Sensibilisierung für Cyber-Sicherheit -
Sind Deutschlands Anstrengungen für eine digitale Sicherheitskultur ausreichend?

Tagungsbericht
verfasst von Verena Diersch

Cyber-Risiken haben in Deutschland eine neue Dimension angenommen: Jede Sekunde werden weltweit zwei Virenprogramme ins Netz eingeschleust, pro Minute werden in Deutschland die Identitäten von zwei Internetnutzern gestohlen. Der Cyberspace wird von Kriminellen und zunehmend auch von Staaten genutzt, um Interessen zu verfolgen und Ziele zu erreichen. Um dem neuen Bedrohungsszenario zu begegnen, ist ein Multi-Stakeholder-Ansatz vonnöten. Zivilgesellschaft, Staat und Wirtschaft müssen für das Thema Cyber-Sicherheit sensibilisiert werden. Ziel der Expertentagung „Sensibilisierung für Cyber-Sicherheit - Sind Deutschlands Anstrengungen für eine digitale Sicherheitskultur ausreichend?“ vom 11. bis 12. April 2013 in Wildbad Kreuth war es daher, Problemfelder zu skizzieren und Möglichkeiten für die Schaffung einer digitalen Sicherheitskultur in Deutschland aufzuzeigen. Die Veranstaltung wurde durch die Hanns-Seidel-Stiftung in Zusammenarbeit mit dem Gesprächskreis Nachrichtendienste in Deutschland (GKND) durchgeführt.

Prof. Dr. Reinhard Meier-Walser, Leiter der Akademie für Politik und Zeitgeschehen der Hanns-Seidel-Stiftung, führte in die Expertentagung ein, indem er die Kooperation zwischen Wissenschaft, Gesellschaft, Wirtschaft, Staat und Diensten für mehr Cyber-Sicherheit in Deutschland in den Vordergrund stellte.
Volker Foertsch, Mitglied des Vorstands des GKND, hob hervor, dass sich seit der letzten Tagung der Hanns-Seidel-Stiftung zum Thema „Cyberwar“ im Jahr 2011 sehr viel getan habe. Die Entwicklungen in der Informationstechnologie (IT) gingen in einem raschen Tempo voran und überforderten daher viele, vor allem im öffentlichen Bereich. Es sei daher ein Umdenken und ein Informationsaustausch zur Schaffung einer digitalen Sicherheitskultur nötig.

Die Einführung in das Thema „Cyber-Sicherheit“ gab Sandro Gaycken, Mitarbeiter im Planungsstab des Auswärtigen Amtes sowie wissenschaftlicher Mitarbeiter im Institut für Informatik der Freien Universität Berlin. Er beleuchtete die außen- und sicherheitspolitischen Aspekte des Themenfeldes Sicherheit im Cyberspace und konzentrierte sich dabei auf Cyber-Angriffe mit strategischer Wirkung, beispielsweise aufgrund geopolitischer Interessen. Der Schutzbedarf in Deutschland sei groß, die Schutzangebote aus dem staatlichen Bereich verbesserungsbedürftig. Die internationale Stabilität werde durch das Anwachsen der Anzahl großer Angriffe durch staatliche Akteure gefährdet. 19 Staaten investieren derzeit in Offensivkapazitäten für den Cyberspace. Zudem gab es von 2004 bis 2011/2012 ein Anwachsen um 120 Cyber-Mercenaries, also Cyber-Söldnerfirmen. Dieser Schwarzmarkt hat Auswirkungen für asymmetrische Angriffe. Sandro Gaycken entwarf das Szenario, dass Talibankämpfer mit den geeigneten Exploits möglicherweise C4ISR-Systeme (also Systeme für Steuerung, Kommunikation, Computer, Informationsbeschaffung, Überwachung) stören könnten. Damit wäre eine neue Stufe asymmetrischer Kriegsführung erreicht. Zu beobachten sei laut Sandro Gaycken außerdem, dass es eine neue Ost-West- Konfrontation gäbe. Russland und China treiben gemeinsam einen sog. „code of conduct“, also Verhaltensregeln, für den Cyberspace voran. Diese Pläne seien jedoch sehr überwachungs- und zensurlastig, so Gaycken. Die USA wiederum seien dabei, ihre

Nachrichtendienste personell aufzurüsten. Man setze sehr auf sog. „human intelligence“ und das sog. „targeted profiling“, das jedoch durch eine „Evolution“ des Tarnens und Täuschens erschwert werde. Gerade im Bereich der Signals Intelligence (SIGINT), also der Gewinnung von Informationen, z. B. aus der Beobachtung der internationalen Kommunikation oder der Erfassung und Analyse elektronischer Daten ganz allgemein, gebe es die Möglichkeit, sie dann zu Angriffen zu verwenden, sich selbst also damit zu tarnen. Neben der Rückkehr zum bipolaren Regimeverständnis des Ost-West-Konflikts ließe sich auch eine Tendenz zum Nationalismus erkennen. Das Auswärtige Amt schlage einen dritten Weg vor, so Gaycken. Er stellte die Prinzipien Freiheit, Verantwortung und Transparenz als maßgeblich vor. Es solle in Deutschland keine Überwachung geben. Man setze auf die Selbstregulierung der Wirtschaft. Zudem werde eine deutlich größere Wissensbasis über Angreifer und ihre Fähigkeiten benötigt. Dies setze neben dem BSI auch einen starken Aufbau des Bundesnachrichtendienstes (BND) voraus. Neben dem Informations- und Wissensausbau gelte es vor allem technische Lösungen zu entwickeln. „Der Schutzbedarf und der gebotene Schutz sollen proportional werden“, erklärte Gaycken. Es soll beispielsweise die Sicherung der „supply chain“, also der international vernetzten Lieferkette der Hardware- und Software-Produkte, im Fokus stehen. Das Lagebild über Cyber-Angriffe auf Unternehmen soll durch eine Meldepflicht verbessert werden. Sandro Gaycken sprach sich in seiner Einführung für eine Stärkung der Rolle des Staates aus. Er halte nicht viel vom Multi-Stakeholder-Ansatz. Lobbyisten würden diese Art der Zusammenarbeit für die Durchsetzung ihrer Industrieinteressen nutzen. Sicherheit zu schaffen sei jedoch eine klassische staatliche Verantwortung, so Gaycken. Desweiteren bevorzuge er technische Lösungen vor rein politischen Willensbekundungen. „Industriespionage ist mit technischen Mitteln absolut lösbar“, erklärte er. Gerade für Deutschland biete sich die Chance, einen Markt für sichere IT-Lösungen aufzubauen.

