Ausschuss für Bildung, Forschung und Technikfolgenabschätzung

Deutscher Bundestag

Ausschussdrucksache 18(18)166 d

27.11.2015

Deutsche Akademie der Technikwissenschaften (acatech)

Stellungnahme

Öffentliches Fachgespräch

zum Thema

„Industrie 4.0“

am Mittwoch, 2. Dezember 2015

Stellungnahme zum Fachgespräch zum Thema Industrie 4.0 des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung

2. Dezember 2015, 09:30 – 12:00

Wir stehen heute an der Schwelle zur vierten industriellen Revolution: das Internet der Dinge zieht in die Fabrik, aus Wertschöpfungsketten werden hochflexible Wertschöpfungsnetzwerke. Deutschlands Wirtschaft sollte seine gute Ausgangsposition als „Fabrikausrüster der Welt" nutzen, um diesen Wandel zu gestalten, statt von der Digitalisierung und der Technologie- und Marktentwicklung in den USA, China oder Japan getrieben zu werden.

Vor rund zwei Jahren hat der von acatech koordinierte Arbeitskreis Industrie 4.0 dazu bereits Handlungsempfehlungen für Wirtschaft und Politik vorgelegt, die auch als eine der Beratungsgrundlagen für dieses Fachgespräch dienen. Der Antrag der Fraktionen von CDU / CSU und SPD „Industrie 4.0 und Smart Services – Wirtschafts-, arbeits-, bildungs- und forschungspolitische Maßnahmen für die Digitalisierung und intelligente Vernetzung von Produktions- und Wertschöpfungsketten" (BT-Drucksache 18/6643) greift viele dieser Empfehlungen auf und benennt entscheidende Handlungsfelder für die Sicherung der Wettbewerbsfähigkeit deutscher Unternehmen im digitalen Zeitalter. Nun gilt es, gemeinsam mit allen beteiligten Akteuren die digitale Transformation der Wirtschaft zu gestalten.

Industrie 4.0 beschreibt die Auswirkungen der Digitalisierung aus der Perspektive der Produktionsprozesse. Die nächste, noch größere Herausforderung für Deutschlands Wirtschaft liegt jedoch im datengetriebenen Wandel der Geschäftsmodelle. Dieser Wandel ist disruptiv: Zukünftig stehen nicht mehr Produkte, sondern deren Nutzer im Zentrum der Geschäftsmodelle. Sie stellen sich entsprechend ihrer jeweiligen Bedürfnisse, Vorlieben und Interessen frei, jederzeit und individuell Kombinationen aus Produkten und Dienstleistungen – Smart Services – mittels webbasierter Dienste zusammen. Smart Services erfordern die flexible Vernetzung von Unternehmen unterschiedlicher Größe und deren weitgehend automatisierte Kollaboration in digitalen Ökosystemen. Sie lagern sich an digitale Plattformen an, auf denen Nutzungsdaten von smarten Gegenständen und Nutzerdaten zusammengeführt und zu neuem Wissen verarbeitet werden (Smart Data), das als Grundlage von Smart Services dient.

Mit Unterstützung des Bundesministeriums für Wirtschaft und Energie wird die Deutsche Akademie der Technikwissenschaften im Projekt „Digitale Serviceplattformen" an konkreten Beispielen zeigen, wie bereits heute auf Basis bestehender digitaler Plattformen neue datenbasierte Dienste geschaffen werden. Der Identifikation von Best Practices wird der Aufbau von Living Labs folgen, in denen Firmen aller Branchen die Entwicklung von Smart Services und die Kooperation in Ökosystemen testen und ihre Erfahrungsgewinne teilen können. Zu den Themen „Digitale Bildung und Qualifikation" sowie „Technologische Enabler" wird der Arbeitskreis Smart Service Welt von zwei Expertengruppen beraten.

Der Aufbau digitaler Plattformen ist ein entscheidendes Kriterium für den erfolgreichen Schritt deutscher Unternehmen in die Welt der digitalen Wertschöpfung. Denn diese Plattformen bilden sowohl entscheidende Daten- als auch Kundenschnittstellen. Für deutsche Unternehmen besteht durchaus die Gefahr, dass sich große IT-Firmen zwischen traditionelle Industrieanbieter und deren Kunden

drängen könnten, weil sie auf Basis großer Datenvolumina die Bedürfnisse der Kunden besser kennen und antizipieren als traditionelle Produktanbieter.

