Bern, 15.12.2023

Digitale Infrastruktur. Geopolitische Risiken minimieren

Bericht des Bundesrates in Erfüllung des Postulates 20.3984 Pult vom 14.9.2020

Zusammenfassung

Das Postulat 20.3984 Pult beauftragt den Bundesrat, einen Bericht darüber vorzulegen, wie geopolitische Risiken im Zusammenhang mit digitalen Infrastrukturen wie 5G und Technologieanbietern wie dem chinesischen Konzern *Huawei* minimiert werden können.

Die Schweiz ist zweifellos geopolitisch geprägten technischen Risiken ausgesetzt, da viele unserer wirtschaftlichen, gesellschaftlichen oder politischen Prozesse über digitale Netzwerke und Systeme gesteuert werden, die Sicherheitslücken aufweisen oder Gegenstand von Cyberangriffen sein können. In einem zunehmend gespaltenen globalen geopolitischen Umfeld ist die Schweiz zudem mit potenziellen geopolitischen Risiken (z. B. Sperrung des Marktzugangs durch die EU) im Zusammenhang mit digitalen und Fernmeldeinfrastrukturen von Anbieterinnen konfrontiert, die als risikobehaftet gelten oder von einem Staat kontrolliert werden, der ein geopolitisches Risiko darstellt.

Um die Resilienz unserer Telekommunikation zu stärken, schlägt der Bundesrat neue Massnahmen vor, die eine Mehrlieferanten-Strategie, Beschränkungen für als risikobehaftet geltende Ausrüstungen sowie die nächste Frequenzausschreibung. Im Übrigen sollte das Schweizer Ökosystem für Cybersicherheit in der Lage sein, langfristig die nationalen Kontroll- und Zertifizierungsstellen bereitzustellen, die unser Land benötigt.

Nach Ansicht des Bundesrates ist es notwendig, nach dem Vorbild der 5G-Toolbox der EU und anderer Regulierungsvorhaben, insbesondere zur Cyberresilienz, im Fernmeldegesetz (FMG; SR *784.10*) eine neue Bestimmung vorzusehen, die ihm die Möglichkeit gibt, bei Eintreten eines geopolitischen Risikos die erforderlichen Massnahmen zu ergreifen. Unter anderem soll er die Beschaffung, die Einrichtung und den Betrieb von Ausrüstungen verbieten können, die von Lieferanten stammen, die als problematisch für die Sicherheit unseres Landes gelten oder die sich im Besitz, unter der Kontrolle oder dem Einfluss eines ausländischen Staates befinden, der ein geopolitisches Risiko für die Schweiz darstellt. In dieser Hinsicht müssen die Wirtschaftsfreiheit und das einwandfreie Funktionieren des Wettbewerbs bestmöglich sichergestellt werden.

Eine internationale Zusammenarbeit ist weiterhin unverzichtbar, um die Sicherheit digitaler Netze und Infrastrukturen angesichts ihrer weltweiten Vernetzung zu gewährleisten.

Inhaltsverzeichnis

Abkürzungen

3GPP	The 3rd Generation Partnership Project
5G	Mobilfunknetz oder -kommunikation der 5. Generation
BAKOM	Bundesamt für Kommunikation
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft
BWL	Bundesamt für wirtschaftliche Landesversorgung
CYD	Cyber-Defence
DDoS	Distributed Denial of Service (Verweigerung des Dienstes)
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EMPA	Interdisziplinäres Forschungsinstitut des ETH-Bereichs für Materialwissenschaften und Technologieentwicklung
ENISA	Agentur der Europäischen Union für Cybersicherheit (European Union Agency for Cybersecurity)
ETH	Eidgenössische Technische Hochschule Zürich
ETSI	Europäisches Institut für Telekommunikationsnormen (European Telecommunications Standards Institute)
EU	Europäische Union
FDV	Verordnung über Fernmeldedienste
FIRST	Forum of Incident Response and Security Teams
FMG	Fernmeldegesetz
GATS	Allgemeines Abkommen über den Handel mit Dienstleistungen (General Agreement on Trade in Services) (WTO)
GATT	Allgemeines Zoll- und Handelsabkommen (General Agreement on Tariffs and Trade) (WTO)
GSMA	The GSM Association
IKT	Informations- und Kommunikationstechnologien
ISG	Bundesgesetz über die Informationssicherheit beim Bund
ISMS	Managementsystem für Informationssicherheit
ITU	Internationale Fernmeldeunion
Kap.	Kapitel
NatCSIRT	National Computer Security Incident Response Team
NCS	Nationale Cyberstrategie
NCSC	Nationales Zentrum für Cybersicherheit
NDB	Nachrichtendienst des Bundes
NESAS	Network Equipment Security Assurance Scheme
NOC	Network Operation Center (Netzwerkbetriebszentrum)
NTC	Nationales Testinstitut für Cybersicherheit
O-RAN	Open Radio Access Network
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
RAN	Radio Access Network (Funkzugangsnetz)
SCION	Scalability, Control, and Isolation on Next-Generation Networks
SOC	Security Operation Center (Sicherheitsbetriebszentrum)
SSFN	Secure Swiss Finance Network
TBT	Übereinkommen über technische Handelshemmnisse (Technical Barriers to Trade Agreement) (WTO)
TF-CSIRT	Task Force Computer Security Incident Response Team
UNO	Vereinte Nationen
VFAV	Verordnung des BAKOM über Fernmeldeanlagen
WTO	Welthandelsorganisation

1 Postulat 20.3984 Pult

Gemäss dem Postulat 20.3984 Pult vom 14. September 2020, das am 17. Juni 2021 vom Nationalrat angenommen wurde, wird der Bundesrat beauftragt, in einem Bericht zu analysieren, wie geopolitische Risiken beim Ausbau und der Weiterentwicklung von digitalen Infrastrukturen wie 5G minimiert werden können. Bei der Auswahl der Technologieanbieter sind die Aspekte Produktqualität, Zuverlässigkeit von Technologie-Lieferketten, Unternehmensstruktur der Anbieter und der Rechtsrahmen, welchem der Hauptsitz des Unternehmens unterliegt, zu berücksichtigen. Insbesondere ist auch zu klären, welche Risiken von Anbietern wie Huawei ausgehen, die in Ländern domiziliert sind, die weder marktwirtschaftlich noch rechtsstaatlich organisiert sind. Letztlich ist die Frage zu beantworten, wie sichergestellt werden kann, dass die Schweizer Technologieinfrastruktur nicht durch den auf absehbarer Zeit stattfindenden geoökonomischen Wettbewerb zwischen den USA und China beeinträchtigt wird.

Das Postulat ist einer von mehreren parlamentarischen Vorstössen, die Fragen zu den geopolitischen Risiken thematisieren, denen die Schweiz in Bezug auf Lieferketten und Infrastrukturen ausgesetzt ist. Ein Bericht des Bundesrates vom 24. November 2021 über die Produktesicherheit und das Supply Chain Risk Management in den Bereichen Cybersicherheit und Cyberdefence beantwortet die Postulate 19.3135 und 19.3136 Dobler. Der Bundesrat hat zudem am 31. August 2022 einen Bericht zur Motion 20.3268 Häberli-Koller zur Rolle der globalen Wertschöpfungsketten für die Versorgungssicherheit der Schweiz mit essenziellen Gütern veröffentlicht.

