Leitplanken Digitaler Souveränität

Ziel und Einordnung

Die digitale Transformation schreitet mit hoher Geschwindigkeit voran und betrifft schon heute nahezu alle Lebens- und Wirtschaftsbereiche. Sie bringt neue Lösungen, neue Produkte und neue Dienstleistungen hervor und verändert Geschäftsmodelle und Kundenbeziehungen grundlegend auf allen Stufen der Wertschöpfungskette. Die Digitalisierung ist längst kein reines Digital- und Infrastrukturthema mehr. Sie ist zu einem branchen- und sektorübergreifenden Querschnittsthema geworden. In jeweils unterschiedlichen Ausprägungen hat sie praktisch alle Branchen erfasst und verändert. Daten sind Ware und Währung zugleich und bilden den Kern einer entstehenden globalen Datenökonomie.

Auch vor dem Hintergrund unterschiedlicher Formen des Datenschutzes dies- und jenseits des Atlantiks ist das Thema Digitale Souveränität zum Gegenstand zahlreicher wirtschafts- und gesellschaftspolitischer Diskussionen geworden. Es ist relevant für den einzelnen Nachfrager, der allgegenwärtige digitale Technologien selbstbestimmt nutzen will, für die anbietenden Unternehmen bei der Gestaltung ihrer Geschäftsmodelle und den Beziehungen zu Kunden und Geschäftspartnern, für die Gesamtwirtschaft vor allem bei der Frage, welche erforderlichen Schlüsselkompetenzen nötig sind, um unsere Wettbewerbsfähigkeit auch in Zukunft zu sichern. Denn nur wenn wir digital souverän agieren können, sind wir in der Lage, unsere Potenziale im globalen Standortwettbewerb erfolgreich umzusetzen und unsere Chancen zu nutzen.

Es drängt sich also die Frage auf, was wir in Deutschland und Europa unter dem Begriff der digitalen Souveränität verstehen und welchen Anspruch wir damit verbinden wollen. Die Fokusgruppe 1 „Digitale Souveränität“ der Plattform „Innovative Digitalisierung der Wirtschaft“ des Nationalen IT-Gipfels hat sich deshalb die Aufgabe gestellt, Leitplanken zu entwickeln und in einem größerem Kreis zur Diskussion zu stellen, die die Schlüsselvoraussetzungen für unternehmerisch und gesellschaftlich souveränes Handeln aller beteiligten Akteure in Deutschland und Europa in einer globalen Datenwirtschaft beschreiben. Ergebnis ist dieses Papier, das von der Fokusgruppe in mehreren Diskussionsrunden entwickelt und anschließend in einem hochrangigen Experten-Workshop überprüft und weiterentwickelt wurde[1].

Unter dem Begriff Souveränität versteht man zunächst allgemein die Fähigkeit zu Selbstbestimmung, die sich durch Eigenständigkeit und Unabhängigkeit ausdrückt. Souveränität grenzt sich einerseits von Autarkie und andererseits von Fremdbestimmung ab. Digitale Souveränität bezeichnet in diesem Sinne die Fähigkeit zu selbstbestimmtem Handeln und Entscheiden im digitalen Raum. Gerade in einer digital vernetzten Welt gibt es keine Autarkie. Gleichzeitig werden die neuen digitalen Möglichkeiten die Freiheit des Einzelnen und von Gesellschaften dauerhaft nur dann erweitern, wenn Schlüsselkompetenzen vorhanden sind, IT-Sicherheit und Datenschutz auf angemessenem Level gewährleistet werden können und innovationsoffener Wettbewerb herrscht.

Souverän zu sein bedeutet daher, zu selbstbestimmtem Handeln und Entscheiden fähig zu sein, ohne dabei ausschließlich auf eigene Ressourcen zurückzugreifen. Dazu gehört, dass Wirtschaft, Wissenschaft und Gesellschaft (digitale) Produkte, Dienstleistungen, Plattformen und Technologien so nutzen können, dass beispielsweise eigene Sicherheits- oder Datenschutzinteressen nicht beeinträchtigt sind, dass keine unausweichlichen Abhängigkeiten entstehen und dass eigene Geschäftsideen und -modelle verwirklicht werden können. Digitale Souveränität bedeutet darüber hinaus, dass Wirtschaft, Wissenschaft (und in einigen Fällen die öffentliche Verwaltung) in der Lage sind, digitale Technologien zu entwickeln, zur Marktreife auf internationalem Spitzenniveau zu bringen und national wie international zu vertreiben.

1 zu den Teilnehmern der Fokus-Gruppe und des Workshops s. Anlage

Das vorliegende Leitplankenpapier greift insbesondere die wirtschaftspolitische Perspektive auf. Ziel ist es, möglichst konkrete Maßnahmen und Handlungsempfehlungen für die Stärkung oder auch Wiedererlangung der digitalen Souveränität in Deutschland und Europa aufzuzeigen. Dabei stehen drei Themenfelder im Vordergrund:

(1) Leistungsfähige und sichere Infrastruktur

(2) Beherrschung von Schlüsselkompetenzen und -technologien

(3) Innovationsoffene Rahmenbedingungen der digitalen Souveränität

1. Leistungsfähige und sichere Infrastruktur

Zu den Grundvoraussetzungen für digitale Souveränität gehören die Bereitstellung einer entsprechenden Infrastruktur, deren sichere Nutzung sowie der Zugang zu sicheren, vertrauenswürdigen digitalen Technologien als solide Vertrauensbasis, etwa zur Etablierung innovativer Geschäftsmodelle.