Der durch digitale Vernetzung getriebene Wandel in den Strukturen der Wertschöpfung sollte sich auch in einer entsprechenden Gewichtung der dieser Herausforderung in den Haushalten der Ministerien niederschlagen.

Infrastruktur

Eine zentrale Voraussetzung für eine digitalisierte Wirtschaft ist die technische Infrastruktur und damit ein beschleunigter, technologieübergreifender Breitbandausbau. Industrie 4.0 und Smart Services beruhen auf der Vernetzung von Menschen, Dingen und Daten untereinander und mit dem Internet. Objekte und Dienstleistungen erhalten einen digitalen Zwilling, der aus Daten entsteht, die in Echtzeit verknüpft werden. Dazu wird aber eine verzögerungsfreie Datenübertragung mit einem minimalen Verlust an Datenpaketen benötigt. Schwankungen in diesem Bereich könnten zukünftig enorme Kosten verursachen.

Entscheidend ist dabei neben der Flächendeckung die Leistungsfähigkeit der Netze, wobei das deutsche Ausbauziel von 50 Mbit/s für Industrie 4.0-Anwendungen nur ein Etappenziel sein kann und mittelfristig Bandbreiten im Gigabitbereich benötigt werden. Im Jahr 2020 sollen nach Schätzungen der Gartner Group weltweit etwa 50 Milliarden Gegenstände mit dem Internet und miteinander verbunden sein. Die Kommunikation zwischen intelligenten Geräten, von Smartphones bis zu Maschinen in der Industrie, intelligente Verkehrsleitsysteme oder Anwendungen des Internet der Dinge im Medizinischen Bereich verlangen nach deutlich größeren Netzkapazitäten.

In der Diskussion zum Thema 5G wird deutlich, dass die neue Generation mobiler Netze insbesondere die Kommunikation von Geräten und die Einbindung von Sensoren smarter Objekte vorsieht und damit über die heutigen Anwendungsmöglichkeiten weit hinausgeht. Darüber hinaus soll der neue Standard hohe Flexibilität besitzen. Netzkapazitäten können dynamisch und intelligent gemanagt und zugewiesen werden: entsprechend der Nachfrage, des Kontextes und nahezu in Echtzeit. Das ermöglicht die technische Garantie von festzulegenden Latenzzeiten für unterschiedliche Domänen wie Energie, Gesundheit oder Verkehr. Sie sind eine Grundvoraussetzung, damit die Datenanalyse und die darauf basierenden Dienstleistungen zuverlässig erbracht werden können. Netzbetreiber sollten Qualitätsdienste mit garantierten Leistungsmerkmalen anbieten dürfen und ein differenziertes Netzmanagement muss möglich bleiben.

Sicherheits- und systemkritische Dienste, etwa in der Flugüberwachung oder im Katastrophenschutz sind auf garantierte Übertragungsraten angewiesen. Deshalb sind die Regeln zur Netznutzung von großer Bedeutung. Das Prinzip der Netzneutralität ist ein hohes Gut. Andererseits wird für bestimmte Dienste und Anwendungsbereiche, etwa für den hochautomatisierten Straßenverkehr, eine garantierte Übertragungsqualität benötigt. Hier müsste differenziert werden: Nicht jede Anwendung und jeder Dienst benötigt die größtmögliche Bandbreite und andererseits darf niemand ausgebremst werden. Eine Mindestgeschwindigkeit für den diskriminierungsfreien Zugang auf alle (legalen) webbasierten Inhalte und Dienste könnte als Ziel des Netzausbaus verankert werden. Höhere Übertragungsraten könnten für Dienste ermöglicht werden, die diese wirklich brauchen. Daraus resultierende zusätzliche Einnahmen sollten verbindlich in den Netzausbau fließen, damit kein Fehlanreiz zugunsten einer langsamen Grundversorgung entsteht.

Die Industrie sollte sich frühzeitig auf einen offenen, globalen Standard für 5G verständigen. Die Politik sollte die nächste Generation des Mobilfunks durch Frequenzvergabe, Forschungsförderung und die Unterstützung internationaler Standardisierung vorantreiben.