Die Motion 22.3414 «Schutz der kritischen Infrastruktur vor Einflussnahme anderer Staaten» der sozialdemokratischen Fraktion wurde am 2. Mai 2023 vom Nationalrat angenommen und am 3. Juli 2023 von der Sicherheitspolitischen Kommission des Ständerates bis zum Erscheinen des vorliegenden Berichts zur Erfüllung des Postulates 20.3984 Pult sistiert. Schliesslich wird der Bundesrat bis Ende 2024 in Beantwortung des Postulates 22.4411 Z'graggen «Strategie Digitale Souveränität der Schweiz» einen Bericht verabschieden. Darin wird er eine Definition des Begriffs «digitale Souveränität» vornehmen, den digitalen Souveränitätsgrad der Schweiz beurteilen und notwendige Massnahmen vorschlagen.

2 Die Fernmeldeinfrastruktur der Schweiz

2.1 Stand der Dinge bei 5G

Die Mobilfunkbetreiberinnen *Salt*, *Sunrise* und *Swisscom* unterhalten in der Schweiz Mobilfunknetze der 5. Generation (5G), um Fernmeldedienste anzubieten. Die Gerätehersteller, die sie mit 5G-Hardware beliefern, sind zahlreich und stammen aus verschiedenen Ländern: *Ericsson* (SE), *Nokia* (FIN) *Huawei* (CN), *Microsoft (eSPIN & Services)* (UK), *A10 Networks* (USA), *Cisco* (USA), *Juniper* (USA), *Commscope* (USA) und *Ceragon* (ISR).

Das Kernnetz (Core Network) ist ein wesentlicher Bestandteil eines 5G-Netzes. Es umfasst die folgenden Hauptfunktionen: Verwaltung der Zugänge und ihrer Sicherheit, Authentifizierung der Nutzerinnen und Nutzer, Weiterleitung von Anrufen und Daten, Verwaltung der Teilnehmerdienste, Kontrolle der Datenströme und ihrer Priori-

sierung, Verwaltung der Interoperabilität mit anderen Netzen, Steuerung der Verbindungsübergabe (handover) zwischen Funkzellen, um die Verbindung während eines Gesprächs oder einer Datenverbindung ohne Unterbrechung aufrechtzuerhalten, sowie Verwaltung der Dienstqualität und der Rechnungsstellung. Eine der Betreiberinnen verfolgt im Hinblick auf das Kernnetz eine Mehrlieferanten-Strategie. Die beiden anderen verwenden ausschliesslich Geräte eines einzigen Lieferanten, entweder zu 100 Prozent von *Huawei* oder zu 100 Prozent von *Nokia*.

Das Funkzugangsnetz (Radio Access Network, RAN) eines Mobilfunknetzes verbindet die Geräte der Endnutzerinnen und -nutzer, z. B. ihre Smartphones, mit der Cloud. Es überträgt die Informationen per Funkwellen zunächst von den Geräten der Endnutzerinnen und -nutzer zu den RAN-Transceivern und dann von diesen zum Kernnetz, das wiederum mit dem Internet oder anderen Betreiberinnen verbunden ist. RAN-Netze führen komplexe Aufgaben bei der Verarbeitung von Verbindungen aus und ihre Entwicklung stützt sich zunehmend auf eine Virtualisierung ihrer Funktionen. Was die in der Schweiz verwendeten RAN-Netze betrifft, so nutzt eine Betreiberin zu 100 Prozent Geräte von *Huawei*, die zweite zu 80 Prozent von *Huawei* und zu 20 Prozent von *Nokia* und die dritte zu fast 100 Prozent von *Ericsson*.[1]

Der Begriff «Backhaul» bezeichnet in Mobilfunknetzen das Übertragungsnetz und die Verbindungen zwischen dem Kernnetz und den Funkzellen des RAN. Backhaul-Netze können auf Glasfaser-, Kupfer- oder Richtfunkverbindungen basieren. Das Übertragungsnetz besteht bei einer Betreiberin aus Ausrüstungen von US-Lieferanten und *Ericsson*, bei der zweiten von *Huawei*, *Ericsson* und *Nokia* und bei der dritten nur von *Huawei*.

Bei den Schnittstellen zu anderen Betreiberinnen oder Diensten (z. B. Zusammenschaltung mit einer anderen Betreiberin, Wartungsarbeiten, Rechnungsstellung, Internetzugang) verwendet eine Betreiberin Ausrüstungen von *Cisco* und *Ericsson*, die zweite von *Cisco* und *Huawei* und die dritte nur von *Huawei*.

Eine Gesamtanalyse der in den 5G-Netzen in der Schweiz verwendeten Ausrüstungen lässt den Schluss zu, dass nur eine der drei Schweizer Mobilfunkbetreiberinnen bei ihren Lieferungen stark vom chinesischen Gerätehersteller *Huawei* abhängig ist. Angesichts dessen, dass auch eine der beiden anderen Betreiberinnen teilweise auf *Huawei*-Ausrüstung zurückgreift, ist an dieser Stelle darauf hinzuweisen, dass jedes Element der 5G-Infrastruktur Zugang zu einem grossen Teil der Gesamtinfrastruktur hat, was in früheren Mobilfunkgenerationen, bei denen die periphere und die zentrale Infrastruktur getrennt waren, nicht der Fall war. Das bedeutet, dass jede Schwachstelle oder Hintertür in einer 5G-Ausrüstung potenziell das gesamte 5G-Netz gefährden kann (vgl. Kap. 2.2).

Die Netzwerkbetriebszentren der Betreiberinnen sind zentrale Infrastrukturen, die für die Fernmeldenetze von grundlegender Bedeutung sind und deren geografischer

[1] Die Open RAN Alliance (O-RAN Alliance) hat zum Ziel, die zukünftige Interoperabilität der verschiedenen Komponenten eines Funkzugangsnetzes zu verbessern. Durch die Standardisierung der Schnittstellen soll der Open-RAN-Standard ermöglichen, dass in einem Mobilfunknetz Hard- und Softwarekomponenten verschiedener Hersteller ohne Anpassungen genutzt werden können.

Standort zur Sicherung der 5G-Netze beiträgt (vgl. Kap. 4.1). Ein Netzwerkbetriebszentrum (Network Operation Center, NOC) überwacht und verwaltet die Leistung und die Verfügbarkeit eines Fernmeldenetzes, während ein Sicherheitsbetriebszentrum (Security Operation Center, SOC) Sicherheitswarnungen und Cybervorfälle sammelt, analysiert und darauf reagiert. Letzteres nutzt fortschrittliche Tools zur Erkennung von Bedrohungen und zum Management von Sicherheitsereignissen, die verdächtige Aktivitäten, Schwachstellen und Versuche, in das System einzudringen oder es anzugreifen, identifizieren.

2.2 Geopolitisch geprägte technische Risiken

Die Digitalisierung hat zur Folge, dass immer mehr für einen Staat sensible wirtschaftliche, gesellschaftliche oder politische Prozesse über digitale Netzwerke und Systeme gesteuert werden, die das Ziel von Cyberangriffen sein können. Solche Angriffe werden professionell von staatlichen, halbstaatlichen oder nichtstaatlichen Akteuren durchgeführt, die Schwachstellen und Sicherheitslücken in Computer- und Telekommunikationssystemen ausnutzen oder Schadsoftware (Trojaner, Spyware und andere «Malware») oder vorinstallierte Hintertüren («Backdoors») einsetzen, um infizierte Systeme zu kontrollieren oder ihre Funktion zu stören.