1.1 Leistungsfähige digitale Infrastruktur

Höchst leistungsfähige, u. U. quasi-echtzeitfähige und sichere digitale Infrastrukturen sind die elementare Basis von innovativen Produkten und Technologien, von Industrie 4.0 und von intelligenten Netzen in den Bereichen Verkehr, Energie, Gesundheit, Bildung und Verwaltung. Dazu gehören vor allem Breitbandnetze unterschiedlicher Ausprägung – auch mobile Netze der fünften Generation.

Breitbandige digitale Infrastrukturen sind die Lebensadern der digitalen Welt. Ihr schnellstmöglicher Ausbau als Teil europaweiter Hochleistungsnetze sollte in einer gemeinsamen Anstrengung von Wirtschaft und Staat Priorität haben.

1.2 Sichere und vertrauenswürdige Infrastruktur

Angesichts der wachsenden Bedeutung des Cyberraums und informationstechnischer Systeme ist es wichtig, Risiken und Bedrohungen der Netz- und Informationssicherheit geeignet zu adressieren und zu minimieren. Elementare Grundlage für souveränes Handeln ist ein sicherer digitaler Raum. Digitale Souveränität setzt voraus, dass Europas Wirtschaft, Staat und Bürger in die Lage versetzt werden, vertraulich und geschützt in digitalen Netzen zu kommunizieren. Darüber hinaus entscheidet vertrauenswürdige IT über den Erfolg der Digitalisierung in Deutschland und somit über die Wettbewerbsfähigkeit der deutschen Wirtschaft. So lange Unternehmen Verlust oder Manipulation ihrer Daten — insbesondere wettbewerbs- und geschäftskritische Informationen — befürchten, werden sie sich nur sehr zurückhaltend oder nur in eigenen isolierten sicheren Räumen digitalisieren. Um die digitale Souveränität Deutschlands und Europas zu wahren bzw. in Teilen wiederzuerlangen und vor allem die betriebliche Datenhoheit sichern zu können, müssen sich Staaten, Unternehmen und Bürger darauf verlassen können, dass bei der Nutzung digitaler und vernetzter Infrastrukturen bestimmte Voraussetzungen und Funktionalitäten gegeben sind, gleichzeitig aber andere, technisch durchaus mögliche, aber unerwünschte Funktionen nicht durchgeführt werden können. Es darf keine Hintertüren oder sonstige Kanäle geben, über die Daten unbefugt eingesehen, kopiert oder verändert werden können.

1.3 Verfügbarkeit und Zugang

Für digitale Souveränität sind auch Verfügbarkeit und Zugang zu digitalen Ökosystemen und deren Plattformen wesentliche Voraussetzung. Wichtiges Instrument sind offene Standards. Sie können herstellerunabhängig entwickelt und angewendet werden. Zudem ermöglichen und erleichtern offene Standards das Zusammenwirken der vielen vernetzten Komponenten und Systeme u.a. in der Industrie 4.0. Die durch ihre Anwendung ermöglichte Interoperabilität ist entscheidend, um bestehende wirtschaftlich-technische Abhängigkeiten für die deutsche und europäische

Wirtschaft zu verringern. Damit ist die Frage von Verfügbarkeit und Zugang eine Grundvoraussetzung digitaler Souveränität im Allgemeinen, und die Fähigkeit zur Entwicklung offener Standards eine Schlüsselkompetenz im Speziellen.

2. Beherrschung von Schlüsseltechnologien und technologischen Schlüsselkompetenzen

Digitale Souveränität bedeutet weiter, zentrale Schlüsseltechnologien und -kompetenzen zu beherrschen. Das heißt, in der Lage zu sein, notwendige Schlüsseltechnologien zu identifizieren und zu beurteilen, diese aufbauen und weiterentwickeln zu können. Zu beachten ist allerdings, dass wesentliche Schlüsseltechnologien nicht mehr in Deutschland und nur noch eingeschränkt in Europa vertreten sind. Deutschland verfügt im Gegenzug über ein hervorragendes Innovationssystem und die notwendigen Ressourcen, auf die wir aufbauen können, etwa in Universitäten, Forschungs- und Entwicklungseinrichtungen, innovationsstarken Klein- und mittelständischen Unternehmen und Start-ups. Entscheidend ist, diese Ressourcen auf die strategisch wichtigen Themenfelder auszurichten. Mit Blick auf die aktuelle globale Marktsituation sind in diesem Kapitel Kompetenz- und Technologiefelder aufgeführt, die aus heutiger Sicht von besonderer Bedeutung sind. Diese Analyse soll in Zukunft laufend aktualisiert und angepasst werden.

2.1 Software-Kompetenzen

Entlang der digitalen Transformation von Geschäftsmodellen, Prozessen und Verfahren stellen Software-Kompetenzen eine zentrale technologische Schlüsselkompetenz dar. Sie umfassen mehr als reine Programmierfähigkeiten. Im Zuge der Verschmelzung digitaler und physikalischer Welt sind vielmehr analytisch/konzeptionelle Lösungskompetenzen im Querschnitt aus Mathematik, Technologie/Technik, Sensorik, Digitalen Medien, Naturwissenschaft und Ingenieurwesen relevant. Die Entwicklung und Erhaltung derartiger Software-Kompetenzen ist v. a. erforderlich, um länderübergreifende Plattformen zu gestalten, Services für intelligente Infrastrukturen zu entwickeln, Datenwertschöpfungsketten zu gestalten, Konzepte sowie geeignete Mensch-Maschinen-Schnittstellen zu erstellen, aber auch Sicherheitslösungen (inkl. Kryptographie und Identitätssicherheit) zu entwickeln, die über reine Softwarelösungen hinausgehen. Darüber hinaus erfordert die digitale Transformation bestimmte Methodenkompetenzen, zu denen insbesondere Hersteller-, Beurteilungs- und Marktgestaltungskompetenzen zählen.