Schlüsseltechnologien

Um Deutschland zum Leitanbieter und Leitmarkt für Industrie 4.0-Anwendungen zu entwickeln und die digitale Wettbewerbsfähigkeit zu stärken, gilt es, die Förderung von Schlüsseltechnologien entsprechend zu gestalten.

Mikroelektronik ist eine Schlüsseltechnologie für die digitalisierte Wirtschaft, da mikroelektronische Bauteile in nahezu jedem Elektro- und IT-Produkt eingebunden sind. Unterschieden werden in der Regel „More Moore"-Technologien (MM), die auf einer stetigen Verkleinerung der Chip-Strukturen basieren und „More than Moore"-Technologien (MtM), bei denen die Funktionalität der Mikrochips wächst. Deutsche Anbieter sind im Bereich von MtM-Technologien zum Teil führend. Jedoch wird die großvolumige (More Moore) Halbleiterfertigung von US-amerikanischen und asiatischen Unternehmen dominiert. Deshalb sollte weiterhin in neue Chip-Funktionalitäten (More than Moore) und frühzeitig in Beyond Moore-Technologien investiert werden, die auf Materialien jenseits von Silizium basieren. Darüber hinaus sollte bei MM-Technologien auf den Erhalt und die Weiterentwicklung der Designfähigkeit fokussiert werden, während bei komplexen und spezialisierten Produkten (MtM) das Ziel sein sollte, die Technologieführerschaft auszubauen und abzusichern.

Im Bereich *Software* liegen die Stärken Deutschlands im B2B-Bereich und in einer leistungsfähigen Forschungslandschaft: bei eingebetteten Systemen, Unternehmenssoftware, Big Data Analytics und semantischen Technologien. Schwächen zeigen sich vor allem im B2C-Bereich: bei Internettechnologien, Betriebssystemen und digitalen Geschäftsmodellen. Zukünftig gilt es, Kompetenzen in den Bereichen Cloud Computing, Big Data Analytics und Echtzeit-Algorithmik auf- bzw. auszubauen und die Schaffung sicherer software-definierter Plattformen zu fördern, die es insbesondere auch kleinen und mittleren Unternehmen (KMU) ermöglichen, digitale Geschäftsmodelle aufzubauen. Allgemein sind Kompetenzen im Softwarebereich von entscheidender Bedeutung für die digitale Transformation der deutschen Wirtschaft. Die Leitanbieterschaft bei strategisch wichtigen Elementen der Wertschöpfung, insbesondere den Engineering- und Systemintegrationsleistungen im Bereich digitaler Plattformen sollte deshalb gesichert werden.

Eine *neue Generation autonomer Systeme* kann in einer alternden Gesellschaft dazu beitragen, gesellschaftliche und wirtschaftliche Herausforderungen in den Innovationsfeldern Mobilität, Produktion und Logistik, Sicherheit, Pflege und Wohnen langfristig zu lösen. Autonome Systeme können komplexe Aufgaben lösen, eigene Entscheidungen treffen und sich in unstrukturierten Umgebungen zurechtfinden, weil sie auf unvorhersehbare Ereignisse reagieren können. Sie unterstützen beispielsweise die Menschen in ihrem Wohnumfeld: Intelligente Assistenzsysteme im Haushalt Patienten und älteren Menschen, in ihrem gewohnten Umfeld zu bleiben. Hebe- und Traghilfen entlasten das Pflegepersonal und intelligente Softwaresysteme nehmen Routineaufgaben der Verwaltung und Aktenführung ab. Robotern in Produktionshallen entwickeln sich von riesigen Maschinen, die nur eine ganz bestimmte Aufgabe abarbeiten, zu flexiblen Helfern. Autonome Systeme könnten auch in menschendfeindlichen Umgebungen agieren und etwa beim Rückbau von Atomkraftwerken unterstützen. Im Fachforum Autonome Systeme innerhalb des Hightech Forums der Bundesregierung erarbeiten derzeit über 60 Expertinnen und Experten aus Wissenschaft, Wirtschaft und Zivilgesell-

schaft Empfehlungen und Anwendungsbeispiele zur Technologieentwicklung im Bereich autonomer Systeme sowie Vorschläge für die Gestaltung gesellschaftlicher und rechtlicher Rahmenbedingungen.
Entscheidend für die Akzeptanz autonomer Systeme durch ihre menschlichen Nutzer ist die *Gestaltung der Mensch-Maschine-Interaktion (MMI)*. Durch eine frühzeitige Integration der Nutzer, bereits in der Phase der Entwicklung der MMI-Technologien, kann die Akzeptanz für diese Anwendungen wesentlich erhöht werden. Neben der ebenso notwendigen öffentlichen Debatte ist für die Akzeptanz neue MMI-Technologien vor allem auch deren Nutzerzentrierung (Stichwort Usability) entscheidend.