In der anschließenden Diskussion brachte Prof. Dr. Michael Meier vom Institute Of Computer-Science der Universität Bonn den Punkt an, dass Industriespionage kein rein technisches Problem sei. Gaycken setzte dem entgegen, die Problematik sei technikbasiert. Viele Angriffe, beispielsweise aus China, werden extern getätigt und könnten durch eine verbesserte Sicherheitsarchitektur verhindert werden. Innentäter seien nicht das gravierende Problem. Gaycken bezeichnete Cyberaußenpolitik als eine Frage um Krieg und Frieden, die für die internationale Sicherheit maßgeblich sei. Desweiteren stellte er fest, dass das Völkerrecht nicht dazu legitimiere, bei Cyber-Angriffen zurückzuschlagen, sondern vorab defensiv tätig zu werden. Dies sei eine Ausgestaltung des Rechtsprinzips „jus ante bellum“. Es sei deshalb durchaus vorauszusetzen, dass der Markt in Sachen Cybersicherheit selbst Investitionen leiste. Software-Giganten wie Google, Microsoft und Apple könnte man den Markzugang für ihre Produkte verwehren, wenn ihre Softwareprodukte gewissen Sicherheitsstandards nicht entsprächen. Gaycken forderte dazu auf sich zu überlegen, welche Kompetenzen im Bereich des Cyberspace renationalisiert werden müssten. Es handele sich um eine Frage der nationalen Sicherheit, dort würden eben andere Regeln gelten. Soft- und Hardware müssten technisch so funktionieren, dass sie möglichst wenig Fehler zulassen. Den Nutzer als größtes Sicherheitsrisiko zu sehen, findet Gaycken daher wenig sinnvoll. Um diesen Punkt zu bekräftigen, nannte er Flugsicherheit als Vergleichsthema. „Hier wird der Pilot zur bloßen Dekoration, für die Sicherheit sorgt die Technik“, so Gaycken.

Deutschlands Stellung im Cyber-Raum
Was tun andere Länder für eine digitale Sicherheitskultur und wie kann Deutschland davon profitieren und daran mitarbeiten?

Alexander Klimburg vom Österreichischen Institut für Internationale Politik (ÖIIP) bekräftigte im Gegensatz zu Sandro Gaycken, dass der Multi-Stakeholder-Ansatz für mehr Cybersicherheit

unverzichtbar sei. Als Beispiel nannte er die Rolle der Internet Engineering Taskforce (IETF), eine Unterinitiative der Internet Society (ISOC). Denn diese zivilgesellschaftlichen Foren seien für den größten Teil des Codes verantwortlich, aus dem das Internet aufgebaut ist. Der Privatsektor wiederum stellt die Infrastruktur für das Internet zur Verfügung. „Die Regierung hat so gut wie keinen Anteil an dem, was im Internet geschieht“, so Klimburg. Einzig Regierungsorganisationen (IGOs) würden durch Regierungsmandate befähigt werden und so habe die Regierung nur mittelbar Einfluss an Entwicklungen im Internet. Die Zivilgesellschaft hat großen Anteil an globalen Tendenzen im Internet: „Die Technikexperten gehen in den Untergrund“, so Klimburg. So würden Cybercrime und Hacktivismus, also die Verwendung von Computern und Computernetzwerken als Protestmittel, entstehen. Doch diese Phänomene und Probleme könnten international angegangen werden.

Ein Beispiel der internationalen Initiative in Sachen Cybersicherheit sei die sog. „World Conference On International Communications “ (WCIT) der Internationalen Fernmeldeunion (ITU), welche 2012 eine Vereinbarung hervorbrachte, die Klimburg als „Internet Yalta“ bezeichnete. Das Forum sei ein Beweis für die starke Rolle des Privatsektors, die Klimburg jedoch auch kritisch sieht. Nach seiner Meinung sollte die Internet Cooperation For Assigned Names And Numbers (ICANN) nicht alleinig für die Vergabe des Domain Name Systems (DNS) verantwortlich sein.

In seinem Anschlussreferat betonte Prof. Dr. Thomas Wingfield vom George C. Marshall Center for Security Studies in Garmisch, dass die NATO keine Cyberpower ist und auch nicht darauf angelegt sei, eine zu sein. Das neue Strategische Konzept der NATO aus dem Jahr 2010 betone lediglich die defensiven Aspekte der Cybersicherheit. Denn wenn die NATO schon keine Cyberpower sein könne, so wolle man doch kein schwarzes Loch im Cyberspace sein, so Wingfield. Im Folgenden stellte er die wichtigsten Cybermächte vor. Die chinesische Regierung beispielsweise verbitte sich jegliche Einmischung in ihre Cyberpolitik. „Die militärische Spionage, die von China ausgeht, wird unterbewertet. Die Industriespionage, die von dem Land ausgeht, wird jedoch überbewertet“, so Wingfield. Anschließend stellt er die russische Initiative „Bribr“ vor, die sich gegen Korruption (englisch: bribe) wendet. Zivilpersonen können online anonym melden, wenn sie zur Korruption aufgefordert wurden oder diese bemerken. Dieses Tool sei jedoch zweischneidig. Denn technisch sei zurückverfolgbar, von wem die Bezichtigung der Korruption komme und diese Information könne in die falschen Hände geraten und dann zur Waffe werden, so Wingfield. Israel, so der Experte, bewerte Bedrohungen der internationalen Sicherheit von Fall zu Fall. Für die USA ließe sich eine enge Verknüpfung des Geheimdienstes National Security Agency (NSA) und dem US Cyber Command (Cybercomm) feststellen, die Wingfield kritisch sieht.
Nach seiner Meinung gebe es einige Missverständnisse in der Diskussion um Cyber-Sicherheit. Er schlug ein sog. Meta-Bezugssystem für mehr Sicherheit im Cyberspace vor. Technik gelte zunächst als Maßstab für das Mögliche. Erst in der Auseinandersetzung mit ihren Grenzen und Herausforderungen würden sich die beiden anderen Kategorien, das Recht als Maßstab für das Zulässige, sowie die Gesetzgebung als Bezugsrahmen für das Wünschenswerte herausbilden. Damit räume man Unstimmigkeiten aufgrund einer unklaren Begriffs- und Diskussionsebene aus. Ein weiterer Punkt, der in der Diskussion um Cyber-Sicherheit immer wieder zu Unsicherheiten führe, sei die Frage der Attribution, also der Rückverfolgbarkeit von Cyber-Angriffen zu ihren Urhebern. Könne man einen Angriff zurückverfolgen, sei schwer nachweisbar, ob es sich um eine staatliche Attacke handle. Zudem sei noch nicht abschließend geklärt, inwieweit die technische Attribution zum wahren Täter führe, da Angriffe umgelenkt oder getarnt werden könnten. Außerdem stehe nicht fest, wie hoch der Verdachtsmoment ausfallen müsse, um rechtlich zu einer Schuldzuweisung oder sogar zur Rechtfertigung einer wie auch immer gearteten Antwort zu kommen. Es gebe im internationalen Recht auch keinen Begriff der Kriegshandlung. Es existierten

