www.heise.de/hintergrund/Digitale-Bildung-Warum-iPads-an-deutschen-Schulen-so-weit-verbreitet-sind-7121719.html?seite=all; abgerufen am 19. April 2023.

67 Siehe Antwort auf Frage 1, Bundestagsdrucksache 20/4821.

68 www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1; abgerufen am 7. Dezember 2022, S. 22; www.bmbf.de/bmbf/de/bildung/studium/zukunftsvertrag-studium-und-lehre-staerken/zukunftsvertrag-studium-und-lehre-staerken_node.html; abgerufen am 25. Oktober 2022; abgerufen am 7. Dezember 2022; https://stiftung-hochschullehre.de/wp-content/uploads/2022/07/stiftunghochschullehre_fbm2020.pdf; abgerufen am 7. Dezember 2022, S. 1f.

69 Ulrich Blum: Wirtschaftskrieg. Rivalität ökonomisch zu Ende denken, Wiesbaden 2020, S. 839f.

70 www.wissenschaftsrat.de/download/2023/1580-23.pdf?__blob=publicationFile&v=11; abgerufen am 7. November, S. 22.

71 www.wissenschaftsrat.de/download/2023/1580-23.pdf?__blob=publicationFile&v=11; abgerufen am 7. November, S. 10, 13.

72 Jakob Kullik (2020): Vernetzte Unsicherheit. Eine Kritik an den deutschen Bemühungen um digitale Sicherheit, S. 662, in: Forschung & Lehre 27 (2020) 8, S. 662.

73 Gerhard Schindler: Wer hat Angst vorm BND? Warum wir mehr Mut beim Kampf gegen die Bedrohungen unseres Landes brauchen. Eine Streitschrift, Berlin 2020, S. 188f.

throughout the whole of government“ und insbesondere „senior officials responsible for developing or influencing cyber legislation, policies or practices“ durch das „Program on Cyber Security Studies“ des deutsch-amerikanischen George C. Marshall European Center for Security Studies dazu ausgebildet werden, „informed decisions on cyber policy, strategy and planning within the framework of whole-of-government cooperation and approaches“ treffen zu können – ein bundesuniversitäres Studium zum Schutz vor Cyberangriffen unter der Aufsicht des Pentagons.[74] Hier gilt nach Auffassung der Antragsteller, was Jäger, Diersch und Liedtke in Bezug auf die deutsche und auf europäische Regierungen festgestellt haben, nämlich „dass die sicherheitspolitische Abhängigkeit von den USA letztlich durch einen fortwährenden Verlust eigener Hoheitsgewalt und eine dauerhafte Einschränkung eigener autonomer Handlungsmacht immer wieder hervorgerufen wird“.[75] Der eigene Handlungsspielraum sei „angesichts der asymmetrisch verteilten Fähigkeiten extrem begrenzt“, was man wissen dürfe, bleibe „in Wirklichkeit außerhalb“ des „eigenen Gestaltungsvermögens“.[76] Angesichts der geschilderten Gefahren, konkreten Bedrohungen und Angriffe, die von US-Behörden und von mit diesen Behörden verflochtenen IT-Unternehmen für deutsche Hochschulen und Forschungseinrichtungen bereits ausgingen bzw. weiterhin ausgehen, ist es nach Auffassung der Antragsteller mit deutschen Interessen unvereinbar, deutsche Entscheidungsträger und Praktiker der Cybersicherheit durch ein regionales Zentrum des US-Verteidigungsministeriums ausbilden zu lassen. Eine Überprüfung der entsprechenden Bildungskooperation zwischen dem BMVg und dem Verteidigungsministerium der Vereinigten Staaten ist nach Ansicht der Antragsteller somit dringend geboten.

Zu Forderung 5

Der Leiter der französischen „École de guerre économique“ (EGE), Historiker, Wirtschaftsberater und ehemalige Geheimdienstmitarbeiter Christian Harbulot verweist hinsichtlich der Frage nach den Bedingungen der Fähigkeit zur hybriden Kriegführung, wozu Spionage- und Cyberangriffe gezählt werden, zum einen auf die Notwendigkeit der Ausbildung entsprechenden Personals in europäischen Nationen wie Deutschland, Frankreich oder Italien und zugleich auf die Unterschiede in den Interessen und Zielen dieser Nationen im Vergleich mit denen Großbritanniens und der USA.[77]