Cyberangriffe stellen geopolitische Risiken dar, die für ein Land wie die Schweiz weitreichende Folgen haben können. Dabei bieten insbesondere die zunehmende Vernetzung und Komplexität digitaler Infrastrukturen und Systeme den Urhebern von Cyberangriffen Möglichkeiten, sich in die Funktionsweise unserer sensiblen oder kritischen Infrastrukturen einzuhacken und diese zu sabotieren. Konkret kann dies insbesondere die Energienetze, die Finanzdienstleistungen oder auch die Wasserversorgungsnetze betreffen, was sowohl wirtschaftliche als auch politische Auswirkungen auf den Staat, die Unternehmen und die Bevölkerung hat. Überdies werden weltweit beträchtliche Cybermittel zu Spionagezwecken eingesetzt. Auch die Schweiz ist davon betroffen, da sie aufgrund ihrer wirtschaftlichen und wissenschaftlichen Leistungen, der Präsenz zahlreicher internationaler Organisationen auf ihrem Territorium sowie ihrer Rolle bei der Durchführung internationaler Konferenzen ein interessanter Standort für ausländische Nachrichtendienste ist.[2]

Die Schweiz hat bereits Cyberangriffe auf ihre digitale Infrastruktur erlebt, von denen einige von ausländischen Staaten durchgeführt worden sein dürften, auch wenn die Urheberschaft nicht abschliessend geklärt werden konnte. Dazu zählen Angriffe auf das Technologieunternehmen RUAG (2014–2016), das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) (2017), das Labor Spiez für den Schutz der Bevölkerung vor atomaren, biologischen und chemischen Bedrohungen und Gefahren (2018), die Vereinten Nationen (UNO) in Genf (2020) und zuletzt auf das Unternehmensnetzwerk der SBB, die Universität Zürich und die Bundesverwaltung über die Schweizer Firma *Xplain* (2023). Ein breit angelegter Distributed-Denial-of-Service-Angriff (DDoS-Angriff) der pro-russischen Gruppierung *NoName* als Reaktion auf die Rede des ukrainischen Präsidenten vor den eidgenössischen Räten betraf im

[2] Bericht des Bundesrates vom 12. Mai 2023 an die eidgenössischen Räte und die Öffentlichkeit: Jährliche Beurteilung der Bedrohungslage, S. 8

Juni 2023 zudem die Websites des Parlaments, der Bundesverwaltung, der Post, des Flughafens Genf, der Armee sowie von Schweizer Kantonen und Städten.

Analog zum US-amerikanischen *Cloud Act* verpflichtet ein chinesisches Gesetz aus dem Jahr 2017 chinesische Unternehmen, mit den Geheimdiensten ihres Landes zusammenzuarbeiten und ihnen Zugang zu den von ihnen gesammelten Daten zu geben, wobei dies auch für ihre Tätigkeiten im Ausland gilt. Das Unternehmen *Huawei*, das 1987 von einem ehemaligen hochrangigen Vertreter des chinesischen Militärs gegründet und vom Staat finanziell stark unterstützt wurde, wird von den USA beschuldigt, für die chinesischen Behörden zu spionieren. Zwar wurden bis anhin keine Beweise für Spionagetätigkeiten oder den Einbau von Hintertüren in die 5G-Infrastruktur durch *Huawei* öffentlich bekannt, aber gewisse Angriffe oder Hintertüren lassen sich nur schwer oder gar nicht erkennen. Zudem ist es für einen Gerätelieferanten durchaus möglich, später gezielt veränderte Software-Updates zu installieren.[3]

2.3 Rein geopolitische Risiken

Die aktuellen Krisen (u. a. Covid-19-Pandemie, Krieg in der Ukraine, Klimawandel, Energiekrise, wirtschaftliche Unsicherheiten und Spannungen um Taiwan) machen zunehmende geopolitische Spaltungen auf globaler Ebene deutlich.[4] Diese Spaltungen wirken sich auf die technologische Entwicklung und Innovation aus und könnten die Verfügbarkeit von Hightech-Gütern einschränken. Die wachsenden Spannungen zwischen China und den USA im Bereich der nationalen Sicherheit und der Technologie könnten unter anderem zu Unterbrechungen in den Lieferketten strategischer Güter wie der Telekommunikationsausrüstung führen, die Vernetzung der Märkte gefährden oder sogar deren Entkopplung zur Folge haben. Da sich der internationale Wettbewerb um Einfluss im digitalen Raum stark verschärft hat, sind die Risiken einer direkten Einflussnahme von Staaten auf die Lieferanten gestiegen.[5]

Die Spaltung gegenüber dem Westen konkretisiert sich im erklärten Willen von Ländern wie China, Russland und einer wachsenden Zahl von Ländern des globalen Südens, stärkeren Einfluss auf eine nach ihrer Auffassung zu «westliche» Weltordnung zu nehmen, was die Schweiz in Bezug auf ihre politische und wirtschaftliche Positionierung vor eine Herausforderung stellt. Diese Herausforderung der Positionierung kann diejenigen Faktoren gefährden, die den Erfolg unseres Landes begründen, nämlich seine auf dem freien Handel basierende Offenheit gegenüber der Welt und seine Innovationsfähigkeit, die vom Zugang seiner Unternehmen zu allen weltweit führenden technologischen Produkten und Dienstleistungen abhängig ist. Der pragmatische

[3] Es ist darauf hinzuweisen, dass *Huawei* anerkannte Sicherheitsstandards wie das Network Equipment Security Assurance Scheme (NESAS) umsetzt, sich an den Arbeiten bezüglich Sicherheit der GSM Association (GSMA) beteiligt und allen Kundinnen und Kunden die Möglichkeit bietet, den Quellcode der Programme, des Betriebssystems oder der Anwendungen in seinen Netzwerkkomponenten einzusehen.

[4] Zum Trend in Richtung einer zunehmend bipolar geprägten Welt vgl. Nachrichtendienst des Bundes NDB, Sicherheit Schweiz 2023 vom 26. Juni 2023, S. 27 ff.

[5] Bericht des Bundesrates in Erfüllung der Postulate Dobler 19.3135 «Haben wir die Cybersicherheit bei Beschaffungen der Armee im Griff?» und 19.3136 «Haben wir die Hard- und Softwarekomponenten bei unseren kritischen Infrastrukturen im Griff?» vom 24. November 2021, S. 8

aussenpolitische Ansatz der Schweiz sollte dabei helfen, diese Spannungen zu bewältigen und einen allgemeinen und nicht-diskriminierenden Ansatz betreffend Sicherheitsrisiken im Zusammenhang mit digitalen Infrastrukturen zu bewahren.

Falls erforderlich muss die Schweiz aber bereit sein, sich angesichts ihres auf Freiheit und Rechtsstaatlichkeit basierenden Wertesystems stärker international zu integrieren und Teil des Innovationssystems der westlichen Hemisphäre zu bleiben. Es muss verhindert werden, dass unser Land als Sicherheitslücke mitten in Europa betrachtet wird[6], dass es im Falle einer Nutzung bestimmter Netzinfrastrukturen aus China wirtschaftlich diskriminiert wird oder dass China unsere potenzielle Abhängigkeit von seiner digitalen Infrastruktur nutzen kann, um politischen Druck auf die Schweiz auszuüben. Letztlich ist nicht auszuschliessen, dass die Schweiz in bestimmten Fällen gezwungen sein wird, sich zwischen der Unterstützung der USA und der Beibehaltung einer unabhängigen Position zu entscheiden.[7]

3 Die aktuelle gesetzliche und politische Regelung

3.1 Internationale Verpflichtungen

Das Allgemeine Abkommen über den Handel mit Dienstleistungen (GATS)[8] regelt den internationalen Handel mit Dienstleistungen, einschliesslich Fernmeldediensten. Das GATS wird durch die verbindlichen Regelungen im Anhang über Telekommunikation und das Vierte Protokoll betreffend den Anhang zu Verhandlungen über Basis-Telekommunikationsdienstleistungen ergänzt, das die spezifischen Verpflichtungen der einzelnen Mitgliedstaaten umfasst (vgl. Art. XVI und XXIX GATS). Abgesehen davon, dass die Schweiz auf der Grundlage dieser verschiedenen Abkommen zur Liberalisierung ihres Fernmeldemarktes verpflichtet ist, muss sie auch Dienstleistungsanbietern und für Dienstleistungen aller Mitgliedstaaten der Welthandelsorganisation (WTO) eine diskriminierungsfreie Behandlung garantieren (Meistbegünstigungsklausel).