lediglich die Tatbestände Gewaltanwendung (die eine unilaterale Selbstverteidigung legitimiert) und bewaffneter Angriff. Letzterer erlaube keinen Gegenschlag mit konventionellen Mitteln. Gewaltanwendung über den Cyberspace, die beispielsweise eintreten könnte, wenn SCADA-Netzwerke gehackt und es in der Folge zu einem immensen Schaden wie einer Explosion kommt, sei theoretisch vorstellbar, erklärte Wingfield abschließend.

Dr. Gustav Lindstrom vom Genfer Zentrum für Sicherheitspolitik gab im Rahmen seiner Präsentation einen Überblick über die „Trends im Cyberspace". Er stellte Präventivmaßnahmen auf technischer und institutioneller Ebene sowie Maßnahmen der Folgenbewältigung auf technischer und institutioneller Ebene anhand einer Übersicht dar, an der viele Stakeholder beteiligt seien. Diese müssen intern sowie extern – mit anderen Staaten – arbeiten. Auf der Seite der technischen Präventivmaßnahmen stehen Sensibilisierung für Cybersicherheit, Schutzsoftware, das sog. Internet Protocol Version 6 (IPv6), das von der IETF seit 1998 verwendet wird. Ebenfalls unter Präventionsmaßnahmen zu nennen ist die Domain Names System Security Extension (DNSSEC) der ICANN. Es handelt sich um eine Reihe von Internetstandards, die Authentizität und Integrität der Daten gewährleisten sollen. Auf der Seite der technischen Maßnahmen der Folgenbewältigung stehen u. a. das Filtern des Internet-Verkehrs und die Zugangsblockierung. Die Präventionsmaßnahmen auf institutioneller Basis betreffen die Einrichtung von Computer Emergency Response Teams (CERTs), von Agenturen wie der European Network and Information Security Agency (ENISA), privaten Stiftungen wie SPAMHAUS und Sicherheitsübungen. Die Maßnahmen der Folgenbewältigung äußern sich auf institutioneller Ebene in der Benutzung von CERTs, dem Informationsaustausch und der Durchsetzung von Gesetzesvorhaben.
Anschließend gab Lindstrom einen Überblick über die bisher geschlossenen Vereinbarungen auf internationaler Ebene. Er hob besonders die sog. Budapest Convention, auch als Übereinkommen über Computerkriminalität des Europarat bekannt, hervor. 39 Staaten haben diese unterzeichnet und ratifiziert, 10 Staaten haben unterschrieben und müssen die Vertragsvereinbarung noch in nationales Recht überführen. Viele Staaten, darunter die Tschechische Republik, Polen und Schweden haben jedoch nicht unterzeichnet. Außerdem nannte Lindstrom den Cyber Security Summit, welchen die Telekom und die Münchner Sicherheitskonferenz erstmalig im September 2012 durchführten, als wichtiges Forum für Cyber-Sicherheit. Auf diesem Gipfel sei eine Basis geschaffen worden, die nun als „rules of the road" umgesetzt werden müssen. Zu diesen zählten ein Verbot von Backdoor-Technologien und die Forderung nach sichererer Hardware sowie einer sicheren Lieferkette. Grundstrukturen dieser Ansprüche habe die IETF bereits vor 30 Jahren vorgetragen, so Lindstrom. Zudem hätten inzwischen über 20 Staaten eine eigene Cyber-Sicherheits- oder Cyber-Information-Strategie vorgelegt, darunter Australien, Kanada, Tschechien, Estland, Deutschland, Luxemburg, die Niederlande, Spanien, Südkorea, die USA, Finnland, Frankreich, Norwegen, Schweden, Uganda und Österreich. Doch auch wenn viele Staaten eine solche Strategie umsetzen wollen, so seien doch verschiedene Zielvorstellungen und Richtwerte zur Zielerreichung zu beobachten. Wichtige Punkte sind der Schutz kritischer Infrastrukturen und nationales Krisenmanagement, Cybercrime und militärische Sicherheitsthemen wie Spionage, Informationserfassung und Offensivkapazitäten. Letztere haben vor allem die USA, Großbritannien, Frankreich und Russland in ihren Cyber-Sicherheitsstrategien ausgestaltet. Viele Staaten heben aber auch die internationale Kooperation für mehr Cyber-Sicherheit hervor.

Dr. Greg Austin, Senior Visiting Fellow am King's College London, hob ebenfalls die internationale Zusammenarbeit im Bereich Cybersecurity hervor. „Das Internet hat die Welt näher zusammengebracht", so Austin. Es sei bedauerlich, wenn das Misstrauen, das durch die neuen Möglichkeiten der Spionage, Kriegsführung und Kriminalität generiert würde, beispielsweise die diplomatischen Beziehungen, die sich zwischen den USA und Russland sowie China seit dem Ende des Kalten

