Fraunhofer SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE
TECHNICAL REPORT

Positionspapier

# Cybersicherheit in Deutschland

Michael Waidner, Michael Backes, Jörn Müller-Quade

FRAUNHOFER VERLAG

CISPA Center for IT-Security, Privacy

CRISP Center for Research in Security and Privacy

KASTEL

Kompetenzzentren für IT-Sicherheit

# Positionspapier
# **Cybersicherheit in Deutschland**

14. Februar 2017

Prof. Dr. Michael Waidner[1,2]
Institutsleiter Fraunhofer SIT *und*
Professor für Informatik an der TU Darmstadt;
Sprecher CRISP
*michael.waidner@sit.fraunhofer.de*

Prof. Dr. Michael Backes[3,4]
Professor für Informatik an der Universität des Saarlandes, Saarbrücken *und*
Max Planck Fellow am Max-Planck Institut für Softwaresysteme;
Direktor CISPA
*backes@cispa.saarland*

Prof. Dr. Jörn Müller-Quade[5]
Professor für Informatik *und* Leiter des Instituts für Kryptographie
und Sicherheit IKS am Karlsruher Institut für Technologie KIT;
Direktor KASTEL
*mueller-quade@kit.edu*

(1) Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75, 64295 Darmstadt

(2) Technische Universität Darmstadt
Rheinstraße 75, 64295 Darmstadt

(3) CISPA, Universität des Saarlandes
Campus E9 1, 66123 Saarbrücken

(4) Max-Planck-Institut für Softwaresysteme (MPI-SWS)
Campus E1 5, 66123 Saarbrücken

(5) Karlsruher Institut für Technologie (KIT)
Am Fasanengarten 5, Geb. 50.34, 76131 Karlsruhe

FRAUNHOFER VERLAG

# Impressum

**Kontaktadresse:**
Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75, 64295 Darmstadt
Telefon 06151 869 100
E-Mail info@sit.fraunhofer.de, URL www.sit.fraunhofer.de

**Bibliografische Information der Deutschen Nationalbibliothek**
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über www.dnb.de abrufbar.
ISSN 2192-8169
ISBN 978-3-8396-1164-7

Hrsg. Michael Waidner
Cybersicherheit in Deutschland, (SIT-TR-2017-01)
Michael Waidner, Michael Backes, Jörn Müller-Quade
Copyright Titelbild: iSock, iconeer

Druck und Weiterverarbeitung: Walter Digital GmbH, Korntal-Münchingen
Für den Druck des Buches wurde chlor- und säurefreies Papier verwendet.


Fraunhofer-Informationszentrum Raum und Bau IRB
Postfach 800469, 70504 Stuttgart
Nobelstraße 12, 70569 Stuttgart
Telefon 0711 970-2500
Telefax 0711 970-2508
E-Mail verlag@fraunhofer.de
URL http://verlag.fraunhofer.de

# Inhalt

# 1 Zusammenfassung

Im Folgenden präsentieren wir sieben Thesen zur Cybersicherheit. Wir richten uns damit an die Politik in Deutschland, aber auch an Gesellschaft, Wirtschaft und Wissenschaft. Wir charakterisieren den heutigen Stand der Cybersicherheit und identifizieren Defizite (Abschnitt 2) und machen Empfehlungen, wie die Cybersicherheit in Deutschland nachhaltig verbessert werden kann (Abschnitt 3). Wir tun dies aus der Perspektive der Wissenschaft, beschränken uns aber in unseren Empfehlungen nicht auf den Forschungsbereich.

Die Digitalisierung und die ihr zugrundeliegenden Informations- und Kommunikationstechnologien (IKT) sind von zentraler Bedeutung für Gesellschaft, Staat und Wirtschaft. Die Medien berichten regelmäßig über Cyber-Kriminalität, gestohlene Passwörter und Kundendaten, Angriffe auf IT-Infrastrukturen, Beeinflussung politischer Wahlen durch Cyber-Spionage und Social Bots und über massive Eingriffe in die Privatsphäre, z.B. in und durch Social Networks. Gerade regulatorisch wird in Deutschland und Europa sehr viel für eine Verbesserung der Cybersicherheit getan – z.B. das IT-Sicherheitsgesetz[1] in Deutschland und auf EU-Ebene die NIS-Richtlinie[2] und die Datenschutzgrundverordnung[3]. Gleichzeitig mehren sich politische Stimmen, die einen Verlust der Überwachungsmöglichkeiten von Verdächtigen beklagen, da natürlich auch Terroristen und andere Kriminelle von einem generellen Mehr an Cybersicherheit profitieren.

All dies legt die Befürchtung nahe, die Entwicklung von Cybersicherheit und Privatsphärenschutz hinkten der Digitalisierung hinterher. Zumindest gefühlt wird die digitale Welt immer unsicherer. Hinzu kommt die Erkenntnis in Politik und Wirtschaft, dass Deutschland und Europa in vielen Bereichen der Digitalisierung und der IKT nicht mehr über die Fähigkeit verfügen, die wichtigsten Schlüsseltechnologien selbst zu entwickeln oder auch nur hinsichtlich ihrer Sicherheitseigenschaften zu beurteilen. Weder Deutschland noch Europa verfügen in diesem Sinne über die digitale Souveränität. Diese Erkenntnis ist umso bedrohlicher, als sich weltweit der Trend zur globalen Zusammenarbeit und

1 »Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)«, 24.7.2015, *https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf*

2 Europäisches Parlament und Europäischer Rat: »Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union«, Richtlinie 2016/1148, 6.7.2016, *http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148&from=DE*

3 Europäisches Parlament und Europäischer Rat: »Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)«, Verordnung 2016/679, 27.4.2016, *http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE*

gemeinsamen Verantwortung umzukehren scheint und nationale Interessen und Protektionismus in den Vordergrund treten.

Auch die Forschung und Entwicklung zur Cybersicherheit und zum Schutz der Privatsphäre scheinen der allgemeinen Entwicklung in der IKT hinterherzuhinken. Grund hierfür ist einerseits die explosionsartige Digitalisierung aller Lebensbereiche. Alles Physische wird digitalisiert und mit allem vernetzt. Die physische und digitale Welt verschmelzen. Damit ergeben sich auch in bislang nie gesehenem Ausmaße neue Angriffsrisiken. Zugleich erhöhen sich in dramatischer Weise die Schutzanforderungen. Die Risiken steigen und damit auch die Ressourcen, die potenzielle Angreifer bereit sind, in Angriffe zu investieren. Staatliche und damit meist sehr ressourcenmächtige Angreifer, z.B. Geheimdienste, spielen eine zunehmend größere, oder zumindest sichtbarere, Rolle. Trends wie Big Data und Cognitive Computing und neue Technologien wie Quantencomputer können auch von Angreifern genutzt werden und zu ganz neuen Angriffstechniken führen. Zugleich sind viele »alte« Forschungsfragen immer noch offen.[4]

Vor diesem Hintergrund formulieren wir die folgenden sieben Thesen, die zu einer nachhaltigen Verbesserung der digitalen Souveränität Deutschlands und Europas beitragen sollen:

1. **Strategisches Ziel »Digitale Souveränität«:** Die Entwicklung der Cybersicherheit muss auf nationaler und europäischer Ebene strategiegetrieben sein. Die Verbesserung der digitalen Souveränität muss dabei ein vorrangiges strategisches Ziel sein. Die Abhängigkeit von IKT, der man mangels Überprüfbarkeit der IKT und ihrer Hersteller blind vertrauen muss, muss reduziert und das vorhandene hohe Potenzial in Deutschland und Europa für Forschung und Entwicklung muss besser genutzt werden. Zugleich muss die enge internationale Kooperation in Forschung und Entwicklung mit Partnern in Europa, aber auch mit in Cybersicherheit führenden Nationen wie USA und Israel, fortgesetzt und ausgebaut werden. Deutschland zeichnet sich durch Offenheit, Schutz von Menschenrechten und gesellschaftliche Stabilität aus – Eigenschaften, die Deutschland zum idealen Standort für Hochtechnologiefirmen und Arbeitsort für hochqualifizierte Mitarbeiter machen. Die Fortschreibung und Ausgestaltung der Cybersicherheitsstrategien brauchen feste, ressortübergreifende Strukturen.

