griephan Edition

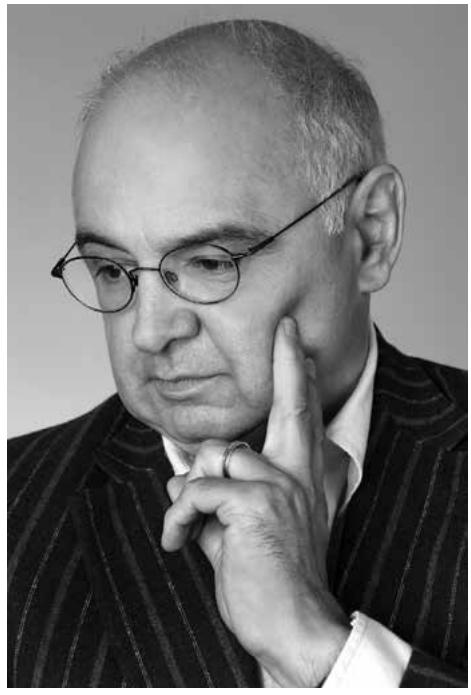
01 | 2015
www.griephan.de

TECHNOLOGISCHE SOUVERÄNITÄT IN DER WIRTSCHAFT

Eine Kooperation DVV | griephan und
dem Bundesverband der Deutschen Industrie (BDI)

BDI

TECHNOLOGIE & SOUVERÄNITÄT – EIN SPANNUNGSFELD



Mit dieser Ausgabe der griephan Edition setzen wir die bewährte Zusammenarbeit mit dem Bundesverband der Deutschen Industrie (BDI) fort. Wieviel Abhängigkeit von Schlüsseltechnologien außerhalb der eigenen Grenzen kann sich ein Industrieland angesichts der Globalisierung leisten? Diese Frage müssen alle entwickelten Länder beantworten. Und Berlin ist besonders gefordert, schließlich ist der hohe Bindungsgrad deutscher Unternehmen in internationalen Wertschöpfungsketten ein Wesenskern des erfolgreichen deutschen Wirtschaftsmodells.

Wir haben mit Gewinn die nachfolgenden Thesen des BDI gelesen. Es geht um Grundsätzliches! Ein offenes Welthandelssystem – konkret der freie Zugang zu Beschaffungs- und Absatzmärkte sowie sichere Handelsrouten – ist maßgeblich für den wirtschaftlichen Erfolg. Daher dürfen die Verhandlungen über ein Transatlantisches Freihandels- und Investitionsabkommen (TTIP) sowie das pazifische Pendant nicht wegen Partikularinteressen scheitern. Wer die Standards setzt, schafft Märkte!

Eine grundsätzliche Erkenntnis nehmen wir nach der Lektüre der verschiedenen Beiträge aus den Reihen des BDI mit: Souveränität ist nicht gleichzusetzen mit Autarkie! Dies ist ein gewichtiges Argument, das einer Abschottung der heimischen Märkte und der Zementierung nationaler Technologien energischen in den Weg tritt. Es besteht die Versuchung, sich mit Hinweis auf technologische Souveränität in die nationale Wagenburg zurückzuziehen. Für Beispiele muss man nicht weit Ausschau halten.

Genau das Gegenteil ist vonnöten: Die Definition nationaler Interessen gepaart mit der Fähigkeit ausgesuchter nationaler Industriepartner zur Technologieabschätzung bilden das Fundament für die Systemfähigkeit: das detaillierte Verständnis der Prozesse und des Gesamtsystems. Auf dieser Grundlage ist dann – minimalistisch und im Dialog zwischen Politik und Wirtschaft – zu entscheiden, welche technologischen Kernfähigkeiten für die nationale Souveränität zu erhalten und zu fördern sind. Minimalistisch, da auch hier gilt: Wer alles verteidigt, verteidigt nichts! Diese Erkenntnis hat angesichts der Globalisierung an Bedeutung gewonnen. Der Dialog über die technologische Souveränität in der Wirtschaft muss in Deutschland geführt werden; andere werden diesen Dialog aufmerksam beobachten.

Heinz Schulte
Chefredakteur
DVV I griephan

griephan Edition ist eine unregelmäßig erscheinende Sonderpublikation von griephan.

Verlag
DVV Media Group GmbH I griephan
Postfach 101609, D-20010 Hamburg
Nordkanalstr. 36, D-20097 Hamburg
www.dvvmedia.com I www.griephan.de
Martin Weber (Geschäftsführer)
Detlev K. Suchanek (Verlagsleiter)

Redaktion
Heinz Schulte (verantw.)
Anna Sturm
E-Mail: anna.sturm@dvvmedia.com

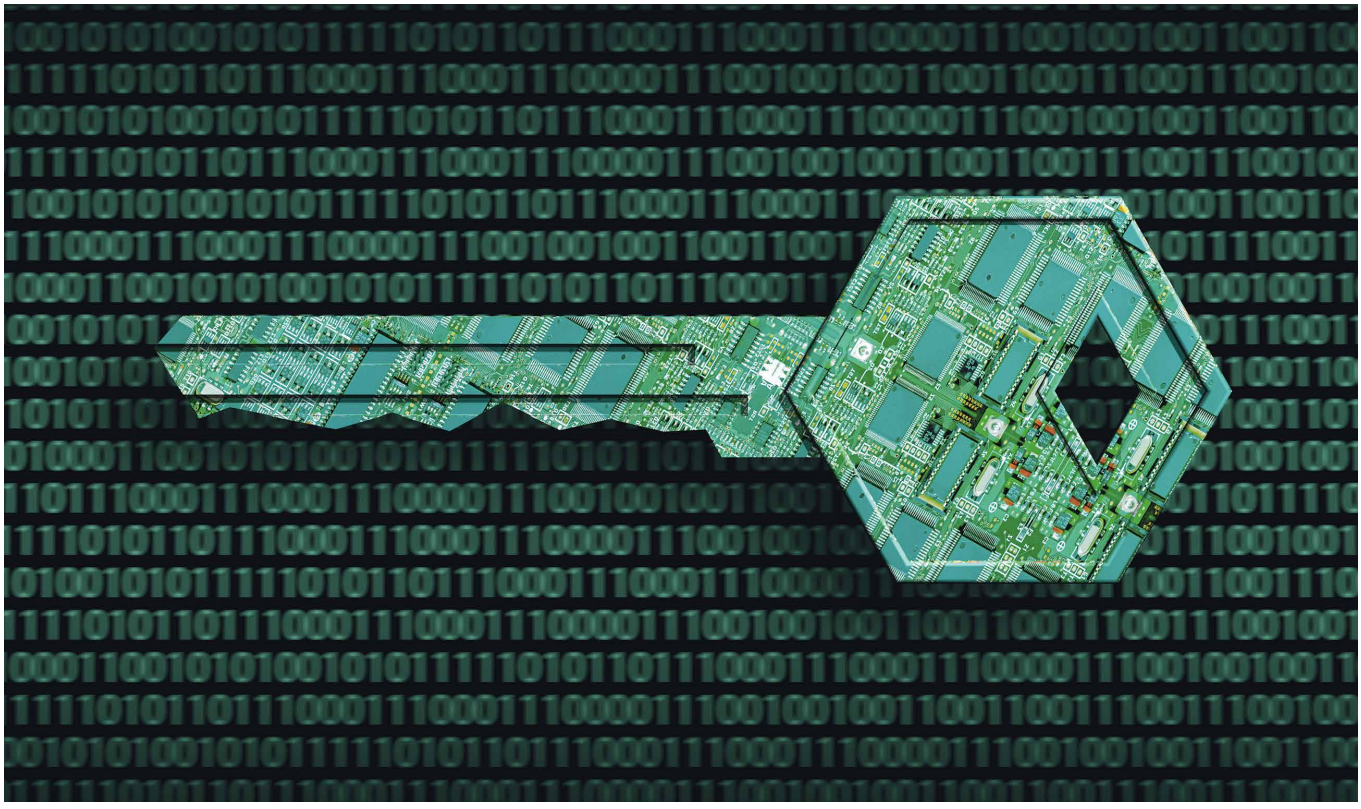
Anzeigen
Nadine Querfurth (Anzeigenleitung)
Dr. Uwe Wehrstedt (Anzeigenverkauf)
E-Mail: wehrstedt@griephan.de

Vertrieb
Markus Kukuk (Vertriebsleitung)

Druck
TZ-Verlag, Roßdorf

Sicherheitstechnologische Souveränität: Innovation, Kompetenz, Wettbewerbsfähigkeit

Ein Eckpunktepapier des Bundesverbandes der Deutschen Industrie (BDI).