2.2 Hardware-Kompetenzen

Die Schnittstelle zwischen realer Welt und ihrer digitalen Entsprechung ist die Hardware. Sensoren und Aktuatoren, Microcontroller, Speicher- und Kryptochips machen die Realität für den Cyberspace verfügbar. Der technologische Fortschritt der Mikroelektronik ist Voraussetzung für die nachhaltige Kostendegression der Hardware und die Verfügbarkeit für Massenmärkte. Die Erfolgsgeschichte weiter Teile der deutschen Systemindustrie hing und hängt von der Kompetenz der deutschen Zulieferindustrie beim Entwurf und der Fertigung kundenspezifischer Mikro- und Nanoelektronik ab. Die darauf aufbauende Kombination von Hardware und Software ermöglicht Alleinstellungsmerkmale und Premiumvorteile.

2.3 IT-Sicherheit

Zentrale Schlüsselkompetenz ist ebenso die Fähigkeit, sichere Produkte und Dienstleistungen entwickeln und anbieten zu können. Qualität, Sicherheit und Verlässlichkeit müssen Markenzeichen auch von digitalen Produkten und Dienstleistungen aus Deutschland und Europa sein. Dazu zählt auch und vor allem IT-Sicherheit. Die deutsche IT-Sicherheitswirtschaft ist technologisch sehr innovativ, aber in ihrer Struktur sehr kleinteilig. Zudem sind deutsche Unternehmen als Anwender noch weit entfernt von einer Sicherung und Entwicklung ihrer Kompetenzen. Zwar haben die großen Unternehmen ihr Bewusstsein in Sachen Cyber-Sicherheit deutlich verbessert; vor allem der Mittelstand hat hier jedoch noch deutliches Potenzial. Der bisher bedenkenlose Einsatz von Technologien im IT-Bereich muss von den Unternehmen hinsichtlich der Datensicherheit und Vertrauenswürdigkeit hinterfragt werden. Gleichzeitig brauchen die Unternehmen der IT-Sicherheitswirtschaft eine größere Marktsichtbarkeit; öffentliche Auftraggeber könnten als

Referenzen entsprechende Signale setzen, damit IT-Sicherheit „made in Europe“ Schlüsseltechnologie und Standortvorteil gleichermaßen werden kann.

2.4 „Big Data“ und „Smart Data“

Daten werden zum Treiber von Innovationen und Wachstum in nahezu allen Wirtschaftssektoren. Konsequente Forschung, Weiterentwicklung der Auswertungsmöglichkeiten und Leistungsfähigkeit der Systeme führen zu enormen Verbesserungen und kundennahen Lösungen, z. B. im Gesundheitsbereich oder in der Industrie 4.0 – unternehmens-, branchen- und marktübergreifend. Voraussetzung für den erfolgreichen Einsatz von Big Data-Lösungen sowohl als eigene Geschäftsmodelle als auch integriert in existierende Geschäftsmodelle sind Kompetenzen bezüglich des Funktionierens und Zusammenwirkens von Big-Data-Wertschöpfungsketten. Auf der Seite der Nutzer sind Vertrauen in einen starken Datenschutz und ein rechtlicher Gestaltungsrahmen nötig, der die wirtschaftliche Datennutzung mit dem Schutzinteresse des Einzelnen in Einklang bringt. Es muss gelingen, dass ganze Datenwertschöpfungsketten gebildet werden können.

2.5 Cloud-Dienste und digitale Produktion

Cloud-Dienste bieten enorme Vorteile, wenn es um die Leistungsfähigkeit und Reaktionsgeschwindigkeit der anwendenden Unternehmen geht. Flexibilität, Skalierung und Kosteneffizienz machen sie zu geeigneten Lösungen bei der Nutzung von verlässlichen Infrastrukturen. Insbesondere bei dem Einsatz von Technologie in Endprodukten mit hoher Stückzahl kann ohne Cloud-Lösungen heute kein annähernd kosteneffizienter Einsatz mehr gewährleistet werden.

Die schnelle Verbreitung muss durch kunden- und bedarfsgerechte Sicherheitslösungen und europaweite Standards gesichert werden. Der Angst vor Datenverlusten bei der Nutzung von Cloud-Lösungen und einem möglicherweise unberechtigten Zugriff Dritter auf sensible Daten muss in der gesamten Nutzungskette entgegengewirkt werden. Daneben sind rechtliche Unsicherheiten bei der Nutzung von Cloud-Diensten ein Hindernis. Es muss deutlich gemacht werden, dass Cloud-Computing und Compliance keine Gegensätze mehr sind.

Mit der Beseitigung dieser Hemmschwellen bekommt Cloud-Computing die Chance, einen zentralen Beitrag zur Realisierung gesamtwirtschaftlicher Vorteile bzw. der Sicherstellung der Wettbewerbsfähigkeit europäischer Unternehmen und damit zur Digitalen Souveränität zu leisten. Ausgehend von Cloud-basierten Lösungen muss zügig die gesamte digitale Produktion als Kompetenzfeld entwickelt werden.

