# Sachverständigengutachten „IT-Infrastruktur"

**zur Anhörung des 1. Untersuchungsausschusses**

Dr. Sandro Gaycken[1], FU Berlin
Berlin, Juni 2014

Zu den Fragen des Untersuchungsausschusses nehme ich wie folgt Stellung:

**Zu Frage (2): Welche technischen Möglichkeiten bestehen, um Kommunikationsdaten und Kommunikationsinhalte ohne Wissen der Nutzer zu erfassen?**

Digitale Daten können durch Nachrichtendienste an allen Orten ihres Vorkommens unbemerkt abgegriffen werden. Die Nachweise sowohl zur Präsenz der Dienste an allen Orten sowie zu den hohen Schwierigkeiten der Detektion sind u.a. durch die Snowden Dokumente eindrücklich belegt. Die technische Möglichkeiten dazu sind überaus zahlreich und werden intensiv genutzt.

Als Beispiele für Orte des unbemerkten Zugriffs sind zu nennen:

- IT- und IT-Sicherheitsprodukte können in der Entwicklung, der Fabrikation oder der Auslieferung mit Schwachstellen infiziert und für einen Zugriff genutzt werden. Dies gilt für Hardware und Software allgemeiner Art wie auch für Spezialtechnologien wie etwa Netzwerkkomponenten. Bezeichnend sind hier die Aktivitäten der TAO-Einheit der NSA sowie die Berichte über das Projekt GENIE. Ebenfalls bezeichnend sind besondere Aktivitäten der NSA zur Infiltration besonders weit verbreiteter oder vermeintlich besonders sicherer Mechanismen, wie die vermuteten Aktivitäten an der Linux Mastercopy 2003 und in Kooperation mit der Firma RSA nahelegen;
- Endsysteme können über direkte externe oder interne Angriffe infiltriert und für einen Zugriff genutzt werden. Bezeichnend sind hier die verschiedenen Infiltrationsmöglichkeiten, die durch den „Shopping Catalogue" der ANT-Division der NSA nachgewiesen sind;
- Direkte oder produktbasierte Angriffe können bei jeder Variante von IT durchgeführt werden, von normalen PCs über Industriesteuerungstechnologien bis hin zu größeren Spezialtechnologien wie Routern. So können auch Daten bei Providern oder an Netzknoten wie dem DE-CIX abgegriffen werden;
- Datenströme können ebenfalls an Kabeln (von den großen Untersee-Datenkabeln bis zu den Kabeln für Tastaturen oder Beamer) oder auf Funkstrecken abgegriffen werden. Auch hier ist der Shopping Catalogue der ANT-Division bezeichnend;

[1] Senior Researcher, Department of Computer Science, Freie Universität Berlin; EastWest Institute Senior Fellow; Oxford University Martin School Fellow und Mitglied der Oxford University Arbeitsgruppe Cybersecurity (Cyberdefense); Associate Fellow des German Council on Foreign Relations; Director im NATO SPS Program on Cyberdefense and Cyberstrategy

- Daten können bei den Betreibern entsprechender IT-Dienstleistung und datenverarbeitender Verfahren (wie Google, Facebook, Firefox etc.) eingefordert oder abgegriffen werden.

In diesem Kontext ist darauf hinzuweisen, dass eine rein technische Betrachtung des Zugriffs zu kurz greift. Viele der Angriffsvektoren basieren auf wirtschaftlichen, politischen oder rechtlichen Grundlagen oder Maßnahmen, die ebenfalls adressiert werden müssen.

