Bundeskriminalamt

Bundeskriminalamt (Hg.)

Cybercrime

Bedrohung, Intervention, Abwehr

BKA

BKA-Herbsttagung 2013

Herausgegeben vom
Bundeskriminalamt
Kriminalistisches Institut

Bundeskriminalamt

Bundeskriminalamt (Hg.)

Cybercrime

Bedrohung, Intervention, Abwehr

Vorträge und Diskussionen anlässlich der
Herbsttagung des Bundeskriminalamtes
vom 12. - 13. November 2013

BKA

Redaktion

Roman Koch
Andreas Kuhn

Bundeskriminalamt
Kriminalistisches Institut

Inhaltsverzeichnis

***Begrüßung und Einführung* in das Tagungsthema:**
Cybercrime – Bedrohung, Intervention, Abwehr

Jörg Ziercke

Wegen der dynamischen phänomenologischen Entwicklung, aber auch wegen der katalysierenden Wirkung, die das Internet als Tatmittel auf die Veränderung der modi operandi vieler Deliktsformen des Strafgesetzbuches, auf den Schadensumfang, auf viktimologische Aspekte sowie auf die Anforderungen an eine effektive Verbrechensbekämpfung hat, ist dies sicherlich ein Thema von hoher Aktualität. Dies zeigen auch die vielen Veranstaltungen in diesem Jahr, die sich mit dem Thema 'Cybercrime' beschäftigt haben. Das belegen viele Sondersitzungen der Polizeien des Bundes und der Länder. Alle reden über eine effektive Verbrechensbekämpfung im digitalen Zeitalter.

Noch vor 10 Jahren wurde in Statistiken der prozentuale Anteil von „Haushalten mit Internetanschluss“ bzw. die „Ausstattung von Haushalten mit PC“ erhoben – heute im Zeitalter von Smartphone, von Tablet, von Wlan-Hotspots, von SmartGrid fast anachronistisch anmutende Erhebungskriterien!

Wir sprechen von flüchtiger Moderne, vom Zeitalter der digitalen Revolution. Dies bringt Umwälzungen, die mit der industriellen Revolution vor 200 Jahren verglichen werden, in allen Lebensbereichen mit sich. Wegen der ihr immanenten Überschreitung jeglicher Art tradierter Ordnungsmuster und der Veränderungsgeschwindigkeit gehen diese Umwälzungen mehr und mehr in eine Nachdenklichkeit über, ob wir bereits in der Lage sind, auf die uns gestellten Fragen hinreichende Antworten zu geben.

Digitale Technologien haben alle Lebensbereiche, Kommunikations- und Interaktionsformen durchdrungen. Sie bieten uns große Chancen und Möglichkeiten. Sie sind eine bedeutende Lebensader unserer Welt geworden, prägen mehr denn je alle Entwicklungen einer rasant fortschreitenden globalen Vernetzung. Ihr Potenzial scheint unerschöpflich. Damit einher gehen aber auch spezifische Abhängigkeiten, Bedrohungen, Verletzbarkeiten und spezifische subjektive Unsicherheitsgefühle.

Das, was wir unter Cybercrime zusammenfassen, ist eine Bedrohung mit unvergleichbarer Dimension: Allein die direkten Kosten, die durch Cybercrime entstehen, sind größer als jene, die der Handel von Kokain, Heroin und Marihuana gemeinsam erzeugen.

Betrugsdelikte und Erpressungen, Eigentum- und Diebstahlsdelikte, illegaler Handel mit Drogen, Kinderpornographie oder Geldwäsche und auch Cybercrime im Bereich der politisch-motivierten Kriminalität: Durch die über das Internet zur Verfügung gestellte digitale Infrastruktur eröffnen sich neuartige modi operandi mit enormen Schadensausmaßen und -potenzialen.

Die Infrastruktur des Internet führt dazu, dass nicht nur Ordnungskriterien wie Zeit und Raum an Bedeutung verlieren. Sie führt ebenso dazu, dass die auf solchen Kriterien basierenden Rechtsordnungen – denken Sie nur an die klassischen Begriffe des Straf- und Strafprozessrechtes wie örtliche Zuständigkeit oder Tatzeit – an funktionale und territoriale Grenzen stoßen, ohne dass alternative Steuerungsmedien und -ebenen erkennbar sind. Das Internet entgrenzt Kriminalität und ist ungebremst entwicklungsoffen.

Unsere BKA-internen Analysen, basierend auf dem Szenario-Projekt zum Thema „Always-on-Gesellschaft“, zeichnen folgende Entwicklungslinien:

1. Die Zahl der potentiellen Einfallstore für Kriminelle steigt weiter: Je mehr Geräte und Schnittstellen wir nutzen, je stärker wir uns digital vernetzen, desto mehr nimmt die Verwundbarkeit der Systeme zu.

2. Der virtuelle Handel, virtuelle Währungen und Cyber-Terrorismus bilden auch künftig Schwerpunkte krimineller Internet-Aktivitäten.

3. Schnellere Übertragungstechnologien erhöhen die Datentransfers. Die Folge sind immer größere Datenmengen. Die Anforderungen an die Recherche- und Analysefähigkeiten im Strafverfahren steigen an.

4. Ein gemeinsames Verständnis, abgestimmte Arbeitsteilung zwischen den Sicherheitsbehörden, wie auch zwischen Behörden und Wirtschaft und anderen Institutionen – auch weltweit – wird immer wichtiger.

Was bedeuten diese Entwicklungslinien für unsere Arbeit?

Um Cybercrime zu bekämpfen, müssen wir die Bedrohungslage differenziert beschreiben und analysieren, müssen intervenieren, Gefahren abwehren und Straftaten verfolgen!

Es geht darum, Antworten auf folgende Fragen zu finden:

- Wie muss kriminalpolizeiliche Arbeit heute und in der nahen Zukunft aussehen?
- Welche kriminaltechnischen und forensischen Möglichkeiten brauchen wir?
- Wie müssen sich die Sicherheitsbehörden aufstellen?
- Welche Kooperationsformen sind notwendig?
- Reicht die bestehende Gesetzeslage aus?

Damit einher geht die Frage: Wie schaffen wir es, das notwendige Vertrauen der Menschen in unserem Land in die polizeiliche Arbeit gegen gewissenlose Cyberkriminelle zu gewinnen und nicht als Totalüberwacher, Datensammelwütige oder Datenprofilneurotiker denunziert zu werden?

Wie gelingt es, in einem solchen Begriffseinheitsbrei Konturen zu bestimmen, die eine sach- und zweckdienliche Auseinandersetzung um den einzuschlagenden Weg erst ermöglichen? Wie schaffen wir es, den Bürgerinnen und Bürgern verstehbar zu erklären, dass bei der Verfolgung von schwerer Kriminalität im Internet derzeit eine Gerechtigkeitslücke entsteht, die wieder einmal nur die Cleveren und Verantwortungslosen begünstigt , aber den rechtstreuen Bürger fassungslos zurücklässt? Die auf Dauer unser Wert- und Normensystem zerstört, ohne das auch eine digitale Gesellschaft nicht zusammenhält.

Mich beschäftigt in diesem Zusammenhang die Frage, ob unsere bisherige Politikberatung wirklich ausreicht. Bund und Länder verständigen sich derzeit auf eine dem globalen Wirkungsraum der Täter entsprechenden Erfassung von Auslandsstraftaten in der Polizeilichen Kriminalstatistik.

Gemeint sind Angriffe auf deutsche Internetuser, Private wie Unternehmen, insbesondere Botnet-Angriffe, bei denen hunderttausende von Rechnern in Deutschland kompromittiert und sabotiert oder als kriminelles Werkzeug benutzt werden. Klare Gesetzesverstöße, die aber heute in keiner Statistik erscheinen. Eine Geschädigtenstatistik soll zukünftig Auskunft geben, ob 1, 2 oder 3 Millionen Menschen oder mehr pro Jahr von Cybercrime in Deutschland betroffen sind. Vielleicht können solche Zahlen die Debatte versachlichen.

Polizei- und auch die Arbeit der Justiz ist „Informationsverarbeitung“. Wir müssen Informationen erheben, selektieren und bewerten. Verdachtsschöpfung, Beweiserhebung, Beweissicherung und Beweisführung folgen im Zeitalter der Cybercrime anderen Logiken, anderen Regeln und Prozessen.
Digitale Spuren und Beweise sind ortsungebunden, flüchtig, veränderbar, zum Teil anonymisiert und kryptiert. Bewährte kriminalistische Methoden und Instrumente stoßen angesichts dieser Charakteristiken an ihre Grenzen.
Zum Beispiel: Maßnahmen der Telekommunikationsüberwachung sind wesentlich für den Ermittlungserfolg in Bereichen schwerer und schwerster Kriminalität. Nach Expertenmeinung ist die Ermittlungsarbeit bei Organisierter Kriminalität zwischen 60 bis 70 Prozent von funktionierender Telekommunikationsüberwachung essentiell abhängig. Doch die zunehmende Verschlüsselung und Kryptierung der Telefonie über das Internet führen dazu, dass Telekommunikationsinhalte mittels klassischer TKÜ-Maßnahmen nicht mehr zu erschließen sind.

In Zusammenarbeit mit den Bundesländern hat das Bundeskriminalamt 167 herausragende Fälle der Schwerkriminalität ausgewertet, in denen Ermittlungsdefizite entstanden sind, weil die Überwachung oder Auswertung von Telekommunikation rechtlich oder technisch aufgrund von Verschlüsselung oder Kryptierung nicht möglich war. In über 70 Prozent dieser Fälle konnte sogar die Art des Kryptierungsdienstes technisch genau belegt werden. Viele schwere und schwerste Straftaten konnten aufgrund des bestehenden Informationsdefizits folglich nicht verhindert und nicht verfolgt werden.

Auch die alternative Nutzung klassischer Maßnahmen wie der Observation oder der Wohnraumüberwachung helfen uns häufig nicht, die notwendigen Daten zu erheben!

Wir brauchen daher andere geeignete Maßnahmen, damit unsere Ermittlungen nicht ins Leere laufen: Ich spreche von der Möglichkeit der Zuordnung von IP-Adressen zu real existierenden Personen – also Mindestspeicherfristen bei den Providern, von Quellen-TKÜ und Onlinedurchsuchung in Fällen schwerster Kriminalität und als ultima ratio mit besonderen Anforderungen an den Grundsatz der Verhältnismäßigkeit.
Wir sind uns der Grundrechtseingriffstiefe und daher der Sensibilität im Umgang mit diesen Instrumenten sehr bewusst. Das Bundesverfassungsgericht selbst hat den Weg für eine verfassungsgemäße Umsetzung aufgezeigt und die Behauptung, die Polizei würde unschuldige Bürger mit einem Generalverdacht überziehen, zurückgewiesen.
Um sicher zu sein, dass die eingesetzte Software für Quellen-TKÜ und Onlinedurchsuchung nicht mehr kann als sie darf, dass technische Vorgaben eingehalten werden, setzen wir darauf, diese Tools selbst zu entwickeln.

Prozesse und Abläufe werden protokolliert, der Kernbereichsschutz wird fortlaufend durch von der ermittlungsführenden Dienststelle unabhängige Einrichtungen überwacht und nicht nur der Bundesbeauftragte für Datenschutz und Informationsfreiheit kann unsere Vorgehensweise jederzeit kontrollieren. Für die Beweiswürdigung durch den Richter müssen wir unsere Vorgehensweise ohnehin dokumentieren und offenlegen. Diese Transparenz sichert die Rechtmäßigkeit der Maßnahmen und den Schutz der Grundrechte der Bürger und das Vertrauen in den Rechtsstaat.
Es wäre allerdings zu kurz gegriffen, sich bei der kriminalistischen Methodenentwicklung ausschließlich auf die Anpassung bzw. Generierung digitaler Ermittlungsinstrumente zu kaprizieren. Diese sind technisch aufwendig und auf Grund der dynamischen Innovationszyklen von geringer Halbwertszeit.

Eine effektive Strafverfolgung und Gefahrenabwehr bedarf selbstverständlich eines ganzheitlichen Ermittlungsansatzes, das heißt einer auf den jeweiligen Einzelfall bezogenen Kombination aus Ermittlungsansätzen der digitalen und der analogen Welt. Beispielsweise durch verdeckte Informationsgewinnung mittels Observationen, den verdeckten Einsatz von Polizeibeamten, durch den Cyber-VE oder die Cyber-VP – Instrumente, die unerlässlich sind angesichts der einfacheren Abschottung der Kommunikation und Interaktion von Tätern im Internet.

Zudem treiben wir den Aufbau einer kriminaltechnischen Servicestelle weiter voran. Das so genannte Cyberlab umfasst die Kryptoanalyse und Dekryptierung von Verschlüsselungen, die Softwareanalyse der Funktionen von digitalelektronischen Asservaten (inkl. „Apps“) und die Administration von Spezialrechnern sowie eines Labornetzes.
Aktuell befasst sich eine Projektgruppe der Polizeien des Bundes und der Länder mit dem Aufbau einer sicheren IT-Infrastruktur zur automatisierten Bearbeitung von Foto- und Videodaten.

Nach den Terroranschlägen in Boston im April dieses Jahres erhielten die US-amerikanischen Sicherheitsbehörden nach einem öffentlichen Fahndungsaufruf innerhalb weniger Stunden über eine Million Fotos und mehr als 1.000 Stunden Videomaterial unterschiedlichster Formate und Quellen. Zur Aufbereitung dieser Datenmengen für die Fahndung und Ermittlungen haben die US-Amerikaner eine Spezialeinheit eingerichtet, die aus über 50 geschulten Videoanalysten besteht und eng mit Universitäten und anderen Einrichtungen kooperiert. Auch die Polizeien von Bund und Ländern müssen bei vergleichbaren Ereignissen – ich erinnere an die Tasche am Bonner Hauptbahnhof – in Deutschland in der Lage sein, solche Informationsmengen, die durch die Bevölkerung nach Fahndungsaufrufen elektronisch übermittelt werden, zu bearbeiten. Das wird eine Herausforderung sein – für alle. Eine

entsprechende Größenordnung lässt sich nur durch eine enge Zusammenarbeit von Bund und Ländern in Form einer Aufrufeinheit von ausgebildeten Videoanalysten und einer gemeinsam genutzten Infrastruktur realisieren.

Zusätzlich müssen die technischen Voraussetzungen für die Datenaufbereitung geschaffen werden: Derzeit gibt es noch keine Analyse- und Auswertetools zur automatisierten Bearbeitung von Foto- und Videodaten verschiedenster Formate. Bund und Länder sind aktuell dabei, Lösungen zu finden.
Der Anschlag in Boston zeigt darüber hinaus noch etwas anderes: Dass die polizeiliche Krisenkommunikation und taktische Öffentlichkeitsarbeit an das veränderte Kommunikationsverhalten der Bevölkerung angepasst werden muss. Der Gefahr von selbst ernannten Fahndern im Internet, die vermeintlich Verdächtige an den Pranger stellen, muss die Polizei mit deeskalierender Öffentlichkeitsarbeit im Internet begegnen. Klassische Medien müssen mit den interaktiven Möglichkeiten des WEB 2.0 und dessen mobiler Nutzung kombiniert werden.

Es ist selbstredend, dass die Verlagerung der Kriminalität in die digitale Welt, strukturelle Anpassungen erfordert. Polizeibehörden benötigen professionelle und zukunftsorientierte Ausrichtungen.
In diesem Jahr haben wir im Bundeskriminalamt einen neuen Kompetenzbereich aufgebaut, der ausschließlich Cybercrime bekämpft. Dabei war für uns entscheidend, ermittlungsunterstützende Auswertung mit operativen Ermittlungen organisatorisch eng zu verknüpfen. Über 150 Spezialisten sollen Cyberkriminelle verfolgen, strafbares Handeln dokumentieren, erwirtschaftete Gewinne aufspüren und Vermögen abschöpfen.
Das für die erfolgreiche Bekämpfung von Cybercrime erforderliche Know-how bauen wir unter anderem durch den Einsatz von Cyberanalysten weiter aus. Diese IT-Experten werden im Team mit Kriminalbeamten in der Fallbearbeitung eingesetzt. Von dieser sogenannten „Tandem-Lösung“ erwarten wir zugleich eine Stärkung einschlägiger Fachkenntnisse bei allen Team-Mitgliedern.

Das Internet als Tatmittel ist inzwischen allgegenwärtig. Deshalb brauchen wir spezifische IuK-Kompetenzen auch in anderen Phänomenbereichen, z.B. zur Bekämpfung der digitalen Verbreitung von Kinderpornographie als besonders widerwärtiger Form eines durch die Spezifika des Verbreitungsmediums auf Dauer dokumentierten Kindesmissbrauchs, des Rauschgifthandels, aber eben auch im Bereich der Spionage, der nachrichtendienstlich gesteuerten Angriffe auf kritische Infrastrukturen sowie beim Extremismus und Terrorismus. Für extremistische und terroristische Organisationen und Gruppierungen ist das Internet das wichtigste Mittel zur Verbreitung von Propaganda und unterschiedlichsten Handlungsanleitungen. Das Gemeinsame Internetzentrum wie auch die Koordinierte Internetauswertung im rechten und linke Extremismusbereich versetzen uns in die Lage, Kommunikationswege von Straftätern, Strukturen, Abläufe, Anschlagsplanungen und sonstige phänomenbezogene Verhaltensweisen frühzeitig zu erkennen und zu bewerten.
Im Phänomenbereich der Cyberspionage sind in Deutschland ausländische Nachrichtendienste unvermindert tätig – nicht erst die aktuellen Debatten legen diesen Fakt offen.

IT-Angriffe mittels Hacking und Malware sind grundsätzlich von jedem Ort der Welt aus und zu jeder Tages- und Nachtzeit möglich. Ernsthafte strafrechtliche Risiken bestehen für die Angreifer kaum, da IT-Angriffe von Nachrichtendiensten dem äußeren Anschein nach nur schwer von allgemeinkriminellen IT-Angriffen zu unterscheiden und die ND-Täter in ihrem Heimatland vor Strafverfolgung weitgehend geschützt sind.