Das Allgemeine Zoll- und Handelsabkommen (GATT)[9] liberalisiert den Warenhandel auf der Grundlage der Listen der Zugeständnisse jedes Mitgliedstaates und gilt gegebenenfalls für Fernmeldeanlagen und andere Geräte aus diesem Bereich. Das GATT wird durch das Übereinkommen über technische Handelshemmnisse (TBT-Übereinkommen)[10] ergänzt, das einen multilateralen Rahmen festlegt, um insbesondere dafür zu sorgen, dass technische Vorschriften, Normen und Konformitätsbewertungen

---

[6] In seinem Bericht vom 9. Juni 2023 zu den Beziehungen zwischen der Schweiz und der EU betont der Bundesrat, dass die EU den wachsenden technologischen Einfluss Chinas mit Besorgnis beobachtet (S. 11). Um künftige Abhängigkeiten zu verhindern oder zu verringern, sollen Entwicklungs- und Produktionskapazitäten im EU-Binnenmarkt gefördert werden (technologische Souveränität). Dies wird auch Auswirkungen auf die Unternehmen und die Konsumentinnen und Konsumenten in der Schweiz haben.

[7] Bundeskanzlei, Schweiz 2035 – Think Tanks beantworten 20 Zukunftsfragen – Lage- und Umfeldanalyse 2022, S. 69 und 72

[8] Das GATS (General Agreement on Trade in Services) ist Teil des Abkommens vom 15. April 1994 zur Errichtung der Welthandelsorganisation (Anhang 1.B; SR **0.632.20**).

[9] Das GATT (General Agreement on Tariffs and Trade) ist Teil des Abkommens vom 15. April 1994 zur Errichtung der Welthandelsorganisation (Anhang 1.B; SR **0.632.20**).

[10] Das TBT-Übereinkommen (Technical Barriers to Trade Agreement) ist Teil des Abkommens vom 15. April 1994 zur Errichtung der Welthandelsorganisation (Anhang 1A.6; SR **0.632.20**).

nicht-diskriminierend sind und nicht zu unnötigen Handelshemmnissen führen. Das TBT-Übereinkommen anerkennt das Recht, technische Vorschriften zu erlassen, um dadurch ein angemessenes Schutzniveau für legitime Ziele wie die nationale Sicherheit festzulegen, wobei die Grundsätze der Nichtdiskriminierung, der Verhältnismässigkeit und der Transparenz zu beachten sind.

Beschränkungen zum oder ein Ausschluss vom Zugang zum Schweizer Markt für Gerätehersteller, die als problematisch für die Sicherheit unseres Landes gelten oder die sich im Besitz, unter der Kontrolle oder dem Einfluss eines ausländischen Staates befinden, der ein Sicherheitsrisiko darstellt, können die GATS-, GATT- und TBT-Verpflichtungen der Schweiz verletzen. Das GATS und das GATT enthalten Ausnahmeklauseln, die es erlauben, unter bestimmten Bedingungen Massnahmen zur Wahrung der öffentlichen Ordnung (Art. XIV Bst. a GATS) oder der Sicherheit (Art. XIV Bst. c Ziff. iii und XIV *bis* GATS sowie Art. XXI GATT) zu rechtfertigen.[11] Diese Ausnahmen werden von den Vergabestellen der WTO streng ausgelegt. Das TBT-Übereinkommen ermöglicht es ausserdem, Erwägungen der nationalen Sicherheit (Art. 2 Abs. 10 und Art. 5 Abs. 4 und 7 TBT) Rechnung zu tragen. Zahlreiche westliche Länder und die EU haben bereits Sicherheitsmassnahmen gegen als problematisch geltende Gerätehersteller ergriffen (vgl. Kap. 3.6), wobei davon auszugehen ist, dass dabei die Bestimmungen des GATS, des GATT und des TBT-Übereinkommens, denen diese Länder ebenfalls angehören, eingehalten wurden.

Das Neutralitätsrecht legt die Rechte und Pflichten eines neutralen Staates im Falle eines internationalen bewaffneten Konflikts fest[12] und hat insofern keine Auswirkungen auf mögliche verbindliche Massnahmen der Schweiz in Bezug auf die Beschaffung und Entwicklung von digitalen und Fernmeldeinfrastrukturen wie 5G.

3.2 Fernmelderecht und Netzsicherheit

Das Fernmelderecht regelt das Angebot von Fernmeldediensten und -anlagen, indem es diese gemäss den internationalen Verpflichtungen, die die Schweiz im Rahmen der WTO (vgl. Kap. 3.1) eingegangen ist, dem Wettbewerb unterwirft. Dieses Recht gewährt dem Bund derzeit keinen Einfluss auf die Beschaffung von Netzausrüstungen durch die Betreiberinnen, die frei wählen können.

Gemäss dem Fernmeldegeheimnis (Art. 13 Abs. 2 BV und Art. 43 FMG) gewährleisten die Betreiberinnen die Vertraulichkeit und Integrität der Informationen, die ihnen von den Teilnehmerinnen und Teilnehmern zur fernmeldetechnischen Übertragung anvertraut werden. Dies verpflichtet die Betreiberinnen, ihre Infrastruktur gegen unbefugte Zugriffe und andere Cyberangriffe zu sichern. Die Ausgestaltung dieser Ver-

[11] Art. 5 Bst. e des Anhangs über Telekommunikation ergänzt diese Schutzmassnahmen, indem er vorsieht, dass der Zugang zu öffentlichen Telekommunikationsnetzen und -dienstleistungen und deren Nutzung Bedingungen unterliegen können, die zum Schutz der technischen Integrität dieser Netze und Dienstleistungen erforderlich sind.

[12] Die dauernde Neutralität ist ein Instrument der schweizerischen Aussenpolitik (Art. 173 Abs. 1 Bst. a und 185 Abs. 1 der Bundesverfassung der Schweizerischen Eidgenossenschaft [BV; SR **101**]). Das Neutralitätsrecht wurde in den Haager Abkommen vom 18. Oktober 1907 (SR **0.515.21** und.**0.515.22**) kodifiziert und ist Teil des Völkergewohnheitsrechts.

pflichtung ist im Fernmelderecht nicht festgelegt, wobei die Betreiberinnen die Massnahmen ergreifen müssen, die unter Berücksichtigung der Sicherheitsrisiken mit vertretbarem Aufwand technisch möglich sind.

Auf der Grundlage eines neuen Artikels 48*a* FMG, der 2021 verabschiedet wurde, konnte der Bundesrat in der Verordnung über Fernmeldedienste (FDV; SR *784.101.1*) bestimmte Massnahmen zur Erhöhung der Sicherheit von Fernmeldenetzen ergreifen. Das System zur Meldung von Störungen des Telekommunikationsbetriebs wurde konsolidiert und die Anbieterinnen von Internetzugängen müssen DDoS-Angriffe bekämpfen. Sie sind berechtigt, Internetzugänge oder Adressierungselemente, die das ordnungsgemässe Funktionieren von Fernmeldeanlagen zu beeinträchtigen drohen, zu sperren oder deren Nutzung einzuschränken, und müssen eine spezialisierte Stelle betreiben, die Meldungen über solche Manipulationen entgegennimmt.