Besonders relevant ist bei diesen Zugriffen, dass diese Variante Angreifer viel Aufwand und Aufmerksamkeit auf eine Vermeidung jeder Detektion legt, indem bekannte Schwächen der Detektionsmechanismen wie Grundrauschen oder blind spots, Vektoren ohne Detektionsmechanismen oder parallele Angriffe auf die Detektionsmechanismen genutzt werden. Leider müssen in diesem Kontext die bestehenden Ansätze zur Detektion als zu ungenau und ineffizient bewertet werden. Es ist auch nicht klar, ob diese Ungenauigkeiten beseitigt werden können. Zwar sind Detektion, Forensik etc. gerade große und wichtige Leitparadigmen im IT-Security Markt, indem dort versucht wird, das Grundrauschen zu beseitigen und alles exakt sichtbar zu machen (hier ist Big Data ein wichtiges Verfahren), alle Vektoren abzudecken und alle potentiell illegitimen Prozesse zu identifizieren, jedoch gibt es einige grundlegende und systematische Bedenken bezüglich der nachhaltigen Wirksamkeit:

- Grundrauschen besteht in vielen verschiedenen Varianten, variiert und erhöht sich kontinuierlich;
- Geschickte Angreifer können ihre Angriffe sehr klein, sehr langsam oder sehr schnell machen, was selbst bei bereits stark reduziertem Grundrauschen immer noch zur Tarnung genutzt werden kann;
- Bei hoher Granularität sind Falschpositive nach wie vor zahlreich und reduzieren die Sensibilität des Systems;
- Anomalien müssen nicht nur gesehen, sondern auch verstanden werden;
- Viele illegitime Prozesse sehen für Maschinen vollkommen legitim aus, da sich ihre Illegitimität erst im außermaschinellen Kontext ergibt;
- Tabellen illegitimen Verhaltens sind oft entweder unscharf oder unvollständig;
- Die Degradierung von Angriffen durch eine Verhinderung der Wiederholbarkeit nach erfolgreicher Detektion ist nicht als effizient nachgewiesen, vor allem nicht für gezielte Aktivitäten;
- Big Data Analysen können durch ein gezieltes, maschinelles Fluten mit strukturierten Fehlinformationen getäuscht werden;
- Forensik kann leicht getäuscht werden;
- Die Detektionsmechanismen laufen in der Regel auf den gleichen Systemen, die sie schützen sollen und sind daher über diese Systeme selbst angreifbar;
- Dieser Fokus ist in der aktuellen Form ein neues Paradigma, auf das Angreifer sich noch beliebig einstellen können.

Weitere Punkte ließen sich anbringen.

Das Dunkelfeld insbesondere im Hinblick auf nachrichtendienstliche Angreifer muss als sehr groß angenommen werden. Ein Indikator dafür ist die Zahl der Operationen des US-Cybercommand 2011 nach den Dokumenten Edward Snowdens (231 Operationen) und die Zahl der detektierten Operationen in selbigem Jahr (1 Operation – „Flame“).

Aber auch die vielen bekannten Schwächen der Detektionsmechanismen bieten ausreichend Raum für entsprechende Spekulationen.

Eine Trennung der Nutzung elektronischer Kommunikation und der Nutzung von Festnetz-, Mobilfunk- und Satellitenkommunikation ist nur begrenzt sinnvoll, da viele dieser Kommunikationsweise gleichartig datenbasiert sind und über gleiche Basisstrukturen mit den gleichen Basisproblemen laufen. Eine Ausnahme bildet zum Teil die Satellitenkommunikation, die allerdings häufig ebenfalls unsicher gestaltet und angreifbar ist.

Während Zugriffe an allen Orten möglich sind, sind sie jedoch nicht an allen Orten gleichartig. Das Abgreifen von Daten ist an unterschiedlichen Orten unterschiedlich voraussetzungsreich, effizient, riskant und kostenintensiv für den Angreifer. Eine Kenntnis dieser Rahmenbedingungen in Kombination mit einer Kenntnis der strategischen Interessen und der taktischen Optionen möglicher Gegner kann bei der Gestaltung kontextuell effizienter Sicherheitsmaßnahmen helfen.