DEUTSCHLAND ALS GLOBALISIERUNGSGEWINNER Das Industrieland Deutschland ist eine der führenden Handelsnationen der Welt. 50 Prozent seines Bruttoinlandsprodukts (BIP) und rund ein Viertel seiner Arbeitsplätze hängen unmittelbar vom Außenhandel ab. Sein wirtschaftlicher Erfolg basiert im Wesentlichen auf drei wechselseitig miteinander verflochtenen Faktoren:

Den ersten Faktor bildet die hohe Innovationskraft deutscher Unternehmen – von großen Systemhäusern bis hin zu mittelständischen Zulieferern. Diese investierten laut dem Stifterverband der deutschen Wirtschaft in 2013 67,5 Mrd € in neue Technologien und Prozesse – in enger Zusammenarbeit mit nationalen wie internationalen Forschungsinfrastrukturen.

Laut BDI-Innovationsindikator gehört Deutschland damit zu den sechs innovativsten Volkswirtschaften der Welt. Dies spiegelt sich auch in der Tatsache wider, dass international von den rund 3.000 in ihren Technologienfeldern führenden Mittelständlern, sogenannte Hidden Champions, die Hälfte aus Deutschland kommen.

Der hohe Einbindungsgrad deutscher Unternehmen in internationale Wertschöpfungsketten – also die Entwicklung, Herstellung und Vertrieb von Gütern aller Art in weltweiter Arbeitsteilung – stellt den zweiten Faktor dar. Der hohe Bestand an deutschen Auslandsinvestitionen in Höhe von 1,2 Bn € in 2013 sowie der Rekordwert von 76 Prozent der deutschen Außenhandelsquote (Anteil der Ex- und Importe am BIP) verdeutlichen dies eindrucksvoll.

Schließlich ist ein offenes Welthandelssystem, das einen möglichst freien Zugang zu

Beschaffungs- und Absatzmärkten sowie sichere Handels- und Transportrouten gewährleistet, der dritte maßgebliche Faktor für den ökonomischen Erfolg des Industrielands Deutschland. Es ist eine politische Rahmenvoraussetzung für die beiden erst genannten Punkte. Jeder dieser Faktoren wird zudem durch neue Technologien begünstigt und getrieben. Insbesondere die voranschreitende Digitalisierung birgt die große Chance, Wirtschaftsprozesse künftig noch schneller, innovativer und effizienter rund um den Globus miteinander vernetzen zu können.

NEUE GLOBALE SICHERHEITSHERAUSFORDERUNGEN Jeder dieser Erfolgsfaktoren ist jedoch mit einer Vielzahl von Sicherheitsherausforderungen verbunden. So weckt die Innovationskraft deutscher Unternehmen bei Wettbewerbern, der organisierten Kriminalität und Drittstaaten Begehrlichkeiten. Laut Bundesregierung steht die deutsche Wirtschaft im Fokus internationaler Wirtschaftsspionage, Sabotage und -kriminalität. Die Akteure kombinieren dabei meist digitale und nicht-digitale Angriffswege. Die Schäden erreichen laut einer jüngsten KPMG-Studie Ausmaße von über 80 Mrd € jährlich.
Die Zunahme dieser vielschichtigen und komplexen Sicherheitsherausforderungen ist auch ein Resultat von Destabilisierungsprozessen der bisherigen, durch westliche Wertesysteme geprägten Weltordnung.
Der Krisengürtel von West- und Nordafrika über den Nahen und Mittleren Osten, die Ukraine und Russland bis nach Südostasien ist mittelfristig kaum für Europa und seine Verbündeten einzudämmen. Die Instabilität der betroffenen Regionen hat massive Folgen: Fehlende Staatlichkeit befördert Terrorismus und Kriminalität. Wirtschaftliches Handeln ist dort immer weniger möglich. Armut und Unsicherheit verursachen eine der größten Flüchtlings- und Migrationswellen der vergangenen Jahrzehnte. Gleichzeitig werden wichtige globale Handels- und Logistikrouten durch die Folgen dieser Krisen bedroht.
Hinzu kommen Gestaltungsansprüche von wirtschaftlich rasant aufsteigenden Schwellenländern wie China oder Indien. Diese fordern eine Mitgestaltung der internationalen Ordnung. Dabei setzen diese Staaten neben wirtschaftlicher vor allem auch auf militärische Stärke, um ihrem Status und – nicht nur regionalen – Machtansprüchen Nachdruck zu verleihen.
Dies geschieht zu einer Zeit, in der die bisherige globale Ordnungsmacht, die USA, die Grenzen ihrer militärischen Möglichkeiten und Einflussnahme realisieren – NATO und EU jedoch weder den Willen noch die Strukturen aufweisen, die sich auftuende machtpolitische Lücke zu füllen.
Es liegt im sicherheitspolitischen Kerninteresse Deutschlands, gemeinsam mit seinen Bündnispartnern in EU und NATO sich selbst und die freie Weltordnung gegen diese Herausforderungen zu schützen.
Wie dies geschehen könnte, ist Gegenstand unterschiedlichster Diskussionen und Konzepte. Die inhaltliche Bandbreite ist groß: Mögliche militärische Einsatzszenarien von Streit- und Sicherheitskräften spielen dabei ebenso eine Rolle, wie die Fragen des zivilen Eigenschutzes gegen Ausspähung und Sabotage für Unternehmen, Bürger und vor allem kritische Infrastrukturen.

SICHERHEITSTECHNOLOGISCHE SOUVERÄNITÄT – EINE DEFINITION Unbeantwortet bleibt jedoch die Frage, welche politische Bedeutung der nationalen Verfügbarkeit und der Beherrschbarkeit von Sicherheitstechnologien im zivilen wie militärischen Bereich zukommt – im Sinne einer „sicherheitstechnologischen Souveränität".
Der Begriff der Souveränität ist dabei strikt abzugrenzen von Autarkie. Letztere würde bedeuten, dass eine Versorgung mit Sicherheitstechnologien ausschließlich mit eigenen Angeboten und eigenen Ressourcen erfolgt – also über einen national oder regional abgeschotteten Markt. Dies ist angesichts einer global vernetzen Welt weder zu erreichen noch anzustreben.
Ein sicherheitstechnologisch souveränes Deutschland und Europa sind aus Sicht des BDI durch die folgenden zwei Merkmale gekennzeichnet:
Erstens: Die Industrie muss über eigene Fähigkeiten auf internationalem Spitzenniveau bei der (Weiter)-Entwicklung und Herstellung sicherheitsrelevanter Schlüsseltechnologien, damit verbundener Services und Plattformen verfügen.
Zweitens: Es muss die Kompetenz bei Staat und Industrie vorliegen, Alternativangebote von Dritten selbstbestimmt hinsichtlich ihrer Leistungsfähigkeit, Integrität, Vertraulich- und Verfügbarkeit zu bewerten, auszuwählen und verantwortungsvoll einsetzen zu können.
Beide Merkmale erfordern eine grundlegende „Systemfähigkeit" – also das detaillierte Verständnis technischer Prozesse in den einzelnen Komponenten und deren Zusammenwirken als Gesamtsystem.
Vor diesem Hintergrund versteht der BDI unter der Sicherheitstechnologischen Souveränität die Fähigkeit des Industrielands Deutschland, selbstbestimmt über die Herstellung, die Weiterentwicklung und die Anwendung von Schlüsseltechnologien, Services und Plattformen entscheiden zu können.