Eine Schlüsseltechnologie für die Realisierung autonomer Systeme und die Gestaltung der MMI ist das *Maschinelle Lernen* (ML). ML-Technologien bilden die Voraussetzung dafür, dass intelligente Systeme direkt aus eingehenden Reizen lernen und sich so auf verschiedenste Situationen einstellen können. Lernende Maschinen passen sich auch an die Bedürfnisse und individuellen Fähigkeiten der Nutzer an. Zwar hat sich der Bedarf an ML-Experten in den letzten Jahren international stark erhöht, doch Forschungs- und Ausbildungskapazitäten wurden überwiegend in den USA erweitert, deren Unternehmen zudem auch Spezialisten vom deutschen Arbeitsmarkt abwerben. Das Forschungsgebiet des Maschinellen Lernens sollte in Deutschland gestärkt und Maßnahmen getroffen werden, um den Zugang zu wissenschaftlichem Nachwuchs aus diesem Feld zu verbessern.

Weltweit werden für das Marktvolumen von MMI-Technologien meist zweistellige Wachstumsraten prognostiziert. Wichtige Anwendungsfelder mit hohen Marktpotenzialen für intelligente autonome Systeme und MMI-Technologien sind der Gesundheitssektor (Weltweites Marktvolumen von deutlich mehr als 200 Mrd. US-Dollar im Jahr 2020), das automatisierte Fahren (Wertschöpfung am Standort Deutschland im Bereich der Fahrerassistenzsysteme im Jahr 2025: 8,4 Mrd. Euro) und die Produktion bzw. der Bereich Industrie 4.0 (270 Mrd. Euro bis 2025).
Zwar verfügt Deutschland auch in diesen Bereichen über eine gute Ausgangsposition, um an der globalen Entwicklung von MMI-Technologien teilzuhaben. Allerdings sollten die vorhandenen Kompetenzen besser vernetzt und in Leuchtturmprojekten gebündelt werden, die Experimentierräume zur Verfügung stellen und sich gut in die bestehende Förderlandschaft integrieren lassen. Diese Räume würden dazu beitragen, Ergebnisse aus der Forschung schneller in Innovationen zu überführen. Entscheidend ist zudem, nicht allein in einzelnen MMI-Technologiefeldern Kompetenzen auszubauen, sondern diese miteinander zu verknüpfen.

Datenpolitik

Bereits heute besteht das Internet der Dinge aus ca. 15 Milliarden vernetzten Objekten. Bis 2050 wird ein Anstieg auf 50 Milliarden Objekte erwartet. Die von diesen Objekten erhobenen Produkt- und Kundendaten werden zur Grundlage neuer Geschäftsmodelle und Smart Services. Diese Geschäftsmodelle stehen in einem Spannungsfeld: Sie sind ohne Informationen über die Kunden nicht zu erbringen und andererseits muss der grundrechtlich verbriefte Schutz sensibler und personenbezogener Daten gewährleistet sein.

Unser heutiges Datenschutzrecht wird jedoch in vielen Teilen der Wirklichkeit global entgrenzter Datenverarbeitung nicht mehr gerecht. Ein wichtiger Schritt, die Unsicherheit, die durch die unterschiedliche Auslegung des Datenschutzrechts in unterschiedlichen EU-Staaten entsteht, zu beseitigen ist die EU-weite Harmonisierung des Datenschutzrechts durch die EU-Datenschutzgrundverordnung. Doch sie muss auch einheitlich ausgelegt und effektiv durchgesetzt werden. ´

Auch der personenbezogene Rahmen des Datenschutzrechts bildet nicht mehr alle wettbewerbspolitischen Implikationen der Fragen nach den Eigentums- und Nutzungsrechten an Daten ab. Es existiert Rechtsunsicherheit beim Einsatz und gerade auch dem unternehmensübergreifenden Austausch von Daten, die besonders bei Start-ups und KMU als ein zentrales Hindernis für die Entwicklung innovativer Geschäftsmodelle angesehen werden.