So ist in diesem Kontext etwa das „Schengen-Routing“ oder das „Deutschland-Routing“ mit einer entsprechenden Verpflichtung aller Dienstleister und Produkte zur Haltung ihrer Daten in Deutschland als effiziente Maßnahme zur Vermeidung einer massenhaften Auswertung der Daten normaler (also nicht in ausgezeichnetem Maße sicherheitsbedürftiger) Nutzerinnen und Nutzer auszuweisen. In diesem Fall wird einerseits eine eindeutige und klare rechtliche Situation und Verfügungsregelung über Daten hergestellt, während zusätzlich eine massenhafte Auswertung von Daten taktisch erheblich erschwert wird, da ein massenhafter illegaler Abfluss schnell detektiert und abgestellt werden kann. Gleichzeitig ist ein solches Routing im Vergleich zu anderen Maßnahmen relativ problemlos und kostengünstig einzuführen. Gegen Massenüberwachung durch ausländische Unternehmen oder über ausländische Datenleitungen ist dies also eine wirksame Maßnahme. Eine wirksame und verlässliche Ende-zu-Ende-Verschlüsselung wird für normale Nutzerinnen und Nutzer ebenfalls eine gute Sicherheitswirkung gegen Massenüberwachung entfalten, da die Nachrichtendienste eine gezielte Unterwanderung oder ein massenhaftes Brechen der Verschlüsselungen als Aufwand nicht aufbringen können.

**Zu Frage (3.1): Wie werden aus massenhaft erfassten Kommunikationsdaten Informationen von nachrichtendienstlichem Interesse generiert?**

In der Regel werden diese Kommunikationsdaten nach verdächtigen Daten, nach verdächtigen Mustern und nach verdächtigen Querverbindungen durchsucht. Die Beschreibungen dessen, was als „verdächtig“ bewertet wird, werden durch die Beobachtung und Analyse bekannter Verdachtsfälle oder durch bereits bekannte Daten zusammengestellt (sog. „strong selectors“). Anders beschrieben: Über andere Quellen bekannte Personen und Netzwerke werden direkt aussortiert und intensiv beobachtet, gleichzeitig über die Jahre aber auch auf typische taktische und kommunikative Muster und weitere Verbindungen und Ausdehnungen hin analysiert, die folgend maschinell formuliert und zur automatischen Massenanalyse genutzt werden können. Entsprechend als potentiell verdächtig ausgewiesene Daten werden von Analysten überprüft, wobei ein Großteil der Daten Falschpositive sind, die wieder verworfen werden.

**Zu Frage (3.2): Weshalb sind bereits Metadaten eine wertvolle Informationsquelle?**

Metadaten liefern etwa grundlegende Informationen über Personen, Autoren von Dokumenten, soziale Netzwerke, genutzte Technologien, einige Verhaltensweisen, geographische Regionen, strategisch relevante Anomalien (zB deutsche Sprache auf religiösen Dokumenten im Iran), Zeiten oder bestimmte Kommunikationsverhaltensweisen. Anhand der zuvor erstellten Suchraster lassen sich so über Musteranalysen bereits einige verdächtige Kommunikationen erkennen und de-anonymisieren, wobei aber häufig weitere gezieltere Aktivitäten wie etwa ein direkter Zugriff auf die Kommunikationen und ihre Inhalte oder auch eine reale physische Identifikation vor Ort folgen müssen.

Die taktische Wertigkeit von Metadaten ist derzeit umstritten. Angreifer haben sich in den letzten Jahren immer besser auf diese Methoden der Analyse eingestellt, und die NSA hat die Maßnahme intern auch als wenig effizient bewertet[2]. Wie bei vielen bereits länger im Umlauf befindlichen Maßnahmen haben sich insbesondere professionellere und damit gerade die gefährlichen Akteure intensiv auf diese Techniken eingestellt und sind effizient in ihrer Umgehung, so dass nur weniger talentierte Akteure damit identifiziert werden. Die umfangreichen Publikationen der NSA-Dokumente werden die Nutzbarkeit weiter beeinträchtigen. Da im Umfeld des Terrorismus aber natürlich auch kommunikationstechnisch weniger talentierte Akteure gefährlich sein können, ist in dieser Hinsicht nach wie vor von einer gewissen Effizienz der Analyse von Metadaten auszugehen. Für andere Akteure, insbesondere höherstehende Terroristen, organisierte Kriminelle und ähnliche, müssen dagegen stärker gezielte technische Maßnahmen wie hochwertige Fähigkeiten des Hacking oder des Hackbacks entwickelt werden. Diese und weitere fortgeschrittene, gezielte Fähigkeiten sowie stärker konventionelle Ermittlungsarbeit werden inzwischen von vielen Seiten als deutlich effizienter empfunden. Ein Ausbau dieser Fähigkeiten ist zu empfehlen, nicht zuletzt auch aufgrund des Umstands, dass diese Fähigkeiten keine Massenüberwachungen erforderlich machen und damit deutlich datenschutzsensibler sind.