SICHERHEITSTECHNOLOGISCHE SOUVERÄNITÄT ALS UMFASSENDEN ANSATZ BEGREIFEN In den bestehenden Diskussionen ist es grundsätzlich unbestritten, dass unsere Streit- und Sicherheitskräfte, Unternehmen und Bürger für ihre Aufgaben und ihren Eigenschutz moderne Technologien benötigen.
Die dauerhafte Verfügbarkeit modernster, vertrauenswürdiger und verlässlicher Sicherheitstechnologien als eine Kernfrage für die Sicherheitsvorsorge durch Staat und Wirtschaft wird allerdings nur ansatzweise diskutiert – oftmals beschränkt auf wenige Technologienfelder wie den künftigen „wehrtechnischen Schlüsseltechnologien" im Rüstungsbereich oder der „digitalen Souveränität" in Bezug auf sichere IT-Systeme [Unter dem Schlagwort der „wehrtechnischen Schlüsseltechnologien" behandeln Bundesregierung und Industrie die Frage, welche Technologien eine besondere Kritikalität für die Einsatzfähigkeit der Bundeswehr haben. Deren Entwicklung, Herstellung und Beschaffung soll dann aus Gründen der Integrität, Leistungsfähigkeit und Verfügbarkeit der Systeme über die nationale Verteidigungswirtschaft erfol-

- Der BDI definiert Sicherheitstechnologische Souveränität als „die Fähigkeit des Industrielands Deutschland, selbstbestimmt über die Herstellung, die Weiterentwicklung und die Anwendung von Schlüsseltechnologien, Services und Plattformen entscheiden zu können". Souveränität ist dabei von einer Autarkie strikt zu unterschieden. Bisherige Ansätze zur Identifizierung von Schlüsseltechnologien greifen zu kurz.
- Der Aufbau und Erhalt sicherheitstechnologischer Souveränität ist eine Kernaufgabe der Sicherheitspolitik in Deutschland und Europa. Moderne, verlässliche und vertrauenswürdige Sicherheitstechnologien sind zur Abwehr zunehmend komplexer Sicherheitsherausforderungen für die Handelsnation Deutschland eine entscheidender Faktor.
- Der BDI fordert die Bundesregierung auf, die Sicherheitstechnologische Souveränität gemeinsam durch Staat und Industrie gezielt aufzubauen. Dazu sind nationale Schlüsseltechnologien anhand klarer Kriterien im Rahmen einer Technologie-Road-Map zu identifizieren, die Wettbewerbsfähigkeit entsprechend eingestufter Unternehmen zu fördern, Exporte zu flankieren und ein tragfähiger EU-Binnenmarkt auszugestalten.

gen, technologisches Know-how so langfristig gesichert werden. Die „Technische/Digitale Souveränität" beschäftigt sich damit, wie angesichts der fortschreitenden Digitalisierung von Gesellschaft und Industrie – der Industrie 4.0. – die technische IT-Sicherheit gestärkt werden kann. Darunter wird die Fähigkeit verstanden, die Vertrauenswürdigkeit, Integrität, Verfügbarkeit der digitalen Datenübertragung, -speicherung und -verarbeitung durchgängig und selbstbestimmt national/EU-weit kontrollieren zu können.). Zudem existiert eine Vielzahl an staatlichen Unterstützungsmaßnahmen vor allem für die zivile Sicherheitsindustrie – sie reichen von nationalen und europäischen Forschungsprogrammen bis hin zur Exportunterstützung. Diese Diskussionen und Maßnahmen sind zu begrüßen. Allein: Es mangelt ihnen bislang, trotz erster positiver Ansätze (Die Bundesregierung hat im Juli 2015 das „Strategiepapier der Bundesregierung zur Stärkung der Verteidigungsindustrie in Deutschland" veröffentlicht (griephan Special 01/15) und darin die Ausarbeitung einer gesonderten Strategie für die zivile Sicherheitsindustrie angekündigt (www.bmwi.de).), an einer gemeinsamen strategischen Grundausrichtung.

Aus Sicht des BDI bedarf es daher einer weiterreichenden Betrachtungsweise, die über diese beiden Bereiche deutlich hinausgeht. Alle Technologiefelder wie neue Werkstoffe, Miniaturisierungsprozesse, Sensorik und Robotik, Energiespeichertechnologien, Biotechnologie oder Herstellungsverfahren wie der 3D-Druck – sie alle haben einen Querschnittsbezug zueinander. Ihr Ausklammern aus einer sicherheitstechnologischen Betrachtung oder Risikoanalyse wäre für die Sicherheit unseres Landes grob fahrlässig.

Derartige Technologiefelder sollten daher stetig in einem gemeinsamen Prozess von Staat und Wirtschaft auf ihre Kritikalität oder auf ihre besondere Eignung zur Gefahrenabwehr geprüft werden. Zudem gilt es, klare Kriterien für deren Einstufung als sicherheitsrelevante Schlüsseltechnologie, sowie für die Folgen einer solchen Einstufung zu entwickeln.

Um zukunftsfähig zu bleiben, muss die sicherheitspolitische Konzeption der „vernetzten Sicherheit" Deutschlands um diese technologische Komponente dringend ergänzt werden: Dem Verständnis von einer umfassenden „Sicherheitstechnologischen Souveränität".

MASSNAHMEN

(1) Nationale Schlüsseltechnologien identifizieren

In einem ersten Schritt gilt es, gemeinsam durch Staat und Industrie die Schlüsseltechnologien zu identifizieren, in denen eine technologische Souveränität auf nationaler Ebene erreicht werden soll. Die Grundlage hierfür müssen aktuelle und zukünftige Bedrohungsszenarien für Unternehmen und Politik und daraus abgeleitete Sicherheitsinteressen bilden.

Diese gilt es, in einer Technologie Road-Map zu skizzieren, die sich an folgenden Punkten orientiert:

Bedarfe: Welche Technologien sind für die Verfolgung nationaler Sicherheitsinteressen zwingend erforderlich („Schlüsseltechnologien")?

Verfüg- und Realisierbarkeit: Welche dieser Technologien sind im Industrieland Deutschland verfügbar? Welche lassen sich unter Vertraulichkeits-, Wettbewerbs- und Wirtschaftlichkeitsaspekten realisieren? Wo sind vorhandene Stärken oder Potentiale für den Aufbau von Leitanbietern vorhanden, die auch auf den Weltmärkten eine Spitzenrolle einnehmen können? Wo bestehen technologische Abhängigkeiten bei Staat und Wirtschaft und wie können diese ggf. reduziert werden?

Rahmenbedingungen: Wie sehen die Rahmenbedingungen oder Hürden für die Erlangung der sicherheitstechnologischen Souveränität in den jeweiligen Schlüsseltechnologien aus? Wie können diese verbessert werden?