4 secUnity Project (*https://it-security-map.eu*): »Key Challenges in IT Security Research – Discussion Paper for the Dialogue on IT Security«, 12.12.2016, *https://www.crisp-da.de/fileadmin/News___Veranstaltungen/PDF_fuer_news_events/Keychallenges_in_IT-security_research_online.compressed.pdf*

2. **Mindeststandards und Produkthaftung:** Berechtigtes Vertrauen in Informationstechnologie entsteht, wenn adäquate Mindeststandards für Sicherheit und Privatsphärenschutz und Testierung nachgewiesen und über Beschaffungsregeln eingefordert werden. Die Verantwortung über Sorgfaltspflichten (z.B. Verwendung von auf die Sicherheitsqualität ausgerichteter Entwicklungsprozesse, verbindliche und schnelle Behandlung sicherheitsrelevanter Schwachstellen) und Haftungsregeln von Produkten und Dienstleistungen müssen festgelegt werden.

3. **Cybersicherheitsinfrastrukturen:** Die digitale Gesellschaft braucht für ihre Cybersicherheit Infrastrukturen, z.B. für digitale Identitäten, Verschlüsselung und die Beurteilung von Produkten und Diensten, die ebenso von Staat und Wirtschaft gefördert werden müssen wie andere öffentliche Infrastrukturen, z.B. Straßen.

4. **Stärkung von Grundrechten:** Grundrechte und Werte können durch Informationstechnologie gestärkt werden. Dies gelingt aber nur, wenn auch der gesellschaftliche Interessensausgleich gelingt. Das Leitprinzip dieses Ausgleichs ist in Deutschland der Wertekanon des Grundgesetzes. Der Schutz der Grundrechte aller Bürger – in Deutschland wie im Ausland – sollte dabei Vorrang haben vor dem Wunsch, datenbasierte Geschäftsmodelle oder die Überwachung von Verdächtigen zu vereinfachen. Insbesondere sollte es keine Einschränkungen der Kryptographie geben, weder im Inland noch – durch Exportkontrolle – im Ausland.

5. **Aus- und Weiterbildung:** Deutschland und Europa brauchen mehr Fachkräfte, die im Bereich Cybersicherheit qualifiziert sind. Mindestbewusstsein von Cybersicherheit sollte in schulischer Ausbildung und beruflicher Weiterbildung fest verankert sein.

6. **Cybersicherheitsforschung:** Angesichts zunehmender Bedrohungen der Cybersicherheit ist mehr exzellente Forschung erforderlich, im Sinne von Grundlagen- und Technologieforschung.

7. **Innovationsrahmen für Cybersicherheit:** Innovation durch Forschung und Entwicklung braucht einen Rahmen, der bewusst wettbewerbliche exzellente Forschung sowie den Transfer aus Deutschland und Europa in den internationalen Markt fördert. Clusterbildung, wettbewerbliche Forschung und die kommerzielle Verwertung von Forschung muss gewollt und im Rahmen der Forschungsförderung unterstützt werden. Die Schaffung von Startups in Cybersicherheit muss gezielt vorbereitet und gefördert werden. Regulatorische Vorgaben, die nationale Lösungen erzwingen und damit die internationale Vermarktung behindern, müssen abgebaut bzw. angepasst werden.

Dieses Positionspapier schreibt in vieler Hinsicht unser Positionspapier von 2013 fort.[5] Viele der damaligen Empfehlungen finden sich heute auch an anderer Stelle, etwa der Digitalen Agenda[6], dem Sicherheitsforschungsrahmenprogramm[7] und der deutschen Cybersicherheitsstrategie[8]. Insgesamt gelten die damaligen Empfehlungen aber unverändert auch heute noch.

**Dank.** Dieses Positionspapier entstand in einer Kooperation der Sprecher der drei Kompetenz- und Forschungszentren für IT-Sicherheit CISPA (Saarbrücken), CRISP (Darmstadt) und KASTEL (Karlsruhe). Diese drei Zentren werden gefördert vom Bundesministerium für Bildung und Forschung BMBF. Das Zentrum CISPA wird zusätzlich von der Saarländischen Staatskanzlei und das Zentrum CRISP zusätzlich vom Hessischen Ministerium für Wissenschaft und Kunst gefördert. Der Forschungstransfer von KASTEL wird zusätzlich vom Ministerium für Wirtschaft, Arbeit und Wohnungsbau Baden-Württemberg gefördert.

Der vorliegende Text entstand in Zusammenarbeit mit Dr. Michael Kreutzer und Dr. Markus Schneider vom Fraunhofer SIT. Für ihre großzügige Unterstützung möchten wir uns sehr herzlich bedanken. Der Text basiert auf zahlreichen Diskussionen insbesondere mit Kolleginnen und Kollegen an den drei Zentren. Auch hierfür möchten wir uns sehr herzlich bedanken. Der Text spiegelt jedoch alleine die Meinung der drei Autoren wider und erhebt nicht den Anspruch, im Namen aller Forscherinnen und Forscher der drei Zentren zu sprechen.

5 M. Waidner, M. Backes, J. Müller-Quade: »Sicherheitstechnik im IT Bereich – Positionspapier aus Forschungssicht«, 9.9.2013, *https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Positionspapier_IT-Sicherheit_Forschung.pdf*

6 Die Bundesregierung: »Digitale Agenda 2014 - 2017«, 2014, *https://www.digitale-agenda.de/Webs/DA/DE/Home/home_node.html*

7 Bundesministerium für Bildung und Forschung: »Selbstbestimmt und sicher in der digitalen Welt 2015-2020«, 2015, *https://www.bmbf.de/pub/Forschungsrahmenprogramm_IT_Sicherheit.pdf*

8 Bundesministerium des Inneren: »Cyber-Sicherheitsstrategie für Deutschland 2016«, 2016, *http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cybersicherheitsstrategie/cybersicherheitsstrategie_node.html*

# 2 Zum Stand der Cybersicherheit

## 2.1 Cybersicherheitslage

Die Digitalisierung und die ihr zugrundeliegenden Informations- und Kommunikationstechnologien (IKT) sind von zentraler Bedeutung für Gesellschaft, Wirtschaft und Staat. Dies gilt für Deutschland ebenso wie für jedes andere Land dieser Welt. Kommunikation, Medien, Produktion, Logistik, Verwaltung, Unternehmenssteuerung, Forschung, Entwicklung, kritische Infrastrukturen – sie alle sind ohne IKT nicht mehr vorstellbar. Die Digitalisierung ist eine notwendige Voraussetzung geworden für gesellschaftliches und wirtschaftliches Wohlergehen und für politische Stabilität und den Schutz unserer Grundwerte.

Die Digitalisierung führt aber auch dazu, dass *unsichere* IKT zu einer Gefahr für Wohlstand und Lebensqualität, für Werte wie Demokratie, Freiheit und Menschenrechte werden kann. Cyberangriffe können zu Krisen, Unfreiheit und Instabilität führen. Viele Konflikte zwischen Menschen, zwischen Unternehmen und zwischen Staaten werden schon heute im Cyberraum ausgetragen. Cybersicherheit spielt nicht nur eine zentrale Rolle für die zukünftige Digitalisierung, sondern auch für unser *heutiges* Leben, für den Fortbestand unserer *heutigen* Gesellschaftsordnung.