Mit der EGE hat sich in Frankreich eine ökonomische Schule zur Ausbildung von Führungskräften im Wirtschaftskrieg etabliert, die aus den strategischen, operativen und taktischen Konzepten des Militärs Erkenntnisse für einen Wirtschaftskrieg ableitet, während in Deutschland laut Prof. Blum nichts Vergleichbares existiert.[78] Unternehmen riskierten ebenso wie Staaten in der Realität stets die Vernichtung des Konkurrenten oder der eigenen Firma.[79] Das Denken in geopolitischen und geostrategischen Kategorien sei für Großmächte wie die USA, China und Russland Normalität und für andere Atommächte wie Frankreich, England, Indien oder Israel gelte dies ebenso.[80] Deutschland werde sich diesem Kalkül nicht auf Dauer entziehen können. Die EGE entstand 1997 als Reaktion auf Praktiken amerikanischer Unternehmen im Globalisierungswettlauf.[81] Der Leiter der EGE Harbulot, betonte bereits vor dem Hintergrund der NSA-Affäre, dass es wichtig sei, nicht in einer „Kultur des Unausgesprochenen zu verharren“, sondern die harten Realitäten zur Kenntnis zu nehmen: „Wir sind in einer neuen Ära angekommen, wo es neben der realen Welt eine neue virtuelle Welt gibt. Das NSA-Programm Prism ist alles andere als ein Einzelfall. Was den Fall so interessant macht: Heute kann man nicht länger ernsthaft behaupten, die Welt der Informationen sei ein sicheres Universum. Die Informationsgesellschaft wird von Amerikanern kontrolliert. Sie beschränken sich nicht darauf, Daten zu sammeln und in die Privatsphäre der Bürger in Europa, Südamerika und Asien einzudringen. Sie versuchen auch, vertrauliche Informationen von Firmen zu bekommen. Viele europäische Politiker haben sich darüber echauffiert. Franzosen und Deutsche wussten aber seit der Gründung des Internets, dass es von den Amerikanern kontrolliert wird. In Frankreich hat das Sécrétariat Général de Défense Nationale, das alle Nachrichtendienste koordiniert, Anfang der 90er-Jahre intern vor der Nutzung des Internets gewarnt. Das zeigt, dass seit 20 Jahren bekannt ist, was Herr Snowden jetzt publik gemacht hat. Diese Empfehlung wurde nicht befolgt, denn es ist unmöglich, ohne Internet zu arbeiten. Aber man kann jetzt auch

---

[74] www.unibw.de/casc/programme/the-master-in-international-security-studies-miss; abgerufen am 27. April 2023; www.marshallcenter.org/en/academics/college-courses/program-cyber-security-studies-pcss; abgerufen am 27. April 2023.

[75] Thomas Jäger, Verena Diersch, Stephan Liedtke: Was Europa wissen darf. Die Geheimdienste der USA und die europäische Politik, Zürich 2020, S. 213.

[76] Thomas Jäger, Verena Diersch, Stephan Liedtke: Was Europa wissen darf. Die Geheimdienste der USA und die europäische Politik, Zürich 2020, S. 214.

[77] www.fr.de/politik/europa-muss-den-hybriden-krieg-denken-92110698.html; abgerufen am 24. Mai 2023.

[78] Ulrich Blum: Wirtschaftskrieg. Rivalität ökonomisch zu Ende denken, Wiesbaden 2020, S. 4.

[79] Ulrich Blum: Wirtschaftskrieg. Rivalität ökonomisch zu Ende denken, Wiesbaden 2020, S. 4.

[80] Ulrich Blum: Wirtschaftskrieg. Rivalität ökonomisch zu Ende denken, Wiesbaden 2020, S. 4.

[81] www.spiegel.de/lebenundlernen/uni/wirtschaftskrieger-hochschule-fuer-hauen-und-stechen-a-470728.html; abgerufen am 25. Mai 2023.

nicht einfach weitermachen, als sei nichts geschehen“.[82] Nach Ansicht der Antragsteller verleihen die bereits aufgeführten Gefahren sowie Cyber- und Spionageangriffe, die von Behörden und IT-Unternehmen fremder Staaten auf die F&E sowie auf das Wissenschaftsorganisationswissen Deutschlands ausgehen, den Ausführungen Harbulots für Deutschland eine hohe Relevanz und Aktualität. Deshalb sollte der Bund dem von der Fraktion der AfD geforderten Forschungsinstitut für geopolitische Studien an der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg[83] einen geoökonomischen Forschungszweig angliedern, in dessen Rahmen analog zur französischen EGE Wissenschaftsspionage und Cyberkriegführung um F&E als Bestandteil der Ausbildung von Führungskräften im Wirtschaftskrieg gelehrt und aus den strategischen, operativen und taktischen Konzepten des Militärs Erkenntnisse für den Wirtschaftskrieg abgeleitet werden.