Wir werden uns durch die Einrichtung eines Arbeitsbereiches Cyberspionage in der Abteilung Polizeilicher Staatsschutz des BKA auch dieser Herausforderung verstärkt annehmen.

Alle Konzepte und Strategien fruchten nicht ohne geeignete, fachkundig ausgebildete Mitarbeiterinnen und Mitarbeiter in den Sicherheitsbehörden und bei der Justiz.
Bereits seit dem Jahre 2006 setzen wir im BKA intensiv das gemeinsam mit den Ländern erarbeitete IuK-Fortbildungskonzept um.

Da am Ende der Prozesskette die Verurteilung des Straftäters für die verübten Taten stehen muss, ist es wichtig, bei Investitionen in den personellen und fachlichen Kompetenzausbau den gesamten Funktionszusammenhang zwischen Polizei, Staatsanwaltschaft und Gerichten im Blick zu haben. Polizeiliche Ermittlungsarbeit ist kein Selbstzweck! Auch die Justiz muss entsprechend aufgestellt sein, sonst produziert die Polizei einen enormen Input an Verfahren und die Justiz ebenso hohe Einstellungsquoten.
Der Aufbau von Expertise bei der Justiz über die Einrichtung von Schwerpunktstaatsanwaltschaften wie die "Zentralstelle zur Bekämpfung der Internetkriminalität" der Generalstaatsanwaltschaft Frankfurt (Main) sind daher Maßnahmen, die unabdingbar sind, wenn wir dem Phänomen jetzt und in Zukunft effektiv begegnen wollen.

Die polizeiliche und justizielle Expertise reicht jedoch allein nicht aus. Um den genannten Bedrohungen zu begegnen, ist eine Ausweitung der Abwehrbemühungen über den Schutz der staatlichen Netze hinaus erforderlich.

Wertvolle Erkenntnisse zu modi operandi, aber auch unverzichtbares Know-how liegen nicht nur bei staatlichen Akteuren, sondern in wissenschaftlichen Einrichtungen und Wirtschaftsunternehmen, insbesondere in den Unternehmen der IT-Branche, die zum Teil erhebliche Ressourcen in Analyse und Sicherheit investieren.
Infrastrukturprovider, Serviceprovider, Contentprovider – private Unternehmen sind wesentliche Akteure bei Auf- und Ausbau, Betrieb und Weiterentwicklung des Internet und der darüber angebotenen Produkte und Dienstleistungen. Gleiches gilt für die Bereiche Hard- und Softwareentwicklung.

Unternehmen können durch ein der Bedrohungslage angemessenes Verhalten einen Beitrag leisten – insbesondere im präventiven Bereich. Beispielsweise durch Einhaltung von Mindeststandards zur IT-Sicherheit.
Darüber hinaus verfügen Unternehmen bei Cyberangriffen über wichtige Informationen für die Polizei. Studien belegen: Unternehmen zeigen Angriffe nur selten an – trotz aller Sensibilisierungsbemühungen der Sicherheitsbehörden.
Der Aufwand einer Anzeige sei zu hoch, der Ermittlungserfolg der Behörden demgegenüber zu unwahrscheinlich, die richtigen Ansprechpartner auf Seiten der Behörden seien nicht bekannt. Es kommt noch ein weiterer Grund hinzu: der befürchtete Ansehensverlust.
So nachvollziehbar diese Begründungen auf den ersten Blick erscheinen, so kontraproduktiv sind die Folgen für die Gemeinschaft: Solange Unternehmen erkannte Angriffe verschweigen, gibt es keinen Ermittlungsansatz für die zuständigen Behörden und damit keinen validen Überblick über die gesamte Bedrohungslage. Die Schadenspotenziale vergrößern sich durch Nichtanzeige!

Mit Zusammenarbeit meinen wir aber nicht nur das Stellen einer Strafanzeige. Zu einem ganzheitlichen Ansatz der Bekämpfung von Cybercrime gehört auch, die in Wirtschaft und Wissenschaft, in Unternehmen und an Forschungsinstituten vorhandene Fachkompetenz mit den polizeilichen Kompetenzen zu bündeln.

Hierzu möchte ich Ihnen zwei Vorhaben des BKA kurz vorstellen:

1. Je nach Angriffsstruktur – beispielsweise denke ich hier an speziell entwickelte Schadprogramme – kann es erforderlich sein, externe Spezialisten mit dem entsprechenden Fachwissen in den Bereichen Programmcode oder Netzwerkforensik hinzuzuziehen. Wir stellen uns hier das Modell einer Aufrufeinheit, einer so genannten „Quick Reaction Force Cybercrime“ vor, bestehend aus Experten der Sicherheitsbehörden von Bund und Ländern, Spezialisten aus der Wirtschaft und Wissenschaft. Die Einrichtung einer Aufrufeinheit würde die Reaktionsfähigkeit bei Eintritt eines Schadensfalles deutlich beschleunigen, da bereits bei Beginn der Ermittlungen die benötigte Expertise zur Verfügung steht.

2. Private und Polizei müssen sich gegenseitig in ihrer Arbeit unterstützen. Wir benötigen einen tagesaktuellen Austausch über Bedrohungen, Sicherheitsmaßnahmen und taktisch wichtige Informationen. Für den Phänomenbereich Cybercrime haben wir deshalb modellhaft und als ersten Schritt eine institutionalisierte Public Private Partnership mit zentralen Akteuren aus dem Bankensektor bereits geschlossen. Hiervon erhoffen wir uns eine Verkürzung der Kommunikationswege, die Bildung von Vertrauen und Verständnis für die Partner und einen effektiven Austausch der Erkenntnisse.

Unbestreitbar ist zudem das Erfordernis, dass Cybercrime im internationalen Verbund bekämpft werden muss. Das Bundeskriminalamt hat in den vergangenen Jahren ein internationales Netz der vertrauensvollen Zusammenarbeit mit Cybercrimedienststellen in aller Welt aufgebaut und wird dies unter Einbeziehung von Europol und Interpol weiter ausbauen.

Auch die Rechtsetzung muss an die Erscheinungsformen von Cybercrime angepasst werden – und zwar auf mehreren Ebenen. Dabei muss die Ungleichzeitigkeit von technologischer Entwicklung und der Reaktionszeit der Politik im Hinblick auf rechtliche Anpassungsnotwendigkeiten als besondere Herausforderung gesehen werden.
Sekundenschnelle Ortswechsel von Informationen über das Internet auf Server oder in Clouds rund um die Welt und die Flüchtigkeit digitaler Spuren kontrastieren mit starren rechtlichen Strukturen der internationalen Zusammenarbeit und den Bürokratismen der internationalen Rechtshilfe.

Wir benötigen daher eine multilaterale Verständigung über einen internationalen rechtlichen Rahmen, der uns eine schnellere und effizientere Strafverfolgung im Bereich Cybercrime ermöglicht. Neben der Harmonisierung des Strafrechts und dem Schließen von Strafbarkeitslücken müssen polizeiliche Eingriffsbefugnisse um Methoden, die den technologischen Entwicklungen entsprechen, technikoffen ergänzt werden.

Der Bundespräsident hat in seiner Rede zum Tag der deutschen Einheit die digitale Revolution als eine der großen Herausforderungen unserer Zeit herausgestellt.
Ich zitiere: „Wir befinden uns mitten in einem Epochenwechsel. Ähnlich wie einst die industrielle Revolution verändert heute die digitale Revolution unsere gesamte Lebens- und Arbeitswelt, das Verhältnis vom Bürger zum Staat, das Bild vom Ich und vom Anderen.“
Genauso real wie die technologischen Fortschritte das Leben erleichtern ist unbestreitbar das damit einhergehende Missbrauchs- und Bedrohungspotenzial.

Die Frage nach informationeller Selbstbestimmung ist angesichts der für den Einzelnen kaum noch durchschaubaren Prozesse der Datenvernetzung und Datenverknüpfung einem diffusen

Gefühl eines hinzunehmenden Ausgeliefertseins gewichen, das Vertrauen tendenziell untergräbt und Misstrauen fördert.

Die potenzielle Abtrennbarkeit eines digitalen von dem realen Selbst ist alles andere als eine positive Verheißung. Autonome Verfügbarkeit über das Identitätsprägende verliert so seine Selbstverständlichkeit. Wegen ihrer Eingriffsbefugnisse war eine omnipräsente und omnipotente Polizei mit unserem Freiheitsverständnis noch nie vereinbar. In einer digitalen Welt ist sie es noch weniger.

Genauso wenig ist aber eine, trotz erkennbarer technologischer Entwicklungen, in ihren Instrumentarien zögerlich limitierte Polizei mit effektiver Verbrechensbekämpfung und Rechtssicherheit in Einklang zu bringen. Weil der Zweck des Rechts in der Stabilisierung von Verhaltenserwartungen und dem Aufbau von Vertrauen liegt, geht es um das Optimierungsgebot zwischen Abwehrrechten und Schutzpflichten, um die Balance zwischen Freiheit und Sicherheit. Im Kern ist die Frage nach der Legitimität unserer Rechtsordnung aufgeworfen, die auf Rechtsetzung und Rechtsdurchsetzung gründet und der vermeintlichen Differenz von analoger und digitaler Welt mit der Einheit der Rechtsordnung begegnet.

Es bedarf mehr denn je eines gesellschaftspolitischen und verfassungspolitischen Diskurses über Fragen der Menschenwürde und der Privatheit in einem digitalen Zeitalter. Auch eines Diskurses über das technisch Machbare und das normativ Wünschbare und Zulässige. Genauso eines Diskurses über den Ausbau des Grundrechtsschutzes durch entsprechende Kontrollverfahren.

Letztlich geht es um Vertrauen: In das Internet, in die Sicherheitsbehörden, in den Rechtsstaat, der seiner Schutzpflicht angemessen genügen muss. Pauschalierende Etiketten werden diesen diffizilen Themen und dem Bemühen um eine Antwort nicht gerecht.

Eröffnungsansprache:
Cyberkriminalität - globale Herausforderungen weltweiter Netzwerke

Klaus-Dieter Fritsche

Einleitung

Die BKA-Herbsttagung beschäftigt sich seit fast 60 Jahren mit aktuellen Fragen zur Bekämpfung und Verhütung der verschiedenen Erscheinungsformen von Kriminalität.

Wenn man sich die Themen der vergangenen Jahre ansieht, fällt auf, dass das Thema Cybercrime mit der diesjährigen Veranstaltung schon zum dritten Mal seit 2003 auf der Tagesordnung steht:

- damals unter dem Titel „Informations- und Kommunikationskriminalität“
- 2007 unter dem Titel „Tatort Internet“
- und heute eben unter dem Titel „Cybercrime“.

Dies hat nun sicherlich nicht damit zu tun, dass den Veranstaltern der Herbsttagung die Ideen ausgingen. Dafür ist die Entwicklung auf allen Kriminalitätsfeldern leider viel zu dynamisch. Der Grund ist vielmehr, dass sich gerade das Gebiet der Cyberkriminalität, den jeweils aktuellen Techniktrends folgend, besonders rasch entwickelt.

Bedeutung Internet

Die Informationstechnik und insbesondere das Internet sind aus unserem Leben nicht mehr wegzudenken. Ob es darum geht, Informationen zu suchen, Einkäufe zu erledigen, Bankgeschäfte abzuwickeln oder einfach mit Freunden und Bekannten oder Kollegen in Kontakt zu bleiben – all diese alltäglichen Handlungen verlagern wir immer mehr ins Internet. Auch die Wirtschaft profitiert von effizienteren Kommunikationswegen und den verbesserten Möglichkeiten für zielgruppengerechte Werbung – nicht zu reden von dem immer größeren Bereich der Internetwirtschaft, der ausschließlich mit dem Internet sein Geld verdient. Der Handel mit Aktien oder anderen Wertpapieren, Rohstoffen oder Emissionszertifikaten, all diese Transaktionen finden mittlerweile selbstverständlich elektronisch statt.

Bedrohungslage I

Angesichts dieser ökonomischen Erfolgsstory überrascht es wenig, dass auch die organisierte Kriminalität versucht, die neuen Kommunikationsformen und Wirtschaftsmodelle auszunutzen. Den virtuellen Bankraub kann man bequem vom Wohnzimmer aus betreiben. Das Risiko, auf frischer Tat ertappt zu werden, besteht quasi nicht. Und wenn man die richtigen technischen Kniffe kennt, hinterlässt man auch kaum Spuren, anhand derer die Polizei einem nachträglich auf die Schliche kommen könnte.

Selbst der Trickbetrüger muss nicht mehr mühselig von Haustür zu Haustür gehen, sondern kann über das Internet – sei es durch gefälschte Inserate bei eBay oder den Versand von Spam – Millionen erreichen. Da verwundert es wenig, wenn sich selbst äußerst plumpe Betrugsversuche noch rentieren – offenbar findet man immer noch genügend Menschen, die darauf hereinfallen, – sei es aus Unerfahrenheit oder weil sie in der Geschwindigkeit, in der ein Geschäft im Internet abgewickelt wird, nicht genügend aufgepasst haben.

Ergriffene Maßnahmen

Repressiv

Nun hat nicht nur die Herbsttagung des BKA das Thema Cybercrime schon frühzeitig entdeckt. Auch in der politischen Diskussion über rechtliche Abwehrmaßnahmen versucht man, mit den Tätern Schritt halten zu können. Dabei standen – und das sind aus meiner Sicht auch heute noch die aktuellen Herausforderungen – zwei Aspekte im Vordergrund:

Zum einen brauchen wir genug Personal bei den Strafverfolgungsbehörden, das in der Lage ist, mit den technisch versierten Tätern mitzuhalten, ihre Fehler zu erkennen und sie letztlich zu überführen. Das mit anderen Worten über die notwendigen Kenntnisse und die notwendige Ausrüstung für die Streife im Cyberraum verfügt.

Und wir brauchen zweitens – auch wenn ich mir mit dieser Aussage heutzutage kaum Freunde mache – Daten. Daten über die Kommunikation der Straftäter, das heißt Verkehrsdaten und Inhalte von Emails und Chats, Login- und Kundendaten von Providern und Telemedienanbietern. Dabei interessieren uns nicht – und ich denke das kann man nicht oft genug betonen – die Daten von unbescholtenen Bürgern. Aber wenn wir einen Verdächtigen haben – das heißt sein Pseudonym, seine Email-Adresse oder vielleicht eine IP-Adresse – müssen die zuständigen Behörden in Deutschland in der Lage sein, herauszufinden, welche Person hinter diesem Pseudonym steckt, welche Identität der vermutliche Straftäter hat.

So hat die Innenministerkonferenz bereits 2010 die Strategie zur Bekämpfung der Informations- und Kommunikationskriminalität beschlossen. Diese legte ihren Schwerpunkt insbesondere auf den fachlichen Austausch – nicht nur zwischen den Behörden, sondern insbesondere mit der IT-Wirtschaft, aber vor allem auf das notwendige fachkundige Personal. Neben der größeren Rolle, die dem Cyber-Thema in der Aus- und Fortbildung seitdem zukommt, sind vor allem die Fachdienstellen hervorzuheben, die in Bund und Ländern die mit dem Phänomen Cybercrime befassten Spezialisten zusammenfassen, um das Know-how entsprechend zu bündeln.

Und dabei kommt auch dem BKA eine besondere Rolle zu. Zum einen ist es als Zentralstelle, insbesondere auch für die internationale polizeiliche Zusammenarbeit, bei den meist länder- und grenzüberschreitenden Sachverhalten gefordert. Darauf sind die Aufgaben des BKA

allerdings nicht beschränkt. Gerade bei neuartigen Begehungsformen und in Fällen, in denen eine Tat noch gar nicht lokalisiert werden kann, übernehmen die Fachleute des BKA auf Bitten der zuständigen Staatsanwaltschaft häufig die polizeilichen Ermittlungen. Insbesondere die Zusammenarbeit mit der ZIT – der Zentralstelle zur Bekämpfung der Internetkriminalität der Generalstaatsanwaltschaft Frankfurt/Main als bundesweiter Schwerpunktstaatsanwaltschaft – hat sich in der Vergangenheit immer wieder als äußerst erfolgreich erwiesen.

Daher setze ich auch große Hoffnungen in den im letzten Jahr gestarteten Ausbau des Cybercrime-Centers im BKA. Hier haben bislang schon die besten „Cybercops“ weltweit gearbeitet. Deren Zahl wollen wir weiter erhöhen, um einerseits den steigenden Kriminalitätszahlen im Cyberraum begegnen zu können, aber auch, um die so wichtige Kooperation mit den Ländern und den Partnerbehörden in anderen Staaten auszubauen.

Letztere ist von ganz besonderer Bedeutung. Denn für den Cyberkriminellen ist es ziemlich gleichgültig, in welchem Land er sein Wohnzimmer hat, er kann von hier aus in jedem anderen Land, das ihm als lukrativer „Markt“ für seine kriminellen Geschäfte erscheint, tätig werden.

Dies ist aber auch ein besonders heikles Thema. Denn die Kriminellen sitzen nicht zwingend in demokratischen Rechtsstaaten, wie wir sie uns wünschen. Und selbst, wenn diese Voraussetzung erfüllt ist: Die Zusammenarbeit erfordert neben einer einwandfreien rechtlichen Grundlage zusätzlich noch besonderes Fingerspitzengefühl und vor allem persönliches Vertrauen, das beständig aufgebaut und gepflegt werden muss.

Doch alleine gute Leute im BKA und den LKÄ genügen nicht, um die Cyberkriminalität wirksam zu bekämpfen. Wir müssen ihnen auch die notwendigen rechtlichen Werkzeuge an die Hand geben. Und das sind, ich erwähnte es bereits, im Cyberraum vor allem Befugnisse, auf die für die Identifizierung und Überführung der Täter notwendigen Daten zugreifen zu können.