Krieges verbessert haben, negativ beeinflusse. Genau das sei jedoch zu beobachten. „Der Weg ist noch nicht voll beschritten, aber bereits vorgezeichnet“, so Austin. „Wir befinden uns in einem Dilemma was Cybersecurity betrifft. Wir haben bereits gute Gesetzgebungsvorhaben voran gebracht und wissen was zu tun ist, wir haben unsere Check-Listen was bei einem Cyber-Angriff zu tun ist, aber den Entwicklungen im Cyberspace begegnet beispielsweise die USA zu langsam und unter erheblichem Kostenaufwand.“ Er halte es für sehr bezeichnend, wenn die größte Volkswirtschaft der Welt in Ausgestaltung der Cyber-Sicherheitspolitik den Angreifern hinterher hinke. Dadurch gerate auch die Idee des Multi-Stakeholder-Ansatzes in eine instabile Schieflage. „Doch die Probleme, die uns neue Unsicherheiten im Cyberspace bescheren, sind meiner Meinung nach einfacher zu lösen als so manche Schwierigkeiten in Zeiten des Kalten Krieges“, zeigte sich Austin zuversichtlich.
Er bemängelte jedoch, dass nationale Cyber-Sicherheitsstrategien oft die internationale Ebene ausklammerten oder zu wenig beachteten. Die Strategie der USA beispielsweise würde ihr so gut wie gar keine Beachtung schenken. Geradezu bedenklich findet Austin, dass im Diskurs über Cyber-Sicherheit Russland und China „auf der einen Seite des Zaunes“ und die NATO- sowie die NATO-Plus-Staaten auf der anderen Seite stehen würden. Die NATO sei zwar keine Cyberpower und wolle keine werden, China sehe das aber möglicherweise anders und könnte befürchten, Länder wie die USA, Frankreich und Großbritannien könnten im Rahmen ihrer nationalen Cyber-Strategien Offensivkräfte gegen ihre Netze und ihre Infrastruktur richten. Wenn China und Russland für „den Westen“ ein Gefahrenpotential bezüglich Cybercrime, Cyber-Spionage und militärischen Cyber-Offensivkapazitäten darstellen würden, dann dürfe man sie unter keinerlei Umständen als Gesprächspartner verlieren.

In der anschließenden Diskussion wies Thomas Wingfield darauf hin, dass Offensive und Defensive im Cyberspace in engem Zusammenhang stehen. Denn Defensivmechanismen können technisch auch immer offensiv genutzt werden. Alexander Klimburg ergänzte, dass man auf Offensivmöglichkeiten angewiesen sei, wenn die Defensive schwach ausgeprägt sei. Deutschland sei davon in der EU besonders betroffen.

Der Cyber-Raum in Deutschland
Was tut Deutschland für eine digitale Sicherheitskultur und was muss noch getan werden?

Dr. Markus Dürig, Leiter des Referats IT-Sicherheit des Bundesministerium des Innern (BMI), gab in seinem Referat einen Überblick über die Cybersicherheitspolitik der deutschen Bundesregierung. Alle zwei Sekunden würde ein neues Schadprogramm entstehen. 20.000 Webseiten werden täglich mit dieser Malware infiziert. Es würden täglich fünf bis zehn Spionageangriffe über das Internet beobachtet. Zudem gebe es zunehmende Angriffe auf die Regierungskommunikation. Als Angreifer benannte Dürig z. B. die „kriminelle Schattenwirtschaft“. Als einen der schwersten Cyber-Angriffe der letzten Monate nannte der Leiter des Referats IT-Sicherheit des BMI die Attacke mit dem Wurm Shamoon auf die Ölförderung des Konzerns Saudi Aramco in Saudi-Arabien, bei dem innerhalb kurzer Zeit 30.000 PC ausfielen. Der Urheber dieses Angriffs sei immer noch unklar. Daraufhin hab es zwar keine Ausfälle in der Ölproduktion gegeben, aber es sei bemerkenswert, dass die Hacker in diesem Fall Administratorenrechte erworben hatten und damit in der Lage waren, erhebliche Manipulationen durchzuführen. Zudem handele es sich bei Saudi Aramco um einen Weltkonzern, der aber offensichtlich nicht in der Lage war, seine Systeme gegen Angriffe zu härten. Es sei doch höchst beunruhigend, wenn man davon auszugehen habe, dass es möglich sei, dass die Ölproduktion eines weltweiten Ölförderers wie Saudi-Arabien plötzlich wegbreche. Als höchst bedenklich stufte Dürig auch die laufenden Attacken auf US-Banken ein. Hier handele es sich um DDos-Angriffe (sog. „denial of service attacks“), durch welche die Verfügbarkeit des

Online-Bankings nicht mehr gegeben sei. Die DDos-Attacken auf das US-Bankensystem könnten aber auch als Beispiel für die internationale Kooperation angebracht werden. Denn als die DDos-Angriffe auf die US-Banken auftauchten, bat die US-Regierung die deutsche Bundesregierung um Mithilfe. Denn deutsche Rechner waren – neben anderen – Teil des Botnetzes gewesen. Dürig sprach deshalb von einem fragilen System, auf dem jedoch die gesamte Weltwirtschaft ruhen würde. Um in Deutschland auf auftretende Probleme in diesem Zusammenhang vorbereitet zu sein, habe man 2011 die Cyber-Sicherheitsstrategie für Deutschland ins Leben gerufen. Der in diesem Rahmen geschaffene interministerielle Austausch – der im Cyber-Sicherheitsrat verortet sei – sei gerade in Zeiten, in denen Industrie 4.0 zum Schlagwort werde, immens wichtig. Der Terminus bezeichnet ein Zukunftsprojekt in der Hightech-Strategie der Bundesregierung, mit dem die Infomatisierung der klassischen Industrien vorangetrieben werden soll. Industrie 4.0 baut in hohem Maße auf Maschine-zu-Maschine-Kommunikation, also auf das sog. „Internet der Dinge“. Dürig wies darauf hin, dass sich noch immer die Frage stelle, wie mit immanenten Problemen der Industrie-4.0-Strategie umzugehen sei. Hier müssten noch Anstrengungen in Sachen Forschung und Standardisierung getätigt werden. Noch immer gebe es kein umfangreiches Lagebild über die Bedrohungslage, die durch Cyber-Angriffe auf kritische Infrastrukturen entstehen könnte. Deshalb befürwortet der Leiter des Referats IT-Sicherheit des BMI die gesetzliche Meldepflicht für erhebliche IT-Vorfälle, besonders wenn sie Auswirkungen auf die Systeme des Endnutzers hätten. Ziel sei es, „innerhalb des BSI ein Gefühl davon zu bekommen, was im Land passiert“, so Dürig. Er verlangte nach einer Stärkung der Rolle des BSI zur IT-Sicherheit bei KRITIS.