2.6 Plattformen

Plattformen spielen in digitalen Märkten eine besondere Rolle und sind die Basis vieler innovativer Geschäftsmodelle in der digitalen Welt. Ein kritischer Erfolgsfaktor für digitale Plattformen ist es, Interessen und Bedürfnisse der Nutzer zu analysieren und darauf Geschäftsmodelle aufzubauen. Digitale Souveränität bedeutet in diesem Zusammenhang, Funktions- und Einsatzweise von Plattformen und zweiseitigen Märkten zu verstehen und sie selbst zur Unterstützung und Weiterentwicklung eigener Geschäftsmodelle zu nutzen. Wettbewerbspolitik spielt hier eine wichtige Rolle, da Marktmacht und Datenmonopole missbraucht werden können, um Märkte abzuschotten. Ziel ist, dass auch Plattformen aus Europa globale Standards setzen und die Marktführerschaft einnehmen.

2.7 Mobile Business

Grundlage neuer digitaler Geschäftsmodelle sind außerdem oft mobile Technologien. Unter Mobile Business-Lösungen (MBS) versteht man in diesem Zusammenhang Prozesse, Technologien, Aktivitäten und Applikationen, die unter Nutzung drahtloser Übertragungstechnologien und mobiler Endgeräte zur Optimierung von geschäftlichen Vorgängen und Entwicklung innovativer Geschäftsmodelle eingesetzt werden. Die Breite der Verteilung bei den Nutzern, die Vielzahl an Lösungen sowie die Geschwindigkeit der Veränderungen bei Endgeräten und Plattformen machen den

Bedarf an Standards und den Aufbau von Wissen bei MBS-Lösungen deutlich. Das „Mobile-Business“ zeichnet sich durch seine Eigenschaften als besonders kritischer Bereich im Rahmen der Digitalisierung aus: Sowohl Endgeräte, Infrastrukturen, Zugänge und die oftmals gemischte private/berufliche Nutzung weisen zwar besondere Chancen in der täglichen Nutzung auf, sind allerdings auch mit deutlich erhöhten Risiken verbunden. Die größten Herausforderungen sind dabei oft die Netzwerksicherheit und der Schutz geschäftskritischer und vertraulicher Daten sowie die Unterstützung einer Vielzahl von mobilen Plattformen.

2.8 Digitale Bildung in der Breite

Die Beherrschung und Entwicklung von Schlüsseltechnologien als Teil digitaler Souveränität setzt über die genannten Felder hinaus, in denen Beherrschung und Entwicklung von Spitzentechnologien nötig sind, auch eine gute digitale Bildung in der Breite voraus. Menschen müssen grundlegend befähigt sein, mit Digitalisierung umzugehen und es verstehen, sie nutzbringend weiterzuentwickeln – als Bürger, als Arbeitnehmer oder auch als Gründer. Das Erwerben digitaler Fertigkeiten in Bildung und Ausbildung, nicht nur, aber vor allem in den MINT-Bereichen, sowie das Erlernen eines sicheren Umgangs mit digitalen Technologien und modernen Kommunikationsmitteln muss eine Priorität der Bildungspolitik werden.

3. Innovationsoffenen Gestaltungsrahmen schaffen

Um im globalen Standortwettbewerb zu bestehen, brauchen digital souveräne Systeme eine „Ermöglichungskultur“ und einen kompetitiven Wirtschaftsraum. Politische Agenden sollten deshalb die Förderung von Innovationen und die Chancen technologischer Entwicklungen stärker in den Vordergrund stellen als die Betrachtung der Risiken.

3.1 Digitaler Binnenmarkt Europa

Der Digitale Binnenmarkt Europa bildet im Idealfall den allgemeinen Ordnungsrahmen eines digital souveränen Europas. Er sollte Garant für ein digital souveränes Europa sein. Auf dem Weg dorthin müssen unangemessene regulatorische Asymmetrien zwischen Anbietern innerhalb Europas aufgelöst und ein marktortbezogenes Level-Playing-Field sichergestellt werden. Das gilt insbesondere für das Datenrecht: Digitale Souveränität benötigt ein Datenrecht, das einen sinnvollen Ausgleich zwischen schützenswerten Persönlichkeitsrechten und der Möglichkeit schafft, Daten für digitale Anwendungen zu nutzen. Die Möglichkeit, mit Daten umgehen und „arbeiten“ zu können, ist essentiell für die Entwicklung eigener Geschäftsmodelle und die Nutzung der Chancen der Digitalisierung. Deshalb dürfen datenbasierte digitale Geschäftsmodelle nicht durch ein unzeitgemäßes Datensparsamkeitsdiktat verhindert werden. Eine wettbewerbsfähige Datenwirtschaft mit Plattformen und intelligenten Diensten braucht vielmehr ein internationales Level-Playing-Field. Gleichzeitig müssen eine intelligente Datenpolitik, Datenschutz und Datensicherheit gewährleistet werden. Bisherige Grundprinzipien des Datenschutzes wie Datensparsamkeit und Zweckbindung müssen überprüft und durch Prinzipien der Datenvielfalt und des Datenreichtums ergänzt und ersetzt werden. Die Förderung datenschutzfreundlicher Anonymisierungs- und Pseudonymisierungstechnologien, Stärkung der Transparenzprinzipien und Verbesserung der Kontrolle und Sanktionsmechanismen bei Verstößen gegen Datenschutzrecht sind Wege zu einer innovativen Datenpolitik.