**Zu Frage (3.3): Wie funktioniert der technische Zugriff auf Nutzerdaten im Rahmen von Projekten wie PRISM und TEMPORA?**

Der technische Zugriff auf Nutzerdaten ist in den unterschiedlichen Projekten je verschieden.

Im Kontext des Projekts PRISM scheinen nach den gängigen Dokumenten vor allem rechtliche Zugriffe auf die Daten bei Providern und Internet-Dienstleistern zu bestehen, die durch den CALEA Act, den Patriot Act und den Protect America Act sowie den FISA konstituiert werden und die zum Teil über automatisierte Verfahren wie das Unified Targeting Tool, zum Teil über operative Kooperationen wie mit der Data Intercept Technology Unit des FBI erreicht werden. Danach werden die Daten automatisiert und manuell innerhalb der Dienste weiterverarbeitet. Möglicherweise existieren auch direkte technische Schnittstellen zu Produkten oder den Datenbanken der Provider und IT-Unternehmen. Die oft gehörten Aussagen der Betreiber und Dienstleister, nicht oder nicht wissentlich kooperiert zu haben, müssen vor dem klaren rechtlichen Hintergrund,

[2] Persönliche, verlässliche Kommunikation

den Indikatoren zu PRISM und dem großen strategischen Interesse an diesen Zugriffen als äußerst fragwürdig gelten.

Im Kontext des Projekts TEMPORA findet vor allem eine Sammlung und Auswertung der Daten statt, die durch die transatlantischen Fiberglaskabel an der Küste Englands laufen, die große Teile der transatlantischen Datenkommunikation beinhalten, aber vermutlich auch eine Sammlung und Auswertung von Daten aus anderen Quellen wie den Daten englischer IT-Unternehmen und Provider. Die Kabel und die Dienstleister, die sie betreiben, gehören unter englische Territorialität und können über den Regulation of Investigatory Powers Act (Ripa) angezapft werden. Entsprechende IT-Firmen und Provider mussten nach Angaben des Guardian dazu kooperieren, so dass unklar ist, ob die Kabel direkt angezapft werden oder ob die Daten bei den Betreibern abgeholt werden.

**Zu Frage (3.4): Wie funktioniert XKeyscore und ähnliche Programme?**

Diese Programme können erneut sehr unterschiedlich ausfallen.
Das Programm XKeyscore hat mehrere Funktionen:

- es dient zur Abfrage von gesammelten Daten an den verschiedenen Standorten (über 700 Server an 150 Standorten werden genannt, auch GPRS und WLAN können angegangen werden) der hier kooperierenden Nachrichtendienste nach verschiedensten Kriterien;
- es dient der gezielten Beobachtung von Zielen in Echtzeit, ihrer Websessions und anderer Aktivitäten, sofern diese Ziele über die angezapften Wege kommunizieren;
- es kann auch ausgewählte Inhalte wie Inhalten von Word-Dokumenten identifizieren, durchsuchen, speichern und verfügbar machen;
- es sortiert eigenständig Daten nach Metadaten und verschiedenen Kriterien und macht sie damit besser handhabbar für die Analysten;
- es kann tief in das Internet eintauchen, also viele Daten an verschiedenen Orten massenhaft sammeln und verarbeiten, dabei sucht es gleichzeitig nach neuen Webdiensten, die von Gegner genutzt werden könnten;
- es kann allgemein große Mengen an Daten verarbeiten und in akzeptabler Zeit durchsuchen;
- es kann über Musteranalysen aus den Datenmengen Anomalien und Auffälligkeiten finden, die einer genaueren Beobachtung unterzogen werden können;
- es ermöglicht eine indexikalisierte Speicherung von Daten;
- es beinhaltet eine abrufbare Datenbank von über Hacking-Angriffe angreifbaren Zielen und ihrer Schwachstellen, die von der TAO-Einheit zusammengestellt wird;
- es soll in Zukunft weitere Internetkommunikationsarten und weitere Internetdienste wie VoIP angreifen können und dabei deutlich mehr Daten und Metadaten abgreifen können.