Datenpolitik muss grundrechtliche Positionen (Recht auf informationelle Selbstbestimmung) ebenso schützen wie sie die Nutzung von Daten für Innovationen und datengetriebene Geschäftsmodelle ermöglicht. Dabei kann auch die Technik selbst als Steuerungsinstrument berücksichtigt und über Anreizsysteme gefördert werden: Datensets können etwa in Silos abgegrenzt oder durch Firewalls separiert werden. Ebenso können Pseudonymisierung, abgestufte Zugriffsberechtigungen und Verschlüsselungsmethoden eingesetzt werden.

Auch Informationen, die öffentliche Stellen erheben, können zur Grundlage innovativer Geschäftsmodelle werden („Open Data“), wenn sie für die private und wirtschaftliche Nutzung weiterverwendet werden dürfen.

Wandel der Arbeitswelt und Aus- und Weiterbildung

Die digitale Vernetzung hat weitereichende Implikationen für die Arbeitswelt und die Beschäftigten. Technologische Entwicklungen sind dabei stets in den gesellschaftlichen Kontext eingebettet. Deshalb müssen auch die gesellschaftliche Perspektive auf die digitale Transformation in die Entwicklung einbezogen und Arbeitswelten als sozio-technische Systeme konzipiert werden.

Der Schlüssel, um die Wachstumspotenziale durch Industrie 4.0 und Smart Services zu heben sind verstärkte Anstrengungen in der Aus- und Weiterbildung. Dabei bestehen jedoch erhebliche Unterschiede zwischen KMU und Großunternehmen hinsichtlich der Kompetenzbedarfe und den Anforderungen für die Qualifizierung von Mitarbeiterinnen und Mitarbeitern.

Zentrale Kompetenzen werden dabei zukünftig nicht allein aus IT-Bereich benötigt. Kommunikative Fähigkeiten und Kompetenzen wie Teamfähigkeit, Selbstorganisation und Systemverständnis sowie lebenslanges Lernen werden zur gewinnen ebenso an Bedeutung. Grundkenntnisse der Datenverarbeitung, das Arbeiten in virtuellen Räumen und die Nutzung digitaler Assistenzsysteme gehören zu den neuen Qualifikationsanforderungen. Interdisziplinäre Kompetenzen müssen gestärkt und IT-Kompetenzen zunehmend vermittelt werden.

Bisher stehen in Unternehmen kaum spezifische Aus- und Weiterbildungsangebote für Industrie 4.0 zur Verfügung, wobei in Großunternehmen mehr Angebote als in KMU vorhanden sind. Einzelne Teilaspekte des digitalen Wandels sind jedoch, wenn auch meist unsystematisch, bereits als Lehrinhalte in bestehende Programme integriert. Wichtig sind deshalb insbesondere ein Ausbau spezifischer Aus- und Weiterbildungsangebote sowie eine stärkere Integration und Ausrichtung bestehender Angebote auf Industrie 4.0.

Auch die Durchlässigkeit zwischen beruflicher und akademischer Bildung sollte gefördert werden. Eine Möglichkeit ist der Ausbau dualer Studiengänge, die durch die Verknüpfung zweier Lernorte –

Hochschule und Betrieb – eine der stärksten institutionellen Abschottungen unseres Bildungssystems überwinden. Es kann reguläre Studiengänge insbesondere dort ergänzen, wo sie auf betriebliche Tätigkeitsfelder zugeschnitten sind. Notwendig sind jedoch übergreifende Qualitätskriterien und -standards, die sicherstellen, dass Studienabschlüsse aussagekräftig und vergleichbar sind.

Dabei muss berücksichtigt werden, dass sich auch der Prozess des Lehrens und Lernens selbst verändern wird. Aus- und Weiterbildung wird zunehmend am Arbeitsplatz und personalisiert stattfinden, wobei digitale Hilfsmittel und Bildungsangebote genutzt werden. Bisher existiert jedoch eine Dominanz traditioneller Instrumente, wie etwa die Durchführung in- und externer Präsenzveranstaltungen. Deshalb sollte die Vermittlung von Digitalisierungswissen mittels digitaler Methoden, die von den Mitarbeiterinnen und Mitarbeitern flexibel genutzt werden können, gestärkt werden und traditionelle Instrumente sinnvoll ergänzen. Dazu gehören etwa digitale Lernplattformen oder Massive Open Online Courses.