Andreas Könen, Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), gab in seinem Referat Einblick in das Gesamtspektrum der Bedrohungen aus dem Cyberspace. Er machte deutlich, dass Software und Hardware zunehmend von Mängeln geprägt seien. 2012 seien 5.257 neue Schwachstellen entdeckt worden. Das entspräche 100 pro Woche. 36 Prozent dieser Sicherheitslücken konnten bisher noch nicht gepatched werden, das heißt, sie stehen Angreifern aktuell noch zur Verfügung. 20 Prozent der Schwachstellen seien als kritisch einzustufen. So treibt etwa der Cyberworm Conficker, der erstmals im Oktober 2008 registriert wurde, noch immer sein Unwesen. „Conficker ist alt, aber immer noch präsent. Er ist die führende Malware im Netz“, so Könen. Noch immer sei die öffentliche Verwaltung von diesem Schadprogramm betroffen. Ein weiteres Problem stelle in Websites eingebettete Malware dar. Sie würde sich meist in Werbebannern verbergen. Infizierte Websites bezeichnet man als „drive by exploit“-Websites. Klicke man auf die Banner, könne man Teil eines Botnetzes werden, wenn der Internet-Browser nicht richtig eingestellt sei. 2012 habe es das BSI mit elf als kritisch zu bewertetenden Exploits – also Schwachstellen, die zur Abschöpfung oder Manipulation von Daten genutzt werden können – zu tun gehabt.
Die derzeitige Angriffskapazität einer DDos-Attacke liege bei 80 bis 300 Gigabit Spitzenlast pro Sekunde. Das sei das 50.000fache der Downloadkapazität eines normalen Hausanschlusses. Diese Menge werde jedoch im Upload geleistet. Es sei eine Tendenz zu beobachten, dass nicht nur PC zur Erstellung eines Botnetzes benutzt werden, sondern zunehmend auch gekaperte leistungsfähige Server mit guter Internetanbindung. Könen sprach von einem „Revival der 'denial of service attack'“. Daher müsse man sich heutzutage präventiv wappnen. Dies setze natürlich erhebliche Kosten und möglicherweise Wettbewerbsnachteile voraus, doch die Beseitigungskosten, die sog. „business recovery“, seien im Vergleich viel kostspieliger. „Alles läuft heute IT-gestützt“, nannte Könen den Grund für die Kostenexplosion infolge eines Cyberangriffs. Durch die Umsetzung der Strategie“ Industrie 4.0“ würde die Anzahl potentieller Angriffsziele sogar noch zunehmen. „Das BSI muss hier involviert sein“, so Könen.
Nach seinem Überblick über die Angriffsvektoren widmete sich der Vizepräsident des BSI der Cybersicherheitslage in Deutschland. Aufgrund der Arbeitsteiligkeit und der Professionalisierung

der deutschen Wirtschaft sei das Land massives Angriffsziel. Zudem werde Deutschland als Mittel zum Zweck, als sog. „Relay-Station“ in Botnetzen, für Cyber-Sabotage-Angriffe genutzt. Könen gab in der Folge einen Überblick über die Lage der Bundesverwaltung. Es sei eine der Kernkompetenzen des BSI, Gegenmaßnahmen gegen Cyber-Angriffe auf allen staatlichen Ebenen durchzuführen. Diese müssten jedoch durch technische Maßnahmen wie die Gewährleistung eines IT-Grundschutzes ergänzt werden. Um die Cyber-Sicherheit in Deutschland auch auf der Ebene des Privatsektors zu garantieren, hat die Bundesregierung im Zusammenhang mit der Cyber-Sicherheitsstrategie für Deutschland die Allianz für Cybersicherheit ins Leben gerufen. Die Maßnahmen des Gremiums zielen insbesondere auf kleine und mittelständische Unternehmen (KMU) ab.

Dr. Kai Grassie, Chief Technology Officer (CTO) bei Giesecke & Devrient in München, stellte die Bedeutung der IT-Sicherheit für die deutsche Industrie voraus. Die IKT-Industrie verfüge hier über einen hohen Stellenwert und eine „immense Hebelwirkung“, wie Grassie betonte. Sie schaffe so viele Arbeitsplätze wie der Maschinenbau und habe eine Wertschöpfung von mehr als 100 Milliarden Euro pro Jahr. Der Maschinenbau wird sich zukünftig zu einem Teil der IT-Industrie wandeln. Sie sei zudem für angelagerte Industrien ein wichtiger „enabler“. Das Internet schaffe Umbrüche in der Gesellschaft. Neue IT-Entwicklungen fordern, dass sich Unternehmen, nicht nur in der IT-Industrie, ständig neu erfinden müssen. Dies bedeute, dass sich interne Strukturen verändern, andere Prozesse umgesetzt und andere Kompetenzen erworben werden müssen. Diese Tatsachen schaffen für Unternehmen riesige Herausforderungen, aber auch Chancen für eine attraktive Positionierung im Markt. Gerade im Zusammenhang mit dem Internet der Dinge werde IT-Sicherheit jedoch immer relevanter. Zehn Milliarden Komponenten und Geräte seien miteinander vernetzt, so Grassie. Diese Zahl werde sich noch vergrößern. Gleichzeitig werden nur noch zehn Prozent der produktiven Wertschöpfung im IT-Sektor in Europa geleistet. „Das entspricht proportional gesehen aber nicht dem, was wir an intellektuelem Eigentum generieren“, so Grassie. Für Deutschland entspricht dies einem Wettbewerbsnachteil. Um dies zu ändern, schlug Grassie eine stärkere Fokussierung auf Forschung und Entwicklung in Deutschland vor. „Wir sind noch weit davon entfernt, in Wirtschaft und Forschung partnerschaftlich zu agieren“, kritisierte Grassie. Zudem gäbe es zu wenige qualifizierte Hochschulabsolventen (ca. 16.000 pro Jahr) und eine zu geringe Sensi-bilisierung im Bereich der Entwicklung neuer Produkte. Für mehr Cyber-Sicherheit sei es aber in Zukunft auch wichtig, die richtige Balance zwischen Regulierung und Überregulierung zu finden.