Um Missverständnissen von vornherein vorzubeugen: Es geht nicht darum, Bürger im Netz flächendeckend zu bespitzeln oder auszuforschen, wie dies manchmal unterstellt wird. Die Strafverfolgungsbehörden interessieren sich weder für die private Kommunikation im Internet noch stehen Schüler, die im Internet heimlich Musik und Filme tauschen, im Fokus – auch wenn letzteres natürlich nicht legal ist und im Zweifel ein Abmahnung der Rechteinhaber nach sich zieht.

Aber wenn die organisierte Kriminalität sich im Internet breit macht und dieses für schwere Straftaten mit hohen finanziellen Schäden missbraucht, sei es in Form des massenhaften Phishings, der Onlineerpressung oder aller Formen der Geldwäsche, dann müssen wir diesen professionell agierenden Tätern auf Augenhöhe begegnen.

Einer der ersten Schritte war sicherlich die schon länger zurückliegende Einführung neuer Computerstraftatbestände in den §§ 202a bis c des Strafgesetzbuches, also das Ausspähen und Abfangen von Daten und deren Vorbereitung. Die Diskussion um diese sogenannten „Hackerparagrafen“ mutete jedenfalls mit der Brille des Juristen betrachtet teilweise etwas bizarr an. So sahen sich Sicherheitsexperten, die ja völlig legal die Sicherheit von Programmen testeten, plötzlich dem Risiko der Strafbarkeit ausgesetzt. Aber auch ein Chirurg hört es ja nicht gerne, dass er in dem Moment, in dem er das Skalpell ansetzt, im

Juristendeutsch tatbestandlich eine Körperverletzung begeht – auch wenn er dies dem Willen des Patienten entsprechend macht und damit natürlich nicht zum Straftäter wird.

Ein Punkt, dem wir uns in der letzten Legislaturperiode angenommen hatten, ist die Bestandsdatenauskunft. Hier hatte das Bundesverfassungsgericht Anfang 2012 Änderungen in den Regelungen des Telekommunikationsgesetzes und Ergänzungen in den Fachgesetzen eingefordert. Das BMI hatte daraufhin einen Entwurf vorgelegt, der vom Bundestag dann auch verabschiedet wurde, so dass das Gesetz rechtzeitig vor Auslaufen der vom Verfassungsgericht gesetzten Frist in Kraft treten konnte. Damit haben wir insbesondere eine normenklare Regelung, die die Provider verpflichtet, auch die Bestandsdaten der Inhaber von IP-Adressen, ggf. unter Rückgriff auf die Verkehrsdaten, zu beauskunften. Dies war im TKG bislang etwas verklausuliert und vom Bundesverfassungsgericht zu Recht als wenig normenklar beanstandet worden.

Prävention

Wir beschränken uns natürlich nicht nur auf die Strafverfolgung. Ein ebenso wichtiges Standbein ist wie bei allen anderen Kriminalitätsfeldern auch die Prävention. Nach einer aktuellen gemeinsamen Studie von PricewaterhouseCoopers und der Universität Halle hat die sogenannte NSA-Affäre hier aktuell einen erheblichen Beitrag geleistet. 25 % der für die Studie befragten Unternehmen schätzen das Risiko von Industriespionage nach den Veröffentlichungen zu den durch Edward Snowden geleakten Dokumenten höher ein als vorher.

Unabhängig von den gegenüber der NSA erhobenen Vorwürfen sind wir uns alle sehr sicher, dass das, was derzeit nur der NSA vorgeworfen wird, von anderen Staaten mit Sicherheit betrieben wird. Nämlich Spionage in Deutschland, und zwar nicht nur gegen Regierungsstellen, sondern insbesondere zu Lasten der deutschen Wirtschaft. Gerade der in Deutschland hoch innovative Mittelstand ist hier bedroht. Und es ist auch eine Tatsache, dass die Bundesregierung bereits seit Jahren vor diesen Gefahren warnt.

Aus diesen Gründen haben wir auch schon zahlreiche Maßnahmen ergriffen, um IT-gestützte Angriffe auf Wirtschaft und Bürger zu verhindern. So veröffentlicht das Bundesamt für Sicherheit in der Informationstechnik regelmäßig zielgruppenspezifisch aufbereitete Warnungen zu aktuellen IT-Risiken. Mit den Grundschutzkatalogen stellt das BSI gerade auch Wirtschaftsunternehmen detaillierte Leitfäden zur Absicherung der Unternehmens-IT zur Verfügung. Und im Nationalen Cyber-Abwehr-Zentrum sitzen seit 2011 Vertreter aller mit Cybersicherheits-Fragen befassten Behörden an einem Tisch, um aktuelle Bedrohungen und Trends frühzeitig zu erfassen und zeitnah Lagebilder zu erstellen.

Internationale Maßnahmen

Auch auf europäischer und internationaler Ebene haben wir bereits viel erreicht. Dank der elektronischen Netze ist es ja selten der Fall, dass sich Täter bei der Begehung von Cyberstraftaten alleine in Deutschland „bewegen“. Vielmehr ist es eher die Regel, dass Opfer und Täter über mehrere Staaten verteilt sind. Und selbst wenn sie sich ausnahmsweise im selben Land aufhalten, liegt dafür die benutzte Technik, liegen die benutzten Server im Ausland oder laufen die virtuellen Zahlungsflüsse über die Staatengrenzen hinweg.

Es wäre nun recht illusorisch, davon auszugehen, dass die Regierungen aller Staaten in der Welt, wenn sie von Cybercrime sprechen, dieselben Delikte meinen. Umso wichtiger ist es daher, wenigstens einen Minimalkonsens zu finden, um Strafbarkeitslücken und damit „sichere Häfen“ für Cyberkriminelle in einzelnen Staaten zu vermeiden, aber auch Länder, die Propagandadelikte im Internet gerne zur Cyberstraftat erklären würden, wenigstens was die internationale Zusammenarbeit angeht, in ihre Schranken zu weisen. Denn es darf auf keinen Fall sein, dass wir beispielsweise die Anfrage einer Behörde eines weniger rechtsstaatlichen Landes zu einem regimekritischen Blogger beantworten, weil die anfragende Behörde dies als Cyberstraftat darstellt.

Auf EU-Ebene haben wir diese Probleme natürlich nicht. Hier haben wir dank der Richtlinie zu Angriffen auf Informationssysteme, deren Novelle jüngst in Kraft getreten ist und jetzt von den Mitgliedstaaten umgesetzt werden muss, einen harmonisierten Katalog von Computerstraftatbeständen einschließlich Vorgaben zum Strafrahmen. Neu ist insbesondere, dass auch die Vorbereitung von Delikten durch das Herstellen oder den Erwerb entsprechender Hacker-Tools einheitlich unter Strafe gestellt werden. Wohlgemerkt, ich erwähnte schon die Diskussion zum § 202c StGB: Es geht um das Herstellen und den Erwerb mit dem Vorsatz, diese auch für entsprechende Straftaten einsetzen zu wollen. Für wissenschaftliche Zwecke im Rahmen der IT-Sicherheitsforschung oder geschäftliche Zwecke, insbesondere zum Testen von Sicherheitsvorkehrungen, bleiben diese Tools natürlich weiterhin verkehrsfähig.

Auch Deutschland wird übrigens zur Umsetzung dieser Richtlinie tätig werden müssen, da die Strafrahmen der §§ 202a ff. StGB teilweise zu niedrig sind.

Durch den Rahmenbeschluss zum Datenschutz im Bereich Polizei und Justiz haben wir einheitliche Datenschutzmindeststandards innerhalb der EU auf rechtlicher Ebene und mit Europol haben wir eine Institution, die auf organisatorischer Ebene den notwendigen Datenaustausch vereinfacht, beschleunigt und sicherer macht. Hoffnungen setze ich vor allem in das europäische Cybercrime-Center bei Europol, das Anfang dieses Jahres in Den Haag seine Arbeit aufgenommen hat.

Dieses soll nicht nur als Drehscheibe für den polizeilichen Informationsaustausch bei schweren und staatenübergreifenden Cyber-Straftaten dienen, sondern die Mitgliedstaaten auch bei technischen und forensischen Themen unterstützten.

Die Zusammenarbeit der zuständigen Polizeien der verschiedenen Staaten auf dem Gebiet der Cyberkriminalität - ich sagte es schon - ist von entscheidender Bedeutung aber eben auch eine besondere Herausforderung. Davon zeugt neben dem Europäischen Cybercrime-Center auch dessen Pendant, das Interpol in Singapur aufbaut.

Entscheidend ist bei allem der Faktor Zeit. Denn digitale Spuren verschwinden, je älter sie sind, weil Daten gelöscht oder überschrieben werden. Insbesondere wenn es – wie auch in Deutschland – keine gesetzlichen Mindestspeicherfristen für derartige Daten gibt.

Und Cybercrime macht natürlich auch nicht an den EU-Außengrenzen halt. Für die internationale Zusammenarbeit haben sich dabei die Regelungen der staatenoffenen Cybercrime-Konvention des Europarates, der sogenannten Budapest-Konvention, als besonderes hilfreich erwiesen.

Die Budapest-Konvention enthält nicht nur einheitliche Definitionen für Cyberstraftaten, sondern auch wichtige verfahrensrechtliche Bestimmungen. Insbesondere enthält sie Vorschriften zur Vorabsicherung von Verkehrsdaten: Denn natürlich dürfen wir mit der Beauskunftung solcher Daten nicht die Regelungen der internationalen Rechtshilfe unterlaufen: Eine Beauskunftung kann erst erfolgen, wenn sichergestellt ist, dass die Daten der Verfolgung von Taten dienen, die auch nach deutschem Recht strafbar sind und der Beschuldigte ein rechtsstaatliches Verfahren erwarten kann. Bis zur Klärung dieser Frage werden die Daten nicht an die anfragende Behörde weitergeleitet, sondern zunächst durch die deutschen Behörden beim Provider gesichert, um einer Löschung aufgrund Zeitablaufs vorzubeugen.

Auf dem internationalen Parkett gab es in den letzten Jahren immer wieder Vorstöße für eine entsprechende VN-Konvention zur Cyberkriminalität. Ich meine, dies ist bedauerlich, da mit der Budapest-Konvention bereits ein etabliertes und bewährtes Instrument zur Verfügung steht. Und zwar allen Staaten der Welt, da die Konvention nicht auf Mitglieder des Europarates beschränkt ist. Dementsprechend haben bereits 51 Staaten die Konvention unterzeichnet. Und die Bundesregierung wird sich auch weiterhin dafür stark machen, weitere Staaten, die an einer Zusammenarbeit bei der Bekämpfung der Cyberkriminalität interessiert sind, von einem Beitritt zur Budapest-Konvention zu überzeugen.

Überleitung

Ist damit bereits alles getan, und können wir uns – vielleicht mit ein paar mahnenden Worten an die Staaten, die noch nicht so weit sind wie wir – zurücklehnen? Sie ahnen es, leider nein. Auch und gerade in Deutschland haben wir noch viele offene Punkte abzuarbeiten: Die zuständigen Polizeibehörden in Bund und Ländern benötigen nicht nur gute Konzepte, sondern müssen adäquat ausgestattet werden. Und der rechtliche Rahmen für die Bekämpfung der Cyberkriminalität weist nach wie vor Lücken auf – sowohl im materiellen Strafrecht als auch in den strafverfahrensrechtlichen Bestimmungen.

Dass wir die Hände nicht in den Schoß legen können, kann man schon bei einem Blick in die Polizeiliche Kriminalstatistik feststellen. Ich werde mich hier kurz fassen, weil sicher noch andere Vortragende die PKS beleuchten werden.

Bedrohungslage II

Zwar sind die Zahlen der PKS in diesem Bereich mit Vorsicht zu genießen, da wir von einem erheblichen Dunkelfeld ausgehen müssen. So fällt es dem Betroffenen oftmals gar nicht auf, dass er sich ein Schadprogramm eingefangen hat, mit dem die Täter seine Daten ausspionieren oder seinen Rechner fernsteuern. Und aus Sorge um das Vertrauen ihrer Kunden zeigen manche Banken, so vermuten wir, Phishing-Vorfälle, in denen der Täter Zugriff auf ein Bankkonto erhalten hat, nicht an, weil sie die Kosten auch übernehmen. Und die betroffenen Kunden erstatten mangels eigenen Schadens in diesen Fällen auch seltener Strafanzeige.

Aber für Trendaussagen ist die PKS gleichwohl tauglich: Sieht man sich die Entwicklung der Cyberkriminalität im engeren Sinne, also der eigentlichen Computerstraftaten an, so fällt ein Jahr sofort ins Auge: Zwischen 2010 und 2011 haben diese stagniert und sind nicht gestiegen. Dies wird von Experten in erster Linie darauf zurückgeführt, dass die Banken flächendeckend neue und sicherere Authentifizierungsmechanismen eingeführt haben, was zu einem

Rückgang bei Phishing-Fällen geführt hat. Das Erschreckende daran ist eher, dass schon 2012 der bis 2010 ungebrochene Aufwärtstrend wieder einsetzt.

Noch viel deutlicher wird die Aufgabe, vor der unsere Polizeien bei der Aufklärung von Cyberdelikten stehen, wenn wir uns die eigentlichen „Hackerparagrafen", also Datenveränderung und Computersabotage ansehen: Hier haben sich die Zahlen in den letzten fünf Jahren nahezu exponentiell entwickelt: Nach moderaten Anstiegen von 2008 bis 2010 haben sich die Zahlen von 2010 zu 2011 verdoppelt, und im letzten Jahr gab es gar einen Anstieg um 134 %.

Auch die Täterstrukturen haben sich verändert. Es agieren nicht mehr wenige hoch spezialisierte Straftäter, sondern überwiegend Kriminelle, die zumeist auf internationaler Ebene arbeitsteilig zusammenwirken. Es hat sich hier eine regelrechte Schattenwirtschaft entwickelt, innerhalb derer die zur Begehung von Straftaten erforderlichen Schadprogramme oder gar komplette kriminelle Infrastrukturen in den einschlägigen Foren zum Kauf oder zur Miete angeboten werden. Dabei sind die angebotenen Werkzeuge aufgrund ihrer relativ einfachen Handhabung auch für Täter ohne fundierte IT-Spezialkenntnisse nutzbar.

Ein Massengeschäft ist mittlerweile die sogenannte Ransomware: Diese Programme – in einer Variante auch als sogenannter BKA-Trojaner im Umlauf – verschlüsseln die Festplatte des Opfers und geben die Daten erst gegen Zahlung eines entsprechenden Geldbetrags frei. Die Geldbeträge sind dabei eher gering – bis zu 100 € –, hier bringt allerdings die schiere Masse den kriminellen Profit.

Auf dem Internet-Schwarzmarkt im sogenannten Dark-Net, einem verborgenen Teil des Internets, der nicht bei einer Google-Suche auftaucht, kann man mittlerweile alles erwerben, was für die Begehung von Cyber-Straftaten – und nicht nur diesen – erforderlich ist:

Dies beginnt mit Zero-Day-Exploits, die Sicherheitslücken in beliebten Programmen ausnutzen, für die es noch keine Sicherheitsupdates gibt.

Was das Schadprogramm dann auf dem Rechner des Opfers anstellen soll – Bankdaten und Passwörter abgreifen, Daten zerstören oder unbrauchbar machen, oder diesen einfach zur Verbreitung von weiteren Schadprogrammen oder Spam-Mails fernsteuern, kann mittels einfach zu bedienender Software-Baukästen bequem konfiguriert werden.

Darüber hinaus kann man Bot-Netze, also unzählige gekaperte und fernsteuerbare Rechner, anmieten, um mit diesen andere Rechner anzugreifen oder einfach nur massenhaft Werbemails zu versenden oder Werbeklicks und damit deren Abrechnung zu manipulieren.

Online-Identitäten, insbesondere massenhaft gestohlene Kundendaten, Zugangsdaten zu Online-Diensten oder auch Kreditkartendaten, können en gros erworben werden – in 1000er-Paketen einschließlich Garantie, dass die Kreditkarten noch nicht gesperrt sind.

Natürlich kann man auch sonstige illegale Güter auf diesen anonymen Schwarzmärkten erwerben, ob Waffen oder verschreibungspflichtige Arzneimittel. Einer der umsatzstärksten Marktplätze der letzten Jahre mit dem passenden Namen Silkroad, Seidenstraße, diente vor allem als Umschlagplatz für Drogen. Durch das so genannte Tor-Netzwerk können die Benutzer dieser Handelsplattform ihre IP-Adressen und damit ihre Identität verschleiern. Derart geschützt, konnten Dealer und Kunden ihre Geschäfte anbahnen und die Bezahlung

abwickeln – Schätzungen gehen von 7-stelligen Dollar-Umsätzen im Monat aus, bis Anfang diesen Jahres der Betreiber verhaftet und der Marktplatz vom Netz genommen werden konnte.

Dieses Beispiel ist natürlich keine Ausprägung der Cyberkriminalität im engeren Sinne mehr, zumal die Ware weiterhin auf mehr oder weniger traditionellen Wegen geschmuggelt werden muss. Aber das Beispiel zeigt, wie sich die organisierte Kriminalität der Vorteile des Internet bedient und so viele Handlungen wie möglich anonym und online abwickelt.

Besonders deutlich wird dies, wenn wir uns den Bereich ansehen, um den es allen Tätergruppierungen am Ende geht: den Geldfluss.
Da eine normale Banküberweisung, nicht zuletzt dank der international koordinierten Bemühungen zur Bekämpfung der Geldwäsche, durch die Strafverfolgungsbehörden noch vergleichsweise einfach nachzuvollziehen ist, mussten sich die Täter frühzeitig nach Alternativen umsehen. Den Anfang machten anonyme Bargeldsendungen zum Beispiel über Western Union – und zu den Zeiten der heute beinahe naiv wirkenden Nigeria-Connection mit ihren miserabel übersetzen Betrugs-Emails noch eine der bevorzugten Methoden.

Ganz andere Dimensionen eröffnen sich bereits, wenn man sich die Schließung der „Liberty Reserve“ Bank in diesem Jahr ansieht. Dieses Unternehmen – mit einer offiziellen Banklizenz Costa Ricas ausgestattet – hatte ein kompliziertes System eigener Umrechnungseinheiten, den sog. „Liberty-Dollars“, und virtueller Wechselstuben aufgebaut, das letztlich offenbar nur einen Zweck verfolgte: Nämlich Geldwäsche und die Anonymisierung von Zahlungsströmen in großem Stil zu ermöglichen.