Die Deutsche Akademie der Technikwissenschaften identifiziert derzeit in Kooperation mit dem Fraunhofer-Institut für Materialfluss und Logistik und der equeo GmbH in einer vom Bundesministerium für Bildung und Forschung geförderten Kompetenzentwicklungsstudie Industrie 4.0 Qualifikationsbedarfe von Unternehmen – vor allem kleiner und mittlerer Betriebe. Dabei steht insbesondere die Frage im Vordergrund, wie künftig ein übergreifender und branchenspezifischer Wissenstransfer sowie die nicht-formale Weiterbildung organisiert werden kann. Die Ergebnisse und Handlungsempfehlungen der Projektgruppe werden von acatech voraussichtlich zur Hannover Messe 2016 veröffentlicht und dokumentiert.

Sicherheit

Industrie 4.0 und Smart Services erfordern die komplexe Vernetzung einer Vielzahl von dezentralen Komponenten über das Internet. Diese tauschen große Mengen von Daten aus, darunter teils sensible Nutzerdaten. Mit der fortschreitenden Vernetzung vermehren sich zudem die potentiellen Angriffspunkte, etwa für Hacker. Damit werden die IT-Sicherheit und Datenschutz zu zentralen Voraussetzungen für die vernetzte Produktion und datengetriebene Geschäftsmodelle. Gerade KMU müssen sich darauf verlassen können, dass Sie im Zuge der zunehmenden Vernetzung sowie der unternehmens- und branchenübergreifenden Kooperation in digitalen Ökosystemen und auf digitalen Plattformen ihr oftmals sehr spezialisiertes Know-How nicht im Zuge von Hackerangriffen oder an Konkurrenten verlieren und dass nur bestimmte Daten zum wechselseitigen Nutzen geteilt werden.

Für Industrie 4.0 und Smart Services muss über alle Ebenen – von der technischen Infrastruktur über die vernetzten Objekte bis hin zu den digitalen Plattformen – eine durchgängige und nahtlose Sicherheitsarchitektur entstehen. Denn eine Lücke auf einer der Ebenen würde das gesamte Angebot korrumpieren, der Endkunde würde das notwendige Vertrauen verlieren. Von der Hardware über die Firmware und die Software bis hin zur mobilen Kommunikation und den Cloud-Diensten muss ein lückenloses Sicherheitsmanagement mit proaktiven Abwehrmechanismen etabliert werden. Eine reine Endpunkt-Sicherheit reicht nicht aus. Ein besonderer Fokus der Sicherheitskonzepte muss dabei auf den digitalen Plattformen liegen, denn hier befinden sich die Schnittstellen zu externen Nutzern.

Entscheidend ist dabei, dass „Security by design“ als Entwurfsprinzip etabliert wird und IT-Sicherheitskonzepte, -architekturen und -standards entwickelt und etabliert werden, die ein hohes Maß an Vertraulichkeit, Integrität und Verfügbarkeit herstellen. Dabei muss sowohl die Angriffssicherheit als auch die funktionale Sicherheit gewährleistet sein.

In einer zunehmend vernetzen Welt sollte zudem ein realistisches Bild der IT-Sicherheit vermittelt werden, um etwa Kundenängste zu vermeiden. So kann zwar ein sehr hoher, aber nie perfekter Sicherheitsgrad erreicht werden, weil sich auch die Angriffe ständig ändern. In einigen Industriezweigen wie dem Maschinen- und Anlagenbau relativer Sicherheit bereits etabliert werden, auch da hohe Standards oftmals gesetzlich vorgeschrieben sind.

Im Zuge der sich schnell ändernden Rahmenbedingungen werden neue proaktive Sicherheitssysteme benötigt, die in der Forschung bereits vorangetrieben, aber noch nicht in die Praxis gebracht worden sind. Aufgrund der unausweichlichen Relativität von Sicherheit ist die IT-Infrastruktur zumindest in den kritischen Bereichen nicht nur sicher, sondern resilient auszulegen.