Zu Forderung 6

Jäger, Diersch und Liedtke stellen fest, dass die USA bei der Zusammenfassung globaler Informationen, die in dieser Art „vermutlich einzigartig“ sei, eine „allumfassende Strategie von Informationsbeschaffung“ verfolgen, deren Ziel sich im Kern als „globale Informationsdominanz durch Technologieüberlegenheit“ zusammenfassen lasse.[84] So lasse sich auch mit Rückblick auf die NSA-Affäre und ihre politischen folgen eindeutig festhalten: „Die NSA und andere amerikanische Geheimdienste haben in ihren Programmen kein Eigenleben außerhalb politisch gesetzter Rahmenbedingungen geführt, sondern sie handelten auf eindeutige und belegbare politische Initiative im Rahmen einer klaren sicherheitspolitischen Strategie und einer eindeutig festgelegten strategischen Rolle“.[85] Während das Kompetenzzentrum Internationale Wissenschaftskooperationen (KIWi) des DAAD im Falle Chinas davor warnt, dass dessen Ziel eines technologischen Großmachtstatus ein Risiko für die Kooperation deutscher mit chinesischen Hochschulen und Wissenschaftseinrichtungen darstelle, scheint das strategische Ziel der USA einer globalen Informationsdominanz durch Technologieüberlegenheit bislang kein entsprechendes Gefahrenbewusstsein hervorzurufen.[86]

Zu Forderung 7

Der Vizepräsident des BfV Sinan Selen suggeriert nach Ansicht der Antragsteller, eingedenk der in der Politikwissenschaft üblichen Unterscheidung des Westens von autoritären Staaten, die Bedrohung für deutsche Wissenschaftseinrichtungen durch Wissenschaftsspionage gehe lediglich von nichtwestlichen Staaten aus: „Die Hemmschwelle für Spionage und Sabotage durch autoritäre Staaten sinkt – das ist Teil der Herausforderung für Demokratien und die internationale Ordnung. Für den Wirtschafts- und Wissenschaftsstandort Deutschland bedeutet das eine erhöhte Gefährdungslage“.[87] Laut dem BMI wird die überwiegende Zahl der in Deutschland festgestellten Cyberangriffe mit mutmaßlich staatlicher Steuerung Russland, China und dem Iran zugeordnet, was ebenfalls Flinks oben genannte Beobachtung bestätigt, wonach vorwiegend diese Staaten als Bedrohung aufgeführt werden.[88] Das BfV erhebt den Anspruch einer „360°-Bearbeitung“ im Rahmen der Aufklärungs- und Abwehraktivitäten der Spionageabwehr, benennt als Akteure der Wissenschaftsspionage gegen Deutschland aber lediglich nichtwestliche Staaten wie Russland, China, den Iran, Pakistan, Nordkorea und Syrien.[89] Westliche Akteure kommen demgegenüber als Bedrohung nicht in Betracht und werden nach Ansicht der Antragsteller implizit als solche für unwahrscheinlich erklärt, da Deutschlands Gefährdung im Bereich der Wissenschaftsspionage mit seiner aktiven Rolle in EU und NATO und damit nach Auffassung der Antragsteller mit Deutschlands Rolle als Akteur innerhalb westlicher Strukturen begründet wird.[90] Auch in der Ausgabe des vom Bereich Prävention in Wirt-

---

[82] Ulrich Blum: Wirtschaftskrieg. Rivalität ökonomisch zu Ende denken, Wiesbaden 2020, S. 4; www.welt.de/print/wams/wirtschaft/article118236120/Frankreich-tut-was-es-kann.html; abgerufen am 24. Mai 2023.

[83] Bundestagsdrucksache 20/6989.

[84] Thomas Jäger, Verena Diersch, Stephan Liedtke: Was Europa wissen darf. Die Geheimdienste der USA und die europäische Politik, Zürich 2020, S. 204f.

[85] Thomas Jäger, Verena Diersch, Stephan Liedtke: Was Europa wissen darf. Die Geheimdienste der USA und die europäische Politik, Zürich 2020, S. 205.

[86] https://hcss.nl/wp-content/uploads/2021/01/BZ127566-HCSS-Checklist-for-collaboration-with-Chinese-Universities.pdf; abgerufen am 25. März 2024, S. 1f.

[87] www.verfassungsschutz.de/DE/themen/wirtschafts-wissenschaftsschutz/wirtschafts-wissenschaftsschutz_node.html;jsessionid=C2CC885C52A99E687E20C491E4327808.intranet252; abgerufen am 12. April 2023; www.ssoar.info/ssoar/bitstream/handle/document/27551/ssoar-2008-kollner-autoritare_regime_-_keine_weltweit.pdf?sequence=1&isAllowed=y&lnkname=ssoar-2008-kollner-autoritare_regime_-_keine_weltweit.pdf; abgerufen am 28. April 2023, S. 1, 2, 5f.

