AUSWIRKUNGEN AUSLÄNDISCHER GESETZGEBUNG AUF DIE DEUTSCHE CYBERSICHERHEIT

Impulspapier | November 2021

Zusammenfassung

Die Cybersicherheit in Deutschland wird nicht nur durch außereuropäische Nachrichtendienste bedroht, sondern auch durch ausländische Unternehmen, die durch gesetzliche Vorgaben gezwungen sind, die Nachrichtendienste ihres Herkunftsstaates zu unterstützen. Um sich gegen diese Bedrohung zu wehren, ist es notwendig, die technologische und wirtschaftliche Abhängigkeit zu verringern und digitale Souveränität zu stärken. Das vorliegende Impulspapier untersucht, mit welchen Zielsetzungen und Mitteln ausländische Nachrichtendienste – direkt oder über in Deutschland operierende Unternehmen – auf die Cybersicherheit in Deutschland Einfluss nehmen könnten. Hierzu werden die jeweiligen Rechtsgrundlagen und rechtlichen Handlungsmöglichkeiten analysiert, auf deren Grundlage die Geheimdienste agieren. Den Nachrichtendiensten der USA, Russlands und Chinas kommt mit ihren Zielsetzungen und Möglichkeiten in der derzeitigen politischen Weltlage die größte Bedeutung zu. Diese drei Staaten unterhalten die drei weltweit größten nachrichtendienstlichen Infrastrukturen. Daher werden deren Rechtsgrundlagen für Auslandsaufklärung und Cyberspionage, soweit dies auch Deutschland betreffen kann, näher vorgestellt. Zu diesem Zweck werden für alle drei Staaten die gesetzlichen Aufgaben und Befugnisse der Nachrichtendienste analysiert sowie ihre Möglichkeiten, Staatsangehörige und Unternehmen zu ihrer Unterstützung zu verpflichten. Dabei beschränkt sich die folgende Analyse auf die Rechtslage in den drei Staaten und stellt keine Spekulationen an, wie die Nachrichtendienste ihre gesetzlichen Aufgaben in der Praxis erfüllen und von ihren Befugnissen Gebrauch machen.

1 Nationale Gesetzgebung für Nachrichtendienste

Das Völkerrecht kennt zwar allgemeine Verbote zur Gewaltausübung, zu Interventionen mit Zwangscharakter oder zu anderen Verletzungen der Souveränität eines anderen Staates. Völkerrechtlich ungeregelt ist jedoch die Spionage oder sonstige Informationssammlung. Sie ist damit völkerrechtlich weder erlaubt noch verboten. Daher steht es den nationalen Gesetzgebern frei, die Informationssammlung und -verarbeitung durch die eigenen Nachrichtendienste zu regeln. Strategische und taktische Vorgaben erfolgen in der Regel durch interne Anweisungen, die nicht für die Öffentlichkeit bestimmt sind. Soweit jedoch Kompetenzen bestimmt, Behörden koordiniert, Mitarbeiter gesteuert und Private verpflichtet werden müssen, erfolgt dies überwiegend in Form von Gesetzen, die auch veröffentlicht werden. Gegenstand dieser Regelungen können zum Beispiel externe Interventionen, Sicherung der Herrschaft über den eigenen digitalen Kommunikationsraum oder Pflichten zur Unterstützung der Nachrichtendienste durch Gestaltung von Informationstechnik oder Sammlung von Daten sein.

2 Gesetzliche Grundlagen in den USA

Die Geheimdienste der USA und ihre gesetzlichen Grundlagen sind sehr heterogen. Die zahlreichen Geheimdienste des Landes kooperieren als US Intelligence Community (IC). Eine Gesamtaufsicht erfolgt durch den Director of National Intelligence (DNI). Einzige unabhängige Geheimdienstorganisation, die nicht einer übergeordneten Bundesbehörde untersteht, ist die Central Intelligence Agency (CIA). Inlandsgeheimdienst ist das Federal Bureau of Investigation (FBI), das auch als dem Justizministerium unterstellte Bundespolizei fungiert. Größter Auslandsgeheimdienst ist die National Security Agency (NSA), die mit der elektronischen Aufklärung betraut ist und den anderen Geheimdiensten zuarbeitet.