Die eigentliche Währung der Unterwelt scheint in diesem Bereich heutzutage aber Bitcoin zu heißen. Ganz egal, wie man zu der Idee dieses „virtuellen Bargeldes“, das durch komplizierte mathematische Methoden berechnet und gehandelt wird, steht: An ihr zeigt sich auch besonders deutlich die Entwicklung der organisierten Cyberkriminalität. Und zwar in beinahe jeglicher Form.

So ist die Berechnung von Bitcoins – das sogenannte Bitcoin-Mining – grundsätzlich so ausgestaltet, dass durch die enorme hierfür erforderliche Rechenkapazität das Tempo des Anwachsens der Geldmenge begrenzt und das virtuelle „Gelddrucken“ nicht wirklich zum Geldverdienen genutzt werden kann.

Doch ein Botnetz namens „ZeroAccess“ hat gezeigt, wie man auch Bitcoin-Mining lukrativ betreiben kann: Indem man gekaperte fremde Rechner für sich rechnen lässt – im Falle von „ZeroAccess“ nach den Angaben von IT-Sicherheitsunternehmen etwa 1,9 Millionen. Zwar werden die Opfer hiervon kaum etwas gemerkt haben – aber insgesamt summierten sich die reinen Energiekosten des Netzwerkes auf über 500.000 $ - pro Tag.

Und wo es virtuelles Bargeld und virtuelle Banken gibt, da braucht man leider auch nicht lange auf virtuelle Taschendiebe und Bankräuber warten. Längst haben es Trojaner neben den herkömmlichen Bankdaten auch auf die auf den Rechnern gespeicherten Bitcoin-Bestände abgesehen. Und da Bitcoins ja als virtuelles Bargeld ausgestaltet sind und Transaktionen dementsprechend anonym und nicht mehr rückgängig zu machen sind, hat das Opfer keine Chance, seine Bitcoins wiederzufinden. Auch die größte Handelsbörse für Bitcoins ist immer wieder Ziel von Hackerangriffen. 2011 waren diese auch erfolgreich. Zwar hüllt sich das Unternehmen in Schweigen, wie viele Bitcoins damals tatsächlich gestohlen wurden. Aber offenbar genügte alleine die Meldung, um den Kurs der Pseudowährung kurzzeitig abstürzen zu lassen.

Vor allem aber erfreuen sich Bitcoins mittlerweile sehr großer Akzeptanz – bei allen erdenklichen illegalen Geschäften. Vom Ransomware-Erpresser über den Handel mit Sicherheitslücken und Schadprogrammen bis hin zum Drogenhandel ist Bitcoin als Währung der Unterwelt auf dem Siegeszug. Und auch wenn die sogenannten „Berufskiller“, die gegen Bitcoins ihre Dienste anbieten, hoffentlich „nur“ Betrüger sind, die es auf eine großzügige Anzahlung abgesehen haben, bieten Bitcoins der organisierten Kriminalität eigentlich nur einen Nachteil: Wenn man sich in der realen Welt etwas von seinem Reichtum kaufen will, muss man die Bitcoins wieder in echtes Geld tauschen. Und hier greifen hoffentlich wieder die Meldepflichten nach dem Geldwäschegesetz,

Diese Beispiele zeigen, dass wir es längst mit Strukturen zu tun haben, die wir auch aus der sonstigen Organisierten Kriminalität kennen: Einzelne Gruppierungen spezialisieren sich jeweils auf „ihren“ Geschäftszweig. Die einen stellen – gegen Geld – die Technik zur Verfügung, die nächsten stehlen mit dieser Hilfe Daten und verkaufen sie weiter, und eine weitere Gruppierung in dieser kriminellen Wertschöpfungskette widmet sich der Aufgabe, die Daten zu Geld zu machen, einschließlich der Geldwäsche.

Dabei gehen die Täter äußerst konspirativ vor. Das Tor-Netzwerk als eine Möglichkeit, seine Spuren im Internet zu verwischen, hatte ich schon erwähnt: Im sogenannten Dark-Net bewegen sich nur Pseudonyme, IP-Adressen führen ins Nichts, Emails werden verschlüsselt. Es gibt Anbieter von Servern, die man mieten kann und die damit Werbung machen, dass sie den Standort ihrer Rechenzentren nicht offenbaren und auf Anfragen von Sicherheitsbehörden nicht reagieren. Und natürlich nutzen die Täter die Tatsache, dass sie dank Internet grenzüberschreitend agieren können.

Selbst die US-Behörden, die – wenn man heutzutage manche Veröffentlichungen liest – angeblich alles aus dem Internet überwachen und speichern können, haben mehrere Jahre benötigt und einen erheblichen Aufwand – einschließlich des Einsatzes verdeckter Ermittler, also Menschen – um den Betreiber der SilkRoad Plattform zu überführen.

Denn die Technik, die hier zum Einsatz kommt, ist mittlerweile so gut, dass die Strafverfolgungsbehörden quasi kaum mehr eine Chance haben, über diesen Weg an die Identität der Täter zu gelangen. Glücklicherweise eint aber auch Cyberkriminelle eine wesentliche Eigenschaft mit gewöhnlichen Straftätern: Aus Eitelkeit und Selbstüberschätzung machen sie Fehler. Und über diese kann man ihnen dann letztlich doch auf die Schliche kommen. Das geht aber eben nicht auf Knopfdruck, sondern erfordert klassische und mühselige Ermittlungsarbeit durch die zuständigen Polizeibeamten. Und diesen müssen auch die notwendigen rechtlichen Ermittlungswerkzeuge zur Verfügung stehen.

Noch ausstehende Maßnahmen / Herausforderungen

Hier besteht aus meiner Sicht dringender Handlungsbedarf!

So kann man diejenigen, die auf den Internet-Schwarzmärkten mit gestohlenen Kreditkartendaten oder ähnlichem handeln, für den Handel selbst strafrechtlich nur schwer belangen, wenn man ihnen nicht nachweisen kann, die Daten selbst gestohlen zu haben. Denn während ein Hehler genauso bestraft wird wie der Dieb, gibt es bislang keine Strafvorschrift für Datenhehlerei. Denkbar wären allenfalls Beihilfehandlungen oder eine Anwendung der nebenstrafrechtlichen Vorschrift des § 44 des Bundesdatenschutzgesetzes. Bei letzterer standen dem Gesetzgeber aber eher Fälle des illegalen Adresshandels vor Augen, was sich auch im Strafrahmen – Geldstrafe oder Freiheitsstrafe bis zu zwei Jahren – niederschlägt. Das

wird der Strafwürdigkeit des organisierten Handels mit Kreditkarten- und Bankzugangsdaten kaum gerecht. Der Bundesrat hatte in der vergangenen Legislaturperiode bereits eine entsprechende Gesetzgebungsinitiative gestartet. Zwar ist diese der Diskontinuität zum Opfer gefallen. Aber wir sollten, wie ich meine, diesen Ansatz schnell wieder aufgreifen.

Ähnliches gilt für das Gros der eigentlichen Computerdelikte. Auch hier hat der Gesetzgeber eher an Hacker gedacht, die ihre Fähigkeiten unter Beweis stellen wollen, als die Nutzung dieser Techniken im Rahmen mafiöser Strukturen. Dementsprechend fehlen den meisten Delikten Qualifizierungstatbestände für gewerbliche oder bandenmäßige Begehungsformen, wie wir sie bei Eigentumsdelikten kennen. Dabei könnten diese Qualifikationstatbestände durch einen entsprechend erhöhten Strafrahmen den höheren Unwertgehalt dieser Form der organisierten Kriminalität berücksichtigen.

Diese Schieflage spiegelt sich auch in den entsprechenden strafprozessualen Befugnissen wieder. Aufgrund des äußerst konspirativen Verhaltens der Täter und insbesondere der Vernetzung und Arbeitsteilung lassen sich diese selten auf frischer Tat ertappen und einfach überführen. Wie auch bei anderen Formen der organisierten Kriminalität lassen sich die Strukturen der Tätergruppierungen oftmals nur durch eine Überwachung ihrer Kommunikation – entweder klassisch beim Provider oder, insbesondere beim Einsatz von Verschlüsselungstechniken, unmittelbar an der Quelle, also auf dem Endgerät, aufklären.

Bislang ist allerdings nur der Computerbetrug eine Katalogtat nach § 100a StPO, die eine Überwachung der Telekommunikation gestatten würde. Die übrigen Computerstraftaten, also das Ausspähen und Abfangen von Daten, Computersabotage und Datenveränderung, sind nicht im Katalog des § 100a StPO enthalten – und dürften es im Zweifel auch gar nicht, da sie angesichts der geringen Strafandrohung teilweise gar nicht mehr als schwere Straftat im Sinne des § 100a StPO zählen. Gegen den „Hobbyhacker“, der als Einzelkämpfer im Zweifel nur sein Können und die ungenügenden Sicherheitsmaßnahmen großer Unternehmen unter Beweis stellen will, müssen wir nicht die schwersten Geschütze der Strafprozessordnung auffahren.

Aber wenn Straftaten im Rahmen organisierter Strukturen im großen Stil begangen werden, dann müssen wir die Strafverfolgungsbehörden in die Lage versetzen, jedenfalls bei Verwirklichung der Qualifikationstatbestände, auch den konspirativ agierenden Profis auf die Schliche zu kommen.

Das gilt übrigens nicht nur für die Telekommunikationsüberwachung. Auch verschlüsselte Festplatten stellen Ermittler vor immer neue Probleme. Zwar können sie im Rahmen einer Wohnungsdurchsuchung auf den Überraschungseffekt setzen und hoffen, dass der Verdächtige seinen Rechner nicht schnell genug ausschalten oder sperren kann. Erfolgversprechender wäre es aber sicherlich, im Rahmen einer Online-Durchsuchung auf dem Rechner nach Hinweisen zu suchen, wenn dieser in Betrieb und damit unverschlüsselt ist. Befugnisse zur Online-Durchsuchung finden sich bislang nur in einigen Polizeigesetzen – unter anderem dem BKA-Gesetz – für Zwecke der Gefahrenabwehr. Als Ultima Ratio sollte dieses Instrument auch in die Strafprozessordnung Eingang finden.

Vorratsdatenspeicherung

Wie Sie wissen, läuft derzeit ein Vertragsverletzungsverfahren gegen Deutschland wegen Nichtumsetzung der Richtlinie zur sogenannten Vorratsdatenspeicherung. Diese Richtlinie verpflichtet die Mitgliedstaaten, Mindestspeicherfristen für Verkehrsdaten, also Daten, wer mit wem wann telefoniert, gemailt oder gechattet hat, zwischen 6 Monaten und 2 Jahren vorzusehen. Denn der wichtige Zugriff auf Daten, ob zur Bekämpfung von Cybercrime oder anderer schwerer Straftaten, geht letztlich ins Leere, wenn die Unternehmen der Telekommunikationsbranche diese zum Zeitpunkt der Anfrage der Behörde bereits gelöscht haben.

Das Bundesverfassungsgericht hatte 2010 die deutschen Vorschriften zur Umsetzung der Richtlinie zur Vorratsspeicherung für nichtig erklärt. Es hat aber zugleich klargestellt, dass Mindestspeicherfristen für Verkehrsdaten per se nicht gegen die Grundrechte verstoßen und aufgezeigt, wie eine verfassungskonforme Umsetzung der Richtlinie aussehen könnte.

Damit haben wir in Deutschland eine klare Rechtslage, dass und unter welchen Bedingungen gesetzliche Mindestspeicherfristen eingeführt werden können. Und müssen dem nachkommen. Und zwar ganz unabhängig vom möglichen Ausgang des Vertragsverletzungsverfahrens. Selbst wenn die EU-Richtlinie morgen aufgehoben würde, müssen wir in Deutschland handeln. Denn für die Verfolgung und Verhütung schwerster Straftaten sind Mindestspeicherfristen ebenso unabdingbar wie für die Aufklärung von Cyber-Straftaten.

Nun sind Mindestspeicherfristen für Verkehrsdaten in erster Linie ein Instrument, um durch die retrograde Abfrage von Kommunikationsverbindungen schwere und schwerste Straftaten aufzuklären. Finden die Ermittler am Tatort ein Mordopfer vor, geben die Verbindungsdaten wertvolle Aufschlüsse über seine Kontakte in den letzten Monaten und dadurch vielleicht erste Anknüpfungspunkte, um einen möglichen Täter zu identifizieren. Dabei sind Verkehrsdaten für sich genommen keine Beweise, auf die alleine später eine Verurteilung gestützt werden könnte. Aber ohne diese Daten wüssten die Ermittler erst gar nicht, wo sie nach weiteren Indizien oder Beweisen suchen müssten.

Daneben spielen Verkehrsdaten aber auch eine gewichtige Rolle bei der Aufklärung von Cyber-Straftaten. Denn wenn man vom Verdächtigen nur ein Pseudonym oder eine anonyme Email-Adresse oder IP-Adresse kennt, ist man auf die Mithilfe der Provider angewiesen, um diese einem Kundenkonto zuordnen zu können. Die Befugnisse hierfür, die Bestandsdatenauskunft hatte ich ja bereits erwähnt, stehen den zuständigen Behörden zur Verfügung. Aber sie nützen nichts, wenn die Provider die hierfür erforderlichen Verkehrsdaten bereits gelöscht haben. Daher sind gerade hier Mindestspeicherfristen so wichtig – wobei der mit der Auskunft verbundene Grundrechtseingriff gleichzeitig geringeres Gewicht hat, wie das Bundesverfassungsgericht festgestellt hat. Deshalb ist eine solche Bestandsdatenauskunft auch für weniger schwere Straftaten verfassungsrechtlich unproblematisch.

Dabei müssen wir übrigens gewahr sein, dass alleine die IP-Adressen zur Identifizierung eines Anschlusses mittlerweile gar nicht mehr genügen, da auch diese teilweise mehrfach vergeben werden. Leider beschränkt sich die Speicherpflicht nach der Richtlinie bislang auf die IP-Adresse. Im Zuge der Wiedereinführung müsste man prüfen, ob hier nicht eine technikoffenere Regelung notwendig ist.

Schluss

Wie Sie wissen, laufen in Berlin derzeit Koalitionsverhandlungen für die Bildung der nächsten Bundesregierung. Aus diesem Grunde darf ich auch an dieser Stelle Bundesinnenminister Dr. Friedrich entschuldigen, der gerne hier persönlich bei der BKA-Herbsttagung gewesen wäre, aber deshalb nicht hier sein kann.

Sie werden mir sicherlich beipflichten, dass die von mir vorgestellten Maßnahmen, die wir zur Bekämpfung der Cyberkriminalität benötigen, ambitioniert, aber gleichwohl unumgänglich sind.

Ich möchte daher meine Einführung mit dem Appell und Wunsch beenden, dass auch dem wichtigen Thema der Bekämpfung von Cybercrime der notwendige Raum in der zukünftigen Koalition gewährt wird und dass wir die erforderlichen Schritte in der jetzt beginnenden Legislaturperiode zügig und bestimmt angehen.

Herzlichen Dank.

Festvortrag:
Freiheit und Grenzen der digitalen Gesellschaft

Prof. Dr. Dr.
Udo Di Fabio

Ist das Grundrecht ein Ladenhüter?

Wirtschaftliche Interessen haben sich mit solcher Macht ins Netz verlagert, dass Privatheit nicht mehr zu garantieren ist. Man kann nur auf die Klugheit der Nutzer setzen.

Der Deutsche Bundestag untersuchte vor kurzem mit einer Enquete das Internet und die digitale Gesellschaft. Im Einsetzungsbeschluss von 2010 war zu lesen gewesen, das Internet sei „das freiheitlichste und effizienteste Informations- und Kommunikationsforum der Welt“ und trage „maßgeblich zur Entwicklung einer globalen Gemeinschaft bei“. Das Internet entwickele sich „zu einem integralen Bestandteil des Lebens vieler Menschen“, gesellschaftliche Veränderungen fänden „maßgeblich im und mit dem Internet statt“.

In der Tat kann von einer digitalen Gesellschaft gesprochen werden, wenn für immer mehr Menschen die digitalisierte und vernetzte Kommunikation sich als eine maßgebliche oder sogar primäre Erlebniswelt entwickelt. Die im Wettbewerb stehenden, durch Verhaltenstrends sich verändernden Netzwerke wie Facebook oder das des WhatsApp-Messengers erzeugen digitale Dauerpräsenz. Die Teilnehmer offenbaren und koordinieren Alltagshandeln, kommunizieren Örtlichkeit, Bewegungsprofile, persönliche Vorlieben und Konsumgewohnheiten, Ansichten und private Schrullen. Die spontan entstehenden Gemeinden, jene Netze im Netz, sind sowohl privat, weil personell begrenzt, aber auch öffentlich. Die Grenzen zwischen Privatheit und öffentlichem Raum verwischen, wenn ein halböffentlicher Raum mit Laufkundschaft so betrachtet wird, als säße man mit engen Freunden zusammen. Jedenfalls wird traditionelles Sozialverhalten, wie die Weitergabe von Informationen, Meinungskundgaben, Weltdeutungen, Normierungen des Alltagshandeln, Moden und Moral, stark ins Netz verlagert: Das, was einstmals schon wegen der Bedingungen einer Face-to-Face-Interaktion als privat galt, wird enträumlicht, simultan zugänglich, speicherbar und verwertbar gemacht. Es findet eine Vergemeinschaftung mit viel Unverbindlichkeit, mit belanglos scheinender Intimität statt, es wächst eine ebenso

kommunikative wie konsumtive Grundstruktur, die eigentlich auf naivem Technikglauben basiert, aber deren Nutzer auch sehr empfindlich auf Enttäuschungen des Vertrauens reagieren können.