**Zu Frage (4): Welche Abwehrmaßnahmen durch Hard- und Software sind verfügbar?**

Insgesamt sind sehr viele Abwehrmaßnahmen prinzipiell verfügbar.

Eher einfach ist eine Abwehr der massenhaften Überwachung normaler Nutzerinnen und Nutzer. Hier helfen wie oben geschildert bereits einfache und verfügbare, beziehungsweise vorrangig rechtliche und organisatorische Maßnahmen wie klare rechtliche Bedingungen der nachrichtendienstlichen Kooperation, ein nationales Routing und eine verlässliche und laientaugliche Ende-zu-Ende-Verschlüsselung, die allerdings als solche noch entwickelt werden müsste.

Ganz anders stellt sich dies bei den stärker gezielten Angriffen der NSA und anderer Nachrichtendienste dar. Hier muss vor jeder Empfehlung von Maßnahmen bedacht werden, dass diese Akteure in voller Kenntnis der Basisverwundbarkeiten sowie der systemischen Defizite der IT und IT-Sicherheit und mit hohen Ressourcen und Fähigkeiten agieren und sich daher auf Vektoren und Techniken ausrichten, die faktisch und konzeptionell außerhalb der konventionellen Perspektiven und Interessen der bestehenden IT-Sicherheit liegen. Konventionelle IT-Sicherheit hilft gegen diese Angreifer nicht. Hier muss Innovation angetrieben werden, vor allem durch staatliche Regulierung und Inzentive.

Die Ausrichtung dieser Innovation ist ein wichtiger und problematischer Gegenstand. Zum einen ist eine rein inkrementelle Innovation bestehender Ansätze (wie die einer Firewall in eine Next-Generation-Firewall) voraussichtlich nicht hilfreich. Sie zwingt Angreifer nicht auf grundsätzlich andere Spielfelder. Erworbene Verfahren, Expertisen, Kontakte können weitergenutzt werden, zudem sind viele prinzipielle und strukturelle Schwächen dieser Ansätze bekannt, die nicht durch Verbesserungen eingeholt werden können. Zum anderen müssen aber auch neuartige Ansätze kritisch bewertet werden. Hier bestehen aufgrund der sehr hohen und vielschichtigen Basisunsicherheiten prima facie ungewöhnlich viele Ansätze zur Innovation. Ohne eine klare vorangegangene Bewertung der Risiken sowie der Effizienz möglicher Maßnahmen und die entsprechende Priorisierung entsteht die Gefahr, dass sich die neuen Ansätze mit nur temporärer Effektivität an kleinere Teilprobleme wenden. Sie können dort zwar gerechtfertigt Effektivität behaupten, es ist aber unklar, wie nachhaltig sie sind, wie effizient sie für ihren Teilausschnitt gemessen an absoluten Sicherheitsanforderungen sind, wie relevant der Teilausschnitt für die Gesamtsicherheit des Systems unter bestimmten Bedrohungsbedingungen ist, wie relevant die Gesamtsicherheit dieses Typs von Systems in der Gesamtmenge der in Deutschland zu beschützenden Systeme ist und auf welche Weise und wie schnell Angreifer sich taktisch und technisch anpassen oder die Schutzmechanismen missbrauchen können. Es besteht folglich die strategische Gefahr, dass „Lösungen“ beschlossen und befördert werden, die etwa nur eine Erhöhung der Sicherheit von 2% an wenig relevanten Stellen und bei Systemen mit niedriger Bedrohungslage produzieren, dabei Aufmerksamkeiten und Ressourcen binden, neue Pfadabhängigkeiten generieren und alte, schädliche Pfadabhängigkeiten vertiefen, während höhere Risiken für den deutschen Staat und die deutsche Wirtschaft gar nicht erst adressiert werden. Insbesondere das Problem der technischen und ökonomischen Pfadabhängigkeiten muss hier als zentral angesehen werden. Wenn neue Sicherheitstechnologien einmal weitflächig eingeführt werden, so sind die Kosten sowie die zugehörigen Prozesse der Umstellung der Systeme, der Ausbildungen und Arbeitsprozesse auf diese Technologien in der Regel umständlich und tiefgreifend für Unternehmen und Institutionen, so dass eine falsche Aufstellung in diesem Bereich nicht einfach wieder rückgängig gemacht werden kann. Das würde hohe Kosten erzeugen, normale Tätigkeiten verlangsamen und erschweren und evoziert daher auch eine