2.1 Gesetzliche Aufgaben

Ein wesentliches Fundament der geheimdienstlichen Tätigkeit in den USA ist der Präsidialerlass „Executive Order 12333“ vom 4. Dezember 1981, weitgehend neu gefasst durch „Executive Order 13470“ vom 30. Juli 2008. Der Erlass betrifft vor allem die Überwachung von Datenströmen außerhalb des Territoriums der USA (Data in Transit). Übergeordnetes Ziel des „United States Intelligence Effort“ („nachrichtendienstliche Aktivitäten der USA“) ist es danach, den Präsidenten, den National Security Council und den Homeland Security Council mit notwendigen Informationen zur Entscheidungsfindung auszustatten. Informationssammlungen über „US-Persons“ (US-Bürger) haben nach einem

vom Attorney General (Generalstaatsanwalt) genehmigten Verfahren zu erfolgen. Ihnen gegenüber sind die „least intrusive collection techniques feasible" („möglichst wenig in die Privatsphäre eingreifende Erhebungsmethoden") einzusetzen. Effektive Restriktionen bezogen auf Non-US-Persons (Nicht-US-Bürger) bestehen nicht. Die „Presidential Policy Directive 28" (PPD-28) aus dem Jahr 2014 betrifft die Signal Intelligence (Fernmelde- und elektronische Aufklärung). Sie formuliert Ziele der „collection in bulk" („Massensammlung"), zu denen auch die Aufdeckung und Bekämpfung von „cybersecurity threats" („Cybersicherheitsbedrohungen") gehört. Ausgeschlossen wird eine Nutzung von Signal Intelligence zu Zwecken der Wirtschaftsspionage. Diese Einschränkung bestand vor 2014 nicht. Interne Zielsetzungen der NSA, die im Zuge der Snowden-Enthüllungen publik wurden, beschreiben unter anderem mit „owning the Internet" („Herrschaft über das Internet") sehr ambitionierte Ziele geheimdienstlicher Tätigkeit mit signifikanten Implikationen für den Bereich der Cybersicherheit.

2.2 Gesetzliche Befugnisse

Rechtliche Rahmenbedingungen der elektronischen Aufklärung wurden erstmals 1978 mit dem FISA Act (Foreign Intelligence Surveillance Act) festgelegt. Größere Überarbeitungen erfolgten durch den USA PATRIOT Act 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act), den Protection of America Act 2007, den FISA Amendments Act 2008, den USA FREEDOM Act 2015 (Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act), den CLOUD Act 2018 (Clarifying Lawful Overseas Use of Data Act) und weitere Gesetze.

FISA ermöglicht in Abschnitt 702 die Aufklärung der Kommunikation von Ausländern ohne richterliche Anordnung. Vor allem die Vorschrift „50 U.S.C. § 1881a" regelt „Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons" („Verfahren zur gezielten Überwachung von Nicht-US-Bürgern außerhalb der Vereinigten Staaten") und ermöglicht den Erlass einer „order requiring the production of any tangible things" („Anordnung, die die Produktion jeglicher greifbaren Dinge vorschreibt"). Mit dem Erlass des FISA erfolgte auch die Einrichtung des Foreign Intelligence Surveillance Court (FISC), dem geheimdienstliche Programme (wie zum Beispiel Planning tool for Resource Integration, Synchronization, and Management (PRISM) oder Upstream) und Maßnahmen zur Genehmigung vorzulegen sind. Dieser tagt nicht öffentlich. Für US-Ausländer besteht kein Rechtsschutz gegenüber US-Nachrichtendiensten.