(2) Wettbewerbsfähigkeit von Unternehmen stärken

Sind die Schlüsseltechnologien identifiziert, muss die internationale Wettbewerbsfähigkeit der Know-how-tragenden Unternehmen gestärkt werden. Hierzu gilt es seitens der Politik entsprechend kohärente Rahmenbedingungen zu schaffen:

Innovationen stärken: Es sollte eine gezielte anwendungsnahe Forschungsförderung für Unternehmen aus den identifizierten Schlüsseltechnologien aufgebaut werden. In Forschungsprogrammen in Deutschland und innerhalb der EU sind über ein „Fokusprinzip" entsprechende sicherheitstechnologische Themen stärker in den forschungspolitischen Mittelpunkt zu rücken. Der technologische Wissensaustausch zwischen Staat und Wirtschaft muss zudem systematisch intensiviert werden. Dazu ist die Vernetzung sicherheitstechnologischer Forschungscluster von Forschungseinrichtungen, Unternehmen (Konzerne, KMU, Start-ups), Kapitalgebern und staatlichen Kunden (Behörden, Streitkräfte) in Deutschland und Europa zu verbessern. Dies schafft Synergie- und Kooperationspotentiale zwischen den Akteuren. Der Technologietransfer zwischen Forschungseinrichtungen und Unternehmen wird so deutlich erleichtert.

Innovationsfreundliche Beschaffung: Das Technologie-Scouting muss seitens der staatlichen Sicherheitsakteure ausgebaut werden. Es ist entscheidend, um sicherheitsrelevante Technologien frühzeitig zu identifizieren sowie bedarfs- und anwendungsgerecht auszugestalten. Im Rahmen staatlicher Beschaffungsvorhaben sollten innovative Referenzprojekte berücksichtigt werden. Dies auch vor dem Hintergrund einer dadurch gestärkten Exportunterstützung.

Finanzierung: Der Zugang für Unternehmen zu staatlichen und privaten Finanzierungsquellen muss sich an den technologiespezifischen Geschäftsmodellen orientieren. Dies betrifft neben der Start-up-Förderung vor allem auch langfristig orientierte, staatlich begünstigte Finanzierungsangebote für KMU.

Zulassungen und Standards: Innovative Technologien müssen nach ihrer Entwicklung zügiger Marktreife erlangen. Hierzu bedarf es schnellere Zulassungs- und Zertifizierungsprozesse auf Grundlage einheitlicher EU-Standards. Diese zu schaffen oder ggf. bedarfsgerecht im Sinne der deutschen Industrie anzupassen sollte das Ziel der Politik sein.

(3) Exportunterstützung aus- und einen tragfähigen EU-Markt aufbauen

Exportunterstützung: Der nationale Bedarf von staatlichen und privaten Kunden reicht für den Technologie- und Kompetenzerhalt in den deutschen Unternehmen in der Regel nicht aus. Dem Export kommt somit eine zentrale Bedeutung zu. Um Exportpotentiale heben zu können, sind im Sicherheitsbereich oftmals staatliche Referenzkunden unabdingbar. Dies gilt es bei nationalen Beschaffungen zu berücksichtigen. Instrumente der Außenwirtschaftsförderung im Bereich Finanzierung und politische Flankierung sind stärker an den spezifischen Anforderungen der Sicherheitswirtschaft auszurichten.

EU-Binnenmarkt: Die Schaffung eines EU-Binnenmarktes für Sicherheits- und Verteidigungsgüter muss zügig abgeschlossen werden. Die Wettbewerbsfähigkeit europäischer Unternehmen nimmt infolge fehlender Skaleneffekte bei abschmelzenden nationalen Sicherheitsbudgets ab. Dem gilt es, durch eine kohärente Ausgestaltung und Optimierung von EU-Standards und Regularien entgegenzuwirken Der Schaffung neuer zusätzlicher Rechtsvorschriften bedarf es hierzu in der Regel nicht. Marktzugangsbarrieren und Wettbewerbsverzerrungen könnten so abgebaut, ein echtes Level-Playing-Field aufgebaut werden. ◂

Sicherheit durch technologische Souveränität

© PM Images / getty images

TECHNOLOGIE Neue sicherheitspolitische Herausforderungen erfordern zu ihrer Bewältigung eine deutsche Außen- und Sicherheitspolitik, die neben den klassischen Themenfeldern auch die Bedeutung von Technologien für die Sicherheit unseres Landes stärker als bisher berücksichtigt.

Dr. Stefan Mair

WACHSTUM DURCH GLOBALISIERUNG

Die Verfügbarkeit, Integrität und Beherrschbarkeit modernster Sicherheitstechnologien ist ein unverzichtbarer Baustein für eine zukunftsgerichtet Sicherheitsarchitektur der Industrienation Deutschland.

Deutschland hat wie kaum ein anderes Land von der Globalisierung der vergangenen Jahre profitiert. Seine Wettbewerbsfähigkeit und sein Wohlstand basieren auf der Einbindung in internationale Lieferketten. So wuchs nach einer Studie der Bertelsmann-Stiftung das reale Durchschnittseinkommen in Deutschland dank seiner internationalen ökonomischen Verflechtungen zwischen 1990 und 2011 jährlich um 1.240 €. 20 Prozent des Wachstums des Bruttoinlandsprodukts (BIP) in dieser Zeit sind auf Globalisierungseffekte zurückzuführen. Rund ein Viertel der deutschen Arbeitsplätze, über neun Millionen, hängen heute vom Außenhandel ab. Der Beitrag der Exporte am deutschen BIP liegt bei über 50 Prozent, das ist ein Rekordwert.

Wesentlicher Faktor dieses Erfolgs war die Schaffung eines stabilen EU-Binnenmarktes sowie die marktwirtschaftliche Öffnung vieler Nachfolgestaaten der Sowjetunion, großer Schwellenländer in Lateinamerika, Afrika und Südostasien – hier vor allem China und Indien. Hinzu kam in unmittelbarer europäischer Nachbarschaft ein stabiles Investitionsumfeld in Mittelosteuropa, das vor allem durch die Aufnahme der dortigen Länder in EU und NATO entstand.

Neben den politischen Aspekten waren aber insbesondere neue Technologien – gerade im digitalen Bereich – der grundlegende Treiber der Globalisierung. Die digitale Vernetzung ist mittlerweile aus dem wirtschaftlichen und gesellschaftlichen Leben nicht mehr wegzudenken.

NEUE RISIKEN Doch so sehr Deutschland von diesen internationalen Verflechtungen profitiert, so sehr sind mit ihnen auch neue sicherheitspolitische Abhängigkeiten und Verwundbarkeiten verbunden.
Inner- und zwischenstaatliche Konflikte führen bereits heute in vielen Regionen zu einer politischen Destabilisierung. Die Krisen in Afghanistan über Syrien, Irak, Nord- und Nordwestafrika bis nach Nigeria und auch im Jemen stellen im Verbund mit dem internationalen islamistischen Terror Europa vor eine komplexe Sicherheitsherausforderung. Die Folgen sind komplex. Aus ökonomischer Perspektive gefährden sie für die Weltwirtschaft wichtige Öl- und Rohstoffmärkte sowie für Europa bedeutsame Handels- und Logistikrouten. Außen- und sicherheitspolitisch stoßen die tradierten Einfluss- und Gestaltungsmöglichkeiten Europas in diesen Regionen immer mehr an ihre Grenzen.
Der wirtschaftliche Aufstieg von Staaten wie China oder Indien verschiebt die globalen Marktgewichte und politischen Machtpole. Das Beispiel China zeigt: Nationales Selbstbewusstsein verkörpert sich dabei auch in einem sicherheitspolitischen Behauptungswillen bei Grenzstreitigkeiten mit Nachbarstaaten und dem Aufbau militärischer Stärke. Russlands Annexion der Krim und die Unterstützung der Separatisten in der Ost-Ukraine sind die bisher größte Herausforderung der europäischen Friedensordnung nach dem Ende des Kalten Krieges. Die aktuelle Flüchtlingsfrage dokumentiert zudem, wie sehr die Welt in Unordnung geraten ist – und wie wenig sich Europa abschotten kann.
Hinzu kommt, dass in einer digital vernetzten Welt Unternehmen, Infrastrukturen und Forschungseinrichtungen immer verwundbarer werden für Ausspäh- und Sabotageangriffe aus dem Cyberraum. Diese finden grenzüberschreitend und rund um die Uhr statt. Die Täter sind dabei ebenso vielfältig wie deren Motive. Die jährlichen Schäden hierdurch liegen allein für die deutsche Industrie in einem hohen zweistelligen Milliardenbereich.
Auf diese Entwicklungen müssen Europa und Deutschland gemeinsame Antworten finden. In einer Situation, in der die Einheit der EU infolge der Wirtschafts- und Finanzkrise und die Krise in Griechenland wie nie zuvor in Frage gestellt wird.