Marco Di Filippo, Geschäftsführer Compass Security Deutschland GmbH, gab in seinem Vortrag einen interessanten Einblick in das sog. „War Googling“, das Auffinden vertraulicher Daten im Netz. Über die Suchmaschine Google suchte er gezielt nach Komponenten kritischer Infrastrukturen, die mit dem Internet verbunden sind, und versuchte, sie zu Zwecken der späteren Aufklärung, per Hack anzugreifen. „Wir beobachten einen hohen Grad an Automatisierung im Alltag“, stellte Di Filippo eingangs fest. Als besonders bedenklich bezeichnete er auch die Finanz-automatik des modernen Weltwirtschaftswesens. Gerade im Bereich kritischer Infrastrukturen glaube er jedoch nicht an den „Super-Gau“ – wie er sagte – und widersprach damit Bedenken des Panel-Moderators Dietrich Läpke, Koordinator Sicherheitsforschung an der Hochschule der Polizei in Münster, der die Frage aufgeworfen hatte, ob die öffentliche Strom- oder Wasserversorgung großflächig via Internet lahmgelegt werden könnte. Dennoch führte er den Teilnehmern der Expertentagung in Wildbad Kreuth vor Augen, dass von 7.500 kritischen Infrastrukturen in Deutschland 45 anfällig für Exploits seien. Wie schnell und häufig Infrastrukturen online angegriffen würden, hat sein Unternehmen anhand von fingierten Selbstversuchen, sog. „Honeypot-Tests“ simuliert. Diese Köder wurden als Infrastrukturen ausgegeben. Informationen

über ihre Steuerungsprozesse wurden bewusst über das Internet zugänglich gemacht. Es habe binnen 24 Stunden 24 Angriffsversuche auf die Anwendungsebene sowie 13 nicht autorisierte Zugriffe auf Sensorik und Motorik gegeben, so Di Filippo. Zudem habe man vier direkte Eingriffe in die Steuerungsmotorik beobachtet. In diesem Zusammenhang wurde der Programmcode verändert. Das „War Googling“ habe zudem ergeben, dass es einige öffentlich zugängliche Systeme ohne Schutzmechanismen in Deutschland gibt. „Auf diese zuzugreifen ist ganz einfach, man muss nur nach namhaften Herstellern im Internet suchen, die Sicherheitslücken haben“, so Di Filippo. So könne man beispielsweise auf die Zentralheizungsanlage einer Schule im Internet einfach so zugreifen. Es wäre so möglich, beispielsweise die Temperatur in den Klassenzimmern über das Internet zu verändern. Die Firmen und Einrichtungen wurden von Compass Security sowie dem BSI benachrichtigt. „Sie sind aber immer noch im Netz zu finden“, bemerkt Di Filippo. Die mangelnde Handlungsbereitschaft, Sicherheitslücken zu schließen, sei ihm unbegreiflich. „Die Bedrohung wird nicht ernst genommen“, so Di Filippo. Auch SCADA-Systeme, zuständig für Steuerungsprozesse in kritischen Infrastrukturen, können in ihrer Visualisierung per Internet aufgerufen werden. Unternehmen machen sich durch die Verfügbarkeit dieser zentralen Informationen im Netz erpressbar, so Di Filippo. Hacker können ihnen androhen, Daten zu manipulieren oder zu löschen. Wenn ein Unternehmen dann über kein Daten-Backup verfüge, könne es verleitet werden zu zahlen, um das operative Geschäft weiterführen zu können.

Der zweite Tag der Expertentagung „Sensibilisierung für Cyber-Sicherheit“ im Bildungszentrum Wildbad Kreuth begann mit einem Einführungsreferat von Prof. Dr. Udo Helmbrecht, Geschäftsführender Direktor der ENISA, der eingangs einen Überblick über das Aufgabenspektrum und das Selbstverständnis seiner Agentur lieferte. Sie wolle den europäischen Sicherheitsmarkt fördern und sicherer machen. Die ENISA verfolge dabei ein industrieorientiertes Konzept. Auf der Policy-Ebene wolle die Agentur politische Rahmenbedingungen für den Cyberspace schaffen. „Erst seit dem Lissabon-Vertrag findet eine vernetzte Zusammenarbeit zu diesem Thema statt. Erst seit 2009 reden wir mit Europol“, erklärte Helmbrecht. Seitdem gibt es immer wieder neue Entwicklungen zu beobachten. Die Kommission habe beispielsweise erst kürzlich die „Network Information Security Directive“ als Entwurf in den EU-Gesetzgebungsprozess eingebracht. Die Direktive wurde im Februar eingebracht und muss noch vom Rat und dem Parlament beschlossen werden, bevor sie von den Mitgliedsstaaten ratifiziert wird. Das Vorhaben soll die Kooperation der Mitgliedsstaaten im Bereich Cyber-Sicherheit stärken, und der ENISA kommt dabei eine starke Rolle zu.
Die Aufgabe der europäischen Agentur ist es, die Kommission im Bereich Netzwerkssicherheit und Informationssicherheit zu beraten und die Mitgliedsstaaten auf technischer Ebene, beispielsweise durch CERTs, zu unterstützen. Die ENISA liefert zudem Analysen und führt Übungen durch. Außerdem hat sie den „Good Practice Guide“ für mehr Sicherheit im Internet herausgegeben. Die Zusammenarbeit im Feld der Netzwerksicherheit und Informationssicherheit basiere auf Vertrauen, so Helmbrecht. Pläne, den Informationsaustausch zwischen den Mitgliedsländern bezüglich Cyber-Angriffen verpflichtend zu machen, steht er deswegen eher skeptisch gegenüber.

In der anschließenden Diskussion stellte Oliver Rolofs, Pressesprecher der Münchner Sicherheitskonferenz, die Frage nach einer gemeinsamen EU-Cyberaußenpolitik. Die brauche Zeit, antwortete Helmbrecht. Er brachte zur Untermauerung seiner These das Beispiel des „EU-Außenministeriums“, dem EEAS. Es habe drei Jahre gebraucht, diesen aufzubauen, so Helmbracht. Ähnlich lange, wenn nicht länger, würden gemeinsame Bemühungen zur Cyberaußenpolitik in Anspruch nehmen.

Investitionen in die Zukunft
Wege zu einer digitalen Sicherheitskultur?