2.3 Indienstnahme von Unternehmen und Staatsangehörigen

Das US-Recht ermöglicht eine umfassende Indienstnahme von US-Unternehmen, insbesondere von Anbietern von Kommunikationsdienstleistungen oder von „remote computing services". Insbesondere der CLOUD Act zielt auf eine eindeutige Rechtsgrundlage für einen weltweiten Datenzugriff. Er etabliert durch Vorschrift 18 U.S.C. § 2713 eine Pflicht der Provider, alle Inhalte elektronischer Kommunikation auf Antrag zu erfassen und zu speichern sowie alle gespeicherten Informationen zur Verfügung zu stellen, unabhängig davon, wo sie aufbewahrt werden. Die Informationen müssen sich lediglich auf einen „customer" (Kunden) beziehen und sich im Besitz, der Obhut oder unter der Kontrolle des Providers befinden. Zur Abmilderung von Konflikten mit anderen Rechtsordnungen sieht der Vorschrift 18 U.S.C. § 2523 sogenannte „executive agreements" („Exekutivverträge") mit anderen Staaten vor. Ein solches „Agreement" wurde bisher aber nur mit Großbritannien geschlossen. Entsteht ein solcher Konflikt, kann der Provider eine gerichtliche Abwägungsentscheidung anstreben. Nach Vorschrift 18 U.S.C. § 2709 kann das FBI zudem sogenannte „National Security Letter" („Brief zur Nationalen Sicherheit") ausstellen, die US-Unternehmen und -Staatsangehörige zur Kooperation mit Sicherheitsbehörden verpflichten. Über Erhalt und Inhalt eines National Security Letter darf der Adressat gegenüber Dritten keine Angaben machen.

3 Gesetzliche Grundlagen in Russland

Die wichtigsten Nachrichtendienste der Russischen Föderation (RF) sind der Inlandsnachrichtendienst FSB (Federalnaja Slushba Besopasnosti), der Auslandsnachrichtendienst SWR (Slushba Wneschnej Raswedki) und der Militärische Auslandsnachrichtendienst GRU (Glawnoje Raswedywatelnoje Uprawlenije).

3.1 Gesetzliche Aufgaben

Seit 2014 sind eine Vielzahl von Gesetzen zum Tätigkeitsbereich der Nachrichtendienste der RF ergangen, die auf die umfassende Überwachung der Informationsgesellschaft abzielen.

Die Aufgaben des FSB umfassen nach dem Föderalen Gesetz (FG) „Über den Bundessicherheitsdienst" vom 3. April 1995 Nr. 40-FZ die Spionageabwehr, die Beobachtung oppositioneller Gruppierungen sowie die Bekämpfung von Extremismus, Terrorismus und Organisierter Kriminalität. Zur Gewährleistung der Informationssicherheit hat der FSB auch die Aufgabe, die eingesetzte Informationstechnik in der RF einschließlich der Kryptografie so zu gestalten, dass er seinen Überwachungsauftrag erfüllen kann. Zudem hat der Nachrichtendienst die Aufgabe, Wirtschafts-, Technologie-

und Militärspionage vom Boden der RF aus zu betreiben. In Einzelfällen führt der FSB Gegenspionage auch im Ausland durch.

Nach dem FG „Über den Auslandsnachrichtendienst“ vom 10. Januar 1996 Nr. 5-FZ ist der SWR für Spionage in den Bereichen Politik, Wirtschaft, Wissenschaft und Technologie zuständig. Zu seinen Zielen gehören ausdrücklich die Unterstützung der wirtschaftlichen Entwicklung, des wissenschaftlichen und technologischen Fortschritts und der militärtechnischen Sicherheit. Weitere Aufgaben sind Gegenspionage, elektronische Aufklärung sowie die Bekämpfung von Proliferation und Terrorismus.

Die Aufgaben des GRU bestehen in der Beschaffung von Informationen in den Bereichen Militär und Sicherheitspolitik. Sie sind in mehreren Gesetzen festgehalten, unter anderem im FG „Über die Verteidigung“ vom 31. Mai 1996 Nr. 61-FZ und im FG „Über die Sicherheit“ vom 28. Dezember 2010 Nr. 390-FZ. Zu den Zielen des GRU zählen auch die Förderung der wirtschaftlichen Entwicklung des Landes, des wissenschaftlichen und technologischen Fortschritts und der militärischtechnischen Sicherheit der RF.