Die Lage spitzt sich zu

Wo so viel soziale Interaktion ins Netz wandert, verlagert sich auch die Welt der Wirtschaft. Die Betreiber der Netzwerke werden milliardenschwer an der Börse gehandelt. Die alten Printmedien müssen im Netz mitspielen oder sich auf eine schrumpfende Nische einrichten. Mit Formaten wie „Facebook Deals“ können auch kommerzielle Freunde am Tisch oder hinter der Kulisse Platz nehmen, Freunde, die großzügig Sonderangebote und Gutscheine offerieren, dabei die Umsonst-Mentalität des Netzes noch mit Geschenken über sich hinaustreiben. Was war da noch mit dem Recht auf informationelle Selbstbestimmung, also dem Recht des Einzelnen, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen? War das nicht die grundrechtliche Fortentwicklung des allgemeinen Persönlichkeitsrechts aus der arg verblassten Zeit der Volkszählung? Was waren das noch für geradezu idyllische Gefahrenlagen! Damals wurde das Bundesverfassungsgericht für seine Innovation und Weitsicht gelobt. Aber ist nicht auch diese Neuheit im Grundrechtekatalog inzwischen ein Ladenhüter der achtziger Jahre, aus der Zeit des Commodore C 64 stammend, von der technischen und gesellschaftlichen Entwicklung geradezu überrollt?

Die Server stehen in den Vereinigten Staaten

Bei Facebook jedenfalls laufen gewaltige Datenmengen zur Zentrale von Facebook Incorporated. Der Datenaustausch der Mitglieder insgesamt wird in zwei riesigen Rechenzentren in den Vereinigten Staaten bereitgestellt. Mit Hilfe des WhatsApp-Messengers werden mehr als siebzehn Milliarden Nachrichten an einem Tag verschickt, Tendenz gerade steigend. Alle Informationen gehen auch hier an einen amerikanischen Server. Auch für das von Google, Microsoft oder Amazon bevorzugte Cloud-Computing sollen neunzig Prozent der Infrastruktur in Amerika befindlich sein und somit dem fortgeltenden Patriot Act unterliegen, der eine recht deutliche Grundrechtsverdünnung für informationelle Eingriffe der amerikanischen Bundesbehörden vorsieht. Die Snowden-Enthüllung hat vielleicht sogar nur einen über der Wasseroberfläche liegenden Teil des Eisbergs auf unseren Flachbildschirm gerückt. Auch wer den Wert der Vereinigten Staaten als Garantiemacht westlicher Werte zu keinem Zeitpunkt wird unterschätzen wollen, kommt nicht umhin, den amerikanischen Rigorismus der nationalen Interessenverfolgung auf wirtschaftlichem und technologischem Gebiet zur Kenntnis zu nehmen. Und hier ist die Infrastruktur des real existierenden Internets ein gewaltiger Hebel, um auch in einem System des Wettbewerbs freier Märkte und kooperierender Staaten sich Vorteile zu verschaffen, die sanft wirken, aber für die anderen unausweichlich sind.

Europa muss ein Gegengewicht schaffen

Man sieht ein weiteres Mal, dass die Vorstellung des Bundesverfassungsgerichts, die Idee der Grundrechte als Selbstbestimmungsrecht der Bürger den technischen und internationalen Entwicklungen folgen zu lassen, keine willkürliche Entgrenzung des Gerichts, also keine Kompetenzanmaßung der Richterinnen und Richter in Karlsruhe, bedeutet. Es waren vielmehr die Demokratien und die Bürger selbst, die die Verhältnisse entgrenzt haben; deshalb droht der Grundrechtsschutz seine praktische Wirksamkeit zu verlieren. In dieser Lage weisen

manche auf staatliche Schutzpflichten hin: Wenn die Verhältnisse sich so ändern, dass wir nicht mehr über unsere Daten praktisch verfügen können, sondern eine scheinbar unkontrollierbare Welt sich entwickelt, dann seien doch wohl die Staaten dazu verpflichtet, eine rechtsstaatliche, freiheitliche Ordnung auch im Internet zu garantieren. Und haben die Staaten Europas sich in der Europäischen Union nicht auch deshalb zusammengefunden, um als größter Binnenmarkt der Welt ein Wort im Rahmen der Global Governance mitzureden? Brauchen wir ein europäisches Airbus-Projekt der digitalen Gesellschaft, also so etwas wie ein EU-Google, damit die transatlantische Partnerschaft eine auf Augenhöhe ist? Solche Gegenmachtsstrategien sind, wenn sie nicht dezentral aus Universitäten und Unternehmen heraus entstehen, als herbeiregulierte politische Projekte überwiegend illusionär. Das Netz ist dezidiert regelungsablehnend. Seine scheinbar anarchische Ordnung lässt eigentlich nur persuasive, anbietende und lockende Techniken zu. Die Abschöpfung und der Zutritt zu den großen privaten Internetakteuren erfolgen nicht selten heimlich; der Druck mancher Regierungen, wie die Amerikas, manchmal auch Chinas, verformt die Netzfreiheit auf wenig transparente Weise. Hier reicht der lange Arm der Netzöffentlichkeit nicht hin, sie ist eben nur digital und informationsbasiert.

Interessen im Widerstreit

Das ist in einer digital vernetzten Gesellschaft viel, aber es umfasst nicht die politische Regelungsmacht und erreicht nicht die Unternehmen, die mit Plattformen und Infrastrukturen das Terrain bereiten. Die Ablehnung einer rechtlich austarierten Ordnung, die auch im Netz gilt, ist seit dem Scheitern von Acta machtpolitisch manifest geworden. Als es mit Acta, einem internationalen Abkommen zum Urheberrechtsschutz, um einen rechtsstaatlichen Einstieg in die Netzwelt ging, haben Internetaktivisten und im Hintergrund wohl auch kommerzielle Interessen dies wirkungsvoll zu Fall gebracht und die Demokratien in Europa mit aus dem Boden schießenden Piratenparteien geradezu in Schrecken versetzt. Wenn das Netz immer mehr zu einer maßgeblich bestimmenden sozialen Lebenswelt mit allen Chancen und Risiken für individuelle Rechtsgüter wird, so steht der Rechtsstaat vor einer unangenehmen Wahl: Muss er einen unregulierten Raum dulden und ihn nehmen, wie er ist? Muss er sich darauf beschränken, mit angepassten Techniken Anonymitätsbarrieren aufzubrechen, wenn es beispielsweise um organisierte Kriminalität geht? Müssen Politiker in Europa darauf warten, was amerikanischen Behörden im Zusammenwirken mit Internetunternehmen auf ihrem Territorium einfällt, oder sollen sie heimlich um der Sicherheit der Bürger willen mit Geheimdiensten kooperieren, wenn anderswo ausgespäht, angezapft wird? Vieles läuft auf eine gegenseitige Rationalitätsblockade hinaus; es bestehen unterschiedlich verkantete Interessen, die im internationalen und digitalen Raum an keinem - und sei es einem virtuellen - Tisch befriedigend ausgeglichen werden können. Demokratische Staaten müssen aufpassen, mit wem sie sich etwa auf der wichtigen Bühne der Vereinten Nationen verbünden.

Wenn Staaten untätig sind, ist der Nutzer gefragt

Auf der Welttelekommunikationskonferenz in Dubai Ende 2012 sollte das Regelwerk der Internationale Fernmeldeunion (ITU) aktualisiert werden. Die besprochenen Neuerungen wurden jedoch insbesondere von westlichen Ländern als Angriff auf das bisherige nichtstaatliche System der Internetregulierung verstanden. Eine stärkere UN-Verantwortung für das Internet könne leicht staatliche Kontrollversuche verstärken, die Entwicklung des Netzes verlangsamen und die Informationsfreiheit gefährden. Als Risiko für die freie Meinungsäußerung etwa wurde die Möglichkeit für Regierungen bewertet, den Nutzern aus

einer Reihe von vage formulierten Gründen den Zugang zum Internet zu entziehen. Im Ergebnis lehnten Deutschland, England, die Vereinigten Staaten und eine Reihe anderer westlicher Länder die Zustimmung ab, wobei der Generalsekretär des ITU das Regelwerk dennoch für verabschiedet erklärte. Hier zeigen sich Spannungen im Staatenensemble, aber auch der Bedarf nach einer Zusammenarbeit von Menschen, denen die Freiheit des Netzes wichtig ist und die genauer als bisher unterscheiden sollten, was ein Rechtsstaat mit seinem Regelungsanspruch ist und was mit ihm gemeinsam als autokratischer Anschlag auf die Netzfreiheit bekämpft werden sollte.

Angesichts der faktischen Regulierungsblockade darf man sich am ehesten etwas von Verhaltensänderungen der Nutzer selbst versprechen. Elternhäuser und Schulen sollen wieder einmal auf bewussten und vorsichtigen Umgang mit Diensten und persönlichen Daten hinwirken: Imperativ der Netzerziehung. In einer Gesellschaft, die auf Freiheit und persönliche Selbstbestimmung setzt, ist ein solches Vorgehen immer richtig, aber nicht immer ausreichend. Wenn Handlungszusammenhänge allzu komplex und allzu dynamisch sind, gaukelt vielleicht sogar der stete Hinweis auf den Erwerb von Netzkompetenz ein Niveau der Sicherheit und der Bewahrung informationeller Selbstbestimmung vor, das so, trotz überlegten Handelns Einzelner, gar nicht besteht. Die Netzwelt fördert die Transparenz der Gesellschaft, sie ist aber möglicherweise selbst schon durch ihr Veränderungstempo und ihre Systembedingungen intransparent, in hohem Maße ebenso zufallsgesteuert wie technik-, interessen- und expertenabhängig.

Den Zugriff der Staatsorgane gilt es einzugrenzen

Wie jeder Raum, in dem Freiheit sich entfaltet, muss auch das Internet selbst vor seiner Deformation geschützt werden. Identitätsdiebstahl, bekannt als Phishing, Computerangriffe, Schadsoftware dürfen nicht nur als technisches Problem privater Sicherheitsprogramme und unternehmerischer Selbstschutzmaßnahmen gesehen werden. Sonst könnte allmählich der Rechtsstaat als partiell verzichtbar oder doch als ohne Funktion erscheinen. Wer angesichts der Schnelllebigkeit von Datenflüssen die Begehung einer Straftat mit Netzhintergrund aufklären will, der muss Datenströme, Verbindungsdaten, vielleicht auch Inhalte konservieren, der ruft nach Vorratsdatenspeicherung. Das Bundesverfassungsgericht sieht in der Speicherung von Verbindungsdaten und im staatlichen Zugriff auf Telekommunikationsunternehmen durch Auskunftsverfahren jedenfalls einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Die mit der NSA-Affäre virulent gewordene Zusammenarbeit von Nachrichtendiensten und Polizei im Rahmen von Rechtshilfe hat das Bundesverfassungsgericht vor kurzem in seiner Entscheidung zur Antiterrordatei behandelt.

Die Zusammenführung von Daten der Nachrichtendienste und der Polizeibehörden erhöhe das Eingriffsgewicht und unterliege verfassungsrechtlich engen Grenzen. Denn Polizeibehörden und Nachrichtendienste hätten verschiedene Aufgaben. Dementsprechend unterlägen sie hinsichtlich der Offenheit ihrer Aufgabenwahrnehmung sowie der Datenerhebung verschiedenen Anforderungen. Die politische Vorfeldaufklärung der Nachrichtendienste sei in der Informationssammlung vergleichsweise breit möglich, weil sie vom polizeilichen Eingriffsinstrumentarium eben getrennt sei. Wer keine Macht gegen die Freiheit des Bürgers hat, darf mehr Informationen sammeln als die Behörde mit dem scharfen Schwert. Insofern ist aber jeder Informationsaustausch auch im Rahmen der Rechtshilfe ein Problem. Denn wenn Nachrichtendienste umfänglich Informationen an Polizei und Staatsanwaltschaft übermitteln, unterspült das die Dämme der Trennung.

Die Utopie einer freien Netzwelt

Vor diesem Hintergrund sollte man sich fragen, wie das polizeipraktisch gut nachvollziehbare Petitum der stärkeren internationalen Zusammenarbeit in rechtsstaatlich und demokratisch unbedenklicher Weise verwirklicht werden kann. Die Frage wird umso dringlicher, wenn man weiß, dass Trennungsgebote wie die zwischen Geheimdienst und Polizei, die in Ländern wie Deutschland geschichtlich gut begründet sind, in anderen Staaten, auch in Demokratien, nicht ganz so streng bestehen und man häufig gar nicht genau weiß, auf welchem Weg die international zirkulierenden Informationen erlangt worden sind. Schaut man nur auf den Problembereich der Internetkriminalität, so wird auch hier und exemplarisch das Spannungsfeld des Themas „Freiheit in der digitalen Gesellschaft“ deutlich. Die Bürger als Nutzer und Akteure im Netz vertrauen auf Sicherheit und Neutralität, hoffen durchaus und nicht ganz ohne Grund auf die spontane Ordnung eines selbstregulativen Prozesses, verstehen sich dabei als eigentliche Zivilordnung, frei von staatlicher Macht. Diese liberale Grundstimmung des Netzes sollte nicht als Naivität abgetan werden; sie ist eine optimistische Kraft, die gerade den Charme dieser dezentralisierten und grenzüberschreitenden Kommunikations- und Interaktionstechnik ausmacht.

Gemeinsam handeln

Aber je bedeutsamer das Netz wird, desto mehr dringen wirtschaftliche Interessen, politische Macht und Kriminalität in diese Welt. Das Netz wird seine eigene Ordnung bei allem selbstregulativen Optimismus nicht garantieren können. Netzregulierung durch die internationale Politik hängt - wenn das Netz solch regulative Anstrengungen überhaupt zulassen wird - nicht nur vom Willen zur Verständigung ab. Die Interessen der Staaten sind so heterogen, dass die Volonté Générale der digitalen Gesellschaft als nicht formulierbar erscheint. Abstimmungen im Internet selbst bringen wenig, sie können Trends markieren und Hinweise geben, aber sie können keine demokratische Legitimität spenden. Eigenwilligkeit der Nutzer und das Bewusstsein von dem, was sie im Netz tun und bewirken, wären auf Dauer die eigentliche positive Prägekraft; aber sie allein bringt vermutlich keine freiheitliche und Sicherheit gewährende Ordnung hervor. Die neue strukturelle Schwäche des Westens seit der Weltfinanzkrise macht es auch nicht wahrscheinlicher, dass ein Standard für den Persönlichkeitsschutz und den sonstigen Rechtsgüterschutz sich ohne Freiheitsverluste wird durchsetzen lassen. Aber die Unionsbürger sollten als Teil des Westens in den Unternehmen, den Universitäten und der Gesellschaft intensiver darüber nachdenken, wie man das Persönlichkeits- und das Selbstbestimmungsrecht im Netz wahren und stärken kann, ohne die Bürokratie einschleusen zu wollen. Europa muss sich allmählich aus dem sanften Protektorat Amerikas herausentwickeln und mit Phantasie eigene Wege der Technik und Kommunikation erproben. Dabei geht es nicht um Antiamerikanismus, sondern um das Selbstbewusstsein einer im Innern plural organisierten und im Verhältnis zu den Vereinigten Staaten komplementären Macht, die das transatlantische gemeinsame Wertefundament nicht aus den Augen verliert.

Cyberterrorismus, Cyberspionage und Cyberwar - eine aktuelle Bedrohungseinschätzung aus Sicht der Wissenschaft

Abschrift des gesprochenen Wortes

Dr. Sandro Gaycken

Hallo meine Damen und Herren,

ich freue mich sehr, hier heute eingeladen zu sein. Meine Vorträge weichen dabei in der Regel etwas von anderen Cyber-Beiträgen ab, denn, wie schon erwähnt wurde – mein Forschungsbereich sind eher die etwas stärkeren Akteure. Die meisten Kollegen beschäftigen sich dagegen eher mit konventionellem Cybercrime, dem empirischen Bodensatz der Cyberdiskussionen – zumindest vor Snowden. Das geht eher in Richtung Taschendiebe und Kleinkriminalität. Ich dagegen beschäftige mich mehr mit großen Jungs, den Nachrichtendiensten, den Militärs, ein wenig auch mit organisierter Kriminalität wie etwa bei Wirtschaftsspionage, viel auch direkt sicherheitspolitisch mit anderen Staaten wie Amerika, Russland, China oder dem Mittleren Osten. Aus diesem Feld werde ich Ihnen heute ein wenig berichten und das Spektrum ein bisschen spannen – Cyberterror, Cyberspionage, Cyber Warfare.

Wir fangen an mit Cyberterror. Cyberterror wurde in der Forschung lange für suspekt gehalten. Es war natürlich populär in der Presse, in den Medien, weil das die beiden Narrative Terrorabwehr und Cyber schön verbunden hat. Da hatten sich viele gedacht, man hätte so eine

schöne Win-Win-Situation und könnte das dann aufbauschen. Allerdings wurde das Szenario in der Fachcommunity für relativ schwierig gehalten und zwar vor allem, weil die Terroristen in den Szenarien, die da gängig besprochen wurden, nicht so einen richtigen Benefit sehen. Ein Blackout etwa ist ja eines der großen Szenarien für diese Geschichten. Man schaltet den Strom ab und dann ist alles dunkel. Das ist für einen Terroristen aber nur mäßig interessant. Einmal ist es unheimlich aufwendig und schwierig und gerade für Terroristen kaum zu leisten, da komme ich gleich noch dazu. Und dann ist halt auch nur der Strom aus. Das ist lange nicht so terroristisch wie eine Bombe, wo dann Blut und solche Dinge zu sehen sind. Von der Terrorwirkung her hat man also immer gesagt, vor dem Kosten-Nutzen-Kalkül von Terroristen ist es eigentlich ein relativ unwahrscheinliches Szenario. Inzwischen allerdings hat sich das weiterentwickelt. Man hat mehr Szenarien erforscht und sich angesehen, auch tatsächlich technisch erforscht, was man da sonst noch machen kann. Die Details kennt natürlich niemand, aber es sind leider einige Szenarien sichtbar geworden, die sog. Megadeath-Optionen bieten.