Am eindrücklichsten versteht man dies, wenn man einige der Cybervorfälle der letzten Monate Revue passieren lässt:

– **Politische Einrichtungen** werden ausspioniert, vermehrt mit dem Ziel, direkten Einfluss auf Politik und Wahlen zu nehmen. 2015 wurde bekannt, dass Angreifer über längere Zeit Zugriff auf praktisch alle Daten des Deutschen Bundestages hatten.[9] 2016 wurden in den USA Systeme der Demokraten angegriffen und erbeutete Daten veröffentlicht, mit dem Ziel, die Präsidentschaftswahl zugunsten des Republikanischen Kandidaten zu beeinflussen. Beide Angriffe wurden Russland zugerechnet.[10,11] Vermehrt werden zudem,

9 Zeit Online: »Hackerangriff - Der Bundestag ist offline«, 20.8.2015, *http://www.zeit.de/digital/datenschutz/2015-08/hacker-angriff-bundestag-computer-system*

10 Zeit Online: »Deutscher Bundestag - Hackerangriff wurde aus Russland gesteuert«, 30.1.2016, *http://www.zeit.de/digital/2016-01/hackerangriff-bundestag-russland-nachrichtendienst-bundesanwaltschaft*

11 Süddeutsche Zeitung: »Das steht im Hacking-Bericht der US-Geheimdienste«, 7.1.2017, *http://www.sueddeutsche.de/politik/hacker-attacken-bei-us-wahl-das-steht-im-hacking-bericht-der-us-geheimdienste-1.3323715*

so z.B. wiederum im US-amerikanischen Präsidentschaftswahlkampf 2016, Social Bots eingesetzt, um die Meinung in Sozialen Netzen über Falschmeldungen und gefälschte Unterstützer dieser Falschmeldungen zu manipulieren.[12]

- Unverändert zeigt sich, dass **persönliche Daten** oft nur unzureichend geschützt sind. 2016 wurde bekannt, dass Hacker bei Yahoo schon 2013 Daten von ca. 500 Millionen Nutzern[13] und 2014 nochmals Daten von ca. 1 Milliarde Nutzern[14] erbeutet hatten. Bei einem Angriff auf Ebay im Jahr 2014 wurde auf die Daten von 145 Millionen Kunden zugegriffen.[15] Im Jahr 2016 ist ein Angriff auf Kundendaten von LinkedIn aus dem Jahr 2012 bekannt geworden, bei dem ca. 177 Millionen Datensätze erbeutet wurden.[16]

- Die **Wirtschaft** wird im großen Stil ausspioniert. BITKOM schätzte 2015, dass bereits mehr als 51% aller Firmen Opfer von Industriespionage waren.[17] Als Angriffsquellen werden häufig China und Russland genannt, aber auch andere Staaten und private Firmen sind in der Wirtschaftsspionage aktiv.

- Ebenfalls im großen Stil werden Server und Infrastrukturen durch **Denial-of-Service-Angriffe** (DoS) lahmgelegt. 2016 wurden dafür erstmals auch Geräte aus dem Internet der Dinge angegriffen.[18] Als Kolateralschaden waren von einem dieser Angriffe Ende 2016 auch 900.000 Kunden der Deutschen Telekom betroffen.[19]

12 Spiegel Online: »US-Wahl und Daten-Ingenieure - Ich ganz allein habe Trump ins Amt gebracht«, 6.12.2016, *http://www.spiegel.de/netzwelt/netzpolitik/donald-trump-und-die-daten-ingenieure-endlich-eine-erklaerung-mit-der-alles-sinn-ergibt-a-1124439.html*

13 New York Times: »Yahoo Says Hackers Stole Data on 500 Million Users in 2014«, 22.9.2016, *http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html*

14 New Yoirk Times: »Yahoo Says 1 Billion User Accounts Were Hacked«, 13.12.2016, *http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html*

15 Heise Security: »145 Millionen Kunden von eBay-Hack betroffen«, 22.5.2015, *https://www.heise.de/security/meldung/145-Millionen-Kunden-von-eBay-Hack-betroffen-2195974.html?view=print*

16 Zeit Online: »Datenleck - Kunden von LinkedIn müssen Passwörter wechseln«, 19.5.2016, *http://pdf.zeit.de/digital/datenschutz/2016-05/linkedin-passwoerter-hacker-angriff-datenleck.pdf*

17 BITKOM: »Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter«, 2015, *https://www.bitkom.org/noindex/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709-Studienbericht-Wirtschaftsschutz.pdf*

18 Heise Security: »Source Code von mächtigem DDoS-Tool Mirai veröffentlicht«, 11.10.2016, *https://www.heise.de/security/meldung/Source-Code-von-maechtigem-DDoS-Tool-Mirai-veroeffentlicht-3345809.html?view=print*

19 Die Welt: »900.000 Router ausgefallen - Telekom prüft Hacker-Angriff«, 28.11.2016, *https://www.welt.de/wirtschaft/webwelt/article159800437/900-000-Router-ausgefallen-Telekom-prueft-Hacker-Angriff.html*

## 2.2 Positive Schritte

Die zentrale Rolle der Cybersicherheit wird auch in der Politik erkannt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) berichtet regelmäßig über die Lage der IT-Sicherheit in Deutschland.[20] Die Verbesserung der Cybersicherheit ist zentrales Thema der Digitalen Agenda[21] und anderer Strategiedokumente des Bundes[22,23,24], aus denen sich teilweise erhebliche Erhöhungen der Investitionen in Cybersicherheit ableiten. Das Bundesministerium für Bildung und Forschung finanziert seit 2011 drei Kompetenzzentren für Cybersicherheitsforschung in Darmstadt (CRISP), Karlsruhe (KASTEL) und Saarbrücken (CISPA) und hat damit eine deutliche Vergrößerung der Forschungskapazitäten in Deutschland ermöglicht.[25] Mitte 2016 kündigte das Bundesministerium für Verteidigung an, das 2013 gegründete Forschungszentrum CODE an der Universität der Bundeswehr in München massiv auszubauen.[26] Auch in der Gesetzgebung sind eine Reihe positiver Entwicklungen zu verzeichnen, etwa das IT-Sicherheitsgesetz[1] und die KRITIS-Verordnung sowie auf EU-Ebene die NIS-Richtlinie[2] und die Datenschutzgrundverordnung[3].

## 2.3 Problemfelder

Trotz vieler positiver Schritte scheint die Cybersicherheitslage in Deutschland und weltweit auf einem nicht zufriedenstellenden Niveau zu stagnieren. Hierfür gibt es eine ganze Reihe von Gründen:

– *Sicherheitsstatus der ausgerollten Technologie:* Der überwiegende Teil der heute ausgerollten und verwendeten Technologie wurde ohne besondere Berücksichtigung von IT-Sicherheitsfragen entwickelt. Vor diesem Hintergrund ist es nicht verwunderlich, dass entsprechende Produkte oder Dienste Schwachstellen haben, die für Angriffe ausgenutzt werden können. For-

20 Bundesamt für Sicherheit in der Informationstechnologie: »Die Lage der IT-Sicherheit in Deutschland 2016«, *https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html*

21 Die Bundesregierung: »Digitale Agenda 2014-2017«, *https://www.digitale-agenda.de/Webs/DA/DE/Home/home_node.html*

22 Bundesministerium für Verteidigung: »Weißbuch 2016«, *https://www.bmvg.de/portal/a/bmvg/start/weissbuch*

23 Bundesministerium für Bildung und Forschung: »Selbstbestimmt und sicher in der Digitalen Welt«, *https://www.bmbf.de/pub/Forschungsrahmenprogramm_IT_Sicherheit.pdf*

24 Bundesministerium des Inneren: »Cyber-Sicherheitsstrategie für Deutschland 2016« *http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cybersicherheitsstrategie/cybersicherheitsstrategie_node.html*

25 Kompetenz- und Forschungszentren für IT-Sicherheit, *http://www.kompetenz-it-sicherheit.de/*

26 Universität der Bundeswehr München: »Größtes Forschungszentrum für Cyber entsteht«, Pressemitteilung vom 28.7.2016, *https://www.unibw.de/praes/service/presse/Pressemitteilungen/groesstes-forschungszentrum-fuer-cyber-entsteht*

schung muss sich daher nicht nur mit der Entwicklung neuer, sicherer IT-Systeme beschäftigen. Sie muss sich ebenso der Herausforderung stellen, wie man Dienste und Produkte, die bereits vorhandene Komponenten verwenden, absichern kann.