3.2 Gesetzliche Befugnisse

Für Aktivitäten im Ausland ist vor allem der SWR zuständig, aber auch der FSB und der GRU haben Kompetenzen, um in der Verfolgung ihrer Aufgaben im Ausland tätig zu werden. Der SWR kann nach den gesetzlichen Grundlagen offene und verdeckte Methoden und Mittel einsetzen, deren konkreter Charakter durch die gegebenen Bedingungen bestimmt wird. Die nachrichtendienstlichen Tätigkeiten führen entweder unabhängige Agenturen oder Mitarbeiter des SWR durch, die in anderen Exekutivorganen der RF – wie etwa dem diplomatischen Dienst – arbeiten.

Befugnisse des FSB ergeben sich aus dem FG 1995 Nr. 40-FZ sowie unter anderem aus dem FG „Über operative Suchaktivitäten“ 1995 Nr. 144-FZ. Sie ermöglichen dem FSB, die technisch unterstützte Kommunikation in der RF vollkommen zu kontrollieren. Telekommunikationsunternehmen sind verpflichtet, Metadaten für die Dauer von drei Jahren und Inhaltsdaten für die Dauer von sechs Monaten zu speichern, Internet-Service-Provider für die Dauer von zwölf beziehungsweise sechs Monaten. Die Unternehmen müssen die Daten in eigenen Einrichtungen auf dem Gebiet der RF speichern und dem FSB zur Verfügung stellen. Sie sind außerdem zum Einbau technischer Mittel verpflichtet. Verschlüsselungstechnik muss durch den FSB genehmigt werden. Der FSB sammelt in großem Umfang biometrische, genomische und biologische Daten – von Ausländern vor allem im Rahmen von Grenzkontrollen –, die zur Identifizierung, zur Überwindung von Zugriffskontrollen oder zur Erpressung genutzt werden können.

Allen Nachrichtendiensten der RF ist erlaubt, zur Tarnung ihrer Aktivitäten Unternehmen, Forschungsorganisationen, Bildungseinrichtungen und ähnliche Organisationen zu gründen und zu betreiben oder in bestehenden Institutionen eigene Abteilungen zu bilden.

3.3 Indienstnahme von Unternehmen und Staatsangehörigen

Nach Artikel 15 FG 1995 Nr. 40-FZ sind Unternehmen, Institutionen und Organisationen unabhängig von ihrer Eigentumsform verpflichtet, den FSB in seiner Aufgabenerfüllung zu unterstützen. Zusätzlich sind natürliche und juristische Personen, die in der RF Postdienstleistungen, Telekommunikation und andere Kommunikationssysteme betreiben, verpflichtet, auf Verlangen des FSB zusätzliche Ausrüstung und Software in ihre Hardware einzubauen sowie andere Bedingungen zu schaffen, die für die operative und technische Tätigkeit des FSB erforderlich sind. Zu diesem Zwecke können zudem Mitarbeiter des FSB in diese Stellen abgeordnet werden.

Dem SWR ist es nach Artikel 6 Abs. 2 FG 1996 Nr. 5-FZ gestattet, Informations- und Kommunikationssysteme sowie Sicherheitstechnik zu entwickeln, herzustellen und zu betreiben sowie zu lizenzieren und zu zertifizieren. Soweit es dem SWR gelingt, solche Geräte oder Systeme zu verbreiten, dürfte er auch auf diese zugreifen, Daten erheben und Funktionen manipulieren können.