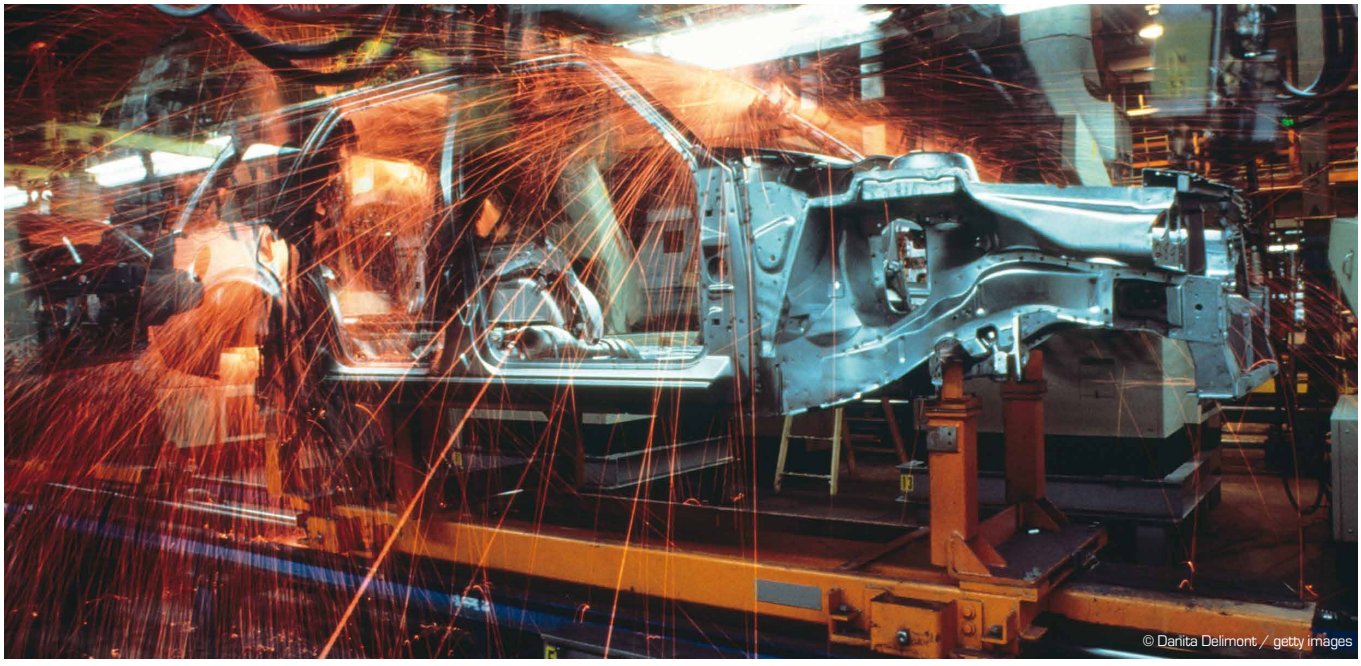
BEDEUTUNG DER SICHERHEITSTECHNOLOGISCHEN SOUVERÄNITÄT Die bestehende offene und freie Weltordnung gegen diese Risiken zu schützen, muss ein außen- und sicherheitspolitisches Kerninteresse der Handelsnation Deutschland sein – gemeinsam mit seinen Verbündeten in EU und NATO.
Bisher unbeantwortet bleibt jedoch die Frage, welche sicherheitspolitische Bedeutung hierfür die Verfügbarkeit und Beherrschbarkeit von Sicherheitstechnologien – im Sinne einer technologischen Souveränität – im zivilen wie militärischen Bereich künftig haben soll.
Zwar betont die Bundesregierung stets die hohe Bedeutung nationaler „Kernfähigkeiten" oder „sicherheitsrelevanter Schlüsseltechnologien" insbesondere im Rüstungsbereich oder hinsichtlich sicherer IT-Systeme. Eine genaue Definition, was genau darunter zu verstehen ist, gibt es jedoch nicht. Auch bleiben wichtige Technologiefelder bzgl. ihrer potentiellen Sicherheitsrelevanz für unser Land außer Betracht: Neue Materialien und Produktionsverfahren wie der 3D-Druck, Sensorik, Robotik und Miniaturisierung, Energiespeichertechnologien, Biotechnologie, Navigations- und Geodatensysteme als Grundlage jeglicher autonomer Fortbewegung – über die Bedeutung dieser Technologien wird derzeit allenfalls unter wirtschaftlichen oder wissenschaftlichen Aspekten diskutiert. Es existieren weder transparente Kriterien für eine Einstufung als „Schlüsseltechnologien" noch gibt es klar artikulierte Ziele, was damit in Folge industriepolitisch verbunden ist.
Das gilt es zu ändern. Aus Sicht der deutschen Industrie bedarf es eines gemeinsamen Prozesses von Industrie und Staat, um Technologiefelder anhand transparenter Kriterien auf ihre Sicherheitsrelevanz und den Grad der notwendigen technologischen Souveränität hin einzustufen. Zudem müssen Ziele und Maßnahmen zur Förderung dieser Technologiefelder entwickelt und umgesetzt werden. Dabei dürfen die Unternehmen, die Schlüsseltechnologien entwickeln und herstellen, nicht dem europäischen Wettbewerb entzogen werden. Vielmehr gilt es, deren Wettbewerbsfähigkeit gezielt im Rahmen von Forschungsprogrammen und einer innovationsfreundlichen Beschaffungspolitik zu fördern.
Dazu gehört aber auch, Unternehmen in Europa einen ökonomisch tragfähigen Heimatmarkt zu schaffen, der ausreichende Volumina aufweist, um Skaleneffekte im Interesse der Unternehmen und Kunden zu heben. Aber auch internationale Exportpotentiale müssen erschließbar bleiben. Hierzu bedarf es einer moderaten weitsichtigen und EU-weit einheitlichen Exportpolitik, die bis heute in vielen der sicherheitsrelevanten Technologiefeldern nicht existiert.
Um es deutlich zu sagen: Technologische Souveränität und tragfähige Marktstrukturen in Europa sind nicht gleichzusetzen mit einer Marktabschottung oder einer technologischen Autarkie. Das wäre angesichts der weltweiten Vernetzung von Wirtschaftsprozessen weder ordnungspolitisch erstrebenswert noch realisierbar.
Vielmehr müssen die betroffenen Technologiesysteme hinsichtlich ihrer Sicherheit, Integrität und Zuverlässigkeit bewertbar, beherrschbar und ggf. Untersysteme substituierbar sein. Eine so verstandene technologische Souveränität ist vereinbar mit einem offenen Welthandelssystem und den Sicherheitserfordernissen einer führenden Handelsnation Deutschland.