- *Komplexität, Dynamik und Methodik:* Die Komplexität und Dynamik heutiger IT-Systeme wie etwa das Internet führen dazu, dass Ingenieure an ihre Grenzen stoßen. Dies betrifft sowohl das Wissen der einzelnen Ingenieure über die im Internet eingesetzten Technologien, als auch die Anwendbarkeit der »klassischen« ingenieurswissenschaftlichen Methoden. Es gibt wahrscheinlich keinen Menschen, der alle internetrelevanten Standards, Methoden und Werkzeuge kennt. Vorhandene ingenieurwissenschaftliche Methoden, Denkweisen und Lösungen, die beispielsweise auf Korrektheit, Exaktheit und Vollständigkeit ausgerichtet sind, sind zur Absicherung komplexer IT-Systeme wie dem Internet nicht mehr hinreichend. Hier muss die Cybersicherheitsforschung neue Wege beschreiten, für welche sie Methoden und Denkweisen empiriebasierter Wissenschaften übernehmen muss.

- *Marktsituation und Abhängigkeit:* Der Markt für IKT-Produkte und Dienstleistungen insgesamt und für Cybersicherheit im Besonderen wird von Herstellern außerhalb Europas dominiert. Heutige IKT-basierte Systeme integrieren typischerweise eine Vielzahl von Komponenten, die aus verschiedenen Ländern stammen. Unter diesen können einzelne Länder sein, die hinsichtlich Zusicherungen oder rechtlicher Bedingungen für Anwender unerwünschte Risiken implizieren. In Bereichen, in denen die Risiken als zu hoch eingeschätzt werden, gibt es einen Bedarf, auf alternative und hinsichtlich Cybersicherheitsanforderungen geeignete Quellen für Informationstechnologie zugreifen zu können.

- *Fachkräfte und Ausbildungsstand:* In Deutschland und Europa herrscht ein erheblicher Mangel an Fachkräften im Bereich Cybersicherheit. In Deutschland war das Fach IT-Sicherheit vor dem Jahr 2000 an den meisten Hochschulen nicht im Fächerkanon der Informatik oder der Ingenieurwissenschaften enthalten. Entsprechend wurden die meisten der heute über Vierzigjährigen als Hochschulabgänger der Informatik und Ingenieurwissenschaften von damals nicht im Bereich Cybersicherheit ausgebildet. Viele heutige Entscheider in Wirtschaft und Behörden gehören dieser Gruppe an. Hier gibt es einen immensen Nachholbedarf.

- *Sicherheitsprozesse in Unternehmen und Behörden:* Unternehmen und Behörden haben in den vergangenen Jahren in der Behandlung von Sicherheitsfragen enorme Fortschritte gemacht. So verläuft etwa die Behandlung

– von Schwachstellenmeldungen oder die Reaktion auf Angriffe in vielen Organisationen inzwischen sehr systematisiert ab. Es ist in diesem Zusammenhang jedoch auch festzustellen, dass für den Umgang mit Schwachstellen und Angriffen betroffene Organisationen jeweils Aufwände für die Behandlung identischer Sicherheitsfragen z.B. für Analyse und Behebung erbringen müssen. Durch diesen ineffizienten Ansatz wird Cybersicherheit in der Praxis teurer als notwendig. Beispielsweise haben die Unternehmen Allianz, BASF, Bayer und Volkswagen zur effektiveren und effizienteren Lösung von Cybersicherheitsproblemen das gemeinsame Tochterunternehmen DCSO[27] gegründet. Dieser Ansatz kann zur Verbesserung der operativen Cybersicherheit weiterentwickelt werden, z.B. in Richtung von öffentlich-privaten Kooperationen.

– *Forschungsrahmen und Forschungssteuerung für Cybersicherheit:* Die Politik hat erkannt, dass die Erforschung von Cybersicherheit und Privatsphärenschutz sowohl wichtig und dringend ist, als auch alle Ministerien betrifft. Forschungsförderprogramme für Cybersicherheit und Privatsphärenschutz mit jeweils vergleichbarer Ausrichtung werden von immer mehr Ministerien aufgelegt und es werden so viele Forschungsmittel investiert wie nie zuvor. Projektskizzen und Anträge für die Forschungsförderung des Bundes sind grundsätzlich auf mehrere Jahre angelegt, der Antragsprozess zieht sich in der Regel über mehrere Monate hin. Die Zyklen der Technologieentwicklung in der Informationstechnologie und speziell im Cybersicherheitsbereich liegen bei bestimmten Themen hingegen im Bereich weniger Monate. Die Rahmenbedingungen der Projektförderung mit festgelegtem Arbeitsprogramm sind nicht mit einer schnellen Reaktion auf tagesaktuelle Ereignisse vereinbar. Die Möglichkeit der Forschung auf gravierende, thematisch zum Forschungsprojekt einschlägige Cybersicherheitsvorfälle schnell unterstützend reagieren zu können, würde den Betroffenen sehr helfen. Direkte wissenschaftliche Konkurrenz kann gerade im Cybersicherheitsbereich fruchtbar wirken. So gibt es beispielsweise in den USA von der DARPA ausgeschriebene Förderungen im Cybersicherheitsbereich mit Wettbewerbscharakter, die sogenannten »Grand Challenges«. An diesen können sich mehrere Einrichtungen beteiligen, die identische angewandte Forschungsaufgaben bearbeiten; dies könnte auch für Deutschland ein Vorbild sein. In Deutschland werden besondere Leistungen aus der Vergangenheit zwar bei der Auswahl von neu beantragten Folgeprojekten berücksichtigt, allerdings gibt es keine Anreizsysteme für Spitzenforschungsergebnisse und gelungenen Transfer während der Projektlaufzeit und an deren Ende. Die aktuelle politische Tendenz

27 *https://dcso.de/de/*

der Entglobalisierung kann dazu genutzt werden, Spitzenforscherinnen und Spitzenforscher (zurück) nach Deutschland zu holen.

- *Organisatorische Einbettung:* Zur Verbesserung der aktuellen Lage der Cybersicherheit genügt es nicht, sich auf die Weiterentwicklung von Technik allein zu beschränken. Es müssen darüber hinaus Instrumente und Mechanismen zur Anwendung kommen, mittels derer Organisationen hinreichend motiviert sind, das Sicherheitsniveau von Produkten, Dienstleistungen und Infrastrukturen entsprechend hoch zu halten. Die der organisatorischen Einbettung zuzuordnenden Instrumente und Mechanismen zur Verbesserung des Sicherheitsniveaus können beispielsweise von rechtlicher oder wirtschaftlicher Dimension sein oder sie können aufgrund von hoheitlichen Aufgaben von staatlicher Seite übernommen werden. Im Bereich der Regulierung können verschiedene Beispiele angeführt werden, mit denen von staatlicher Seite der Rahmen für Sicherheit und Datenschutz gestaltet wurde, wie etwa durch das IT-Sicherheitsgesetz, die KRITIS-Verordnung, den »Hackerparagraphen« im Strafgesetzbuch (§202c StGB) oder die Datenschutzgrundverordnung der EU. Bereits in der Anwendung befindliche Instrumente zur Verbesserung der Cybersicherheitslage, die der wirtschaftlichen Dimension zuzuordnen sind, sind uns nicht bekannt. Diese wurden unserer Kenntnis nach bisher nur in anderen Technologiebereichen oder Wirtschaftsbranchen angewendet, wie etwa bei der Abwrackprämie für PKW oder bei der Förderung regenerativer Energien. Im Bereich der hoheitlichen Aufgaben zur Verbesserung von Infrastrukturen mit Bezug zu Cybersicherheit und Datenschutz sind etwa der neue Personalausweis oder die elektronische Gesundheitskarte zu nennen.