Im Hinblick auf die Sicherheit der 5G-Netze sind die Betreiberinnen verpflichtet, ein Managementsystem für Informationssicherheit (ISMS) nach anerkannten Standards und den Anforderungen des Bundesamtes für Kommunikation (BAKOM) zu betreiben. Zudem müssen sie ihre Netzwerk- und Sicherheitsbetriebszentren (NOC und SOC) ausschliesslich in Staaten betreiben, deren Gesetzgebung ein angemessenes Datenschutzniveau gewährleistet, wobei die aktuellen Rechtsgrundlagen es aber nicht erlauben, den Betrieb ausschliesslich in der Schweiz vorzuschreiben.

Schliesslich müssen die Betreiberinnen von 5G-Netzen sicherstellen, dass die von ihnen betriebenen sicherheitskritischen Fernmeldeanlagen nach anerkannten Sicherheitsnormen zertifiziert sind. Das BAKOM kann die betroffenen Anlagen definieren, bei Bedarf in Zusammenarbeit mit der Branche. Diese Verpflichtung umfasst die Entwicklung eines Verfahrens zur Zertifizierung oder Konformitätsbewertung von kritischen Geräten in Mobilfunknetzen (vgl. Kap. 4.3). Diesbezüglich wäre es angesichts des Gewichts des europäischen Marktes und der Abkommen mit der EU über die gegenseitige Anerkennung im Bereich der Fernmeldeanlagen sinnvoll, die schweizerische Regelung derjenigen der EU anzugleichen. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) bereitet ein Zertifizierungsverfahren für die 5G-Cybersicherheit vor, das auf die Verabschiedung des Instrumentariums für 5G-Sicherheit (5G-Toolbox) folgt. Es wird zu prüfen sein, ob die Schweiz dieses Zertifizierungsverfahren, das auf anerkannten Standards beruhen soll, nutzen kann oder ob die Zusammenarbeit mit dieser Agentur nicht gar formalisiert werden sollte.

3.3 Resilienz der kritischen Infrastrukturen

Das Informationssicherheitsgesetz (ISG; SR *128*) soll die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten. Es sieht insbesondere eine Risikobeurteilung für Betriebe vor, die öffentliche Aufträge erfüllen, die empfindlich für die Sicherheit des Bundes sind.[13] Dieses Gesetz, das noch nicht in Kraft getreten ist, muss noch geändert werden, um die Resilienz der Schweiz gegenüber Cyberrisiken zu stärken.

[13] Mit dieser Beurteilung sollen Betriebe ausgeschlossen werden, die Aufträge mit hoher Wahrscheinlichkeit vorschriftswidrig oder unsachgemäss ausführen werden. Dies kann der Fall sein, wenn der Betrieb von ausländischen Staaten in einer Weise kontrolliert oder beeinflusst wird, die nicht mit dem Schutz der Interessen der Schweiz vereinbar ist (Art. 57 Abs. 2 Bst. b ISG).

Dabei geht es darum, die Aufgaben und Kompetenzen des künftigen neuen Bundesamtes für Cybersicherheit (BACS) gesetzlich zu verankern und eine Meldepflicht bei Cyberangriffen auf kritische Infrastrukturen einzuführen. Als kritische Infrastrukturen gelten dabei unter anderem Prozesse und Systeme, die essenziell für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung sind.

Das Bundesamt für wirtschaftliche Landesversorgung (BWL) hat einen Minimalstandard für den Schutz der Informations- und Kommunikationstechnologien (IKT) vor Cyberrisiken veröffentlicht, dessen Einhaltung das künftige ISG für kritische Infrastrukturen aber nicht vorschreibt. Die Bundesverwaltung nimmt dennoch Rücksicht auf diesen Minimalstandard, da sie dafür sorgen muss, dass ihre Organe und Systeme eine angemessene Resilienz gegenüber Cyberrisiken aufweisen (Art. 6 ISG). Zudem wird das BACS subsidiäre Unterstützung für Betreiberinnen von kritischen Infrastrukturen bieten müssen (Art. 74 ISG). Werden Computersysteme und Computernetzwerke, die sich im Ausland befinden, für Angriffe auf kritische Infrastrukturen in der Schweiz verwendet, so kann der Nachrichtendienst des Bundes (NDB) in diese Computersysteme und Computernetzwerke eindringen, um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen (Art. 37 Abs. 1 des Nachrichtendienstgesetzes [SR *121*]).

Der Entwurf des ISG und die neue Nationale Strategie zum Schutz kritischer Infrastrukturen, die der Bundesrat am 16. Juni 2023[14] gutgeheissen hat, konkretisieren die Nationale Cyberstrategie (NCS), indem sie Massnahmen vorschreiben, die die Resilienz kritischer digitaler Infrastrukturen stärken. Im Übrigen ist es Sache des Bundesrates, zu prüfen, in welchen Bereichen zusätzlicher Regelungsbedarf besteht, und dem Parlament bei Bedarf und Zuständigkeit des Bundes Modelle für verbindliche Vorgaben in Bezug auf die Anwendung von Standards bei kritischen Infrastrukturen vorzuschlagen.

Das SCION-Protokoll (Scalability, Control, and Isolation on Next-Generation Networks), das von der Eidgenössischen Technischen Hochschule (ETH) Zürich entwickelt wurde, ist ein hervorragendes Beispiel dafür, wie kritische Infrastrukturen gesichert werden können. Es ermöglicht die Schaffung einer neuen Internetarchitektur, die die Eigenschaften von geschlossenen und privaten Netzwerken in der Infrastruktur des öffentlichen Internets anbietet. SCION erhöht die Sicherheit des Internets, indem es den Absenderinnen und Absendern die Möglichkeit bietet, selbst zu entscheiden, welche Wege ihre Daten nehmen, und so die Kontrolle über den Informationsfluss auszuüben. Die Schweizerische Nationalbank (SNB) nutzt SCION seit Juni 2022 für das Secure Swiss Finance Network (SSFN) und arbeitet dabei eng mit dem Schweizer Börsenbetreiber SIX Group, den Betreiberinnen Swisscom und Sunrise sowie der Stiftung SWITCH zusammen, die die Internet-Domain «.ch» verwaltet.

3.4 Sicherung von Fernmeldeanlagen und anderen IKT-Produkten

Die Eindämmung von Cyberrisiken erfordert die Sicherung von Fernmeldeanlagen und -ausrüstungen sowie anderer IKT-Produkte, die nach wie vor zahlreiche Sicher-

[14] BBl **2023** 1659

heitslücken in Bezug auf Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit von Daten aufweisen. Dabei tragen die Annahme und Anwendung von Sicherheitsstandards für solche Anlagen, Ausrüstungen und Produkte und deren Zertifizierung oder Konformitätsbewertung durch anerkannte Stellen dazu bei, ihre Sicherheit und ihre reibungslose Integration in die digitale Infrastruktur zu verbessern.