»Es ist nicht Aufgabe von Unternehmen, deutsche Sicherheitspolitik zu definieren.«

FAZIT Es ist nicht Aufgabe von Unternehmen, deutsche Sicherheitspolitik zu definieren. Dies ist das Primat der Politik. Eine solche Definition kann jedoch nur auf der Basis zentraler Werte und auf Grundlage abzugleichender nationaler Interessen erfolgen. Dafür ist es unabdingbar, diese gesellschaftlichen aber eben auch die ökonomischen Interessen und Fähigkeiten zu artikulieren. Letzteres ist die Aufgabe und der sicherheitspolitische Beitrag der Wirtschaft – gerade im Bereich der technologischen Souveränität.

Dr. Stefan Mair
Mitglied der Hauptgeschäftsführung
Bundesverband der Deutschen Industrie

Digitale Souveränität – Wunschtraum oder Wirklichkeit?



(UN)ABHÄNGIGKEIT Über Digitale Souveränität wird derzeit heiß diskutiert, auf nationaler wie europäischer Ebene. Jetzt geht es darum, einen vernünftigen Mittelweg zu gehen.

Dr. Magnus Harlander

KOMPROMISS Der Mittelweg bedeutet, sich einerseits aus der Abhängigkeit der „digitalen Platzhirsche" zu befreien, aber andererseits nicht in die völlige Autarkie zu gehen. Denn Arbeitsteilung und Kooperation über Grenzen hinweg kann allen Beteiligten neue Chancen eröffnen.

Seit dem Koalitionsvertrag der aktuellen Regierung, allerspätestens aber seit der von den Bundesministerien des Inneren (BMI), für Verkehr und digitale Infrastruktur (BMVI) und Wirtschaft (BMWi) vorgelegten Digitalen Agenda ist die Stärkung Digitaler Souveränität eines der erklärten Ziele der Bundesregierung. Gleichzeitig wurde damit eine breite Debatte in verschiedenen Bereichen der Wirtschaft ausgelöst, die sich meist darum dreht, was der Begriff bedeuten soll, was zur Erreichung einer Digitalen Souveränität geschehen soll, was machbar und was unmöglich ist.

EUROPA AM ZUG Nicht nur die Wirtschaft wird aktiv, auch die Politik hat erste Maßnahmen ergriffen. Die europäische Cybersecurity-Strategie enthält im Hinblick auf die Stärkung der europäischen Fähigkeiten bereits viele begrüßenswerte Ansätze, die sich bisher allerdings vor allem im Forschungsumfeld und in legislativen Initiativen niederschlagen. Eine Stärkung der ohnehin schon schmalen, meist mittelständisch geprägten industriellen Basis ist bisher noch nicht in ausreichendem Maße erfolgt, die Europäische Agentur für Netzwerk- und Informationssicherheit (ENISA) startet hierzu aber nun die ersten Aktivitäten. Konkrete Fördermaßnahmen sind hier nach jetzigem Stand allerdings nicht zu erwarten.

BEWEGUNG IN DER DEUTSCHEN POLITIK National findet man im Organigramm des BMWi neuerdings ein eigenes Referat, das

sich neben ökonomischen Fragen der Digitalen Agenda auch mit technologischer Souveränität auseinandersetzen soll. Dabei hat das BMWi naturgemäß die Gesamtwirtschaft im Blick und wird die Aktivitäten zugunsten einer Digitalen Souveränität an den Bedürfnissen vor allem der produzierenden Industrie ausrichten. Dem BMI in seiner Zuständigkeit für Cybersicherheit geht es vor allem um den Zugang zu vertrauenswürdiger Informationstechnologie. Folgende Punkte sind dem Innenministerium dabei besonders wichtig:

- Die Verbindung internationaler Technologien mit nationalen Sicherheitsankern und die damit einhergehende Öffnung internationaler Anbieter.
- Die Identifizierung vertrauenswürdiger Anbieter, die, so unterstreicht das Ministerium, nicht zwangsläufig aus Deutschland kommen müssen.
- Die Schaffung einer Bewertungsfähigkeit von vertrauenswürdigen Produkten in Deutschland.

NATIONALE SCHLÜSSELTECHNOLOGIEN NICHT AUFGEBEN Eine Betrachtung der in Deutschland und Europa noch vorhandenen Fähigkeiten unterstreicht den technologischen und industriepolitischen Handlungsbedarf: Nur wenige große Technologieanbieter sind verblieben, als Beispiele sollen Alcatel-Lucent oder Nokia Siemens Networks oder auch unbekanntere Namen wie Kontron aus Bayern dienen. Im Bereich der IT-Sicherheit findet sich ein breites und qualitativ sehr gutes Know-How, das jedoch meist durch kleine und mittelständische Unternehmen gestellt wird. Diese alleine sind nicht in der Lage, die dringend benötigten Technologien europaweit auszurollen. Dabei können wir nicht davon ausgehen, die gesamte Wertschöpfungskette der IT-Welt durch deutsche oder europäische Produkte abzubilden, ein solcher Ansatz würde die Augen vor den Realitäten des Marktes verschließen. Aber die noch vorhandenen Bereiche sollten auch nicht ohne Not aufgegeben werden. Das verlangt zunächst jedoch eine Weitung des Begriffs der Schlüsseltechnologien über Panzer und U-Boote hinaus.

KEIN WIDERSPRUCH: DIGITALE SOUVERÄNITÄT UND INTERNATIONALE KOOPERATION Für uns führt der Weg zum Erfolg über eine klare Analyse der Bereiche, die Deutschland als Staat weiterhin in seinem Industrieportfolio halten will, auch im Bereich der IT-Sicherheit. Sind diese identifiziert, sollten diese auch mit staatlicher Unterstützung in den europäischen Katalog aufgenommen werden. Auch stehen wir einer Kooperation mit weltweiten Anbietern offen gegenüber, denn nur so kann der eigene Markt erfolgreich ausgeweitet werden. Damit können auch internationale Anbieter ihr Portfolio für bestimmte Märkte und Sicherheitsinteressen erweitern. Notwendig wird dafür allerdings ein gedanklicher Neuansatz sowohl bei der Forschungsförderung als auch bei der Industrie-, Exportförderungs- und Beschaffungspolitik.

»Eine Betrachtung der in Deutschland und Europa noch vorhandenen Fähigkeiten unterstreicht den technologischen und industriepolitischen Handlungsbedarf.«

Doch nicht nur die Politik hat Hausaufgaben. Auch die produzierende Wirtschaft sollte nicht nur im Hinblick auf eigene schützenswerte Güter und Know-how stärker auf den heimischen Lösungsmarkt blicken. Auch die IT-Sicherheitswirtschaft muss sich an die eigene Nase fassen und vielleicht bei großen Projekten eher auf Kooperation als auf gnadenlosen Verdrängungswettbewerb setzen. Quasi-Monopolisten haben noch keinem geholfen, schon gar nicht dem Fortschritt.
Digitale Souveränität ist also sinnvoll gelebt kein Wunschtraum. Fest steht aber, dass sie nicht mit einem einfachen „weiter so“ auf allen Seiten erreicht werden kann.