- *Verständnis der Implikationen neuer Technologien für grundrechtliche Werte:* Die Anwendung von und der Umgang mit neuen Technologien und insbesondere Cybersicherheitstechnologien in der Praxis hat oftmals erhebliche Auswirkungen auf Werte, die im Rahmen des Grundgesetzes oder der Menschenrechte gelten, wie etwa Meinungsfreiheit, Privatsphärenschutz, Schutz von Minderheiten oder Schutz unserer demokratischen Grundordnung. So können etwa Werte durch bestimmte Anwendungen von neuen Technologien bedroht werden. Da Interessen oder Rechte hierbei konkurrieren können, müssen sie sorgfältig gegeneinander abgewogen werden, z.B. wirtschaftliche Interessen gegen das Recht auf Datenschutz, Interesse zur präventiven Überwachung gegen Datenschutz oder rein defensive gegen offensive Handlungsfähigkeit. Das erfordert ein tiefes Verständnis potenzieller Auswirkungen dieser Technologien auf grundrechtlich verankerte oder sons-

tige Werte. Bestimmte Fragestellungen zur Dualität konkurrierender Werte konnten in der Vergangenheit im Rahmen von öffentlich geförderten Forschungsprojekten immer wieder interdisziplinär untersucht werden, z.B. im Rahmen des BMBF-Projektes »Forum Privatheit«[28].

Ausgehend von diesem Stand muss sich der Rahmen für Cybersicherheit weiter entwickeln, damit die folgenden Ziele verfolgt werden können:

- *Steigerung von Sicherheit und Privatsphäre:* Das tatsächliche Sicherheitsniveau praktisch verwendeter Technologie muss verbessert werden. Hierzu müssen durch Stärkung von Grundlagenforschung und anwendungsorientierter Forschung im Bereich Cybersicherheit Ergebnisse produziert werden, durch welche die aktuelle Cybersicherheit verbessert werden kann. In diesem Zusammenhang müssen neue Wege gefunden und beschritten werden, über welche diese Ergebnisse in die praktische Anwendung gelangen.

- *Berechtigtes Vertrauen:* Durch die Weiterentwicklung der Cybersicherheitsforschung soll ein Zustand erreicht werden, in dem Anwender – also Unternehmen, Behörden und Bürger – ein berechtigtes Vertrauen in neue Technologien und Dienste haben. Die Digitalisierung darf nicht dazu führen, dass für Bürgerinnen und Bürger das reale Sicherheitsniveau absinkt.

- *Gestaltung von Cybersicherheit und Datenschutz durch Strategie und Umsetzung:* Die effektive Gestaltung des Rahmens zur Verbesserung von Cybersicherheit und Datenschutz erfordert die Identifikation der relevanten Ansatzpunkte für Maßnahmen zur Steuerung. Hierbei können die drei Kompetenzzentren unterstützen.

## 2.4 Prognosen

Wir gehen davon aus, dass sich die Rahmenbedingungen für Cybersicherheit zukünftig folgendermaßen weiterentwickeln werden:

- *Verbreitung von Angriffswerkzeugen und Organisation von Angreifern:* Waren für Angriffe früher ausgeprägte Hackerkenntnisse erforderlich, so wird es zunehmend Angriffswerkzeuge geben, auf die man zur Durchführung von Angriffen zurückgreifen kann. Darüber hinaus werden sich Angreifer der Zukunft durch einen immer höheren Organisationsgrad auszeichnen, sie

28 *https://www.forum-privatheit.de/forum-privatheit-de/index.php*

verfügen über mehr finanzielle Mittel und ihre Angriffstechniken werden sich permanent weiterentwickeln.

- *Zukünftige Durchbrüche bei Angriffstechniken:* Mit der Entwicklung neuer Angriffstechniken wird es zukünftig immer wieder Quantensprünge hinsichtlich neuer Bedrohungen geben. Diese Durchbrüche tragen dazu bei, dass Angreifer immer mächtiger werden.

- *Vergrößerung der Angriffsfläche:* Informationstechnologie wird immer weiter in vernetzte Geräte verschiedener Technologie- und Anwendungsbereiche diffundieren, die früher keine Informationstechnologie verwendet haben. Bei vielen dieser auf den Markt gebrachten Geräte wurde Cybersicherheit nicht berücksichtigt.

- *Zunahme datenzentrierter Geschäftsmodelle:* Die Weiterentwicklung von datenzentrierten Geschäftsmodellen auf Basis neuer Big-Data-Algorithmen wird die Privatsphäre von Bürgerinnen und Bürgern immer stärker bedrohen.

- *Unzureichendes Lifecycle-Management im Internet der Dinge:* Die Geräte in dem sich immer weiter vergrößernden Internet der Dinge bieten keine hinreichenden Funktionen, um die Schutzmechanismen der Geräte zu aktualisieren.

- *Weitere Zunahme von Komplexität:* Die Menge der IT-Systeme, deren Sicherheit nicht mehr nur mit klassischen ingenieurmäßigen Methoden und Denkweisen behandelt werden kann, wird zunehmen.

- *Entglobalisierungstendenzen der Weltwirtschaft:* Im Rahmen protektionistischer Ansätze vereinzelter Länder wird der Markt für die stark exportorientierte Wirtschaft Deutschlands kleiner. Dadurch kann sich der Wettbewerb verschärfen. Cybersicherheit ist ein wichtiges Qualitätsmerkmal von Produkten und Diensten im Wettbewerb.

# 3 Sieben Thesen zur Cybersicherheit in Deutschland

## 3.1 These 1: Strategisches Ziel »Digitale Souveränität«

**These 1:** Die Entwicklung der Cybersicherheit muss auf nationaler und europäischer Ebene strategiegetrieben sein. Die Verbesserung der digitalen Souveränität muss dabei ein vorrangiges strategisches Ziel sein. Die Abhängigkeit von IKT, der man mangels Überprüfbarkeit der IKT und ihrer Hersteller blind vertrauen muss, muss reduziert und das vorhandene hohe Potenzial in Deutschland und Europa für Forschung und Entwicklung muss besser genutzt werden. Zugleich muss die enge internationale Kooperation in Forschung und Entwicklung mit Partnern in Europa, aber auch mit in Cybersicherheit führenden Nationen wie USA und Israel, fortgesetzt und ausgebaut werden. Deutschland zeichnet sich durch Offenheit, Schutz von Menschenrechten und gesellschaftliche Stabilität aus – Eigenschaften, die Deutschland zum idealen Standort für Hochtechnologiefirmen und Arbeitsort für hochqualifizierte Mitarbeiter machen. Die Fortschreibung und Ausgestaltung der Cybersicherheitsstrategien brauchen feste, ressortübergreifende Strukturen.

Um die Cybersicherheit und den Schutz der Privatsphäre nachhaltig verbessern zu können, ist eine Fortschreibung der deutschen und europäischen Cybersicherheitsstrategie erforderlich. Diese Strategie muss in einem Top-Down-Ansatz die wesentlichen Handlungsfelder ressortübergreifend angehen und die ressorttypischen Perspektiven und Anwendungsfelder umfassen. Für die Entwicklung und Fortschreibung dieser Strategie sollte es feste Strukturen geben, in denen alle relevanten Interessensvertreter eingebunden sind. Zur Implementierung dieser Struktur braucht es die Fähigkeit, innerhalb von komplexen technischen und organisatorischen Gemengelagen die wesentlichen Problemfelder und Ansatzpunkte zur Verbesserung der IT-Sicherheitslage identifizieren zu können, die darüber hinaus in der Umsetzung durch geeignete Instrumente zentral gesteuert und koordiniert werden können. Diese Steuerung und Koordinierung sollte sich auch auf die Forschungsgestaltung der Cybersicherheit auswirken.