3.2 Innovationsförderung

Europa wird nur dann eine Führungsrolle in der Digitalen Wirtschaft übernehmen können, wenn eine aktive Forschungsförderung betrieben wird und Start-ups sowie Wachstumsunternehmen intensiv gefördert werden. Etablierte Klein- und mittelständische Unternehmen müssen aktiv von Branchenverbänden, Kammern und Ministerien dabei unterstützt werden, die Möglichkeiten der Digitalisierung in ihre Geschäftsmodelle und Produktionsprozesse zu integrieren.

Leistungsfähige, schnell wachsende und international orientierte Tech-Start-ups sind mit entscheidend für ein funktionsfähiges digitales Ökosystem, die Stärkung der internationalen Wettbewerbsfähigkeit und damit die Stärkung digitaler Souveränität. Im gleichen Maße sind Investitionen in Forschung und Entwicklung elementarer Bestandteil für innovationsgetriebenes, nachhaltiges Wachstum.

4. Forderungen

Zur Stärkung unserer digitalen Souveränität in Deutschland und Europa sind entlang der oben beschriebenen Ziele vielfältige politische Maßnahmen zu ergreifen:

4.1 Leistungsfähige und sichere Infrastruktur

4.1.1 Infrastruktur

- Als europäischer Wirtschaftsmotor sollte Deutschland sich zum Ziel setzen, innerhalb der nächsten zehn Jahre der Flächenstaat mit den im weltweiten Maßstab leistungsfähigsten digitalen Infrastrukturen vor allem in den Bereichen Breitband, Verkehr, Energie, Industrie 4.0, Gesundheit, Bildung und Verwaltung zu werden.

- Wo ein wirtschaftlicher Ausbau von Breitbandinfrastrukturen nicht möglich ist, sind technologie- und anbieteroffene Förderprogramme nötig. Im Bereich digitaler Infrastrukturen werden weitere Anstrengungen notwendig sein, um vor allem in der Frage der Latenzzeiten die Bedürfnisse der Wirtschaft adäquat abbilden zu können.

- Für den Wettbewerb und die erfolgreiche Vernetzung der Branchen sind differenzierte Lösungen unerlässlich. Nur auf der Grundlage von qualitätsgesicherten Netzwerkdiensten (Quality of Service) können erfolgreiche Geschäftsmodelle auf Basis von cyber-physikalischen Systemen entstehen.

- Der Aufbau einer eigenständigen, regulierten und sicheren Netzumgebung, z. B. als Grundlage für die vernetzte Produktion und um Produkte und Service mit hohen Sicherheitsstandards aufzubauen, in der u. a. eine eindeutige, urheberbezogene Identifizierung der gesamten technischen Kommunikation sichergestellt ist, würde diesen Prozess stützen.

4.1.2 Sicherheit und Vertrauenswürdigkeit

- Für den Standort Deutschland und Europa ist eine kohärente Cybersicherheitspolitik unerlässlich.

- Ein Mindestmaß an Sicherheit und Vertrauen muss gewährleistet werden. Für eine ganzheitliche Sicherheitsbetrachtung der Wertschöpfungskette der digitalen Welt ist es erforderlich, alle relevanten Marktteilnehmer bei der Umsetzung von Sicherheitsanforderungen zu berücksichtigen, die Produkte oder Dienste im Cyberraum anbieten. Es genügt nicht, die Betreiber kritischer IT-Infrastrukturen einzubinden; auch entsprechende Hard- und Software-Zulieferer müssen Bestandteil der IT-Sicherheitsarchitektur Deutschlands werden.

- Eine eigene Prüfkompetenz bei der Bewertung von IT Sicherheit muss gegeben sein, Anforderungen an Sicherheit, Zuverlässigkeit und Verfügbarkeit von CoTS (= consumer off the shelf) Systemen und Produkten müssen bereits in der Design-Phase (Security by Design) klar definiert und einheitliche verbindliche Sicherheitsstandards unter stärkerer Einbeziehung deutscher und europäischer Unternehmen geschaffen werden.

- Politik als Vorbild: Bewusster Einsatz von Security-Referenzprojekten in Heimatmärkten. Aufgrund ihrer Signalwirkung dienen sie als wichtiges Element der Wirtschafts-und Exportförderung. Dennoch müssen grenzüberschreitende Telekommunikationsdienste trotz nationaler Bedürfnisse bspw. bzgl. Öffentlicher Sicherheit gewährleistet sein.

- Schlüsseltechnologien im Bereich der IT-Sicherheit müssen identifiziert und bereitgestellt werden. Ein Anbieter-Anwender-Forum als offizielle Plattform kann politische Impulse aufnehmen und die notwendigen Technologien und Strategien weiterentwickeln. Dabei sind die einschlägigen Beratungen und Ergebnisse der Plattform Industrie 4.0 des Nationalen IT-Gipfels zu berücksichtigen.

- Stärkung der ENISA (European Network and Information Security Agency) Kooperationsplattform Cyber-Security für den regelmäßigen Erfahrungsaustausch zwischen IT-Sicherheitsfachleuten.

4.1.3 Verfügbarkeit und Zugang

- Die Verfügbarkeit offener Standards unterstützt einen innovationsoffenen Gestaltungsrahmen und ist ein Wettbewerbs-liberalisierendes Element. Offene Standards sind innovationsfördernd und eine wichtige Bedingung für digitale Souveränität. Ihr Einsatz in Wirtschaft und öffentlicher Verwaltung muss daher gefördert werden.