Ich bringe Ihnen ein paar Beispiele. Eines der Beispiele sind Flugzeuge. Da sind inzwischen mehr Sachen an die Öffentlichkeit gegangen, auch mehr Sachen an die Community gegangen, und es gibt in der Tat einige Optionen, Flugzeuge zu hacken, kritische Softwarefehler dort zu verursachen. Das ist sehr schwierig und knifflig und für Laien nicht zu leisten, für gute Fach-Hacker allerdings ist das inzwischen möglich. Gerade dadurch, dass Flugzeuge immer stärker informatisiert werden, auch immer stärker vernetzt werden – die funken z.B. auch über Internet inzwischen mit den Bodenstationen hin und her – gibt es immer mehr Optionen, da einzusteigen. Das Schlimmste, von dem ich bis jetzt gehört habe, ist Air Mexico. Fliegen Sie nicht Air Mexico. Die haben anscheinend ein Verfahren, da kriegt der Pilot den Flugplan auf sein iPad, abends über unverschlüsselte Verbindung im Internet im Hotel, das wird dann da rauf geladen und die stöpseln dann am Flugtag das iPad direkt in das Fly-by-Wire-System des Flugzeugs. Dann fliegt also das iPad, das vorher am Abend über die ungeschützte Verbindung von der Website die Flugdaten bekommen hat. Das sind Szenarien, wo der Fortschritt uns einmal wieder ein bisschen überholt hat. Das passiert mit Sicherheit häufig. Dann wurden noch ein paar andere Szenarien entdeckt, z.B. Chemiewerke, da gibt es teilweise auch kritische Punkte. Schleusentore z.B. öffnen, bestimmte Mischungen verursachen, auch in der Pharmaindustrie bestimmte Mischungen von Pharmazeutika zu verursachen oder so etwas. Da ist es dann natürlich immer ein bisschen schwierig, die Terrorwirkung auch zu kommunizieren. Aber auch da lassen sich durchaus recht signifikante Schäden gestalten, die man auch tatsächlich für Terrorangriffe und für eine Terrorwirkung gut nutzen kann. Und schließlich, müssen wir leider sagen, sind auch Atomkraftwerke nicht so cybersicher wie wir denken. Es gibt im Moment eine relativ große Initiative innerhalb der Staaten, die sich mit Nuklear-Cybersecurity beschäftigt. Das geht einmal um die zivile nukleare Cybersicherheit, da geht es also um die Atomkraftwerke, dann aber auch um die militärische nukleare Cybersicherheit, auch da musste man leider Schwächen in den Systemen finden. Die sind natürlich alle nicht so leicht auszubeuten. Man kann sich jetzt nicht von hier, von der Herbsttagung, da reinhacken und den Melt-Down verursachen. Aber für ein gutes Team müssen wir festhalten, dass das durchaus möglich ist. Hinzu kommt, dass sich viele zivile Atomkraftwerke immer stärker digitalisieren.

Wenn Sie jetzt mit den Fach-Ingenieuren der Firmen sprechen, sagen die, das ist alles Quatsch, nie passiert, gibt es nicht. Aber das ist gelogen. Da können Sie auch gerne nachgucken, das hier sind ein paar Fälle, die dokumentiert sind, wo also Softwarefehler und Hacker fast zu kritischen Vorfällen geführt hätten. Die IAEA hat noch einmal ein Dossier, das ist dreimal so dick, von Vorfällen, die beinahe kritisch waren. Und viele Atomkraftwerke,

natürlich nicht mehr in Deutschland, aber am Rand von Deutschland, in Frankreich und Polen z.B., werden jetzt intensiv digitalisiert und vernetzt.

Aber sehen wir auch ein Interesse bei Terroristen? Etwa in Ankündigungen, in strategischen Planungen? Im Moment noch nicht. Es gab Schriften von einem Terrorfürsten, die bei einer Razzia in Afghanistan gefunden wurden. Der hat gesagt: Wir müssen das Internet nutzen, aber er hat nicht gesagt wie und wozu. Da hat man also doch mehr diesen Vektor der Propaganda und der Gewinnung von Nachwuchs. Es gibt allerdings ein intensives und pragmatisches Interesse daran, Drohnen fernzusteuern und vom Himmel zu holen. Es haben sich ja die Gerüchte gemehrt, dass man Drohnen tatsächlich hacken kann. Und wir wissen natürlich, dass diese Drohnen nicht auf einer speziellen Hochsicherheits-Pentagon-IT fliegen, sondern auf chinesischen Komponenten mit Windows-NT oder so etwas. Die haben sichere Kryptokanäle und solche Dinge, kompartimentalisierte Sicherheitskonzepte. Aber da sind viele zuversichtlich, gerade, wenn sie so ein bisschen Unterstützung aus organisierten Kreisen oder von Nachrichtendiensten sympathisierender Staaten bekommen können, so dass sie in die Kryptokanäle einbrechen oder andere Angriffe auf die IT fahren können.

Davon abgesehen ist es allerdings für Terroristen nach wie vor schwierig, Cyberziele mit einer hinreichend interessanten Terrorwirkung anzugreifen. Terroristen sind eine Extrem-Form des Guerillakrieges. Man ist auf bestimmte taktische Prinzipien angewiesen, muss in sehr kleinen Gruppen arbeiten, hochmobil sein und eine hohe Tarnung beibehalten, sonst sieht einen die CIA. Diese Prinzipien sind entgegengesetzt zu den Prinzipien, die man braucht, um Hochsicherheitsziele oder hochkritische Ziele in Cyber anzugreifen. Wenn man Kraftwerke angreifen will, Flugzeuge oder solche Dinge, ist das technisch sehr anspruchsvoll. Die haben viele Safety- und Securitymechanismen eingebaut, das ist nur etwas für Experten. Da muss man größere Gruppen von Experten zusammenziehen, über einen längeren Zeitraum, in einem Lab, wo diese Sachen kontinuierlich entwickelt werden können. Man muss Zugang zu den Materialien haben, die man angreifen will. Das kann man nicht einfach von außen versuchen oder erraten. Für Angriffe auf Flugzeuge benötigt man außerdem Flugzeugingenieure mit Erfahrungen, Wissenschaftler und teilweise sogar die Angestellten der Hersteller bestimmter Bauteile, damit man das richtig versteht. Da steckt also dann immer viel Expertise drin, viel impliziertes Wissen. Wenn man das nicht mit abholt, kann man diese Dinge meist nicht erfolgreich angreifen. Daher denken wir, dass wir im Moment noch relativ sicher sind vor Cyberterror. Das ist einfach zu schwierig und zu anspruchsvoll. Selbst wenn man einmal drei oder vier Hacker entführt, wird man damit nicht glücklich, denn so wenige sind nicht ausreichend, um kritische Effekte zu verursachen.

Sieht man das dann auch noch im Kosten-Nutzen-Verhältnis relativ zu dem, was Terroristen sonst machen, dann sind Cyberoperationen viel unsicherer und sehr viel teurer als eine Bombe. Alleine schon aus diesen Kosten-Nutzen-Verhältnissen heraus wird dieses Szenario also auch in Zukunft nicht sehr wahrscheinlich sein.

Es gibt allerdings Probleme für die Zukunft dieses Problems, mit denen wir uns auseinandersetzen müssen. Eines der größeren Probleme ist, dass es weltweit viele Hacker gibt, die nicht einmal auf dem Schwarzmarkt sind, sondern die ganz legal IT-Sicherheitsbuden betreiben, Penetration-Testing-Buden, die frei nach Auftragslage Angriffe auf Wunschzielsysteme anbieten. Normalerweise würde man natürlich fordern, dass man das nur auf die eigenen Systeme tun kann, und die Firmen, die da vollständig sauber sind, machen das auch nur auf die eigenen Systeme. Aber es gibt eben auch welche, die sehen das nicht so eng – leider auch im Silicon Valley, wie mir letztens jemand aus dem Pentagon erzählt hat. Die entwickeln für jeden, der mit einem Koffer voller Bargeld ankommt, Angriffe

und diese Angriffe sind sogar laientauglich, mit einer schönen grafischen Oberfläche. Ich kann einfach nur klicken, was ich alles drin haben will. Das ist ein Markt, den wir im Moment noch nicht unter Kontrolle haben und der sich neu orientiert. Wir hören auch immer wieder aus diesen Buden, die weltweit verteilt sind – in Europa viele, auch in Asien – dass da immer wieder Leute mit Koffern voller Bargeld vor der Tür stehen, dieses und jenes bestellen wollen, und da sagen natürlich nicht alle nein. Das ist viel mehr Geld als die normalerweise verdienen, wenn sie ihre Bugs an Microsoft verkaufen. Bei Microsoft kriegen sie 50.000 Dollar oder eine ähnliche Bounty-Prämie, wenn sie nicht verklagt werden. Aber Nachrichtendienste geben schon einmal ein paar 100.000 Dollar dafür aus.

Wir müssen hoffen, dass wir über Außenpolitik „Waffenkontrollen“ in diese Szene bekommen. Das sollte möglich sein, denn das ist kein Schwarzmarkt, sondern ein Weißmarkt. Diese Hacker wollen auch nicht kriminalisiert werden. Viele finden das im Moment opportun, solange es nicht reguliert ist. Aber wenn es reguliert werden würde, dann würden viele von denen sich auch wieder an die Regeln halten. Das wäre doch etwas, was man dringend in diesem Bereich tun könnte. Ein zweites Problem, das sich anbahnt, ist eine viel stärkere Verbreitung des Offensivwissens. Wir haben im Moment noch die glückliche Situation, dass eigentlich gar nicht so viele Leute wissen, wie man richtig gut hackt. Insbesondere die sogenannten Wizards sind noch sehr wenige – das sind in der Hacker Community die, die so richtig gut hacken können, die nicht einfach nur versuchen. irgendwas nachzubauen, sondern ein ganz intuitives Verständnis von den Systemen haben. Aber es gibt natürlich gerade bei den Militärs und den Nachrichtendiensten weltweit ein sehr starkes Bemühen, diese Wizards anzuheuern und herauszukriegen, was die für eine Intuition haben, um das dann zu methodologisieren und um das seinen anderen Truppen beibringen zu können. Das hat in anderen Technologiebereichen auch funktioniert. Viele Technologiebereiche sind auf ähnliche Weise groß geworden. Da gab es erst ein paar Hobbybastler, die das intuitiv verstanden haben und ein technisches Thema in einer Vorphase als Enthusiasten nach vorne gebracht haben. Dann wurde das Thema kommerzialisiert, wie jetzt das Hacken kommerzialisiert wird, und man hat eben versucht rauszufummeln, was die implizierten Wissensbestände ausmacht, die impliziten Verfahren, um dieses Wissen in die Masse der Ingenieure zu bringen. Das ist also etwas, das dann sehr interessant sein wird, für diese Kräfte und auch für Terroristen, denn so wird das Wissen leichter verständlich, und es werden wesentlich mehr sehr gute Hacker auf dem Markt sein. In dieser Situation ist es einfacher, sich selbst größere Teams zusammenzubauen. Wenn man das noch kombiniert mit vorher eingekauften Angriffen, könnte sich der Cyberterror in der Zukunft noch entwickeln. Das sollte man in den nächsten 5 bis 10 Jahren beobachten.

Schließlich haben wir leider auch das Problem – das ist etwas, das ich aus Jordanien berichten kann – dass es auch große Befürchtungen gibt, dass Staaten Cyberangriffe benutzten, um so zu tun, als wären diese Terrorangriffe, um so bestimmte Reaktionen zu provozieren – sogenannte False-Flag-Operationen. Das kann man in Cybersecurity sehr einfach machen, weil die Spuren insbesondere für Nachrichtendienste leicht zu fälschen sind. Es fällt mir relativ leicht, so zu tun, als wäre ich Al Qaida oder so etwas und entsprechend die Spuren zu streuen und zu setzen. Ein kritischer Cyberangriff kann dann entsprechende Reaktionen nach sich ziehen, die ich mir als False Flag Angreifer außenpolitisch wünsche. Im mittleren Osten befürchtet man, dass so einige Gruppen versuchen werden, andere Staaten mit in die dortigen Konflikte zu ziehen. Problematisch hieran ist auch, dass Cybereskalationen nicht gut berechnet oder vorbestimmt sind: Wie schnell reagiert man dann, wie reagiert man, wie kommuniziert man, wie bewertet man das und solche Dinge? Da gibt es noch keine vereinbarten Regeln. Die internationale Gemeinschaft ist gerade intensiv dabei, sich darüber zu unterhalten, was es für Regeln gibt und was für Kriterien man angeben muss, wenn man

entsprechende Behauptungen aufstellt oder darauf reagieren will. Aber da ist man noch nicht sehr weit. Von daher wäre zumindest im Moment noch die Gefahr einer Eskalation, einer schnellen unbedachten Eskalation in diesem Bereich relativ hoch.

So weit zum Cyberterror. Jetzt kommen wir zu dem etwas aktuelleren und nicht ganz so hypothetischen Szenario Cyberspionage. Ich habe Cyberspionage und Cyber Warfare zusammengefasst, weil das in den Bereichen, in denen ich arbeite, immer als eins behandelt wird. Man redet im angloamerikanischen Sprachgebrauch auch inzwischen mehr von Cyberkonflikt. Das ist eine Fusion aus beidem und das hat damit zu tun, dass die Fähigkeiten, die man hier nutzt, eigentlich klassische nachrichtendienstliche Fähigkeiten sind: Spionage und Sabotage, also ganz klassisches nachrichtendienstliches Denken. Aber die Wirkungen dieser Tätigkeiten haben klar geostrategisches Potential. Und das ist auch eine Neuheit auch an diesem Bereich. Man geht eigentlich mit nachrichtendienstlichen Methoden und ganz klassischem nachrichtendienstlichen Wissen daran, aber das, was man tut, hat eben so eine enorme Wirkung, kann ungeheuer eskalieren und auch an so kritischen Punkten stattfinden, dass sich das wiederum militärisch nutzen und verstehen und in militärische Taktiken und Strategien einbauen lässt. Die Fusion findet sich auch in der Organisation der Truppen. Wir haben etwa in den USA das Cyber Command, von General Alexander geleitet, der auch gleichzeitig bei der CIA war. Auch bei den Russen sehen wir, dass diese Truppen gleichzeitig militärisch-nachrichtendienstlich aufgespannt sind und auch bei vielen anderen Staaten sehen wir so eine enge Verbindung aus militärischen und nachrichtendienstlichen Elementen in diesem Bereich. Von daher lässt sich das nicht klar trennen. Es lässt sich natürlich nachher wieder klar trennen, in den Folgen, in den Wirkungen, in den Aktivitäten. Da kann man wieder sagen: das gehört jetzt in den Bereich Warfare, das gehört in den Bereich Spionage. Da gibt es dann aber auch zwei verschiedene Arten, das einzuordnen. Das eine ist nämlich die rechtliche, da kommen dann die Juristen und behaupten, dass es gar keinen Cyberwar gibt, weil man die Akteure nicht identifizieren kann. Das gehört ja zu einer Kriegshandlung. Oder weil die Wirkungen sehr schleichend sind, mehr Erosionsgeschichten als große Explosionen, so dass man die Angriffe nicht mit einem militärischen Angriff mit einer kinetischen Wirkung und mit einem klar uniformierten Akteur vergleichen kann. Aber das sind eben nur die Juristen. Daneben gibt es noch die strategische Einordnung, bei der man auch anonyme Aktivitäten mit militärischem Kalkül wie militärische behandelt, diese aus einer strategischen Perspektive einordnet und dann entsprechend agiert.

Was wollen die denn eigentlich machen, diese Cyber-Spione, Cyber-Krieger? Da haben wir inzwischen ein bisschen bessere Kenntnisse. Einmal natürlich durch die ganzen Leaks der NSA und auch durch andere, die vorher stattgefunden haben. Dann mehren sich natürlich auch die einzelnen Vorfälle, die detektiert, gefunden und besprochen werden, so dass wir also jetzt ein bisschen besser sehen können, was da eigentlich alles gemacht wird. Wir sehen einmal verschiedene Varianten der Kooperationen. An der NSA haben wir ganz klar gesehen, dass es eine sehr enge Kooperation z.B. mit der Wirtschaft gibt. Es gibt eine sehr enge Kooperation mit den Telekommunikationsunternehmen. Da wurde auch berichtet, auch aus Großbritannien, dass die freundschaftlich und sehr zuvorkommend waren. Die IT-Unternehmen waren natürlich viel unwilliger. Das wissen wir aus Hintergrundgesprächen. CIA-Hintertüren sind für globale Unternehmen ökonomischer Selbstmord. Von daher waren die da sehr gegen solche Kooperationen und haben sich gesträubt. Aber wir wissen ja, dass das nicht unbedingt mit Erfolg gekrönt war. Wir wissen nicht genau, wer wann, wie, wo, mit wem verflochten ist, insbesondere nicht bei den IT-Herstellern. Das ist schwierig nachzuverfolgen. Aber wir sehen aus den NSA-Dokumenten und aus den Sachen, die vorgefallen sind, dass man, wenn man nicht freiwillig kooperiert hat, auch dazu gezwungen werden kann. Man hat die Unternehmen etwa infiltriert. Hat sich da reingehackt, hat auch

teilweise Leute angeheuert, um dann da Hintertüren einbauen zu können oder Sachen umlenken zu können. Das hier z.B. ist ein belgisches großes Routingunternehmen, das also Datenströme im Internet hin und her lenkt, das man infiltriert hat, um vermutlich Datenströme Richtung Amerika zu lenken. Dann hat man in den USA selber auch die Option, Firmen per Patriot Act oder CALEA Act zu zwingen, zu kooperieren. Das ist im Moment sehr schlecht für die US-Wirtschaft. Ich war letzte Woche gerade im Silicon Valley, habe da mit einigen Leuten geredet und alle haben gesagt, für die Industrie sei die NSA-Affäre ein Nine-Eleven. Man erwartet dort riesige Einbußen und hat auch bereits einen Knick gemerkt in den Bestellungen. Im Moment leben diese Akteure in kritischen Bereichen eigentlich nur noch davon, dass es keine richtigen Alternativen gibt zur amerikanischen IT – bzw. ist die einzige Alternative chinesisch, und das ist dann gehüpft wie gesprungen für die meisten. Aber sobald einmal einer genug Geld in die Hand nimmt, um eine Alternative aufzubauen, der vertrauenswürdiger ist, was seine Nachrichtendienste angeht und keine Supermachtallüren an den Tag legt, dürften diesem Markt große Umwälzungen bevorstehen. Wenn man eine Alternative hätte, die eine Souveränität gestattet, eine Integrität aller kritischen Daten und Prozesse, hat man als Staatslenker oder als Unternehmenslenker die Pflicht, auf solche Technologien umzuschalten.