Die Cybersicherheitsstrategie sollte hierbei durch das Ziel geleitet sein, die technologische Abhängigkeit von Deutschland und Europa insbesondere in kritischen Bereichen zu reduzieren. Spätestens seit den Enthüllungen von Snowden ist bekannt, wie massiv und mit welchen Mitteln andere Länder ihre Interessen gegenüber Deutschland und Europa durchsetzen. Aktuelle politische Entwick-

lungen wie die Brexit-Entscheidung[29] oder die Ankündigungen von Donald Trump, internationale Abkommen zu stoppen bzw. aufzukündigen,[30] legen die Vermutung nahe, dass der Protektionismus in der Welt zunehmen wird.[31] Daher ist es wichtig, dass sich Deutschland und Europa technologisch weniger abhängig machen. Das bedeutet auch, dass sich Deutschland und Europa hinsichtlich Cybersicherheit durch eigene Aktivitäten besser schützen müssen.

Grundsätzlich sind Deutschland und Europa für diese Herausforderungen gut aufgestellt; es sind viele Stärken vorhanden. Im Rahmen der Cybersicherheitsstrategie muss es daher auch darum gehen, die relevanten Stärken zu identifizieren und in geeigneter Weise zu bündeln. Dort, wo es noch entscheidende technologische Lücken gibt, sollten die Lücken geschlossen werden. Dies kann mit geeigneten Instrumenten und Anreizsystemen unterstützt werden. Hierbei kann es sich um Instrumente handeln, die im Wirtschaftssystem (z.B. durch Subventionen) oder im Wissenschaftssystem (z.B. im Wettbewerb um die besten Köpfe; siehe hierzu auch These 7) ansetzen.

Die internationale Zusammenarbeit in der Forschung und Entwicklung zur Cybersicherheit bleibt im Bereich der Cybersicherheit entscheidend. Insbesondere die Zusammenarbeit mit den europäischen Partnern und den in Cybersicherheit führenden Nationen wie Israel und USA muss auch weiterhin gefördert werden.

Weitere positive Effekte können durch eine Verbesserung von Rahmenbedingungen und des Innovationsklimas erreicht werden. Deutschland zeichnet sich durch Werte aus wie Meinungsfreiheit, Demokratie, offene Gesellschaft und Schutz von Minderheiten. Angesichts des Trends zu Entglobalisierung sind diese Werte wichtige Argumente für kluge Köpfe im Ausland, nach Deutschland zu kommen und hier zu arbeiten.

29 Süddeutsche Zeitung: »May kündigt Austritt aus dem EU-Binnenmarkt an«, 17.1.2017, *http://www.sueddeutsche.de/politik/brexit-may-kuendigt-austritt-aus-dem-eu-binnenmarkt-an-1.3336155*

30 Süddeutsche Zeitung: »Trump verordnet Ausstieg aus Freihandelsabkommen TPP«, 23.1.2017, *http://www.sueddeutsche.de/wirtschaft/usa-trump-verordnet-ausstieg-aus-freihandelsabkommen-tpp-1.3346340*

31 Matthias Hartwig: »Tendenz zur Abschottung«, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht 18.11.2016, *https://www.mpg.de/10831101/voelkerrecht-verbindlichkeit*

## 3.2 These 2: Mindeststandards und Produkthaftung

> **These 2:** Berechtigtes Vertrauen in Informationstechnologie entsteht, wenn adäquate Mindeststandards für Sicherheit und Privatsphärenschutz und Testierung nachgewiesen und über Beschaffungsregeln eingefordert werden. Die Verantwortung über Sorgfaltspflichten (z.B. Verwendung von auf die Sicherheitsqualität ausgerichteter Entwicklungsprozesse, verbindliche und schnelle Behandlung sicherheitsrelevanter Schwachstellen) und Haftungsregeln von Produkten und Dienstleistungen müssen festgelegt werden.

In allen Branchen führen risikoadäquate Mindeststandards bezüglich Cybersicherheit zu einem erheblichen Vertrauenszuwachs. Die Notwendigkeit für solche Standards liegt beispielsweise für die Finanzdienstleistungsbranche auf der Hand, wie auch die Erklärung der G7-Staaten vom 7. Oktober 2016 besagt.[32] Die Beschaffung im IT-Bereich muss sowohl in der öffentlichen Hand als auch in allen Branchen passende IT-Sicherheitsmechanismen für Produkte und Dienste als Kriterien enthalten. Dies ist eine notwendige Bedingung für die Wirtschaftlichkeit einer Lösung, nur bei Einhaltung dieser Kriterien können Gestaltungsziele der Cybersicherheit erreicht werden. Dementsprechend sind nachgewiesene Sicherheitsgarantien für den Betrieb von IT und die Nutzung von IT-Services erforderlich. In kritischen Anwendungsbereichen müssen zudem Sicherheitstests nachgewiesen werden. Hierfür sollten Standards für Tests entwickelt werden, die nicht schwerfällig sind, sondern praktisch anwendbar. Standards müssen zudem Möglichkeiten zur Weiterentwicklung von Software, Hardware und Diensten berücksichtigen, so dass folgende Fragen geklärt werden können: Ab wann sind neue Tests erforderlich, bis wann sind partielle Tests hinsichtlich veränderter Teile möglich und schließlich ab wann muss ein komplettes Produkt (erneut) getestet werden. Zudem kann es ein großer Beitrag für die Cybersicherheit sein, wenn leicht feststellbar ist, welche Produkte und Dienste (sicherheits-)kritisch für den Betrieb sind.

Klare Haftungsregeln bezüglich Cybersicherheit implementieren Verantwortlichkeit und erhöhen damit zwangsläufig das Sicherheitsniveau. Die weit ausgereiften Regelungen zur Arzneimittelhaftung und Medizinproduktehaftung können hier Orientierungspunkte und Vorbilder sein.

[32] »G7 Fundamental Elements of Cybersecurity for the Financial Sector«, 11.10.2016, *http://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Internationales_Finanzmarkt/Internationale_Finanzpolitik/2016-10-11-Cyber-Sicherheit-download.pdf*

## 3.3 These 3: Cybersicherheitsinfrastrukturen

**These 3:** Die digitale Gesellschaft braucht für ihre Cybersicherheit Infrastrukturen, z.B. für digitale Identitäten, Verschlüsselung und die Beurteilung von Produkten und Diensten, die ebenso von Staat und Wirtschaft gefördert werden müssen wie andere öffentliche Infrastrukturen, z.B. Straßen.

Ähnlich wie der Staat mit Straßen und Autobahnen Infrastrukturen für den Verkehr bereitstellt, diese unterhält und durch Verkehrsregeln und Kontrolle der Einhaltung dieser Regeln zur Sicherheit von Verkehrsteilnehmern beiträgt, sollte der Staat auch für den Aufbau und den Betrieb von Cybersicherheitsinfrastrukturen sorgen. Durch den Betrieb solcher Infrastrukturen kann der Staat dazu beitragen, dass Bürgerinnen und Bürger und auch Unternehmen bei der Nutzung von Informations- und Kommunikationstechnologie besser geschützt sind. Den Aufbau von entsprechenden Infrastrukturen durch nichtstaatliche Akteure voran zu treiben ist schwierig und hat sich in der Realität bisher als nicht praktisch erwiesen. Ohne entsprechende Infrastrukturen für Cybersicherheit wie etwa Public-Key-Infrastrukturen sind bestimmte sichere Varianten von IT-Anwendungen wie der vertraulich durchgeführte Austausch von Nachrichten praktisch nicht möglich.