Die Bestimmungen, die 2022 in die Verordnung des BAKOM über Fernmeldeanlagen (VFAV; SR *784.101.21*) aufgenommen wurden, erhöhen die Cybersicherheit bestimmter drahtloser Geräte (Smartphones, Smartwatches, Fitness-Tracker und drahtlose Spielzeuge), die auf dem Schweizer Markt erhältlich sind. Solche vernetzten Geräte müssen Funktionen aufweisen, die eine Beeinträchtigung der Kommunikationsnetze verhindern, damit deren Resilienz gestärkt wird. Diese Bestimmungen der VFAV gelten auch für 5G-Anlagen. Sie haben die Angleichung der Schweizer Gesetzgebung an jene der EU ermöglicht (vgl. Kap. 3.6). Um die Konformitätsbewertung von Anlagen und ihre Markteinführung zu erleichtern, erarbeiten die europäischen Normenorganisationen harmonisierte Normen, die der europäischen und schweizerischen Industrie zur Verfügung gestellt werden sollen.

Es wäre sinnvoll, wenn die Schweizer Gesetzgebung beispielsweise im Bundesgesetz über die technischen Handelshemmnisse (THG; SR *946.51*) oder im ISG (vgl. Kap. 3.3) die Problematik der Cybersicherheit von Produkten mit kritischen digitalen Komponenten berücksichtigen und nach dem Vorbild des EU-Projekts zur Cyberresilienz (Kap. 3.6) Anforderungen an die Hersteller solcher Produkte vorsehen würde.

3.5 Nationale Cyberstrategie

Gemäss der strategischen Stossrichtung der Legislaturperiode 2023–2027 antizipiert der Bund Cyberrisiken und unterstützt und ergreift wirksame Massnahmen, um die Bevölkerung, die Wirtschaft sowie die kritischen Infrastrukturen zu schützen.[15] Diese strategische Stossrichtung wurde in der NCS[16] vom April 2023 konkretisiert. Dank dieser Strategie soll die Schweiz vor Cyberbedrohungen geschützt werden.

Die NCS beschreibt die wichtigsten Cyberbedrohungen, die Quelle geopolitischer Risiken sind. Dazu zählen Cyberspionage, Cybersabotage, Cybersubversion, die darauf abzielt, das politische System eines Staates zu unterminieren, sowie Cyberoperationen in bewaffneten Konflikten (vgl. Kap. 2.2). In der NCS wird betont, dass die Entwicklung der Cyberbedrohung wesentlich durch geopolitische Veränderungen und technologische Innovationen geprägt ist und dass mit zunehmenden Spannungen zwischen Ländern zu rechnen ist, die zu den wichtigsten Herstellern von Hard- und Software-Produkten zählen. Es wird von einem risikobasierten, umfassenden Ansatz ausgegangen, der zum Ziel hat, die Resilienz der Schweiz hinsichtlich Cyberbedrohungen zu verbessern. Gemäss der NCS sollte geprüft werden, in welchen Bereichen über Standards oder Regulierungen Vorgaben gemacht werden müssen. Der vorliegende Bericht befasst sich mit dieser Fragestellung.

---

[15] Bundesrat, Leitlinien und Ziele für die Legislaturplanung 2023–2027 vom 11. Januar 2023, Ziel 18

[16] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-94237.html

3.6 Im Ausland ergriffene Massnahmen

Die USA haben im Mai 2019 die Produkte und Dienstleistungen der chinesischen Unternehmen *Huawei* und *ZTE* in ihren Telekommunikationssystemen verboten. Dieses Verbot wurde 2022 auf alle chinesischen Telekommunikations- und Videoüberwachungsprodukte ausgeweitet. Die Gründe für das Verbot sind neben dem Spionageverdacht auch Überlegungen betreffend die Dominanz chinesischer Unternehmen auf dem Markt für 5G-Technologie und den Rückstand der US-Unternehmen in diesem Bereich. Andere Länder sind dem Beispiel der USA gefolgt, unter anderem Kanada, Grossbritannien, Japan und Australien.

Die EU-Mitgliedstaaten haben ihrerseits in einer im Januar 2020 verabschiedeten Toolbox einen umfassenden Ansatz für den Umgang mit Risiken im Zusammenhang mit 5G-Netzen festgelegt.[17] Die darin vorgeschlagenen Massnahmen zielen vor allem darauf ab, die Sicherheitsanforderungen zu verschärfen, die Risikoprofile der Lieferanten zu bewerten, Beschränkungen bis hin zum Ausschluss für Lieferanten anzuwenden, die als mit einem hohen Risiko behaftet gelten, und Strategien für eine Diversifizierung der Lieferanten sicherzustellen. Zwar haben die meisten EU-Mitgliedstaaten in ihren Gesetzen eine Beschränkung und/oder ein Verbot der Nutzung von Hochrisiko-Lieferanten für den Aufbau der nationalen 5G-Infrastruktur oder ihrer kritischen Elemente wie den Kernnetzfunktionen erlassen. Allerdings hat nur ein Teil von ihnen diese Vorrechte auch tatsächlich genutzt, um Hochrisiko-Lieferanten zu beschränken oder auszuschliessen. Die Europäische Kommission ist der Auffassung, dass *Huawei* und *ZTE* wesentlich höhere Risiken bergen als andere 5G-Lieferanten und dass die Beschränkungen und Ausschlüsse, die ihnen von zehn Mitgliedstaaten auferlegt wurden, gerechtfertigt sind und mit der 5G-Toolbox in Einklang stehen. Sie fordert die anderen Mitgliedstaaten und die Telekommunikationsbetreiberinnen angesichts des Risikos für die kollektive Sicherheit der EU nachdrücklich dazu auf, ebenfalls solche Massnahmen zu ergreifen.[18]

Die Richtlinie 2014/53/EU über Funkanlagen (RED), an die die Schweiz ihre Gesetzgebung angeglichen hat (vgl. Kap. 3.4), schafft einen Regelungsrahmen für das Inverkehrbringen von Funkanlagen, der technische Anforderungen für den Schutz der Privatsphäre, den Schutz personenbezogener Daten und den Schutz vor Betrug umfasst. Die EU hat zudem einen Vorschlag für ein Gesetz über Cyberresilienz[19] vorgestellt, das Verpflichtungen für Hersteller von Produkten mit digitalen Elementen vorsieht. Diese Verpflichtungen betreffen insbesondere die Konzeption, Entwicklung und Herstellung solcher Produkte, das Lebenszyklusmanagement und die Meldung von Schwachstellen. Die Vereinigten Staaten verlangen von den Lieferanten auf der

[17] Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures (https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures)
[18] Mitteilung vom 15. Juni 2023 (https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox)
[19] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen an Produkte mit digitalen Bestandteilen und zur Änderung der Richtlinie EU/2019/1020 (COM[2022] 454 final – 2022/0272[COD])

Grundlage einer «executive order» vom Mai 2021 zur Verbesserung der Cybersicherheit auch Transparenz bezüglich der Komponenten von Software, die an die Regierung verkauft wird (Software Bill of Materials).

3.7 Kurzer Überblick über das derzeitige rechtliche und politische System

Die Schweiz hat zwar bereits gewisse Massnahmen zur Sicherung ihrer digitalen Infrastruktur getroffen, aber es bestehen weiterhin Sicherheitsrisiken im Zusammenhang mit der Fernmeldeinfrastruktur, die Möglichkeiten zum Hacking oder zur Sabotage unserer kritischen Infrastrukturen sowie zur wirtschaftlichen oder auch politischen Erpressung bieten (vgl. Kap. 2.2). Angesichts der sich daraus ergebenden geopolitischen Risiken für unser Land müssen die Mittel zur Bekämpfung dieser technischen Risiken in einem allgemeinen und nicht-diskriminierenden Ansatz verstärkt werden.