4 Gesetzliche Grundlagen in China

Die Volksrepublik China (VRC) unterhält mehrere Geheimdienste, die in der Lage sind, Cyberspionage durchzuführen. Das Ministerium für Staatssicherheit (MSS) ist für die Auslandsaufklärung, die nichtmilitärische Auslandsspionage und die politische Sicherheit zuständig. Die ihm unterstehenden „Ämter für Staatssicherheit“ sind sowohl in China selbst als auch im Ausland aktiv. Auch sind mehrere Abteilungen der Volksbefreiungsarmee mit militärischen Aufklärungs- und Spionageabwehroperationen sowie Wirtschaftsspionage befasst. Bis 2014 war das chinesische System der Geheimpolizeien und Nachrichtendienste zum größten Teil gesetzlich ungeregelt. Ihnen dienten allgemeine Ministerialanweisungen zur Orientierung in der Praxis. Seit 2014 erließ die VRC jedoch sukzessive ein Paket von Gesetzen zur nationalen Sicherheit, insbesondere zur Cybersicherheit. Diese Gesetze zielen darauf ab, die rechtliche Grundlage für Chinas Sicherheitsaktivitäten zu stärken und chinesische und ausländische Bürger, Unternehmen und Organisationen zur Zusammenarbeit zu verpflichten.

4.1 Gesetzliche Aufgaben

Das Gesetz zur Spionageabwehr 2014 (CEL), das Gesetz zur nationalen Sicherheit 2015 (NatS), das Gesetz zur Terrorismusbekämpfung 2015 (CTL), das Gesetz zur Cybersicherheit 2016 (ergänzt 2018) (CSL), das Kryptografiegesetz 2020 (CrypL), das Gesetz zur Sicherheit personenbezogener Informationen 2021 (PIPL) und das Gesetz zur Datensicherheit 2021 (DSL) beschreiben die Aufgaben der Sicherheitsbehörden und Nachrichtendienste und die Pflichten von Organisationen, Unternehmen und Staatsangehörigen für die Abwehr von Spionage und die Gewährleistung innerer Sicherheit. Das NatS gibt vor, dass die nationale Sicherheit aufrechtzuerhalten und die demokratische Volksherrschaft und das sozialistische System mit chinesischen Merkmalen unter der Führung der Kommunistischen Partei Chinas zu schützen sind.

Geheimdienstliche Aktivitäten im Ausland regelt vor allem das Nationale Geheimdienstgesetz von 2017 (NIL). Danach sollen die Nachrichtendienste nicht nur politische Ziele verfolgen, sondern auch wirtschaftliche und soziale Interessen Chinas unterstützen. Sie sollen vor allem nachrichtendienstliche Informationen zur Entscheidungsfindung für nationale Instanzen liefern. Sie haben aber auch die Aufgabe, eine Informationsbasis aufzubereiten, die hilft, problematische Personen und Institutionen zu identifizieren sowie ihre Aktivitäten zu verhindern und zu bestrafen.

4.2 Gesetzliche Befugnisse

Für diese Aufgaben können die Sicherheitsbehörden und Nachrichtendienste auf alle notwendigen Befugnisse zurückgreifen. Sie können zum Beispiel technische Ermittlungsmaßnahmen anwenden und ihre Identität verschleiern. Sie können Nachforschungen bei allen relevanten Institutionen, Organisationen und Personen anstellen, alle Orte betreten und alle relevanten Akten, Materialien oder Gegenstände lesen und sammeln. Sie können auch Kommunikationsausrüstungen, Transportmittel, Gebäude und andere Einrichtungen beschlagnahmen. Das CTL ermächtigt, Anti-Terror-Operationen auch im Ausland durchzuführen.

Das CryptL regelt den Einsatz von Verschlüsselungstechnologien und -produkten in China und gibt der chinesischen State Cryptography Administration (SCA) Zugriff auf alle verschlüsselten Daten. Artikel 18 CTL bestimmt, dass Internet-Service-Provider den Anti-Terror-Behörden technische Schnittstellen, Entschlüsselung und andere technische Hilfe und Unterstützung anbieten müssen.