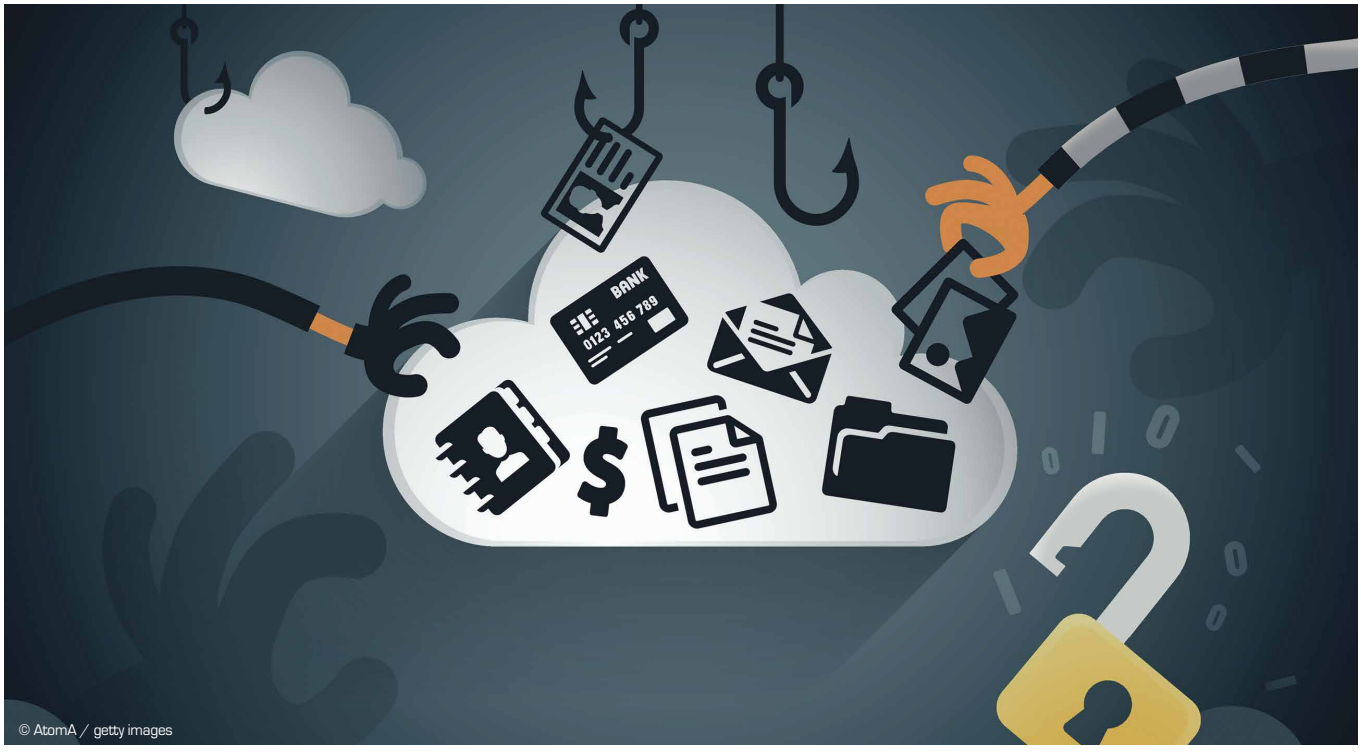
Wie kann ein Plan hierzu aussehen?

1. Wir müssen die aktuell verfügbaren Kompetenzen und Ressourcen im Hard- und Software-Bereich sichten, bewerten und zusammenführen.
2. Es gilt, den Bedarf und die aktuellen Defizite zu identifizieren, damit konzentriert und ergebnisorientiert an den wichtigsten Stellen gearbeitet werden kann. Nur so können zum Beispiel im Bereich Open Source die richtigen Impulse gesetzt werden, um Sicherheit in den Bereichen Infrastruktur, Verschlüsselung, Netzwerkabsicherung, Desktop und mobile Systeme voranzubringen.
3. Die Nutzer (Industrieunternehmen, Telekommunikations-Wirtschaft, Systemhäuser und Behörden) müssen von vornherein mit den Anbietern zusammenarbeiten, um zu passenden Lösungen zu kommen und flankierende Maßnahmen zu finden, die auch zum Einsatz der eigens entwickelten Systeme führen. Nur mit einer ausreichenden Nachfrage in der Heimatregion kann man auch international erfolgreich werden, und das sollte das Ziel sein.
4. Unter Führung großer (auch internationaler) Systemhäuser sollten möglichst umfassende sichere Gesamtlösungen anhand von weltweit vermarktbaren Use-cases erarbeitet werden, die das hohe Sicherheitsniveau deutscher Produkte als Wettbewerbsvorteil in den Markt bringen. Dabei muss nicht zwangsläufig alles „Made in Germany“ sein, kritische Komponenten vertrauenswürdiger Hersteller können das Angebot in Sachen Sicherheit jedoch aufwerten.
5. In der stark zersplitterten, meist mittelständisch geprägten Anbieterlandschaft muss eine neue Kultur der vertrauensvollen Zusammenarbeit geschaffen werden, die von kurzfristigem Konkurrenzdenken Abschied nimmt und auf mittel- und langfristige Synergieeffekte setzt.

All diese Schritte werden allerdings nur dann von Erfolg gekrönt sein, wenn es eine starke Moderation auf europäischer Ebene gibt, die alle leistungsstarken Partner (sowohl Unternehmen als auch Mitgliedsstaaten) einbindet und den industriepolitischen Prozess straff führt, um Einzelinteressen vorzugreifen. Die Weichen müssen allerdings jetzt, und nicht erst in 2020 gestellt werden.

Dr. Magnus Harlander
Geschäftsführer
genua

Souverän ist, wer selbst-bestimmt entscheidet



© AtomA / getty images

DIGITALISIERUNG Mit zunehmender Digitalisierung von Wirtschaftsprozessen und unserer Kommunikation steigt das Risiko, dass digitale Systeme zum Einfallstor für Straftaten oder nachrichtendienstliche Aufklärung werden.

Dr. Tim H. Stuchtey

RISIKO DURCH WACHSENDE VERNETZUNG Die Späh-Affäre um die NSA oder der Angriff auf den Bundestag haben verdeutlicht, welche Möglichkeiten Nachrichtendienste, organisierte Kriminalität oder Konkurrenzunternehmen haben, Informationen zu sammeln und diese zum Zwecke der Aufklärung, Sabotage, Industriespionage oder der Erpressung zu nutzen. Gleichzeitig sehen Beobachter die Gefahr, dass Deutschland mit wachsender Vernetzung und Digitalisierung an Souveränität verliert. In der Konsequenz wird nach einer Intervention des Staates gerufen, um die technologische Souveränität allgemein und besonders bei sicherheitssensitiven Bereichen des Staates und der Streitkräfte aufrechtzuerhalten oder aufzubauen. Bei allen Veränderungen, die der digitale Wandel für Wirtschaft, Staat und Bürger mit sich bringt, ist die Frage nach der Notwendigkeit einer nationalen Souveränität in einzelnen Branchen kein Novum. Derartige Diskussionen gibt es seit es Nationalstaaten gibt. Von jeher wird z. B. darüber nachgedacht, ob ein Staat nicht bei der Nahrungsmittelversorgung oder der Energieerzeugung unabhängig sein müsse. In der Debatte sollte zwischen sicherheitspolitischer Notwendigkeit und industriepolitischer Hoffnung unterschieden werden.

NATIONAL VS. INTERNATIONAL Es gibt Verfechter die eine autarke Lösung favorisieren. Ähnlich dem Vorbild des Airbus-Konzerns (einstmals die europäische Antwort auf die Dominanz der amerikanischen Luftfahrtindustrie) müsse es auch ein „europäisches Google" geben. Europa – oder gar einzelne Staaten – solle sich in allen Bereichen auch technologisch abkoppeln, eigene Sicherheitssysteme und Informationstechnologien entwickeln. Allein die Analogie mit Airbus zeigt, dass es sich hier weniger um ein sicherheitspolitisch motiviertes Argument handelt, als um ein industriepolitisches.
Andere meinen, dass zumindest in sicherheitssensitiven Bereichen wie dem IT-Netz des Bundes ausschließlich auf nationale Anbieter zurückgegriffen werden müsse.