4.2 Schlüsseltechnologien und technologische Schlüsselkompetenzen

- Digitale Souveränität bedeutet, dass unsere Unternehmen in entscheidenden Bereichen sowohl wirtschaftlich als auch technologisch eine Marktposition besitzen, die es ihnen erlaubt, ihre Geschäftsmodelle weiterzuentwickeln und neue Dienstleistungen sicher anzubieten. Dazu gehört, dass bestimmte digitale Schlüsseltechnologien in Deutschland und Europa beherrscht oder zumindest verstanden werden sollten. Gelingt dies nicht, besteht die Gefahr, dass unsere Unternehmen in niedrigere Stufen der Wertschöpfungskette abrutschen.

- Voraussetzung für die Beherrschung der zuvor genannten Schlüsseltechnologien ist in erster Linie der Erwerb der relevanten Software- und Hardware-Kompetenzen. Dabei ist zunächst zu analysieren, welche speziellen Softwarekompetenzen erforderlich sind. Darauf basierend ist dann gemeinsam mit Stakeholdern zu prüfen, wie der Erwerb der erforderlichen Kompetenzen in Bildungssystemen, durch Unternehmen (z. B. Anreize für internen Aufbau von Softwarekompetenzen) oder durch Kooperationen mit Bildungseinrichtungen staatlich und von privater Seite gefördert werden kann.

- Konkret kann dies gemeinsam mit den betroffenen Branchen und Stakeholdern – unter anderem über die Plattformen „Innovative Digitalisierung der Wirtschaft“ und „Industrie 4.0“ des IT-Gipfels und in Zusammenarbeit mit anderen relevanten Foren wie dem „Hightech-Forum“ der Bundesregierung – geschehen. Ziel ist die Entwicklung einer strategischen Technologie-Agenda, die für die strategisch wichtigen Schlüsseltechnologien in einer jeweiligen Roadmap festlegt, wie und in welchem Zeithorizont diese erarbeitet und gesichert werden können. Als Bestandteil dieser Roadmap sollte auch ein fortlaufendes Kompetenzmonitoring entwickelt werden.

4.3 Innovationsoffener Gestaltungsrahmen

Grundsätzlich müssen die politischen und rechtlichen Rahmenbedingungen entsprechend dem Ziel der digitalen Souveränität ausgestaltet und optimiert werden. Gesetzesnovellen müssen hinsichtlich des Ziels „Sicherung der digitalen Souveränität“ geprüft und im Bedarfsfall angepasst werden. Dies kann neben den oben genannten zentralen Feldern unter Umständen auch Felder wie Urheber- und Wettbewerbsrecht, den Außenwirtschaftsschutz sowie die Telekommunikations- und Medienordnung, betreffen.

4.3.1 Digitaler Binnenmarkt

- Erforderlich ist ein echter digitaler Binnenmarkt mit EU-weit einheitlichen Bedingungen vom Daten- und Verbraucherschutz bis zur Besteuerung, der Europa sehr viel näher an große, homogene Märkte wie die USA und China heranbringen würde. Ziel sollten die Harmonisierung direkter Steuern in der EU und die Schaffung international einheitlicher Regelungen und Maßnahmen gegen die sogenannte Aushöhlung der Steuerbasis und die

Gewinnverlagerung *(Base Erosion and Profit Shifting – BEPS)* sein. International agierende digitale Unternehmen sollten angemessen besteuert werden (etwa im Hinblick auf die Praxis von Gewinnverlagerung mittels konzerninterner Verrechnungspreise).

- Für einen schnellen Ausbau der Digitalinfrastruktur ist eine Deregulierung bei der Preis- und Zugangsregulierung zu Telekommunikationsnetzen erforderlich. Im gleichen Kontext bedarf es einer Harmonisierung der Spektrumspolitik in Europa, d.h. konkret Harmonisierung beim Design der Spektrumsauktionen, der Vergabezeitpunkte sowie der Lizenz-Bedingungen für die Spektrumsnutzung.

- Vor dem Hintergrund immer leistungsfähigerer Datenverarbeitungstechnologien und -geschäftsmodelle brauchen wir vor allem auch eine rasche Anpassung unseres Datenschutzsystems an die Gegebenheiten der globalen Datenökonomie. Für Europa besteht mit der Datenschutzgrundverordnung die große Chance, ein hohes Datenschutzniveau zu sichern und gleichzeitig neue digitale Geschäftsmodelle wie Big Data zu ermöglichen. Eine rasche Verabschiedung der EU-Datenschutzgrundverordnung zwecks Harmonisierung der sehr unterschiedlichen nationalen Bestimmungen ist zwingend erforderlich. Dabei sollten im Entwurf gleichzeitig die Bestimmungen z.B. für die Pseudonymisierung oder Anonymisierung von Daten –überarbeitet werden, um unnötige administrative Hemmnisse abzuschaffen und im Sinne einer anreizorientierten Datenpolitik die Verarbeitung pseudonymer und anonymer Daten zu priorisieren. Sonst werden sich Erfolge bei Industrie 4.0, wo Daten als „Rohstoff der Zukunft“ eine zentrale Rolle spielen, nicht einstellen können. Das gilt für individualisierte Produktion, vorausschauende Wartung bis hin zum autonomen Fahren. Die Wettbewerber, die sich in diesen Märkten etabliert haben und sich zunehmend etablieren, basieren ihr Geschäftsmodell ganz wesentlich auf die Verfügbarkeit großer Datenmengen und deren intelligente Verwertung. Wir müssen aus Europa heraus in der Lage sein, Industriedaten, die einen Verbraucherbezug aufweisen können, auch zukünftig ohne komplizierte bzw. unrealistische Einwilligungsmechanismen nutzen zu können.