Sowohl das CSL als auch das PIPL und das DSL regeln, wann Datenübertragungen aus China in Drittländer erfolgen dürfen und welche Anforderungen an die Datenlokalisierung gelten. Generell ist es in China nicht verboten, Daten außerhalb des Staatsgebiets zu übertragen. Eine Datenlokalisierung gilt jedoch für die Betreiber von Kritischen Infrastrukturen. Sie müssen persönliche Informationen und wichtige Daten in China speichern. Dagegen sind Netzwerkbetreiber nur verpflichtet, eine Sicherheitsbewertung durchführen, wenn sie personenbezogene Daten außerhalb Chinas übertragen. Wenn die Datenübertragung die nationale Sicherheit oder das öffentliche Interesse beeinträchtigen könnte, sollen die Netzwerkbetreiber allerdings die Übertragung unterlassen. Dies gilt ebenso, wenn die Datensicherheit während der Datenübertragung gefährdet ist. Vorgaben zur Datenlokalisierung in China gibt es in vielen bereichsspezifischen Regelungen wie zum Beispiel für Staatsgeheimnisse, für medizinische Daten, für Finanzdaten und Daten von Kreditauskunfteien. Auch für Daten von Online-Taxi-Plattformen, von Fahrrad-Verleihern und von Internet-Kartenanbietern gibt es besondere Regelungen.

4.3 Indienstnahme von Unternehmen und Staatsangehörigen

Fast alle Sicherheitsgesetze begründen rechtliche Pflichten für chinesische Staatsangehörige, Unternehmen und Organisationen, in einigen Fällen auch für ausländische Akteure, die in China tätig sind, nachrichtendienstliche Aktivitäten zu unterstützen. Dabei müssen sie „alle Geheimnisse der staatlichen Geheimdienstarbeit, von denen sie Kenntnis haben“, wahren. Diese Klauseln legen nicht fest, dass nur chinesische „Organisationen“ diesen Anforderungen unterliegen. Daher ist davon auszugehen, dass das NIL für alle Organisationen in China gilt, unabhängig von den Eigentumsverhältnissen. Das Gesetz gilt weltweit für alle chinesischen Konzerne und ihre Tochtergesellschaften und auch für sich im Ausland befindliche Staatsangehörige.

5 Schlussfolgerungen für die Bedrohung der Cybersicherheit

Für die Cybersicherheit in Deutschland ergeben sich allein schon aus der Analyse der gesetzlichen Regelungen in den drei untersuchten Staaten wichtige Schlussfolgerungen:

In allen drei Staaten sind einheimische Unternehmen und Staatsangehörige verpflichtet, mit den Nachrichtendiensten weltweit zusammenzuarbeiten. Die Nachrichtendienste können außerdem eigene (Tarn-)Unternehmen gründen oder eigene Mitarbeitende in bestehende Unternehmen einschleusen. Diese Pflichten können auch für ausländische Töchter deutscher Organisationen gelten, die in den untersuchten Staaten tätig sind. Mit dieser Indienstnahme erweitern die Nachrichtendienste ihre Reichweite und ihre Aktionsmöglichkeiten erheblich. Sie wirken in Deutschland oder in der Kommunikation mit deutschen Stellen als „Trojanische Pferde“. Ihnen ist ihre Funktion für die nachrich-

tendienstliche Tätigkeit nicht anzusehen. Gerade dadurch können sie in besonderer Weise zu nachrichtendienstlichen Erfolgen beitragen.

In Russland und China beherrschen die Nachrichtendienste den nationalen Kommunikationsraum beinahe vollständig. In beiden Staaten müssen Daten im eigenen Land gespeichert werden, um jederzeit auf sie zugreifen zu können. Dort können die Nachrichtendienste den Kommunikationsraum jederzeit weitgehend abschotten und die Kommunikation mit anderen Staaten unterbinden – mit starken Auswirkungen zum Beispiel auf erforderliche Datenübertragungen (etwa beim Cloud-Computing). In den USA können die Nachrichtendienste von allen Providern Unterstützung einfordern.

Schließlich haben die Nachrichtendienste in den drei untersuchten Staaten potenziell Zugriff auf alle dort gespeicherten Daten. Dies gilt auch für alle die Daten, die Organisationen aus diesen Staaten und ihren Tochterorganisationen anvertraut werden – insbesondere, wenn diese eine gewisse Bedeutung für nachrichtendienstliche Zwecke haben, wie zum Beispiel Wirtschafts-, Finanz-, Forschungs- und Gesundheitsdaten.