Wir sehen dann auch eine sehr enge Kooperation mit der Wissenschaft. Insbesondere in den USA gibt es viele neue Labs. Die NASA hat da viel gebaut, auch große Programme wie CRASH, hinter denen viel Geld steht, ein 100 bis 1000-faches der europäischen Fördersummen. Vieles davon geht allerdings nicht in die Defensive, sondern in die Offensive, in die Entwicklung von Angriffs- und Aufklärungsfähigkeiten. Da haben sich auch viele private Forschungsinstitute gegründet. Auch dort sehen wir eine starke Verflechtung mit einem Private-Sector, der sich neu gebildet hat. Das war ja bei Snowden auch das Problem, dass man sehr viele Subunternehmer brauchte, weil man die Gehaltsstrukturen teilweise nicht liefern konnte in den staatlichen Einrichtungen, deswegen halt eben Ausgründungen brauchte, die dann bessere Gehälter zahlen konnten. Da hatte man schon befürchtet, dass man da vielleicht einmal einen Leak hat, denn den Private Sector kann man natürlich nicht so gut kontrollieren wie die Leute, die man im eigenen Gebäude hat. Da hatte ich schon vor Jahren Gespräche mit US-Militärs, die da Bauchschmerzen hatten. Die sehen sich jetzt natürlich bestätigt. Für strategische Geheimhaltung sind solche Public-Private-Modelle eben problematisch, denn man muss eben doch viele kritische Daten mit diesen Subunternehmern teilen, wenn man da vernünftige Operationen betreiben will. Dazu hat man noch das neue Paradigma der „Responsibility to share“ in den USA, das auch so seine Blüten treibt, vor allem technisch und organisatorisch.

Wir haben auch in unserer unmittelbaren Nachbarschaft eine enge Kooperation von Wissenschaft und Offensiventwicklung, nämlich in Frankreich. Da gibt es eine lustige Schule in Paris, die School of Economic Warfare. Die behaupten zwar immer, das sei rein defensiv und nur zum Schutz der eigenen Wirtschaft. Komischerweise haben sie aber dieses Jahr z.B. einen Kurs zu subversiven Techniken für ökonomische und Cyber-Destabilisierung. Das klingt erst einmal nicht defensiv, und derjenige, den ich da kenne, hatte mir auch gesagt, die wären ziemlich irre, und man müsste die dringend ein bisschen beobachten und an die Kandare nehmen. Es ist also durchaus nicht nur ein Problem mit der NSA, dass man versucht, helle Köpfe in die Offensiventwicklung hineinzubringen.

Auch großartig an den Snowden-Leaks ist, dass wir inzwischen viel mehr wissen über die Truppengrößen und die Aktivitäten. Da ist sehr viel bekannt geworden in den USA. In der NSA alleine arbeiten angeblich bereits 4000 Hacker. Wir wissen nicht, wie viele dann noch links und rechts bei anderen Truppenbeständen oder in Firmen ausgelagert sind und andere

Dinge tun – und man hired ja weiterhin, das hier war gerade eine Anzeige, die ich auf einer IT-Fachwebsite gesehen habe. Da konnte man dann klicken und direkt sich einschreiben für die NSA. In diesem Batch Leaks war der für spektakulärste der Snowden-Leaks. Der ist von der Presse so durchgewunken worden, weil die alle nicht verstanden haben, was da drin stand. Das war die Zahl der Operationen des Cybercommand im Jahr 2011. Sie müssen wissen, Operationen im militärischen Kontext bedeutet, dass man ein bestimmtes militärisches Ziel hat und dann eine Serie von Aktivitäten und Taktiken unternimmt, um dieses Ziel in Angriff zu nehmen oder zu erreichen. Das ist also nicht ein einzelner Angriff, sondern eine Serie von Angriffen mit einer bestimmten Absicht. Stuxnet z.B. war eine Operation, wahrscheinlich noch flankiert von Spionageaktivitäten zu Reconnaissance und solchen Dingen. Auch Flame war eine Operation, die ja viele Systeme im Mittleren Osten infiziert hat und da jahrelang Informationen gesammelt hat. Jetzt überlegen Sie einmal, wie viele Operationen in dieser Größenordnung denn so ein Cybercommand pro Jahr durchführen kann. Ich hatte vor einiger Zeit einmal meine Kollegen gefragt – die haben gesagt: vielleicht 10 oder 20. So ein Angriff ist ja wahnsinnig aufwendig in der Entwicklung und braucht Betreuung. Aber es waren nicht 10 oder 20 – es waren 231 Operationen! Nur im Jahr 2011! Dreiviertel davon waren in China, Russland, Nordkorea, Iran. Das ist eine spektakulär große Zahl. Dann hatten wir noch eine andere schöne Zahl im gleichen Leak, da wurde auch noch das „Genie“-Projekt der NSA erwähnt. Das Projekt Genie hatte zum Ziel, „covert implants“ einzubauen, also Schwachstellen als versteckte Hintertüren. Dafür wurden 652 Millionen US-Dollar ausgegeben! Jetzt kann man sich als Laie, nicht viel darunter vorstellen. Das ist so eine Hausnummer für ein US-Militärbudget. Aber 652 Millionen Dollar für Schwachstellen sind schon sehr substanziell. Dafür kriegen Sie eine ganze Menge hin. Das sind ein paar Hundert bis ein paar Tausend Backdoors, die Sie dafür kriegen. Und dann müssen Sie sehen, dass die natürlich nicht einzelne Backdoors in einzelnen Maschinen bauen, sondern breit nutzbare Typen-Backdoors für diese Typen von Maschinen.

Zudem wird man eine systematische Ökosysteminfektion anstreben. Die beginnt relativ früh in der Supply Chain, also möglichst in der Fabrik, wo das Ding gebaut wird, in der Mastercopy einer Software, oder man verteilt breit mit einem Update – das sind gängige Mechanismen für Nachrichtendienste. Dann wird man auch versuchen, möglichst unten im Systemstack anzusetzen, also Hardware zuerst, dann Betriebssysteme, dann Anwendungen, um erneut möglichst breite Wirksamkeit zu erzielen. Dann können Sie mit 652 Millionen Dollar viel machen. Sie können alle Betriebssysteme nachhaltig infizieren, mit mehreren Vektoren, Hardware, alles, was gängig und breit verteilt ist.

Diese Summe bedeutet also, dass ein größerer Teil des bestehenden IT-Ökosystems bereits nachhaltig verseucht ist. Das ist einfach jetzt ein Fakt. Da können wir nichts mehr machen, die Schwachstellen werden kaum zu finden sein.

Ja, das sind so ein paar Zahlen, die wir aus den USA haben. Dann haben wir natürlich auch ein paar Kenntnisse über die anderen, China zum Beispiel. Wir müssen bei China davon ausgehen, dass die mindestens so aktiv sind wie die USA, wenn nicht noch sehr viel mehr. Man weiß nicht so viel über die. Es gibt ja immer wieder Meldungen, China hier und China da, insbesondere aus den USA. In der Wirtschaft werden sie auch relativ häufig beobachtet, aber dann halt nicht gemeldet. Das Interessante an den Chinesen ist, dass sie recht schlau vorgehen. Diese Angreifer sind erst einmal opportunistisch. Sie sind nicht wie die Amerikaner oder die Russen, die sehr sorgfältige, sehr hochwertige Angriffe bauen, die man nie sieht, solange nicht Edward Snowden dann losläuft. Die chinesischen Wirtschaftsspione machen relativ einfache Angriffe. Das sieht dann oft auch ein bisschen so aus, als hätten die Chinesen keine Ahnung von dem, was sie machen, weil die sozusagen mit der Holzkeule einbrechen.

Aber die nehmen halt das, was reicht. Die packen sozusagen nicht die Silver Bullet aus, wenn sie die gar nicht brauchen, und bei den meisten Unternehmen, selbst bei Rüstungsunternehmen, kommen sie mit relativ einfachen Maßnahmen dann doch noch irgendwie an die Kronjuwelen.

Das bedeutet aber auch, dass es ihnen relativ egal ist, dass wir sie die ganze Zeit sehen, denn solche einfachen, opportunistischen Aktivitäten sind deutlich eher sichtbar. Es scheint also der Fall zu sein, dass es ihnen nicht so viel ausmacht, wenn wir sie beobachten. Tatsächlich sind ja auch die internationalen diplomatischen Reaktionen eher moderat. Man will sich diesen großen Handelspartner nicht verscherzen, und die Chinesen sagen ja auch immer, sie hätten damit nichts zu tun. Aber wir hatten im letzten Jahr einen Fall, der präsentiert wurde: APT-1. Das war von einer Firma Mandiant in den USA, ein freigegebener Bericht über eine Militäreinheit in China, die Electronic Warfare-Geschichten gemacht hat und die aber seit einiger Zeit für die chinesische Regierung Industriespionage im Westen betrieben hat. Bei Hochtechnologieunternehmen, Rüstungsunternehmen usw.

Die Russen sind eine andere Großmacht in diesem Bereich. Wir denken, dass die ebenfalls sehr fähig sein müssen. Russland hat sehr viele gute Mathematiker, Ingenieure und Wissenschaftler. Wir haben aber unklare Zahlen, wie viele militärische Hacker es bei denen gibt. Das weiß keiner so richtig. Wir wissen, dass die traditionell stark sind in Signals Intelligence und auch traditionell viel Gewicht legen auf Information Operations, weil sie ja damals immer viel mit Propaganda zu tun hatten. Sie sind auch sehr interessiert an klassischer Spionage und an Wirtschaftsspionage. Wir sehen aber sehr wenig von den Russen in diesem Bereich. Im Cybercrime sieht man viel russische Aktivität, aber bei diesen hochwertigen Sachen sieht man sie fast gar nicht. Es kann allerdings gut sein, dass sie sich im Strom des Cybercrime tarnen. Wir hatten schon mehrfach Angriffe, die sehr hoch qualifiziert waren, aber von außen, wenn man draufgeguckt hat, erst einmal aussahen wie ganz normale Cybercrime-Aktivitäten. Stuxnet zum Beispiel sah von außen aus wie ein ganz normaler Bankingtrojaner, wenn man einfach so draufgeguckt hat. Da hat dann einmal ein deutscher Forscher, übrigens aus Langeweile, in den Code reingesehen und hat dann gefunden, dass der nicht nach Bankdaten sucht, sondern nach SCADA-Steuerungsdaten. Und so ist dann erst aufgeflogen, dass das ein Industriesabotagewurm war. Von daher kann man gut davon ausgehen, dass hier also viel Spionage-Aktivität als kriminell getarnt wird. Und dann haben wir natürlich auch noch viele andere Akteure weltweit neben den Supermächten, die sich hier aufbauen. Insbesondere die Schwellen- und Entwicklungsländer haben großes Interesse, hier aktiv zu werden. Das ist auch etwas, das uns in Zukunft noch mehr beschäftigen wird.

Kommen wir zu Strategie und Taktik – da sehen wir auch einiges an Entwicklung. Wir sehen viel „First Order-Strategie“, also was man erst einmal so damit machen kann, auch die Taktik ist insbesondere bei den Supermächten schon weit entwickelt. Bekannte strategische Interessen und Verfahren werden etwa entwickelt für konventionelle Spionage, da sind die schon sehr weit, aber auch Electronic Warfare ist sehr weit und da müssen wir leider sagen, dass das Verhältnis von Offensivfähigkeiten zu Defensivfähigkeiten bei den Militärs herausragend schlecht ist. Ich würde im Moment mein Gehalt darauf verwetten, dass wir kein funktionierendes Militär haben im gesamten Westen, dass die alle nachhaltig unterwandert und nicht mehr funktionsfähig sind. Davon müssen wir ausgehen. Die haben massiv auf kommerzielle Komponenten gesetzt, haben keine Ahnung von IT-Security, kein Geld, um das irgendwie zu lösen, kein Personal und teilweise reicht ein einziger Insider, um das gesamte System dauerhaft zu grillen. Und das ist natürlich für Nachrichtendienste ein Klacks, irgendwo in so einem riesigen Militär einen Innentäter an einer kritischen Stelle zu installieren. Man ist also im Moment glücklich, dass man nur mit den Taliban zu tun hat und

nicht mit irgendwelchen Hightech-Nationen. Aber man muss hinterfragen, ob das noch das ist, was wir eigentlich wollen bei den Militärs. Zur Lösung muss man substanzieller investieren, um die wieder zu sichern.

Daneben haben wir eine ganze Reihe von neuen strategischen Überlegungen, die früher auch schon da waren, aber nicht so eine große Rolle gespielt haben. Information Operations zum Beispiel ist so eine Sache, die ganz wichtig geworden ist, indem man im Web so tut, als wäre man jemand anders und dann versucht, Kampagnen zu leiten, um Meinung zu steuern. Wir haben im Mittleren Osten eine ganze Reihe von Aktivitäten in dieser Richtung gesehen, insbesondere in der Infiltration und Nutzung von Social Media zur Identifikation und Desinformation von Aktivisten und Oppositionellen.

Ein anderes Szenario, das uns viel Sorge bereitet, sind Economic Operations. Dies sind militärische und nachrichtendienstliche Operationen an der Wirtschaft. Das war immer eher ein Stiefkind im Kalten Krieg, weil es schwierig war, andere auf diese Weise ökonomisch zu ruinieren. Inzwischen müssen wir allerdings sagen, dass die Wirtschaft gegen hochwertige Cyberangreifer absolut ungeschützt ist, so dass wir da also einen offenen Vektor haben. Viel Industriespionage, Wirtschafts- oder Handelsspionage könnte einen strategischen Hintergrund haben – in Zukunft auch in Kombination mit Sabotage. Auch hier ist es schwierig, kriminelle von staatlichen Aktivitäten klar zu trennen. Aber aus Hintergrundgesprächen mit IT-Sicherheitsleuten in den Banken und den Börsen wissen wir, dass da so oder so bereits viel läuft. Die Banken geben sich viel Mühe und heuern die besten Leute und die besten Technologien an, um dem einen Riegel vorzuschieben. Aber das klappt leider sehr schlecht, weil da natürlich auch Akteure dahinterstehen, die entsprechend investieren können und weil die Banken und Börsen sehr intensiv und umfangreich IT-abhängig sind. Dann haben wir zwei Varianten, strategisch, wozu man das nutzen kann. Das eine ist als Economic Equalizer. Das ist das, was viele Schwellen- und Entwicklungsländer sich vorstellen, dass man also Industriespionage macht, um sein eigenes Land voran zu bringen. Economic Erosion ist die andere Variante, wo man dann das Konkurrenzland auch konkret schwächen will, in diesem Fall durch strategische Konkurrenz. Auch die NSA scheint da nicht ganz abgeneigt zu sein. Natürlich nicht so umfangreich wie andere, aber zum Beispiel kam gerade vor einigen Tagen heraus, dass auch die OPEC beobachtet wurde und da ist erst einmal keine Terroraktivität unmittelbar zu befürchten. Da geht es vermutlich eher um Handelsaktivitäten.

Wir sehen dann auch Kombinationen aus alten und neuen Methoden, also auch die gute alte nachrichtendienstliche Arbeit am Boden, Human Intelligence, spielt eine Rolle. Zum Beispiel gab es verschiedene Einbrüche bei Silicon Valley-Firmen, wo der Source Code geklaut wurde, und bei Sicherheitsunternehmen. Es wurden auch verschiedene Innentäter erwischt, die den Source Code von High-Frequency-Trading Software geklaut haben. Dieser klassische Innentäter spielt eine sehr große Rolle in diesem Bereich. Wir hatten auch schon den Fall, dass ganz konventionell kinetisch ein Cyber Commander erschossen wurde. Der Cyber Commander der Iraner wurde gerade vor ein paar Wochen mit Kopfschuss in der Wüste aufgefunden. Also auch diese Methoden kommen jetzt so langsam in diese Cyberspiele rein.

Leider sind dies aber nur unmittelbare militärisch-strategische Betrachtungen. Strategie höherer Ordnung, die große politische Ebene, eine Einbettung in eine Grand Strategy oder auch in größere wirtschaftspolitische, außenpolitische Ziele – das findet oft nicht statt. Das ist auch eine Gefahr. Das haben wir an der NSA gesehen. Die NSA hat ja fast freie Hand gehabt. Da gab es auch Gespräche mit den Leuten des Oversight Committee, die ja eigentlich darauf hätten gucken müssen und das politisch hätten einordnen müssen. Die haben gesagt, sie hätten zu viele Nachrichtendienste, die zu viele Sachen machen. Sie wären nicht in der Lage, das

alles zu lesen und dann gerade diese technischen Geschichten mit diesem IT-Kram hat sowieso keiner verstanden, also wurde das vom Tisch, von links nach rechts, geschoben. Das ist jetzt aber etwas, das sehr schmerzhaft ist, was politisch zurückkommt in Problemen mit der Glaubwürdigkeit, dem Export etc.