Im zunehmend gespaltenen geopolitischen Kontext besteht zudem das Risiko, dass unser Land als Sicherheitslücke in der Mitte Europas betrachtet und bei der Nutzung bestimmter digitaler oder Netzwerkinfrastrukturen wirtschaftlich diskriminiert wird oder bei einer potenziellen Abhängigkeit von einem oder mehreren bestimmten Ausrüstungslieferanten politisch unter Druck gesetzt werden könnte (vgl. Kap. 2.3). Eine Berücksichtigung dieser geopolitischen Risiken im FMG wird unter diesen Umständen prioritär und unumgänglich.

4 In Betracht zu ziehende potenzielle Massnahmen

4.1 Den Kampf gegen technische Risiken verstärken

Angesichts der geopolitisch geprägten technischen Risiken (vgl. Kap. 2.2 und 3.7) sollten die Kompetenzen des Bundesrates im FMG präzisiert und erweitert werden, damit neue Instrumente und Anforderungen nach dem Vorbild der 5G-Toolbox der EU und anderer Regulierungsvorhaben, insbesondere im Bereich der Cyberresilienz, festgelegt werden können, die für eine Verbesserung der Sicherheit unserer Fernmeldeinfrastrukturen erforderlich sind. Dies umfasst insbesondere Folgendes:

- Telekommunikationsbetreiberinnen dazu verpflichten, Geräte, Anlagen und Software im Zusammenhang mit dem Angebot von Fernmeldediensten von verschiedenen Lieferanten zu beschaffen und zu betreiben (Mehrlieferanten-Strategie);
- die in der FDV für 5G-Netze vorgesehenen Sicherheitsanforderungen (vgl. Kap. 3.2) auf alle Fernmeldenetze erweitern, insbesondere die Verpflichtung, sicherzustellen, dass sicherheitskritische Geräte, Anlagen und Software dem Stand der Technik entsprechen und angemessenen Zertifizierungsverfahren für Cybersicherheit unterzogen werden;
- zusätzliche Beschränkungen für Geräte, Anlagen und Software im Zusammenhang mit der Bereitstellung von Fernmeldediensten vorsehen, die als risikobehaftet gelten;
- erhöhte Sicherheitsanforderungen für die Beschaffung und den Betrieb von Geräten, Anlagen und Software für die nächste Ausschreibung von Mobilfunkfrequenzen im Jahr 2028 vorsehen (Konzessionen);

- die Möglichkeit einer Standortpflicht bezüglich der NOC und SOC in der Schweiz prüfen – sofern die internationalen Verpflichtungen der Schweiz dies zulassen –, wobei diese von der Betreiberin selbst oder von einem von den Lieferanten unabhängigen Beauftragten betrieben werden müssen.

Die Umsetzung dieser neuen Anforderungen, die letztlich die Sicherheit unserer Fernmeldeinfrastrukturen erhöhen, erfordert einen Ausbau der technischen Zertifizierungs- und Kontrollkapazitäten in unserem Land (vgl. Kap. 4.3) und eine verstärkte Aufsicht durch das BAKOM.

Angesichts der technologischen Kosten und des Innovationsniveaus, die für den Aufbau digitaler Infrastrukturen notwendig sind, wäre es unrealistisch, eine Industriepolitik in Erwägung zu ziehen, mit der die technologische Abhängigkeit unseres Landes von ausländischen Ausrüstungslieferanten verringert werden könnte. Hingegen ist nicht ausgeschlossen, dass in der Schweiz spezielle Sicherheitslösungen im Zusammenhang mit Fernmeldeanlagen, -software oder -diensten erarbeitet werden können. In diesem Kontext wäre es sinnvoll, wenn die Forschung und Entwicklung solcher Schweizer Sicherheitslösungen nach dem Vorbild des an der ETH Zürich entwickelten SCION-Protokolls (vgl. Kap. 3.3) über geeignete bestehende Finanzierungsinstrumente (Schweizerischer Nationalfonds, Innosuisse).

4.2 Die geopolitischen Risiken antizipieren

Angesichts der potenziellen geopolitischen Risiken, denen die Schweiz ausgesetzt ist (vgl. Kap. 2.3 und 3.7), sollte sie über die rechtlichen Mittel verfügen, um diese Risiken bei Bedarf mit der gebotenen Sorgfalt anzugehen, auch wenn der allgemeine und nicht-diskriminierende Ansatz für Sicherheitsrisiken weiterhin so weit wie möglich bevorzugt werden sollte (vgl. Kap. 4.1). Deshalb sollte im FMG eine neue Bestimmung vorgesehen werden, die dem Bundesrat die Möglichkeit gibt, bei Eintreten eines potenziellen geopolitischen Risikos unter Einhaltung der internationalen Verpflichtungen der Schweiz die erforderlichen Massnahmen zu ergreifen. Letztlich geht es darum, dass die Schweiz über den Bundesrat nötigenfalls rasch handeln kann, um ihre Interessen, ihre innere und äussere Sicherheit sowie ihre Unabhängigkeit zu wahren.

Der Bundesrat sollte daher im FMG die Befugnis erhalten, nach dem Vorbild der 5G-Toolbox der EU und der diesbezüglichen Gesetze der EU-Mitgliedstaaten die folgenden potenziellen Schutzmassnahmen zur Erhöhung der Sicherheit der digitalen und der Fernmeldeinfrastrukturen auf dem Verordnungsweg zu ergreifen:

- Die Telekommunikationsbetreiberinnen dazu verpflichten, Geräte, Anlagen und Software im Zusammenhang mit dem Angebot von Fernmeldediensten nur von bestimmten Lieferanten oder Kategorien von Lieferanten zu beschaffen, einzurichten und zu betreiben;
- die Beschaffung, die Einrichtung und den Betrieb von Geräten, Anlagen und Software im Zusammenhang mit dem Angebot von Fernmeldediensten von Lieferanten, die als problematisch für die Sicherheit unseres Landes eingestuft werden oder die sich im Besitz, unter der Kontrolle oder dem Einfluss eines ausländischen Staates befinden, der ein geopolitisches Risiko für die Schweiz darstellt, einschränken, aussetzen oder verbieten;

- die Betreiberinnen dazu verpflichten, Geräte, Anlagen und Software im Zusammenhang mit dem Angebot von Fernmeldediensten aus ihrer Infrastruktur zu entfernen, die von Lieferanten stammen, die als problematisch für die Sicherheit unseres Landes eingestuft werden oder die sich im Besitz, unter der Kontrolle oder dem Einfluss eines ausländischen Staates befinden, der ein geopolitisches Risiko für die Schweiz darstellt.

Die Ergreifung der hier in Betracht gezogenen Massnahmen könnte erhebliche wirtschaftliche Folgen für die betroffenen Betreiberinnen sowie weitreichende betriebliche Auswirkungen auf ihre Netze und ihr Angebot an Fernmeldediensten haben. Die Massnahmen sollten mit Bedacht und unter Wahrung der Grundrechte der betroffenen Unternehmen konzipiert und die damit verbundenen Umsetzungsfristen ausreichend lang sein.

4.3 Die technischen Prüfungs- und Zertifizierungskapazitäten ausbauen

Um digitale Infrastrukturen, Telekommunikationsgeräte und -anlagen sowie IKT-Produkte zu sichern, müssen sie zertifiziert oder muss ihre Konformität in Bezug auf die Sicherheit bewertet werden (vgl. Kap. 3.2 und 3.4). Dies erfordert Kompetenzen, Ressourcen und Fachkenntnisse, über die die Schweiz in ihren Hochschulen, im öffentlichen Sektor oder in ihren Unternehmen weitgehend verfügt.