6 Empfohlene Cybersicherheitsmaßnahmen

Zur Stärkung der Cybersicherheit Deutschlands und Europas sind die üblichen Sicherheitsmaßnahmen zum Erkennen von Angriffen und zu deren Abwehr durch ausländische Nachrichtendienste sowie zur Begrenzung von möglichen Schäden zu ergreifen. Außerdem ist zu versuchen, durch internationale Abkommen Cybersicherheit zu gewährleisten und massenhafte Ausspähung zu verhindern. Zudem gilt es, auf diplomatischem Weg bilateral mit den untersuchten Staaten Verbesserungen der gegenseitigen Sicherheit zu erreichen. Darüber hinaus sei auf folgende Aspekte hingewiesen.

Gegenüber den Handlungsmöglichkeiten von US-Nachrichtendiensten erlangen vor dem dargestellten Hintergrund die Bemühungen in Deutschland und der Europäischen Union um digitale Souveränität besondere Bedeutung. Für dieses Thema hat sich Deutschland zum Beispiel in seiner Präsidentschaft im Rat der Europäischen Union im Jahr 2020 besonders stark gemacht. In gewisser Weise muss die digitale Souveränität auch mit Blick auf chinesische Nachrichtendienste zentrale Bestrebung sein. Digitale Souveränität ist nicht nur eine Frage der Wettbewerbsfähigkeit, der politischen Selbstbestimmung, der Innovationskraft und der Sicherung der Rechtsstaatlichkeit, sondern sie ist auch zentral zur Gewährleistung von Cybersicherheit. Vorschläge für Maßnahmen hierzu unterbreitete die Wissenschaftliche Arbeitsgruppe Nationaler Cybersicherheitsrat bereits in ihrem Impulspapier „Technologische Souveränität: Voraussetzung für die Cybersicherheit“ vom Dezember 2019. Diese umfassten unter anderem

- die Bereitstellung sicherer Dateninfrastrukturen und die Zertifizierung kritischer Netzkomponenten,
- die Entwicklung sicherer Hardwarealternativen, basierend auf Open-Source-Hardware,
- die Zertifizierung von KI-Systemen,
- eine gezielte Industriepolitik für sichere Infrastrukturen und alternative Produkte und Dienste,
- eine transferorientierte Förderung von Forschungs- und Entwicklungsanstrengungen,
- die Stärkung der Fachkräfteausbildung und
- geeignete rechtliche Rahmenbedingungen.

Die Notwendigkeit, digitale Souveränität zu erlangen, hat auch das Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 (C-311/18 – Schrems II) zur Unionsrechtswidrigkeit des Abkommens der Europäischen Union mit den USA „Privacy Shield“ betont. Dieses verbietet die Übertragung personenbezogener Daten in alle Drittstaaten, wenn nicht durch ausreichende Garantien ein Zugriff der Nachrichtendienste ausgeschlossen werden kann. Da dies durch bilaterale Absprachen mit den Datenempfängern nicht möglich erscheint, kann dem Gebot nur dadurch entsprochen werden, dass

- die Datenverarbeitung in der Europäischen Union erfolgt,
- die Daten technisch-organisatorisch vor dem Zugriff von Nachrichtendiensten geschützt sind (zum Beispiel durch Verschlüsselung und Treuhänder) oder
- keine Datenverarbeitung durch Unternehmen erfolgt, die den jeweiligen Nachrichtendiensten verpflichtet sind.

Dies ist realistisch nur dann möglich, wenn die technologische Abhängigkeit von solchen Unternehmen reduziert wird und Alternativen aus der Europäischen Union unterstützt werden. Als ein Beispiel hierfür kann die Initiative Gaia-X zur Vereinbarung von Standards dezentraler Cloud-Angebote gesehen werden, die sich an europäischen Werten orientieren. Darüber hinaus sollten die öffentlichen Stellen im Bund und in den Ländern mit guten Beispielen vorangehen (zum Beispiel Vergabeverfahren, eigene IT-Nutzung, Auftragsverarbeitungen) und ihre IT-Nutzung schrittweise auf diese Alternativen umstellen.