Prof. Dr. Michael Waidner, Leiter des Fraunhofer-Instituts für Sichere Informationstechnik (Fraunhofer SIT) sowie Inhaber des Lehrstuhls für Sicherheit in der Informationstechnik an der Technischen Universität Darmstadt, erläuterte in seinem Referat Gründe für die Unsicherheit der IT. „Web-Anwendungen sind mehrheitlich verwundbar“, erklärte er. 86 Prozent der Fehler, die zur Unsicherheit der Informationstechnik führten, seien Konfigurationsfehler, entstünden also im Zusammenhang mit der Erstellung von Daten und Zugriffsmöglichkeiten. Große Sicherheitslücken gebe es beispielsweise bei der Software Java. Für die Unsicherheit der IT nannte Waidner folgende Gründe: Zunächst seien Informationen die neue Währung. Der Handel mit Sicherheitslücken und Konsumentendaten boome. Zudem würden gerade starke Angreifer immer Lücken im System finden, daher sei ein schneller Austausch über Sicherheitslücken vonnöten. Darüber hinaus sei das Internet für Robustheit und nicht für Sicherheit gebaut worden. Es sei daher ein „geordneter Neuanfang“ nötig, so Waidner. IT sei so komplex, dass die Auswirkungen von Angriffen kaum vorhersehbar seien. „IT wird wie eine Kunst entwickelt und nicht wie eine Wissenschaft“, so Waidner. Die einzige Möglichkeit, mehr Cyber-Sicherheit zu schaffen sei daher, die Idee der „security by design“ durchzusetzen. Die Architekturen müssten so gestaltet sein, dass möglichst viele Fehlerquellen ausgeschlossen werden können. So sollten z. B. nicht mehr große Systeme mit einer einzigen Datenbank, sondern Strukturen mit mehreren Teilsystemebenen geschaffen werden. Auch auf der Integrationsebene müsse die Leitlinie „security by design“ besser umgesetzt werden. Hier sieht Waidner ein großes Forschungs- und Entwicklungspotenzial in Deutschland. „'security by design' ist die einzige Möglichkeit, die Kostenexplosion bei der Fehlerbehebung zu begrenzen“, bekräftigte er.

„Es fehlen Umgangsformen und Verhaltensweisen im Cyberspace“, bemerkte Oliver Rolofs in seinem Tagungsbeitrag. Er sprach sich zudem für eine Fokussierung auf eine Präventions- und Sensibilisierungskultur anstatt einer Sicherheitskultur aus. Zudem sprach er sich dafür aus, die Governance des Internets in den Mittelpunkt zu stellen. Die derzeitige internationale Zusammenarbeit für Cyber-Sicherheit, etwa auf Basis der CERTs, entspräche eher einem Pragmatismus denn einem Leitbild. Rolofs störte sich zudem an der „inflationären Verwendung des Begriffes Krieg“ und sprach damit die andauernde Begriffsverwirrung im Feld der Cyber-Sicherheit an, in dem oft von „Cyberwar“ die Rede sei. Dies könne zu einem Sicherheitsdilemma führen, so Rolofs. Er sprach sich in diesem Zusammenhang für eine „verbale Abrüstung“ aus. Auch er befürwortete, wie am Tag zuvor bereits Sandro Gaycken, eine stärkere Rolle des Staates im Bereich Cyber-Sicherheit. „Es muss die Möglichkeit geben, das Thema Vorratsdatenspeicherung unter den sicherheitsrelevanten Aspekten unemotional zu diskutieren“, so Rolofs. Er sprach sich zudem für eine stärkere Zentralisierung der Kompetenzen aus. „Institutioneller Wildwuchs und der deutsche Föderalismus erschweren den Informationsaustausch“, so Rolofs. Zudem halte er die Angst vor einer Meldepflicht für unbegründet. Er schlug deshalb vor, „die Cyber-Expertise in einer Lead-Funktion beim Bundeskanzleramt anzusiedeln.“

Dieter Schneider, Präsident des Landeskriminalamts Baden-Württemberg, näherte sich in seinem Referat dem Thema der Tagung an, indem er den Begriff „digitale Sicherheitskultur“ zu definieren versuchte. Hierfür erklärte er, dass der Begriff Sicherheitskultur erstmalig in Zusammenhang mit dem Reaktorunfall in Tschernobyl verwendet worden sei. Die derzeitige Situation sei durchaus überspitzt mit der damaligen zu vergleichen, so Schneider. „Wir leben in digitaler Unsicherheit“, erklärte er. Besonders besorgniserregend für das Landeskriminalamt sei die „digitale Schattenwirtschaft“. „Beim Bürger macht sich Unsicherheit breit“, bemerkte Schneider. Denn wo liege der

Unterschied, ob man nach dem Geldabheben am Automaten seiner Barschaft beraubt werde oder ob der gleiche Effekt diskreter erfolge, nachdem die Kartendaten am Automaten ausgelesen wurden? Eine Unterscheidung sei lediglich in der Reaktion der Geschädigten zu beobachten. Denn obwohl die Geschädigten zunächst berechtigterweise wütend wären, setze oft wenig später Resignation ein. Aufgrund der Anonymität des Verbrechens und der – wie Schneider sagte – „Eigendynamik des Technischen" – mache sich bei den Opfern Ohnmacht breit.
Aufgabe der Landeskriminalämter sei es daher, den Nutzer vor der Zweckentfremdung seiner Daten und vor der Schädigung seiner Systeme zu schützen. „Es darf online nicht das Recht des Stärkeren gelten", so Schneider. Derzeit liefen die Ermittlungsbehörden den Entwicklungen jedoch eher hinterher, als ihnen Herr zu werden. „Ein Rechtsstaat 2.0 mit einer digitalen Sicherheitskultur kann nur gemeinsam mit allen gesellschaftlichen Kräften gelingen. Der Staat hat ein Gewalt-, aber kein Sicherheitsmonopol", fasste Schneider die Situation zusammen. Die einzige Möglichkeit, Cyberkriminalität, für die das Landeskriminalamt zuständig ist, zu bekämpfen liege darin, mehr Know-How zu generieren. „Wir müssen uns updaten für die Bekämpfung von Cyber-Kriminalität", so Schneider. Zudem warf er die Frage auf, ob auch vom privaten Internetnutzer mehr Kenntnisse für sicheres „surfen" verlangt werden dürfte. „Brauchen wir einen Internetführerschein?", fragte er.