- Auch die Datenschutzgrundverordnung wird nur eine Momentaufnahme sein. Daher muss schon heute auch über einen „zukünftigen Gestaltungsrahmen“ der Datenpolitik nachgedacht werden. Gerade das Urteil des EuGH in Sachen Safe Harbor zeigt, dass der Umgang mit Daten an etablierte Systemgrenzen führt und das Nationalstaatlichkeitsprinzip an dieser Stelle neu definiert werden muss.
  Zur Stärkung der Wettbewerbsfähigkeit europäischer Unternehmen sollten EU-weite Datenschutzzertifikate für neue Technologien geschaffen werden, die von Datenschutzbehörden anerkannt und von externen Prüfern angewandt werden. Nach dem Vorbild des EU Cloud-Zertifikats sind weitere Bereiche wie z. B. Industrie 4.0 und Big Data denkbar.

- Bürgernahe europaweite Big Data Leuchtturmprojekte bspw. in den Bereichen personalisierte Medizin oder Smart Cities sollen Aufklärungsarbeit leisten und den Menschen die Möglichkeiten von Big Data näher bringen.

- Eine Studie sollte alle horizontalen und sektoralen Barrieren für den freien Datenfluss (Gesetze, Verordnungen, Praktiken) identifizieren, aus der ein Arbeitsplan für den Abbau unangemessener Barrieren entwickelt werden sollte.

- Einsetzung einer Expertengruppe durch die Bundesregierung, die vor allem bei Datenschutzfragen im Kontext der Datenökonomie Institutionen berät und wichtige Impulse für die Weiterentwicklung des regulatorischen Rahmens gibt.

- Die öffentliche Hand sollte eine Vorreiterrolle einnehmen: Mit einem „Cloud First“ Programm für die öffentliche Verwaltung würden nicht nur Effizienzgewinne eintreten, sondern gleichzeitig ein Schub für die Marktdurchdringung von Cloud-Diensten entstehen.

4.3.2 Innovationsförderung

- Derzeit existierende Forschungs- und Entwicklungsstrukturen erschweren häufig die erforderliche schnelle Umsetzung relevanter Forschungsaktivitäten. Eine im Hinblick auf die Stärkung der digitalen Souveränität orientierte Neugestaltung ist erforderlich. Hierzu gehören insbesondere Maßnahmen, die zu einer Beschleunigung und Neugestaltung von Forschungsprozessen führen können.

- Es müssen innovative Anreizsysteme für eine erfolgreiche Forschungs- und Entwicklungsarbeit geschaffen werden. Damit innovative Unternehmen entstehen und v.a. wachsen können, ist eine im regulatorischen Rahmen (z.B. Steuersystem) institutionalisierte Förderung von Innovationen und Forschungsprojekten erforderlich.

- Steuerliche Förderung von Innovation senkt für Unternehmen die Risiken, die sie mit Forschungs- und Entwicklungsprojekten tragen, insbesondere technologische Unwägbarkeiten und unsichere Marktaussichten. Länder, die Innovationen steuerlich fördern, stoßen damit zusätzliche private Forschungs- und Entwicklungsinvestitionen an. Daher wären EU-weite Steueranreize zu begrüßen; bislang gibt es solche nur in elf Mitgliedsstaaten.

- Die Gründungsphase von Start-ups ist trotz erfolgreichen Bürokratieabbaus nach wie vor zu stark bürokratisiert und reglementiert: Für ein schnelles, internationales Wachstum fehlt teilweise das Geld. Einige Gesetze sind nicht zeitgemäß und verhindern innovative Geschäftsmodelle. Für Start-ups sollten in den ersten vier Jahren ihres Bestehens grundsätzlich wachstumsfördernde Sonderregeln gelten. Sie sollten steuerliche und arbeitsrechtliche Erleichterungen ebenso umfassen wie eine Befreiung von Zwangsmitgliedschaften bei Kammern und Berufsgenossenschaften.

- Das Augenmerk der Förderung von Unternehmen liegt z.T. zu stark auf der Gründungsphase. Für die Wachstumsphase von Unternehmen sowie für Kleine und mittelständische Unternehmen brauchen wir zusätzliche Unterstützung, damit diese Unternehmen (international) wachsen und skalieren bzw. digitalisieren können. Notwendig ist ein attraktiver Rechtsrahmen für potenzielle Investoren und Wagniskapitalgeber, am besten durch ein Wagniskapitalgesetz. Die Veräußerung von Streubesitzanteilen muss weiterhin steuerfrei sein. Außerdem sollte die unterschiedliche steuerliche Behandlung von Eigen- gegenüber Fremdkapitalfinanzierung verringert und eine gezielte Verlustnutzung bei der Beteiligung an innovativen Unternehmen zugelassen werden.

- Eine Initiative „Start-ups Digitale Wirtschaft“ zur Förderung von IKT B2B Start-ups sollte ins Leben gerufen werden. Diese Startups könnten dann lokale Partner für die Digitalisierung der europäischen Industrie werden (Abhängigkeit von Silicon Valley reduzieren) und den Pool für die nächste Generation europäischer Weltmarktführer in der Digitalen Wirtschaft bilden. An der Initiative könnten sich die öffentliche Hand, IKT- und Industrieunternehmen beteiligen.