SELBSTÄNDIGKEIT ODER KOOPERATION? Politik und Unternehmen zugleich müs-

sen sich fragen, was das Konzept der technologischen Souveränität konkret umfassen soll. Meines Erachtens ergibt es – weder für die Wirtschaft noch für den Staat – ökonomisch Sinn, alles selbst – also autark – entwickeln und herstellen zu wollen. Denn sowohl im IT-Sektor als auch bei Waffensystemen sind die Forschungs- und Entwicklungskosten ein dominanter Kostenfaktor, sodass in der Produktion erhebliche Skaleneffekte anfallen. Anbieter mit einem großen Heimatmarkt (und einer passenden industriellen Basis) haben somit oft einen Kostenvorteil. Dies ist ein wesentlicher Grund dafür, warum sowohl in der Rüstungsindustrie als auch im digitalen Bereich amerikanische Unternehmen auf dem Weltmarkt eine derart starke Stellung haben. Dieser zu begegnen, indem man in sicherheitssensitiven Bereichen den eigenen Markt vor ausländischer Konkurrenz aus partnerschaftlich verbundenen Staaten abschottet, kann für eine Nation, die ansonsten auf die Offenheit von Grenzen angewiesen ist, kaum eine überzeugende Lösung sein.

In der Konsequenz heißt das, dass im Bereich der Verteidigung ein offener einheitlicher Markt innerhalb von EU und NATO von Vorteil wäre. Wichtig ist, dass man möglichst zwei veritable Anbieter erhält, um sich nicht bei aller staatlichen Souveränität in die Abhängigkeit von einem (teuren) Monopolisten zu begeben. Natürlich benötigt dieser Ansatz eine politische Begleitung, schon um die Einflussnahme anderer Staaten auf das Marktergebnis auszugleichen.

Bei der IT-Sicherheit – vor allem in der Wirtschaft – sieht es anders aus: Die Gruppe potentieller Angreifer ist heterogener und Angriffe können unerkannt die Produktion sabotieren oder F&E-Daten entwenden. Eine Unterscheidung zwischen „In- und Ausland" ergibt keinen Sinn. Die Realität zeigt, dass ein Angriff ebenso von partnerschaftlich verbundenen Geheimdiensten, wie von halbstaatlichen Hackern oder von konkurrierenden inländischen Unternehmen ausgehen kann. Hier ist ein hohes Schutzniveau angemessen – sowohl auf der Staats- als auch auf Unternehmensebene. Technologische Souveränität muss sich daher in diesem Bereich auf die Beurteilungsfähigkeit sowie die Bewertungskompetenz der eigenen Systeme und deren Grad an Sicherheit beziehen.

FESTLEGUNG DES SCHUTZNIVEAU Ein weniger restriktives Verständnis technologischer Souveränität reduziert sich darauf, bei der beschafften Technik in sicherheitssensitiven Bereichen ein Wissen darüber zu haben, wie diese Technik funktioniert und welche Informationen wohin fließen oder welche Eingriffsmöglichkeiten auf das System bestehen. Wenn sich ein IT-System nicht vollständig verstehen oder kontrollieren lässt, dann gilt es, auf einer unsicheren Infrastruktur die Daten entsprechend des eigenen (unternehmerischen wie staatlichen) Schutzbedürfnisses aufwendig zu verschlüsseln. Wird dies staatlicherseits untersagt oder der Schlüssel verlangt, dann besteht kein Zweifel mehr, mit wem man seine Unternehmensdaten teilen muss und die Unternehmensentscheidungen sind entsprechend auszurichten.

»Es gilt, Bedrohungen den jeweils adäquaten Schutz entgegenzusetzen.«

ADÄQUATER SCHUTZ Es stellt sich die Frage, ob für jede Form des Informationsaustausches eine absolute Sicherheit notwendig oder erstrebenswert ist. Letztlich war dies bei der Post und Telefonie auch zu keinem Zeitpunkt der Fall. Wie in allen Sicherheitsfragen gilt es, ein unter Berücksichtigung der Kosten verhältnismäßiges Maß an Sicherheit durch entsprechende Schutzmaßnahmen zu erreichen. Eine 100-prozentige Sicherheit ist weder wünschenswert noch effizient. Es gilt, Bedrohungen den jeweils adäquaten Schutz entgegenzusetzen. Nicht für jedes Unternehmen ist es realistisch oder sinnvoll, jeden Gegner aus seinem Netzwerk raushalten zu wollen. Der finanzielle Aufwand stünde in keinem Verhältnis zur potenziellen Bedrohung. Doch die geistigen Kronjuwelen des Unternehmens gilt es, vor Industriespionage oder Kriminellen zu schützen.

Die Knappheit qualifizierter inländischer Arbeitskräfte in Deutschland, der Wunsch vieler Bürger nach informationeller Selbstbestimmung oder der Mangel an Eigenkapitalfinanzierungsquellen führen dazu, dass angebotsseitig nicht die Voraussetzungen existieren, den USA als Standort für die digitale Wirtschaft den Rang streitig zu machen. Anstatt mit großem industriepolitischen Aufwand zu versuchen, das Silicon Valley nach Deutschland zu holen, muss es einer offenen Volkswirtschaft wie Deutschland darum gehen, bestehende Stärken weiterzuentwickeln. Deutschland hat einen komparativen Konkurrenzvorteil im Bereich des Maschinen- und Anlagenbaus sowie der Automobilindustrie. Diesen gilt es auch in einer digitalen Zukunft mit einer „Industrie 4.0" zu sichern. Digitale Souveränität verstanden als die Fähigkeit, die Produktions- und Mobilitätsprozesse der Zukunft sicher zu gestalten, stellt die Basis der zukünftigen Wettbewerbsfähigkeit der deutschen Industrie dar. Die kann dann auch zukünftige Exporterfolge begründen, wenn auch Kunden ertüchtigt werden, souverän zu wirtschaften.

Das soll nicht heißen, dass einzelne deutsche IT-Sicherheitsunternehmen weltweit nicht wettbewerbsfähig sind. Gerade diese Unternehmen sind die Wachstumstreiber der Sicherheitswirtschaft in Deutschland. Die Bundesregierung sollte stabile und vorhersehbare Rahmenbedingungen vor allem bei der eigenen Beschaffung bieten. Gleiches gilt für die wehrtechnische Industrie. Forschungs- und Entwicklungsprogramme können angepasst werden, um Dual-Use-Forschung zu erlauben. Zudem sollte sich die Bundesregierung für verbesserte Marktzutrittschancen deutscher Sicherheitsunternehmen in Europa und Nordamerika einsetzen.

FAZIT Technologische Souveränität im Sinne einer eigenverantwortlichen Entscheidungsmöglichkeit ist notwendig, wo originäre Sicherheitsbedürfnisse des Staates oder der Wirtschaft betroffen sind. Verkürzt mit den Worten von Peter Sloterdijk: „Souverän ist, wer selbst entscheidet, worauf er hereinfallen will." Souveränität als ein Argument zur Abschottung von Märkten schafft hingegen keinen Wohlstand, sondern zerstört ihn.

Dr. Tim H. Stuchtey
Geschäftsführender Direktor
Brandenburgisches Institut für Gesellschaft und Sicherheit (BIGS)

Medien für einen bewegten Markt.