niedrige Grundbereitschaft der Verantwortlichen zur Reform, selbst wenn diese faktisch notwendig erscheint. Billigere und periphere Maßnahmen werden dann erneut zur „Ergänzungslösung", die zwar ebenfalls mit temporärer Basiseffektivität verkauft werden, aber erneut keinen echten systemischen und nachhaltigen Sicherheitseffekt erzeugen können. In diesem Kontext muss auch als grundlegend angemerkt werden, dass in der Cybersicherheit nicht der Grundsatz „etwas ist besser als gar nichts" gilt. „Etwas" kann kurzfristig besser sein als gar nichts, langfristig aber deutlich schlechter. Uninformiert Vorschläge zu befördern, die nicht aus einer strategischen Vorausschau, sondern aus spontanen Ideen und vorhandenen Fähigkeiten generiert werden, bringt daher nicht notwendig einen echten Gewinn an Sicherheit, sondern birgt möglicherweise eher ein Risiko für die Sicherheit und die Nachhaltigkeit des IT-Sicherheitsmarkts.

**Zu den Fragen (5) und (6): Welche Änderungen staatlicher Rahmenbedingungen und gesetzlicher Regelungen wären erforderlich, um IT/IT-basierte Kommunikation noch sicherer als bisher zu machen?**

Angesichts der zuvor gemachten Beobachtungen muss an der gestellten Frage die Wendung „sicherer als bisher" zur kritischen Revision empfohlen werden. Die einfache Vorgabe „ sicherer als bisher" ist zu offen und variabel und wird keine nachhaltige und effiziente Sicherheit und keinen erfolgreichen IT-Sicherheitsmarkt produzieren. Schlechte IT-Sicherheit wird zudem auch eine Verschlechterung der Security anderer deutscher technischer Produkte zur Folge haben, sofern diese mit IT ausgestattet werden, so dass als größere transitive Gefahr einer falschen Ausrichtung Deutschlands Exportkapazitäten im Maschinenbau, im Autobau sowie im Aerospace nachhaltig beeinträchtigt wären. Auch in diesem Interesse sollte also nicht irgendeine, sondern die richtige Sicherheit gefunden werden.

Um zu einem informierten und strategischen Ansatz zu kommen, müssen vor der technischen Entwicklung detaillierte Überlegungen und Forschungen angeschoben werden, die Wirtschaft und Regierung gemeinschaftlich initiieren und verfolgen sollten. Die folgenden Themen sollten beachtet werden:

- Bedrohungsmodelle: welche Risiken bestehen ad abstractum, welche bestehen real, wie sind diese in Bezug auf spezifische Sektoren und Technologietypen zu werten, wie verfahren und wie entwickeln sich die Angreifer?
- Grundlegende Probleme der Implementierung: warum wurde IT-Security so lange vernachlässigt, welche Gründe lassen sich für das darunterliegende und als Phänomen bekannte Markt- und Politikversagen anführen, wie können diese Probleme angegangen werden?
- Verwundbarkeiten: wie schlimm verwundbar sind Basistechnologien, lassen sich diese Verwundbarkeiten deutlich reduzieren, wie soll mit hochverwundbaren Basistechnologien umgegangen werden?
- Exposition: wie exponiert sind informationalisierte, vernetzte Prozesse, wie können securityeffiziente Segregationen eingeführt werden, wo bestehen verdeckte Übergänge, welche Rolle spielen Innenvektoren?
- Security Effizienz: wie gut ist ein Sicherheitssetting, wie effizient und wie passend ist eine Dienstleistung oder Technologie, wie kann Effizienz überhaupt gemessen werden, was bedeutet „angemessene Sicherheit"?
- Systematische Security Innovation: wie kann Security Bestandteil allgemeiner technischer Innovationsprozesse werden, nach welchen Methoden und auf Basis

welcher Risikomodelle und Annahmen müssen IT-Security entwickelt werden, wie viel müssen IT-Security Hersteller über spätere Anwendungskontexte wissen und wie kann dieses Wissen implementiert werden?