5. Ausblick

Das vorliegende, zum Nationalen IT-Gipfel 2015 entstandene Papier fasst einige konkrete Maßnahmen und Handlungsempfehlungen zur Stärkung der digitalen Souveränität in Deutschland und Europa zusammen. Sie sind zunächst als Grundlage vertiefender Diskussionen in der Fokusgruppe 1, aber auch in anderen thematisch verwandten oder betroffenen Fokusgruppen zu verstehen. Über den Nationalen IT-Gipfel hinaus kann das Papier darüber hinaus eine wichtige Basis für die Fortentwicklung und Umsetzung der geforderten Maßnahmen sein. Dies gilt nicht nur für eine stetige Verankerung in der nationalen politischen Agenda, sondern v.a. auch auf der europäischen Ebene. Einzelne Bereiche können durch detaillierte, wissenschaftliche Studien weiter vertieft werden. Die Fokusgruppe 1 hat sich zum Ziel gesetzt, weitere Schritte auch zukünftig konstruktiv zu begleiten.

Mitglieder der Fokusgruppe 1

Vorsitzende

Matthias Machnig, Bundesministerium für Wirtschaft und Energie

Dr. Bernhard Rohleder, Bitkom Bundesverband Informationsgesellschaft, Telekommunikation und neue Medien e.V.

Sherpas

Bernd Weismann, Bundesministerium für Wirtschaft und Energie

Dr. Ulrike Engels, Bundesministerium für Wirtschaft und Energie

Björn Siebert, Bitkom Bundesverband Informationsgesellschaft, Telekommunikation und neue Medien e.V.

Dr. Joachim Bühler, Bitkom Bundesverband Informationsgesellschaft, Telekommunikation und neue Medien e.V.

Mitglieder

Oliver Frese, Deutsche Messe AG

Reinhard Clemens, T-Systems International GmbH

Prof. Dr. Helmut Krcmar, Technische Universität München, MÜNCHNER KREIS

Peter Ganten, OSB Alliance – Open Source Business Alliance e.V.

Mike Cosse, SAP AG

Dr. Thomas Endres, VOICE – Verband der IT-Anwender e.V.

Sherpas

Thomas Mosch, Deutsche Messe AG

Dr. Wolfgang Kubink, Deutsche Telekom AG

Thomas Schauf, Deutsche Telekom AG

Thomas Bendig, Fraunhofer-Verbund IuK-Technologie

Isabel Netzband, Fraunhofer-Verbund IuK-Technologie

Pamela Krosta-Hartl, LANCOM Systems

Dr. Rahild Neuburger, Ludwig-Maximilians-Universität München, MÜNCHNER KREIS

Konstantin Böhm, Ancud IT-Beratung GmbH

Dr. Andreas Herschel, SAP AG

Christoph Hecker, VOICE – Verband der IT-Anwender e.V.

Teilnehmer des Expertenworkshops am 22. September 2015 in Berlin

Thomas Bendig, Fraunhofer IuK-Verbund

Peter-J. Bisa, TACTUM GmbH

Konstantin Böhm, Ancud IT-Beratung GmbH

Nils Börnsen, BMWi

Juliane Braun, BMI

Dr. Joachim Bühler, BITKOM

Robert Dehm, BMWi

Dr. Robert Diemer, deep Innovation GmbH

Dr. Thomas Endres, VOICE e.V.

Dr. Ulrike Engels, BMWi

Prof. Mike Friedrichsen, Stuttgart Media University

Teilnehmer des Expertenworkshops am 22. September 2015 in Berlin (Forts.)

Elmar Geese, OSBA
Thomas Götz, IBM Deutschland GmbH
Dr. Andreas Goerdeler, BMWi
Karsten Häcker, Forschungsverbund Berlin e.V.
Christoph Hecker, VOICE e.V.
Dr. Andreas Herschel, SAP SE
Jörg Heuer, Deutsche Telekom AG
Steffen Heyde, ZVEI e.V.
Marco Hoffmann, Nokia Solutions and Networks
Prof. Helmut Krcmar, MÜNCHNER KREIS, TU München
Pamela Krosta-Hartl, LANCOM Systems GmbH
Marta Kujawa, BMWi
Dr. Sicco Lehmann-Brauns, Siemens AG
Dr. Martin Matzke, Atos Deutschland
Jochen Michels, Fujitsu Technology Solutions GmbH
Thomas Mosch, Deutsche Messe AG
Isabel Netzband, Fraunhofer IuK-Verbund
Dr. Rahild Neuburger, MÜNCHNER KREIS, LMU München
Alexander Nouak, Fraunhofer IGD
Martin Olff, The unbelievable Machine Company GmbH
Prof. Torsten Oltmanns, Roland Berger Strategy Consultants GmbH
Juliane Petrich, BITKOM
Dr. Christoph Peylo, Deutsche Telekom AG T-Labs
Dr. Hans-Joachim Popp, Deutsches Zentrum für Luft- und Raumfahrt e.V.
Thomas Schauf, Deutsche Telekom AG
Prof. Martin Schell, Fraunhofer HHI
Dr. Haya Shulman, Fraunhofer SIT
Fabian Schmidt, Software AG
Björn N. Siebert, BITKOM
Prof. Heinz Thielmann, Emphasys GmbH
Prof. Michael Waidner, Fraunhofer SIT
Bernd-Wolfgang Weismann, BMWi
Dr. Malthe Wolf, TNS Deutschland GmbH, D21
Prof. Stefan Wrobel, Fraunhofer IAIS
Torsten Wunderlich, DATEV eG