Unternehmen in der Europäischen Union sind gegenüber Direktiven aus dem Ausland zur Übermittlung von personenbezogenen Daten durch Art. 48 DSGVO geschützt.

Dieser Schutz schließt jedoch nicht aus, dass ausländische Unternehmen in der Europäischen Union, die einer solchen Direktive nicht folgen, in ihrem Heimatstaat sanktioniert werden.

Die Europäische Kommission wird von Art. 50 DSGVO und Art. 40 JI-RL (2016/680) aufgefordert, internationale Maßnahmen zum Schutz personenbezogener Daten in Drittländern zu vereinbaren. Die beiden zentralen Kritikpunkte des Europäischen Gerichtshofs an der Rechtslage in den USA sind jedoch die unbestimmten und unverhältnismäßigen Zugriffsrechte der Nachrichtendienste auf alle erreichbaren Daten und der Ausschluss eines adäquaten Rechtswegs von US-Ausländern (EuGH C-311/18 Rn. 165 ff.). Solange diese Rechtslage bestehen bleibt, wird auch ein dritter Versuch der Europäischen Kommission zu einem Datenschutzabkommen mit den USA (nach Safe Harbor und Privacy Shield) scheitern. Das Gleiche gilt auch für alle anderen Staaten, in denen die Datenschutzregelungen deutlich unter dem Niveau der Europäischen Union liegen.

Gegenüber russischen Nachrichtendiensten ist weniger die digitale Abhängigkeit ein Problem, sondern die Probleme liegen vielmehr in der Beeinflussung der demokratischen Willensbildung durch Desinformation. Dies gilt mit Abstrichen auch gegenüber chinesischen Nachrichtendiensten. Vorschläge für Maßnahmen hiergegen unterbreitete die Wissenschaftliche Arbeitsgruppe Nationaler Cybersicherheitsrat bereits in ihrem Impulspapier „Gefährdung demokratischer Willensbildung durch Desinformation“ vom Dezember 2019. Diese umfassten neben dem verbesserten Netzwerkdurchsetzungsgesetz unter anderem

- technische und organisatorische Maßnahmen zum Erkennen von Trollen, Social Bots und Microtargeting sowie zum Unterbinden rechtswidriger Aktionen,
- Kennzeichnungspflichten für den Einsatz von Social Bots und Microtargeting,
- weitere Forschungen, wie technisch – auch mit Künstlicher Intelligenz – Desinformationen, Manipulationen, Deep Fakes, Trolle und Malicious Social Bots und ihre Verbreitungswege erkannt, gekennzeichnet, gesperrt und gelöscht werden können,
- eine Pflicht der Betreiber von Social Networks – anonymisierte oder pseudonymisierte – Kommunikationsdaten aus ihren Netzwerken der Forschung zur Verfügung zu stellen,
- die Steigerung von Medienkompetenz, zu der auch die Sensibilisierung gegenüber Desinformation und eine Vermittlung der Charakteristik journalistischer Qualitätsstandards gehören,
- Hinweise für Bürgerinnen und Bürger, wie Desinformationen erkannt werden können und wie mit Desinformationen umzugehen ist (nicht weiterverbreiten, Freunde warnen, dem Betreiber des Social Networks melden, Anzeige erstatten).

Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat

Seit Oktober 2018 unterstützt die Wissenschaftliche Arbeitsgruppe den Nationalen Cyber-Sicherheitsrat. Sie berät aus Perspektive der Forschung zu Entwicklungen und Herausforderungen im Hinblick auf eine sichere, vertrauenswürdige und nachhaltige Digitalisierung.

Mitglieder der Wissenschaftlichen Arbeitsgruppe sind: Prof. Dr. Gabi Dreo Rodosek, Prof. Dr. Claudia Eckert, Thomas Caspers, Prof. Dr. Jörn Müller-Quade, Prof. Dr.-Ing. Christof Paar, Prof. Dr. Alexander Roßnagel (Hauptautor dieses Impulspapiers), Prof. Dr. Michael Waidner