Über diese Infrastrukturen hinaus sollte der Staat seine Bürgerinnen und Bürger und seine Unternehmen durch das Angebot von Dienstleistungen unterstützen. Immer wenn heute Schwachstellen oder Angriffe bekannt werden, von dem viele Personen oder Unternehmen betroffen sind, müssen entsprechenden Informationen zu den Anwendern gelangen. Bei den heute hierfür verwendeten Strukturen müssen entsprechende Informationen dann von vielen Anwendern parallel zusammengetragen werden. Der Großteil von Bürgerinnen und Bürgern kann diese Informationen nicht selbsttätig zusammentragen, die Informationen entsprechend einordnen und bewerten sowie darauf aufbauend Entscheidungen treffen. Innerhalb von Unternehmen kann man dies prinzipiell zwar typischerweise etwas einfacher umsetzen, jedoch bedeutet dieser Schritt, dass in den betroffenen Unternehmen parallel dieselbe Arbeit durchgeführt wird. Dieses Vorgehen ist nicht effizient; aufgrund der wiederholten Bearbeitung der gleichen Aufgabe werden dadurch Werte vernichtet. Für die Behandlung von solchen Anfragen, die sich auf tagesaktuelle Begebenheiten beziehen, können zunächst einmal Werte dadurch geschützt werden, indem entsprechende Arbeiten zentralisiert im Rahmen von Diensten durchgeführt und potenziell betroffenen Anwendern angeboten werden. Um diese umzusetzen müssten Strukturen geschaffen und aufgebaut werden, welche die Fähigkeit besitzen sollten, entsprechend agil auf die Bedarfe von Anwendern einzugehen.

## 3.4 These 4: Stärkung von Grundrechten

> **These 4:** Grundrechte und Werte können durch Informationstechnologie gestärkt werden. Dies gelingt aber nur, wenn auch der gesellschaftliche Interessensausgleich gelingt. Das Leitprinzip dieses Ausgleichs ist in Deutschland der Wertekanon des Grundgesetzes. Der Schutz der Grundrechte aller Bürger – in Deutschland wie im Ausland – sollte dabei Vorrang haben vor dem Wunsch, datenbasierte Geschäftsmodelle oder die Überwachung von Verdächtigen zu vereinfachen. Insbesondere sollte es keine Einschränkungen der Kryptographie geben, weder im Inland noch – durch Exportkontrolle – im Ausland.

Die Weiterentwicklung des Verständnisses des Dualismus von Themen der Cybersicherheit und des Privatsphärenschutzes ist eine dauerhafte gesellschaftliche Aufgabe.

Beispielsweise ist Ende-zu-Ende-Verschlüsselung ein wichtiger Mechanismus zur Erreichung der grundgesetzlich garantierten Vertraulichkeit individueller Kommunikation. Gleichzeitig schafft die Bundesregierung eine eigene Stelle, die Strafverfolgern und Staatsschützern zum Zwecke der Strafverfolgung oder der Gefahrenabwehr bei der Dechiffrierung von verschlüsselter Kommunikation helfen soll.

Ein weiteres Beispiel ist das Spannungsfeld zwischen Freiheit, Privatsphärenschutz, Versammlungsfreiheit und dem Schutz von Leib und Leben. Die Verantwortlichen zur Planung von Polizeieinsätzen stehen immer wieder vor der Frage, wie viel Personal sie für bestimmte Ereignisse einplanen sollen. Ein Beispiel, bei dem es eine gravierende Fehleinschätzung bei der Einsatzplanung gab, waren die Silvesterereignisse 2015/16 in Köln. Die unzureichende Planung hat dazu geführt, dass nicht genügend Einsatzkräfte vor Ort waren, um Bürgerinnen und Bürger in angemessener Weise schützen zu können. Die Polizei soll zum Wohle der Gesellschaft präventiv einwirken. Der Einsatz moderner Informationstechnologie (z. B. die anonymisierte Auswertung von Informationen aus sozialen Netzen) kann dazu beitragen, dieses Ziel ressourcenschonend und balanciert zu den anderen gesellschaftlichen Interessen wie Freiheit, Privatsphärenschutz und Versammlungsfreiheit zu erreichen.

Ein von der Forschung begleiteter Diskurs vermag Orientierung für den gesellschaftlichen Ausgleich in diesen und in anderen Fällen der Kollision zwischen Werten des Grundgesetzes zu bringen. Als Leitprinzip muss hier die Priorisierung von Vorhaben zur Verteidigung der Werteordnung des Grundgesetzes als tragende Säule unserer Gesellschaftsordnung gelten. In allen staatlichen geförderten Vorhaben sollte der Schutz der Grundrechte aller Bürger – in Deutschland wie im Ausland – Vorrang haben vor dem Wunsch, datenbasierte Geschäftsmodelle oder die Überwachung von Verdächtigen zu vereinfachen. Ins-

besondere sollte es keine Einschränkungen der Kryptographie geben, weder im Inland noch – durch Exportkontrolle – im Ausland.

## 3.5 These 5: Aus- und Weiterbildung

> **These 5:** Deutschland und Europa brauchen mehr Fachkräfte, die im Bereich Cybersicherheit qualifiziert sind. Mindestbewusstsein von Cybersicherheit sollte in schulischer Ausbildung und beruflicher Weiterbildung fest verankert sein.

Am dringendsten werden aktuell Bildungs- und Weiterbildungsangebote für Cybersicherheit benötigt, die Fachkräfte schnell und bedarfsspezifisch in der Thematik qualifizieren. Staatliche Hochschulen und Universitäten in Deutschland haben ihre Kernkompetenz in der Lehre vor allem in der akademischen Erstausbildung; von daher ist es aussichtsreich und effizient, Qualifizierungsmöglichkeiten im Weiterbildungsbereich jenseits von Hochschulen zu verstärken bzw. neu aufzubauen. Diese müssen breit angelegte Programme für verschiedene Empfängergruppen anbieten, die zudem einen möglichst hohen Praxisbezug haben, damit das Gelernte unmittelbar in der Arbeitsumgebung angewendet werden kann. Die Aus- und Weiterbildung in allen Informatik- und informatiknahen Fächern muss die Vermittlung von grundlegenden Cybersicherheitskenntnissen beinhalten. In allgemeinbildenden Schulen ist die frühe Sensibilisierung bezüglich des Themenfeldes durch die Integration in Lehrpläne zu erzielen. Dies wirkt dem digitalen Analphabetismus in einem Schlüsselbereich entgegen, denn Kenntnisse über Cybersicherheit sind eine Grundvoraussetzung für die mündige Nutzung von Informationstechnologie.

## 3.6 These 6: Cybersicherheitsforschung

> **These 6:** Angesichts zunehmender Bedrohungen der Cybersicherheit ist mehr exzellente Forschung erforderlich, im Sinne von Grundlagen- und Technologieforschung.

Die anhaltende massive Diffusion von Informationstechnologie mit all ihren Schwachstellen und die vielen real stattfindenden Angriffe tragen dazu bei, dass der Bedarf an Cybersicherheitsforschung und -entwicklung steigt. Die immer mächtiger werdenden Angreifer und die sich stets weiter entwickelnden Angriffsmethoden bei immer komplexer werdenden IT-Systemen können ansonsten nicht effektiv behandelt werden. Hier sind Forschung und Entwicklung

in allen Technologiereifegraden[33] gefordert, von der erkenntnisorientierten Grundlagenforschung über die angewandte Technologieforschung bis hin zur Erprobung und Einführung im Markt.

Um exzellente und letztlich verwertbare Ergebnisse produzieren zu können, muss sich die Cybersicherheitsforschung an möglichst realistischen Rahmenbedingungen orientieren.

Die Cybersicherheitsforschung muss die Sicherheit der IT-Systeme von morgen behandeln, sie muss sich aber in mindestens gleichem Maße um die Sicherheit der bereits vorhandenen Informationstechnologie kümmern. Es müssen hierbei die typischen, realen Bedingungen heutiger IT-Entwicklung und Integration berücksichtig werden, bei denen viele technische Komponenten verschiedener Hersteller für einzelne Produkte und Dienstleistungen verwendet werden. Gerade die Verbesserung der Sicherheit von bereits vorhandener Technologie stellt die Forschung vor besondere Herausforderungen. Aufgrund der gegebenen technischen Ökosysteme, mit denen sich die Cybersicherheitsforschung hier auseinanderzusetzen hat, ist davon auszugehen, dass das klassische Repertoire von Methoden und Denkweisen der Cybersicherheitsforschung, die sich an Korrektheit und Vollständigkeit orientieren, um neue Ansätze zu erweitern ist, die in den empirisch orientierten Naturwissenschaften angewendet werden, z.B. der Biologie und Physik. Bei wissenschaftlichen Untersuchungen rücken zunehmend Gegenstände wie Implementierungen in Form von relevanten IT-Produkten oder deren Konfigurationen in den Mittelpunkt der Analyse.