Dr. Hans-Peter Uhl, Mitglied des deutschen Bundestages und innenpolitischer Sprecher der CDU/CSU-Fraktion, bemängelte, dass die Anstrengungen Deutschlands für eine digitale Sicherheitskultur nicht ausreichend seien. Auch seien die Haushaltsmittel für diesen Bereich zu gering. Wie schon der Referent Sandro Gaycken sprach sich auch Hans-Peter Uhl dafür aus, einen IT-Hochsicherheitsmarkt für Deutschland zu generieren. Damit könne das Problem der Unzuverlässigkeit der im Ausland gefertigten Software- und Hardware-Komponenten umgangen werden. Zudem schlug er eine Art TÜV für das Internet vor. Ein Gremium solle Soft- und Hardware-Produkte sowie Systeme auf ihre Sicherheit hin überprüfen.
Der Schutz der Schwächeren durch Mindestsicherheitsanforderungen habe höchste Priorität. Der Staat habe hierfür schon einiges getan. So sei etwa 2007 das IT-Sicherheitsmanagement für die Bundesregierung eingeführt worden. Zudem arbeitet man seit 2005 zum bundesweiten Schutz kritischer Infrastrukturen zusammen. Es wurden seit 2009 große Anstrengungen im Bereich der IT-Sicherheitsforschung in einer finanziellen Höhe von 30 Milliarden Euro getätigt. Das BSI wurde personell aufgestockt. 2002 waren es noch 392,5 Stellen, 2013 verfügt die Behörde über 536,5 Planstellen. 2009 wurde das BSI per Gesetzesnovellierung zudem mit neuen Befugnissen als Zentralstelle, als verantwortliche Behörde für IT-Sicherheitswarnungen sowie für den IT-Sicherheitsschutz des Bundes ausgestattet. Ebenfalls zu nennen ist das dem Wirtschaftsverwaltungsrecht zugeordnete DE-Mail-Gesetz, das die Zulassung und die Arbeit so genannter De-Mail-Dienstanbieter reguliert.
Größter Fortschritt sei die 2011 verabschiedete Cyber-Sicherheitsstrategie für Deutschland. Sie zeichne sich durch einen ganzheitlichen Ansatz im Sinne des Cyber-Sicherheitsbegriffs und der internationalen Handlungsnotwendigkeiten aus. Dennoch müsse auf gesetzgeberischer Seite noch einiges getan werden, betonte Uhl. Auf seiner innenpolitischen Agenda stünden u. a. die Einführung der Vorratsdatenspeicherung, der Online-Durchsuchung sowie der Quellen-Telekommunikationsüberwachung. Diese Maßnahmen seien laut Uhl „unabdingbar". Uhl forderte darüber hinaus die Schaffung gesetzlicher Grundlagen für die Benutzung und Bereitstellung von offenen drahtlosen Netzwerken inklusive der Klärung der Rechtsstellung und Haftung des Anbieters zum Schutz des privaten Nutzers. Zudem wolle er durch geeignete Maßnahmen das eigenverantwortliche Handeln in der digitalen Gesellschaft, z. B. durch frühe Förderung der Medienkompetenz in der Schule, erreichen und dazu staatliche Angebote stärker mit der Wirtschaft abstimmen.

In der anschließenden Diskussion widersprach Waidner der Aussage Schneiders, man müsse über einen „Führerschein“ für das Internet nachdenken. „Das Problem sind nicht die Nutzer, sondern die Entwickler“, betonte der Informatik-Professor. Diese sollten gezwungen werden, sichere Produkt- und Software-Lösungen anzubieten. Der Schaffung eines IT-Hochsicherheitsmarktes „Made in Germany“ erteilte er eine Absage. „Wir können nicht autark werden. Das ist nicht finanzierbar“, sagte er. Rolofs fügte hinzu, dass die Schaffung eines IT-Sicherheitsmarktes nur mithilfe von Subventionen durchführbar sei. Dies aber wahrscheinlich nicht nachhaltig sei.

Zum Abschluss der Tagung zog Prof. Dr. Reinhard Meier-Walser ein Fazit der Veranstaltung. Das Thema Cyber-Sicherheit sei im Kontext weiterer neuer sicherheitspolitischer Herausforderungen, wie etwa Terrorismus, Pandemien, Piraterie etc., zu sehen. „Im Unterscheid dazu verkörpert Cyber-Sicherheit jedoch eine extreme Komplexität“, erklärte er. Das Themenfeld sei nur mit einem multiperspektivischen Blick voll umfänglich zu begreifen. Volker Foertsch bemerkte zum Ende der Veranstaltung, dass die Rolle des Staates in dem Maße, in dem die Sensibilisierung für Cyber-Sicherheit fortschreite, immer stärker werde. Es sei zudem als positiv zu bewerten, dass seit der letzten Kooperationsveranstaltung der Hanns-Seidel-Stiftung und des Gesprächskreises Nachrichtendienste im Oktober 2011 Öffentlichkeit, Medien und Politik deutlich für das Thema Cyber-Sicherheit sensibilisiert worden seien. Trotzdem gebe es in diesem Feld noch viel zu tun.

Die Beiträge der Tagung lassen den Schluss zu, dass internationale Zusammenarbeit und nationalstaatliche Bemühungen, beispielsweise der Drang nach Regulierung, einander zuwider laufen können. Ebenfalls noch nicht abschließend geklärt ist die Rolle des Privatsektors sowie der Zivilgesellschaft zur Förderung der Cyber-Sicherheit, nicht nur in Deutschland. Wollen wir einen „Whole of nation approach“, der private Akteure mit einschließt? Oder brauchen wir einen „whole of government approach“, der Aktivitäten der Exekutive, privatwirtschaftliche und zivilgesellschaftliche Akteure zu mehr Sicherheit zu verpflichten, hervorhebt? Auf internationaler Ebene kann zudem beobachtet werden, dass erneut ein bipolares Denken einsetzt, wonach „der Westen“ die Freiheit im Internet postuliert und ein Abschreckungsszenario gegen potentielle Angreifer aufbaut, während „der Osten“ in bilateralen Verhandlungen zwar Verhaltensregeln fordert, diese Argumente aber vor allem zur Förderung der staatlichen Kontrolle anbringt. Zudem kann in der deutschen Debatte festgestellt werden, dass fundamentale demokratische Fragestellungen wieder eine Rolle spielen. Es geht darum, wer im Zusammenhang mit dem Streben nach größerer Sicherheit ein Mitspracherecht hat. Steht die Private-Public-Partnership vor dem Aus? Außerdem wurde deutlich, dass die Revolution Industrie 4.0 eine Weiterentwicklung ist, deren Folgen wohl nicht zu Ende gedacht wurden. Die stärkere Vernetzung wird Risiken bergen. Die Frage für die Zukunft wird sein: wie und in welchem Rahmen gehen wir mit diesen Herausforderungen um?