[88] www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/cyberspionage/cyberspionage-node.html; abgerufen am 19. April 2023.

[89] www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2023-06-20-verfassungsschutzbericht-2022.pdf?__blob=publicationFile&v=9; abgerufen am 25. März 2024, S. 278, 281, 304, 306f.

[90] www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2023-06-20-verfassungsschutzbericht-2022.pdf?__blob=publicationFile&v=9; abgerufen am 25. März 2024, S. 278.

schaft, Wissenschaft, Politik und Verwaltung des BfV herausgegebenen Magazins SPOC vom März 2023 mit dem Themenschwerpunkt Spionage in Wirtschaft und Forschung werden unter dem Gesichtspunkt des Interesses anderer Länder, sich Zugang zu deutschen wissenschaftlichen Erkenntnissen und Erfindungen zu verschaffen, lediglich Russland und China aufgeführt.[91] Westliche Staaten wie die USA werden lediglich als Referenzen für die Bedrohung Deutschlands und der „westlichen Staatengemeinschaft" durch Russland und China genannt.[92]

Der MAD-Report 2021/22 des BAMAD benennt die Bereiche Wissenschaft, Forschung und Entwicklung explizit als Gründe für die Notwendigkeit von Maßnahmen zur Spionage- und Cyberabwehr, nennt als Angreifer aber lediglich China.[93] Westliche Akteure kommen auch hier als Bedrohung nicht in Betracht und werden nach Ansicht der Antragsteller erneut implizit als solche für unwahrscheinlich erklärt, da Deutschlands Gefährdung im Bereich der Wissenschaftsspionage mit seiner aktiven Rolle in EU und NATO und damit nach Auffassung der Antragsteller mit Deutschlands Rolle als Akteur innerhalb westlicher Strukturen begründet wird.[94]

Im Falle des BND unterliegen konkrete Angaben zu den Staaten, die nachrichtendienstlich aufzuklären sind, zwar der Geheimhaltung.[95] Vor dem Hintergrund der Kooperation mit den anderen Nachrichtendiensten im Rahmen des Nationalen Cyber-Abwehrzentrums und der Initiative Wirtschaftsschutz zum Schutz vor Wissenschaftsspionage und Cyberangriffen sowie angesichts dessen, dass neben der Geheimhaltung der Aufklärungsziele zugleich explizit „enge Verbindungen zu Institutionen der Europäischen Union und der NATO" seitens des BND bestehen, ist nach Auffassung der Antragsteller Grund zu der Annahme gegeben, dass Zutrauen und Gefahreneinschätzung gegenüber den genannten Staaten hier ähnlich verteilt sind.[96]

In ihren Stellungnahmen vor dem Parlamentarischen Kontrollgremium im Deutschen Bundestag verwiesen die Präsidenten der für Cyber- und Spionageabwehr zuständigen Behörden BfV, BAMAD und BND in den letzten Jahren zwar regelmäßig auf die Bedrohung durch Cyber- und Spionageangriffe, die u.a. mit dem Ziel des Zugriffs auf Informationen des Bereichs F&E erfolgen würden, wie bspw. Militärtechnologie und militärisch nutzbare Forschungsergebnisse, medizinisches Forschungs- und Organisationswissen.[97] Als Angreifer wurden aber lediglich nichtwestliche Staaten wie Russland, China und der Iran benannt, während westliche Staaten wie die USA nur implizit und im Rahmen von Kooperations- und Bündnisstrukturen, nicht aber als Angreifer genannt werden.[98] Demgegenüber warnen Experten des Max-Planck-Instituts für ausländisches und internationales Strafrecht Hochschulen und andere Wissenschaftseinrichtungen vor Wissenschaftsspionage auch durch westliche Staaten wie die USA und solche aus dem europäischen Ausland.[99]

Zu Forderung 8

Gehemmt wird der Ausbau der Cybersicherheit mithilfe der IT-Sicherheitsforschung zudem durch die geltende Rechtslage, gemäß der auch das wohlmeinende Identifizieren, Melden und Schließen von Sicherheitslücken potenziell einen Strafbefehl zur Folge haben kann. Die Bundesregierung hat im Koalitionsvertrag zwar angekündigt, das „Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z. B.

---

91 www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2023-03-23-spoc-magazin.pdf?__blob=publicationFile&v=4; abgerufen am 13. April 2023, S. 9ff.