Die Audit- und Zertifizierungskapazitäten werden in unserem Land gegenwärtig ausgebaut. Beispiele dafür sind die kürzlich erfolgte Gründung des Nationalen Zentrums für Cybersicherheit (NCSC), das über hochspezialisierte Kompetenzen im Bereich der Cybersicherheit verfügt, oder das exponentielle Wachstum des privaten Angebots an Dienstleistungen für IT-Schwachstellenanalysen und Penetrationstests.[20] Der Cyber-Defence Campus (CYD Campus) von armasuisse arbeitet zudem eng mit Hochschulen und der Wirtschaft zusammen, um ein auf Cybersicherheit ausgerichtetes Technologiemonitoring aufzubauen, und die Akademien der Wissenschaften Schweiz sind beauftragt, die Chancen und Risiken neuer Technologien zu evaluieren.

Dieses Schweizer Ökosystem für Cybersicherheit sollte in der Lage sein, der Schweiz langfristig die erforderlichen unabhängigen nationalen Kontroll- und Zertifizierungsstellen bereitzustellen, um die Software- und Hardware-Sicherheit ihrer digitalen Infrastruktur, ihrer Fernmeldeausrüstungen und ihrer IKT-Produkte zu evaluieren. Parallel dazu sollte die Schweiz internationale Abkommen zur Anerkennung von technischen Zertifizierungen entwickeln, insbesondere im Rahmen des Abkommens zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Union über die gegenseitige Anerkennung von Konformitätsbewertungen (MRA CH-EU; SR *0.946.526.81*).

[20] Ein Beispiel ist das Nationale Testinstitut für Cybersicherheit (NTC) mit Sitz in Zug, das die Zuverlässigkeit und Sicherheit von vernetzten Produkten und digitalen Anwendungen überprüft. Die Tests werden in Kooperation mit der Wirtschaft, IT-Sicherheitsfirmen und Hochschulen gestartet und orientieren sich an den gängigen internationalen Standards. Das NTC prüfte im Auftrag des NCSC im Juni 2021 das Covid-19-Zertifikat und im April 2023 die chinesische App TikTok.

4.4 Die internationale Zusammenarbeit intensivieren

Die internationale Zusammenarbeit ist weiterhin unverzichtbar, um die Sicherheit von digitalen Netzen und Infrastrukturen angesichts ihrer weltweiten Vernetzung zu gewährleisten. Gemäss der Strategie Digitalaussenpolitik 2021–2024[21] will die Schweiz die Cybersicherheit stärken, indem sie sich für die konkrete Anwendung völkerrechtlicher Normen einsetzt.[22] So nimmt sie an den Verhandlungen zur Ausarbeitung einer UNO-Konvention zur Cyberkriminalität teil, verhandelt über die Aktualisierung der Global Cybersecurity Agenda der ITU, beteiligt sich aktiv an der Umsetzung der vertrauensbildenden Massnahmen im Bereich der Cybersicherheit der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) und unterstützt zahlreiche internationale Initiativen zur Bewahrung eines offenen, freien und sicheren Cyberspace.[23] Die Einbindung der Schweiz in das internationale Regelwerk erfolgt auch über das internationale Genf, das eine wesentliche Plattform für Debatten über Cybersicherheit auf globaler Ebene darstellt.

Staaten können die Sicherheit des digitalen Raums insofern nicht alleine garantieren, als privatwirtschaftliche Akteure diesen Bereich durch ihre globalen Standards, Produkte und Dienstleistungen entscheidend mitprägen. Die Schweiz setzt sich deshalb für einen Multistakeholder-Ansatz ein und fördert den Dialog mit den Unternehmen. Von grosser Bedeutung ist auch die Zusammenarbeit mit privaten internationalen Initiativen und technischen Kompetenzzentren für Cybersicherheit (u. a. FIRST, TF-CSIRT, NatCSIRT) sowie die Beteiligung an der Standardisierung von Fernmeldenetzen in verschiedenen Organisationen (ITU, ETSI, 3GPP usw.) in Zusammenarbeit mit den Lieferanten von Anlagen.

5 Schlussfolgerung

Gemäss der strategischen Stossrichtung für die Legislaturperiode 2023–2027 muss der Bund Cyberrisiken antizipieren und in diesem Bereich wirksame Massnahmen zum Schutz der Bevölkerung, der Wirtschaft sowie der kritischen Infrastrukturen ergreifen. Die Nationale Strategie zum Schutz kritischer Infrastrukturen 2023 und die Nationale Cyberstrategie 2023 gegen Cyberbedrohungen greifen diesen präventiven Ansatz auf, beauftragen den Bundesrat aber zugleich, Cyberrisiken und -verwundbarkeiten zu analysieren und unter Berücksichtigung von Bedürfnissen und Gesetzeslücken notwendige Regelungen vorzuschlagen.

Der Bundesrat ist angesichts der geopolitisch geprägten technischen Risiken, denen die Schweiz im Zusammenhang mit ihrer Fernmelde- und digitalen Infrastruktur ausgesetzt ist, überzeugt, dass die Mittel zur Bekämpfung dieser Risiken verstärkt werden müssen. Er schlägt Massnahmen vor, die auf der Grundlage des FMG zu treffen

---

[21] Bericht des Bundesrates in Erfüllung des Postulates 17.3789 vom 4. November 2020 «Strategie Digitalaussenpolitik 2021–2024»

[22] In diesem Zusammenhang ist auch die durch die UNO-Generalversammlung beauftragte Arbeitsgruppe «Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security» (UN OEWG) zu erwähnen, in der sich die Schweiz aktiv einsetzt.

[23] Die Schweiz sponsert insbesondere ein UN-Programm zur Förderung eines verantwortungsbewussten Verhaltens von Staaten im Cyberspace und engagiert sich in der *Counter Ransomware Initiative*.

sind (Mehrlieferanten-Strategie, Beschränkungen für als risikobehaftet geltende Ausrüstungen, verstärkte Sicherheitsanforderungen bei der nächsten Frequenzausschreibung). Im Übrigen sollte das Schweizer Ökosystem für Cybersicherheit in der Lage sein, langfristig die nationalen Kontroll- und Zertifizierungsstellen bereitzustellen, die unser Land benötigt.

Nach Ansicht des Bundesrates ist es notwendig, nach dem Vorbild der 5G-Toolbox der EU und anderer Regulierungsvorhaben, insbesondere zur Cyberresilienz, im FMG eine neue Bestimmung vorzusehen, die ihm die Möglichkeit gibt, bei Eintreten eines geopolitischen Risikos unter Einhaltung der internationalen Verpflichtungen der Schweiz die erforderlichen Massnahmen zu ergreifen. Unter anderem soll er die Beschaffung, die Einrichtung und den Betrieb von Ausrüstungen verbieten können, die von Lieferanten stammen, die als problematisch für die Sicherheit unseres Landes gelten oder die sich im Besitz, unter der Kontrolle oder dem Einfluss eines ausländischen Staates befinden, der ein geopolitisches Risiko für die Schweiz darstellt. In dieser Hinsicht müssen die Wirtschaftsfreiheit und das einwandfreie Funktionieren des Wettbewerbs bestmöglich sichergestellt werden.

Schliesslich muss sich die Schweiz weiterhin in der internationalen Zusammenarbeit engagieren, die angesichts der weltweiten Vernetzung von digitalen Netzwerken und Infrastrukturen für deren Sicherheit unverzichtbar ist.