Die Verfügbarkeit kritischer Infrastrukturen hat eine zunehmend zentrale Bedeutung für die Wertschöpfung. Mit dem IT-Sicherheitsgesetz hat die Bundesregierung einen Ordnungsrahmen verabschiedet, der zur weiteren Erhöhung der IT-Sicherheit dieser Infrastrukturen beiträgt. Aufgrund deren räumlicher Ausdehnung und Verteilung sind sie für Angriffe besonders verwundbar und es werden oftmals hohe Investitionen für entsprechende Sicherungsmaßnahmen erforderlich. Daher sollten Methoden entwickelt werden, die eine Bewertung und Verbesserung der Effizienz von Sicherheitsmaßnahmen erlauben.

Angriffe erfolgen nur, solange sie sich für Angreifer lohnen. Neben der Entwicklung von entsprechenden Sicherheitstechnologien ist es deshalb sinnvoll, die Transaktionskosten für Angreifer zu maximieren, sodass sich Cyberangriffe nicht mehr lohnen, obwohl sie weiterhin technisch möglich sind. Zu den betriebs- und volkswirtschaftlichen Wirkzusammenhängen der organisierten Cyberkriminalität steht die Forschung noch am Anfang. Dieses Wissen ist jedoch grundlegend für nachhaltige Abwehrmechanismen, denn Angriffe lassen sich wirksam reduzieren, wenn die hinter den Attacken stehenden „Geschäftsmodelle“ – und insbesondere die Monetisierung der erbeuteten Daten – unterbunden werden können.

Industrie 4.0 und Smart Services werden nicht ohne Cloud Computing-Infrastrukturen auskommen. Vertrauen in solche Lösungen könnte insbesondere durch Zertifizierung, vor allem von Backdoor-freien Lösungen, geschaffen werden. So gibt es erste Initiativen, die von der Selbsterklärung und -verpflichtung über den Ansatz „Sicherheit made in Germany“ bis zu entsprechenden Zertifizierungsstellen reichen. Im EU-Kontext kann dadurch ein Wettbewerbsvorteil entstehen, im US-Markt herrscht dagegen noch die Backdoor-Pflicht vor. Heutige Ansätze, vertrauenswürdige Cloud-Services nur alle zwei bis drei Jahre zu zertifizieren, sind aufgrund der ständigen Veränderungen nicht ausreichend. Mit dem Technologieprogramm „Trusted Cloud“ nimmt sich das BMWi der Frage an, wie das für die Smart Service Welt wichtige Vertrauen in Cloud-Dienste insbesondere im Mittelstand (wieder-)gewonnen werden kann.

In den drei vom BMBF geförderten Kompetenzzentren zur Sicherheit CISPA (Saarbrücken), EC Spride (Darmstadt) und KASTEL (Karlsruhe) werden langfristige Strategien der IT-Sicherheit entwi-

ckelt und zugehörige Forschungsprojekte durchgeführt. Allerdings sollten die Kompetenzzentren noch besser vernetzt und deren Expertise gebündelt werden.

Die Bekämpfung von Cyberkriminalität wird in der Industrie 4.0 und Smart Service Welt eine Daueraufgabe sein, die nicht alleine Forschungs- und Kompetenzzentren oder klassische Behörden bewältigen können. Der Aufbau von Fachdienststellen als operative Sicherheitszentren ist dafür ein erster wichtiger Schritt. Sie können auf Grundlage der jeweils neuesten Forschungsergebnisse aktiv Angriffe gegen kritische Infrastrukturen des Staates und der Wirtschaft abwehren und Cyberkriminelle der Strafverfolgung zuführen. Deutschland sollte seine effizienten und zivilen Überwachungs- und Abwehrzentren für Cyberattacken ausbauen, wie sie bspw. in den USA und Japan schon operativ tätig sind.

Ausblick

Mit der digitalen Agenda und ihrer Hightech-Strategie hat die Bundesregierung zentrale Handlungsfelder und Schwerpunkte definiert, um Deutschland zu einem digitalen Wachstumsland zu entwickeln und die Bürgerinnen und Bürger und die deutsche Wirtschaft auf die digitale Transformation unserer Gesellschaft und Wertschöpfung vorzubereiten. Einige darauf basierende konkrete Maßnahmen und Programme wie der Technologiewettbewerb Smart Service Welt des BMWi wurden bereits umgesetzt, doch es gilt auch zukünftig die digitale Agenda und Hightech-Strategie mit weiteren konkreten Maßnahmen zu unterlegen und eine entsprechende Mittelallokation einzuleiten.