Wurde in der Vergangenheit eher defensiv-orientierte Cybersicherheitsforschung durchgeführt, so wird die Cybersicherheitsforschung zur Stärkung von Prävention, Detektion und Reaktion auch verstärkt offensiv ausgerichtet sein müssen.

Für eine Diskussion aktueller Forschungsthemen sei auf das Positionspapier verwiesen, das im Rahmen des BMBF-geförderten Projektes SecUnity entstand.[4]

33 *https://de.wikipedia.org/wiki/Technology_Readiness_Level*

## 3.7 These 7: Innovationsrahmen für Cybersicherheit

**These 7:** Innovation durch Forschung und Entwicklung braucht einen Rahmen, der bewusst wettbewerbliche exzellente Forschung sowie den Transfer aus Deutschland und Europa in den internationalen Markt fördert. Clusterbildung, wettbewerbliche Forschung und die kommerzielle Verwertung von Forschung muss gewollt und im Rahmen der Forschungsförderung unterstützt werden. Die Schaffung von Startups in Cybersicherheit muss gezielt vorbereitet und gefördert werden. Regulatorische Vorgaben, die nationale Lösungen erzwingen und damit die internationale Vermarktung behindern, müssen abgebaut bzw. angepasst werden.

Mit der Schaffung von drei Kompetenzzentren durch das BMBF und eines Kompetenzzentrums durch das BMVg (siehe Abschnitt 2.2) unterstützt die Bundesregierung bereits die Entstehung exzellenter Forschungscluster. Diese Strategie muss fortgesetzt und auch die operationale Einbindung der existierenden Zentren in die Cybersicherheitsstrategie muss ausgebaut werden.

Der Forschungsförderrahmen in Deutschland zielt ab auf die Förderung wohldefinierter, sich inhaltlich möglichst wenig überlappender Projekte mit möglichst geringem Risiko des Scheiterns. Dies gilt auch für die o.g. Kompetenzzentren des BMBF, deren Finanzierung sich aus solchen Projekten zusammensetzt. Dieser Rahmen muss so erweitert werden, dass auch gezielt exzellente Projekte unterstützt werden, die miteinander im Wettbewerb um die beste Lösung desselben Problems stehen.

Für die Förderung von in diesem Sinne wettbewerblichen Projekten gibt es gut funktionierende Vorbilder aus anderen Ländern. Ein Beispiel sind die sehr erfolgreich durchgeführten »Cyber Grand Challenges« von DARPA in den USA. An diesen können sich mehrere Einrichtungen beteiligen, die identische angewandte Forschungsaufgaben der Cybersicherheit bearbeiten. Mehrere erhalten hierfür eine Förderung und treten am Ende wettbewerblich gegeneinander an. Es gibt in den USA keine Vorbehalte bezüglich Mehrfachförderung der Erforschung desselben Themas bei verschiedenen Einrichtungen. Mehrfachförderung wird in vielen Fällen weltweit sogar bewusst initiiert, weil sie in vielen Bereichen die besten Ergebnisse erzielt. Beispielsweise wurden in der Kryptographie die anerkanntesten und stabilsten Verfahren über Wettbewerbe unter parallel entwickelten Verfahren gefunden.

Neben der Förderung wohldefinierter Projekte sollte für die Zentren und generell für exzellente Köpfe auch ein »freies« Budget zur Verfügung gestellt werden, so dass diese die Mittel nach eigener freier Entscheidung und bei aktuellem Bedarf für strategisch drängende Fragen der Cybersicherheitsforschung einsetzen können. So erfordert beispielsweise das Bekanntwerden neuer An-

griffsmethoden oder Schwachstellen immer wieder Reaktionen, die *ad hoc* erfolgen müssen. Die Anforderung zur schnellen Reaktionsfähigkeit ist in der Cybersicherheitsforschung wie in keinem anderen Forschungsgebiet gegeben. Wir erwarten, dass sich dieses Extra-Budget in einem besonders hohen Maße für die Cybersicherheit auszahlen wird.

Bislang noch zu selten gelingt in Deutschland und Europa der Transfer von Forschungsergebnissen in den Markt.

Hürden, die einer Verwertung von Forschungsergebnissen im Cybersicherheitsbereich entgegenstehen, sollten abgebaut werden. Der Verwertungsweg sollte in Projekten nahtlos implementierbar sein und im Rahmen von Forschungsprojekten ausdrücklich gefördert werden.

Für Forschungseinrichtungen und junge Firmen sind die Anforderungen von Unternehmen und des Staates für Testinstallationen und Beschaffung oftmals unüberwindbare Hürden und stellen gerade gegenüber den etablierten, großen Anbietern einen entscheidenden Nachteil dar. Diese Hürden sollten generell gesenkt werden und gerade jungen Firmen und über nationale oder europäische Programme geförderten Technologien sollte der Markteintritt erleichtert werden.

Verwertungserfolge können auch durch Anreizsysteme für die beteiligten Forscher und Einrichtungen für Markt- und Verwertungserfolge erzielt werden; dies gilt für alle Forschungsprojekte der Cybersicherheit, unabhängig davon, ob sie eher grundlagenorientiert oder anwendungsorientiert ist.

Von besonderer Bedeutung ist auch die Schaffung neuer Unternehmen im Bereich der Cybersicherheit, also von Startups. Die entsprechenden Voraussetzungen (Ausbildung, Kapital, Infrastruktur, Vermarktungshilfen) müssen geschaffen und die daraus entstehenden Firmen gefördert werden. Die drei Zentren des BMBF können hier eine besondere Rolle spielen.

In Deutschland gibt es nur eine sehr kleine Zahl von in der Cybersicherheit auch international erfolgreicher Unternehmen. Dies ist besonders deutlich sichtbar, wenn man Deutschland z.B. mit Israel vergleicht: Deutschland hat grob zehnmal mehr Einwohner als Israel. Eine Studie von Cybersecurity Ventures ver-

zeichnet unter den Top-500 Anbietern weltweit 25 aus Israel, davon 8 unter den Top-100, aber nur 11 aus Deutschland, davon keines unter den Top-100.[34]

Um die Chancen deutscher und europäischer Firmen – Startups wie etablierter Unternehmen – zu verbessern, müssen deren Chancen im internationalen Markt verbessert werden. Dazu müssen insbesondere regulatorische Vorgaben, die nationale Lösungen als Sonderwege implizieren, bzw. die internationalen Anforderungen unberücksichtigt lassen und damit die internationale Vermarktung behindern, abgebaut bzw. international angepasst werden. Dies gilt auch für die Anforderungen an die Zertifizierung und die behördliche Zulassung von Produkten. Regulatorische Vorgaben und internationale Marktentwicklung sollten hierfür noch stärker synchronisiert und abgestimmt werden.

Anreizsysteme werden auch für den Bereich der Gewinnung von exzellenten Köpfen der Cybersicherheitsforschung empfohlen. Zudem lassen sich die Bedingungen für exzellente Köpfe verbessern, indem ihnen besondere Freiräume und ein Vertrauensvorschuss gewährt werden. Analog empfehlen wir auch bestimmte Projekte mit hohem Risiko gezielt zu fördern, wenn diese bei Erfolg hohe Potenziale versprechen.

[34] Cybersecurity Ventures: »World's Hottest Cybersecurity Companies to Watch in 2017«, 15.11.2016, *http://cybersecurityventures.com/cybersecurity-500/*

ISBN 978-3-8396-1164-7