92 www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2023-03-23-spoc-magazin.pdf?__blob=publicationFile&v=4; abgerufen am 13. April 2023, S. 10, 20, 49.

93 www.bundeswehr.de/resource/blob/5361404/4fa2a6e88f8fc77863022395942e6241/mad-report-2020-data.pdf; abgerufen am 12. Mai 2023, S. 17, 28.

94 www.bundeswehr.de/resource/blob/5631036/e06fcba5e41b279b28d823b9298083c2/mad-report-2021-2022-data.pdf; abgerufen am 25. März 2024, S. 20.

95 www.bnd.bund.de/DE/Die_Themen/Laender_Regionen/Auftragsprofil/staaten_node.html; abgerufen am 12. Mai 2023.

96 www.wirtschaftsschutz.info/DE/Home/home_node.html; abgerufen am 12. Mai 2023; www.bnd.bund.de/DE/Die_Arbeit/Kooperationen/kooperationen_node.html;jsessionid=33416433D6D160D0662A4A1F443CC11A.internet972; abgerufen am 12. Mai 2023.

97 www.bundeswehr.de/resource/blob/5511988/f1769b95a327078a44d74312e13db60f/eingangsstatement-pkgr-2022-data.pdf; abgerufen am 11. Mai 2023, S. 5; www.bundeswehr.de/resource/blob/5232150/65cbc456991e8c2171e589912e5b78a4/eingangsstatement-pkgr-2021-data.pdf; abgerufen am 11. Mai 2023, S. 7; https://youtu.be/iHKVnvnkZXc?t=1992; abgerufen am 11. Mai 2023; https://youtu.be/iHKVnvnkZXc?t=9488; abgerufen am 12. Mai 2023; www.bnd.bund.de/SharedDocs/Downloads/DE/Statement_Bruno_Kahl_2022.pdf?__blob=publicationFile&v=5; abgerufen am 11. Mai 2023, S. 3; www.verfassungsschutz.de/SharedDocs/reden/DE/2021/statement-haldenwang-oeffentliche-anhoerung-durch-das-parlamentarische-kontrollgremium.html; abgerufen am 11. Mai 2023; www.verfassungsschutz.de/SharedDocs/reden/DE/2022/2022-10-17-haldenwang-pkgr.html; abgerufen am 11. Mai 2023.

98 Bundestagsdrucksache 20/310, S. 10; www.bundeswehr.de/resource/blob/5511988/f1769b95a327078a44d74312e13db60f/eingangsstatement-pkgr-2022-data.pdf; abgerufen am 11. Mai 2023, S. 4, 5, 7; www.bnd.bund.de/SharedDocs/Downloads/DE/Statement_Bruno_Kahl_2022.pdf?__blob=publicationFile&v=5; abgerufen am 11. Mai 2023, S. 2, 3; www.verfassungsschutz.de/SharedDocs/reden/DE/2022/2022-10-17-haldenwang-pkgr.html; abgerufen am 11. Mai 2023.

99 www.mpg.de/12584445/Handlungsleitfaden_Wissenschaftsorganisationen_final.pdf; abgerufen am 13. April 2023, S. 14 www.zeit.de/campus/2021-06/russischer-geheimdienst-spionage-verdacht-universitaet-augsburg/komplettansicht; abgerufen am 12. April 2023.

in der IT-Sicherheitsforschung, soll legal durchführbar sein".[100] Dieses Vorhaben wurde bislang jedoch nicht umgesetzt.[101] In ihrer Antwort auf eine Schriftliche Einzelfrage erklärte die Bundesregierung, in der ersten Jahreshälfte 2024 hierzu einen Gesetzentwurf vorlegen zu wollen.[102] Hier besteht nach Auffassung der Antragsteller dringender Handlungsbedarf seitens der Bundesregierung, das Identifizieren, Melden und Schließen von Sicherheitslücken im Rahmen der IT-Sicherheitsforschung dergestalt legal zu ermöglichen, dass die Durchführung von in gutem Glauben durchgeführten IT-Sicherheitstests keine Strafverfolgung oder Ermittlung durch die Staatsanwaltschaft begründen kann.

[100] www.bundesregierung.de/resource/blob/974430/1990812/1f422c60505b6a88f8f3b3b5b8720bd4/2021-12-10-koav2021-data.pdf?download=1; abgerufen am 9. November 2023, S. 16.

[101] Kipker, D.; Rockstroh, S. (2023): Es bedarf klarer Regeln. Strafbarkeitsrisiken von IT-Sicherheitsforschern, S. 575, in: Forschung & Lehre 30 (2023) 8, S. 574–575.

[102] Antwort auf die Schriftliche Frage Nr. 11/379.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333