- Systemische und wertsensible Innovation: wie kann Security im Lichte aller verfügbaren Optionen und den korrespondierenden Kosten-Nutzen-Verhältnissen gestaltet werden, wie können digitale Werte und Bürgerrechte als leitende Paradigmen in Security Innovation eingebunden werden?

Viele Kernfragen zur Klärung des Innovationsprozesses sind erkennbar nicht technisch. In dieser Hinsicht sind inter- und transdisziplinäre Ansätze wichtig, die allerdings grundlegend anders aufgesetzt werden müssen, als das gegenwärtig der Fall ist. Aktuell arbeitet interdisziplinäre Forschung in Deutschland meist so, dass die technischen Wissenschaften, insbesondere aus der Anwendungsforschung, größere Projekte aufsetzen mit festen technischen Ideen, bei denen dann ein geringer Anteil auf eine nicht-technische Begleitforschung verwendet wird, die durch Ethiker oder Anwaltskanzleien wahrgenommen wird und die nur eine ex post facto Kommentarfunktion hat, ohne in irgendeiner Weise auf den Innovationsprozess selbst einwirken zu können. Dieser problematische Umstand ist in der Technikbegleitforschung seit Langem bekannt und kritisiert. Einer vorschnellen Anwendungsforschung muss aber – gerade bei Cybersicherheit – eine „Anwendbarkeitsforschung" vorangestellt werden.

Außerdem ist zu beachten, dass an einigen dieser Fragestellungen mehrere Dunkelfelder zum Tragen kommen, die sich zum Teil in „Superdunkelfeldern" überschneiden. So ist grundsätzlich kaum abzuschätzen, wie viele und was für Angreifer mit welchen Interessen angreifen, wie viel die Detektionstechnologien tatsächlich sehen, was das Gesehene bedeutet, wie und wo Angriffe ausgebeutet und mittel- und langfristig schädlich für das Opfer werden, wie effizient bestimmte Sicherheitstechnologien konkret operativ sind, wie sich bestimmte Schwachstellen und kritische Abhängigkeit real ausprägen etc. Diese Punkte sind theoretisch und statistisch nicht eindeutig zu belegen, sondern nur punktuell und anekdotisch und daher mit ungewöhnlich großen Spielräumen für folgende Einzelbewertungen. Überschneiden sich viele dieser Undeutlichkeiten in Superdunkelfeldern (wie etwa im Fall der Industriespionage), so kann alles Mögliche über Risiken und Effizienzen behauptet werden.

Statt auf eine zwar einsetzende, aber voraussichtlich nur sehr langsame Verbesserung der Datenlage zur Bewertung zu warten, ist hier zu empfehlen, unabhängige Bewertungsmaßstäbe zu entwickeln, die Dunkelfelder und Superdunkelfelder systematisch umgehen können, ohne an Aussagekraft zu verlieren. Dies wird mitunter schwierig sein, ist aber eine wichtige Aufgabe für nicht-technische juristische, ethische und ökonomische Argumentationen. So kann etwa aus Prinzipien der Haftung, der Verantwortung oder des nachhaltigen Wirtschaftens qualitativ argumentiert werden, um zu hohen Sicherheitsstandards zu gelangen. An dieser Stelle kann auch eine wichtige und leitende politische Frage lokalisiert werden, nämlich danach, ob man bei der Anwendung dieser Prinzipien eine eher sicherheitssensible und starke Haltung zu Regulierung oder eine unsicherheitstolerante und offene Haltung zur Regulierung einnehmen möchte.

Eine unsicherheitstolerante und offene Haltung wird die Entscheidungen weitestgehend der IT-Branche überlassen und nur bei konkreten Vorfällen punktuell nachregulieren.

Für eine stärker sicherheitsbetonte Haltung dagegen ließen sich aus bestehenden Prinzipien einige erste Empfehlungen für Regulierungen treffen, die aus regulären Safety-Anforderungen parallelisiert werden können:

- IT-Security Produkte und Dienstleistungen müssen jenseits der Zertifizierungen nach absoluten und risikorelativen Effizienzkriterien evaluierbar und agil bewertbar gemacht werden;
- Restrisiken müssen sichtbar und verständlich gemacht werden;
- Basisunsicherheiten (Verwundbarkeiten und kritische Verwundbarkeiten) in IT-Produkten müssen unabhängig abgeschätzt und ausgewiesen werden, um informierte Akquisitionen zu ermöglichen;
- Mindestens für Neuentwicklungen muss eine Haftbarkeit für zu hohe Basisverwundbarkeiten eingeführt werden, um Anreize zu besserer Entwicklung zu generieren;
- Safety-Anforderungen für kritische Prozesse und kritische Maschinen müssen in Security-Anforderungen gleicher Qualität übersetzt werden;
- Security-Anforderungen für sicherheitskritische Prozesse und Institutionen müssen für Informationstechnik genauso hart und eindeutig vorgegeben werden wie für anderes Gerät oder entsprechende Verfahren;
- Der IT-Markt darf keine Machbarkeitsgrenzen und Realitäten vorschreiben, sondern muss sich an gesetzlichen und gesellschaftlichen Vorgaben orientieren und diese umsetzen;
- Verfügbare Hochsicherheitstechniken sollten für kritische Kontexte zu Standards erhoben werden, die mittelfristig umzusetzen sind;
- Soll ein Endnutzer für die Security eines IT-Systems verantwortlich gemacht werden, so müssen die Sicherheitsmechanismen des Systems so entwickelt sein, dass sie mit wenig Zeit und niedriger Aufmerksamkeit von ungeschultem oder gering geschulten Personal fehlerfrei korrekt und effizient implementiert und bedient werden können. Ist dies nicht möglich, ist die Schuld nicht beim Nutzer, sondern beim Entwickler der Technologie zu suchen;
- IT-Security Fachpersonal muss als solches ausreichend spezialisiert oder geschult sein, um entsprechende Aufgaben wahrnehmen zu dürfen;
- Forschung und Entwicklung könnten „Top Down“ anfangen statt „Bottom Up“ und stärker die in Theorie und Forschung härtesten Ansätze beforschen. Da viele dieser Ansätze bereits bekannt sind (wie etwa durch das CRASH Programm und ähnliche Initiativen), müssen Forschung und Entwicklung vor allem die Bedingungen und Möglichkeiten der technischen und ökonomischen Implementierbarkeit dieser Konzepte untersuchen, um dort zu Empfehlungen zu gelangen, die eine echte Migration erlauben;
- Besonders zu bevorzugen wären stärker disruptive Ansätze, die vor allem nicht nur unsichere Systeme mit ad hoc Maßnahmen absichern wollen, sondern die grundlegend sichere System neu bauen wollen. Diese sind zwar in der deutschen Entwicklungslandschaft ebenfalls vorhanden – Mikrokerne, Separationskerne und „Security By Design“ sind Beispiele – spielen aber in der Gewichtung keine hinreichend zentrale Rolle, um einen tiefgreifenden Wandel des Spielfeldes und seiner Bedingungen und Möglichkeiten zu erzeugen;
- Formate und Foren für einen vertraulichen Austausch von sensiblen Informationen müssen geschaffen werden.

Zudem lässt sich als übergreifende Empfehlung und unabhängig von allen anderen und weiteren Maßnahmen raten, dass dringend deutlich mehr Spezialisten und Experten der IT-Sicherheit generiert werden müssen, für Entwicklung und Betrieb. Es muss deutlich mehr spezialisierte Ausbildung an den Universitäten stattfinden, Trainings- und Weiterbildungskonzepte müssen entwickelt werden. Ohne eine ausreichende Menge prüfbar hinreichend geschulten Personals lassen sich viele Probleme gar nicht erst angehen.