Der Stand der Offensive ist tatsächlich sehr hoch. Wir haben hier eine weit fortgeschrittene Ausgangslage, technisch, organisatorisch und ökonomisch. Es ist übrigens gerade ein neuer Angriff im Feld: Bad BIOS. Das können Sie sich einmal ansehen, vor ein paar Tagen wurde der entdeckt. Der hat ein paar interessante Features dabei. Eine ganz tolle Sache, die er macht: er kann Systeme miteinander kommunizieren lassen, die keine Datenverbindung dazwischen haben. Kein Kabel, kein WLAN, kein Bluetooth. Wie macht er das? Er sendet hochfrequente Tonsignale über die Lautsprecher, die dann das Mikrofon von einem anderen Rechner empfängt, der vorher ebenfalls infiziert wurde. Also quasi wie eine Fledermaus, durch Tonsignale über einen ganz normalen Lautsprecher. Eine ganz tolle Geschichte und funktioniert anscheinend auch zwischen verschiedenen Fabrikaten. Das ist also noch einmal eine neue Variante, macht so eine Art Software Defined Radio aus ihrem Rechner und funkt dann. Und das macht Sinn, wenn Sie verschiedene Hochsicherheitssysteme kennen. Die haben nämlich teilweise einen Rechner da stehen, der direkt ins Internet geht und auf ihrem Arbeitsplatz direkt daneben den Rechner, der ins Hochsicherheitsnetz geht. Dazwischen sind überhaupt keine Kabel, kein WLAN. Aber wenn die sich einfach über den Lautsprecher mit Tönen austauschen können, dann haben sie da natürlich eine Brücke geschaffen, mit der sie dann die Hochsicherheitssysteme umgehen können.

Es gibt auch eine deutliche Evolution in diesem Bereich. Es gibt große Investitionen und die Akteure, die in diesem Bereich tätig sind, bemühen sich, die Methoden aus der kommerziellen Softwareindustrie zu adaptieren, um selber effizienter zu werden. Cyberwar ist eigentlich nichts anderes als das Entstehen eines Marktes für hochqualifiziertes Hacking und entsprechend denkt man daran, die Methoden aus der normalen Softwareentwicklung zu übernehmen.

Leider müssen wir sagen, ist gegen diesen Akteur das, was wir haben an IT-Sicherheit, der Stand der Defensive, sehr, sehr schlecht. Wir haben einmal das Problem, dass wir immer noch mit sehr komplexen Commercial-Of-The-Shelf-Produkten arbeiten. Selbst im Hochsicherheitsbereich sind wir gezwungen, mit diesen Produkten zu arbeiten. Die sind strukturell defizitär, haben mehrere Tausend Angriffsvektoren pro System. Die können Sie also gar nicht absichern. Wir haben dann noch das Problem, dass wir glauben, mit Detektion weiterzukommen. Die meisten Konzepte, die sie hören zur IT-Sicherheit, sind CERTs oder SOCs oder Intrusion-Detection-Geschichten usw. Aber das funktioniert in diesem Bereich einfach nicht. Weiter ist dann gerade der Irrglaube, dass man mit diesen Systemen viel tun kann, eher ein Teil des Problems als ein Teil der Lösung. Dann haben wir auch das Problem, dass unsere IT-Sicherheit, die wir haben, immer noch in einem sehr infantilen Status ist. Das meiste ist reaktiv, das nützt Ihnen schon nicht viel. Das ist alles technologisch sehr unsystematisch, sehr unreif, man schraubt immer dem hinterher, was letzte Woche in den Medien war oder im Sommer in der Cebit und versucht sich daran irgendwie zu orientieren. Man hat gar keine Vision, wo das hingeht, kein systematisches Wissen darüber, was damit passiert. Dann haben wir auch die lustige Beobachtung gemacht, dass diese ganzen IT-Sicherheitsprodukte nicht nur ineffizient, sondern selber völlig unsicher sind. Es gibt entsprechenden Studien in den USA von Imperva oder NSS, aber auch die Saudis hatten mir da etwas erzählt. Die haben so einen typischen Saudi-Ansatz an IT-Sicherheit gemacht, haben einfach alles gekauft, was irgendwie auf dem Markt ist und das zusammengeschraubt. Das hat ein furchtbares Chaos hinterlassen. Sie konnten das meiste nicht bedienen, dann gab es

tausend Kompatibilitätsprobleme, mit denen die dauernd beschäftigt waren. Und dann haben sie vor allem aber herausgefunden, dass Hacker schlechte Programmierer sind. Einen Sicherheitsfehler bei dem einen zu finden heißt noch lange nicht, dass man selber keine macht. Und von daher waren also viele dieser Sicherheitsprodukte, die entwickelt worden sind, selber unsicher, hatten eine teilweise um 60 % höhere Fehlerrate als normale kommerzielle Software, so dass man also über diese Sicherheitsprodukte noch viel besser in die Systeme einsteigen konnte als ohne. Sie haben also nur die Zahl ihrer Angriffsvektoren erhöht und nicht ihre Sicherheit.

Dazu kommt dann auch ein ganzes Set anderer Probleme, die wir in diesem Bereich haben. Wir haben etwa nicht genug gute Entwickler, um gute Software zu entwickeln. Wir haben kaum Awareness. Die Angreifer und ihre Konsequenzen sind kaum sichtbar. Wir orientieren uns ja meistens an dem, was wir sehen können, was aber natürlich nur das untere Ende der Angreifer ist. Wir sind nach wie vor dabei, alles mit allem zu vernetzen, weil uns nichts Neues mehr einfällt, um unsere IT noch weiter zu verkaufen. Wir sind auch dabei, überall Features dranzuschrauben, wobei wir damit natürlich noch mehr Verwundbarkeiten verursachen. Alles muss auch smart sein, dabei nutzen wir trotzdem immer nur die gleichen Monokulturen, d.h. wir haben überall die gleiche, breite Basis von Verwundbarkeiten eingezogen. Das Ganze bewegt sich sehr schnell, sehr agil. Wir haben auch einfach unglaublich schlechte Arbeitskräfte im Bereich IT-Sicherheit. Es gibt nur wenig gute Leute und leider auch bis jetzt noch keine besonders gute Ausbildung in diesem Bereich.

Damit haben wir insgesamt eine schlechte Situation. Das ist die Asymmetrie, von der man redet, wenn man sagt, das ist also „offense dominated“. Die Offensive ist viel agiler, besser finanziert, geht systematisch vor, ist unglaublich innovativ, macht auch Disruptive-Innovationen, die orientiert sich nicht an den Kleinkriminellen und deren Dynamiken. Die haben sehr viele Optionen, sind kaum sichtbar, die müssen nur ein einziges Mal gewinnen, um in ihrem System für immer drin zu sein und die haben ausreichendes Personal, weil sie da gar nicht so viel brauchen. So eine Truppe von 20 Personen, wenn die gut sind, reicht aus, um Hochsicherheitsziele zu penetrieren und da drin zu bleiben. Auf der anderen Seite haben sie eine Defensive, die ist langsam, hat keine Ahnung, keine Vision, ist schlecht finanziert, hat keine Datenlage über diese Angreifer, geht völlig unsystematisch vor, ist kaum innovativ. Die machen alle nur die Firewall, dann die next-generation Firewall und dann die next-next-generation Firewall – alles sehr konservativ. Tut mir leid, wenn hier Industrievertreter sind. Das ist meine Meinung. Wir haben dabei aber gleichzeitig sehr viele Vektoren zu sichern, insbesondere bei Nachrichtendiensten, wo dann Innentäter mit reinkommen.

Das ist insgesamt eine unschöne Situation. Haben wir denn Optionen für den Strafverfolger? Wenn wir sagen:. Okay, die technische Sicherheit ist so miserabel, dann müssen wir halt mit Strafverfolgung ansetzen und versuchen, die Angreifer zu identifizieren und dann entsprechend abzuschrecken oder zu verfolgen. Aber da müssen wir leider auch sagen, dass es hier ebenfalls keine Option gibt. Das hat einfach damit zu tun, dass Angreifer in diesem Segment sich nicht identifizieren lassen. Wenn die sich schon nicht detektieren lassen, können Sie sich auch vorstellen, dass die auch nur sehr schwer zu identifizieren sind. Wir haben auch Beweise dafür, dass die unsichtbar und trotzdem da sind. Der Nasdaq-Hack zum Beispiel 2011, da gibt es eine Anekdote. 2011 war ein Hack aufgeflogen. Dann gab es ein Team von Analysten, die sich das angesehen haben. Als die reingeguckt haben, haben die sechs andere da drin gefunden, die nicht aufgeflogen sind, weil die ihre Angriffe besser designed haben. Das waren alles sehr hochqualifizierte Angreifer, hätten die nie gefunden. Und sie vermuten, dass noch einmal einige drin sind, die sie auch nicht gefunden haben. Dann haben Sie das beste Beispiel, die Operationen der NSA 2011. 231 Operationen im Jahr 2011 – hatte ich

vorhin schon erwähnt. Die einzige, die wir gesehen haben oder die zumindest in der Öffentlichkeit angekommen ist, war Flame. Die anderen 230 Operationen hat niemand weltweit gesehen, niemand. Da können Sie mir nicht erzählen, dass diese Paradigmen mit Detectionen und Intrusion Detection usw. gut funktionieren. Und dann haben wir natürlich auch die Detektionszeiten. Wir wissen auch von den einigen hochqualifizierten Angriffen inzwischen, wie lange die in diesen Systemen sind. Bad BIOS z.B. war schon seit 3 Jahren aktiv, bevor er jetzt das erste Mal detektiert wurde. Die meisten anderen Angriffe liegen auch zwischen 3 Jahren und 5 Jahren bis sie das erste Mal gefunden werden, das ist natürlich auch dramatisch schlecht.

Außerdem wird viel daran entwickelt, alles zu tun, um Sie zu täuschen. Ein Freund von mir macht z.B. ein Projekt in Frankreich. Das ist ein System, das setzt sich zwischen einen Angreifer und ein Opfer, also sagen wir einmal Amerika und China. Die beiden behaken sich gegenseitig. China spioniert, Amerika versucht mit Big Data und allem möglichen Krimskrams Beweise zu finden. Der setzt jetzt sein System dazwischen, guckt genau wie die sich abtauschen miteinander, zeichnet alles auf, unterbricht dann irgendwann diese Geschichten, greift selber die USA an und spielt dabei aber vollständig die Signale aus China. Der hat sogar eine Sphäre der Selbsttäuschung um sich herum, wo das System merkt, wenn es Signale absendet, die nicht chinesisch aussehen. Dann fährt es sich herunter und macht noch einmal alles neu, rechnet es noch einmal um, damit es dann wieder chinesisch aussieht. Sie haben natürlich eine gewisse Fehlerquote, aber er meinte, er kriegt es hin, dass 95 bis 98 % der Signale, die sie kriegen aus diesem System „nach China“ aussehen. Jetzt haben Sie das Problem, wenn Sie auf der Seite der Analysten sitzen und Sie haben 95 % Ihrer 1000 Signale, die sie mit Big Data gesammelt haben und Querverbindungen weisen nach China und 5 % sind Noise mit ein paar Signalen aus Frankreich – wen greifen Sie denn dann an? Und wie wollen Sie das jemandem erklären, dass Sie dann doch lieber Frankreich angreifen mit 5 % Signalen als China mit 95 %.

Das ist etwas, was man in diesem Bereich sehr gängig macht. Man legt großes Gewicht auf Tarnung und Täuschung und von daher müssen wir sagen, dass es für Strafverfolgung, für Attribution, also die Zuschreibung von Angriffen, hier wenig Optionen gibt. Selbst die USA, die viel machen mit Big Data, sind da nicht besser dran. Ich war gerade letzte Woche bei Palantir zum Beispiel, die machen viel mit Big Data, sammeln alles, was irgendwie geht unter gröbsten Datenschutzverletzungen, hacken sich in andere Länder ein und greifen sich alles, was man irgendwie kriegen kann, was für uns schon alles gar nicht mehr gangbar ist. Selbst die haben schlechte Quoten für saubere harte Identifikation und noch weit schlechtere Quoten für Verhaftungen und Verurteilungen. Das ist in diesem Bereich, wenn Sie es mit sehr hochqualifizierten Angreifern zu tun haben, fast unmöglich.

Wir brauchen also auch andere Lösungen. Da will ich Ihnen jetzt noch zum Schluss meine Idee mitgeben. Erst mal sollten wir uns bei anderen Lösungen darum bemühen, das Problem zu verstehen, das ist immer noch nicht richtig passiert. Wir haben keine richtige Bedrohungs- und Risikomodellierung. Man guckt halt immer nur, was letzte Woche passiert ist und das ist dann das Risiko. Aber wir müssen natürlich eine theoretische Modellierung anstreben, eine quantitative Modellierung, um halt eben auch genau zu sehen, was denn eigentlich die großen Risiken und was die kleinen Risiken sind. Worum müssen wir uns zuerst kümmern und worum erst später? Wir müssen klassifizieren. Wir müssen auch Metriken ganz dringend entwickeln, um die Effizienz von Offensive und Sicherheit zu messen. Es gibt gar keine Metriken, um diese ganzen IT-Sicherheitsprodukte, die Ihnen dauernd angedreht werden, zu prüfen. Die selbst messen sich mit den Zahlen ihrer gefangenen Viren, aber das sagt kaum irgendetwas Brauchbares über den Sicherheitsstand des Systems aus. Die wissen überhaupt

gar nicht wie gut die sind oder wie schlecht, ob die selber sicher sind und solche Dinge. Das sind also alles Desiderate, die wir erst mal erfüllen sollten, bevor wir in irgendwelche Produkte investieren, damit wir wissen, ob die Lösung, die wir kaufen, auch wirklich Lösungen sind. Da hätte ich auch Zweifel, ob die Priorisierungen, die wir im Moment haben, noch so gültig sind. Im Moment haben wir die Priorisierung IT-Grundschutz. Alle sollen sich erst einmal gegen das Botnetz von nebenan schützen und gegen Cyber-Kleinkriminalität. Das ist natürlich trotzdem viel und ein wichtiger Punkt, aber es ist eben dann immer nur Betrug, kleinere, mittlere Kriminalität. Ob das wirklich unsere Priorität ist oder ob wir uns nicht lieber um Hochsicherheit kümmern müssen, um Industriespione und um mögliche Kriegsfälle – das wird nicht einmal richtig diskutiert. Dabei sollte klar sein, dass wir das vielleicht einmal ein bisschen höher setzen in der Liste der Dinge, die wir tun können und tun müssen. Zu einer echten Lösung gehört dann auch, dass man versteht, dass dieses Problem nicht rein technisch ist, sondern dass es sehr viele andere Dimensionen hat. Die technischen Probleme haben ihre Ursachen im Markt und in der Politik. Es gibt ein konsequentes Marktversagen, das ist auch selber schon gut erforscht, es gibt eine eigene Forschungsrichtung in der IT, die sich nur mit diesem Marktversagen in der IT-Sicherheit beschäftigt, die Economics of IT-Security. Dann sehen wir ein Politikversagen. Gerade die Entscheider haben keine Lust, sich mit diesem IT-Zeug zu beschäftigen. Wenn sie es tun oder versuchen, haben sie plötzlich Horden von Lobbyisten um sich rum, die ihnen alle etwas anderes erzählen. Wenn Sie selber kein Experte sind, können Sie das nicht beurteilen – und dann wollen Sie natürlich keine mehrstelligen Millionenbeträge ausgeben. Das ist verständlich, bringt uns aber natürlich nicht weiter. Man versucht dann eher, den „most common denoninator“ zu finden, also das, worauf sich alle einigen können, und dabei möglichst wenig Geld auszugeben. Das hilft aber nicht bei der Behebung des Problems. Und dann haben wir eben auch ein kognitives Versagen. Wir verstehen dieses Problem noch nicht, wir haben viel zu wenig Daten, viel zu wenig Fälle sind publik und auch in der Wissenschaft gibt es leider noch viel zu wenig Geld und viel zu wenig Möglichkeiten, um entsprechende Angriffe zu verstehen. Das wäre also das erste, was man tun sollte. Man muss das Problem viel besser verstehen. Und wenn man das dann hat, kann man auch strategisch vorgehen. Wenn man eine Priorisierung hat, wenn man die Risiken und die Probleme kennt und nicht nur die technischen Probleme, sondern auch die Probleme in Wirtschaft, Politik und Wissenschaft und man kann die alle adressieren und richtig klar formulieren, dann kann man erst eine Strategie formulieren.

Meine persönliche Strategie gegen diese Angreifer, insbesondere, weil Strafverfolgung nichts nützt und weil IT-Sicherheit in diesem Bereich so furchtbar defizitär ist, ist Hochsicherheits-IT. Das ist so meine persönliche Idee. Es gibt sehr viel, was man da tun kann, sehr viel wird auch schon getan. Mikrokerne zum Beispiel, da haben wir verschiedene Projekte, man kann aber auch noch mehr tun: Harvardarchitekturen, sichere Sprachen, solche Dinge. Eine Trusted Hardware Foundry wäre ebenfalls wichtig für Deutschland oder für Europa. Das ist eine abgesicherte Chipfabrik, so dass man eine vertrauenswürdige Hardwareproduktion hat.

In der Vergangenheit hat man immer gesagt, das ist zu sperrig, zu teuer. Aber die Forschung ist inzwischen so weit, dass das alles nicht mehr stimmt. Außerdem ist das eine vollständig privacy-freundliche, freiheitsfreundliche Lösung dieser ganzen Probleme. Der Widerspruch zwischen Freiheit und Sicherheit löst sich hier völlig auf. Wenn Sie den Computer so sicher machen, dass die Angriffe darauf so teuer werden wie in den 80er Jahren, dann haben Sie das Problem aus dieser Richtung gelöst und dann brauchen Sie keine Überwachung mehr, denn der Akteur, der dann bei der Kostenstufe noch einsteigen kann, den identifizieren Sie auch nicht. Das heißt, das ganze Überwachungsproblem ist passé. Sie brauchen das immer noch für die Kleinkriminellen usw., aber für diese besonders guten Kriminellen und Staaten können Sie sich das sparen. Dann gibt es inzwischen auch viele Hochsicherheitssysteme, die

hochperformant sind, laientauglich sind, usable sind, die messbar sind und die auch ökonomisch sind. Dafür haben wir ausreichend Nachweise. D.h. die ganzen Argumente von gestern, dass es nicht funktioniert, dass es nicht geht, dass es zu teuer ist, die gibt es alle nicht mehr und wir sollten uns das vielleicht einfach noch mal überlegen, ob wir das nicht so priorisieren wollen. Das wäre eine „disruptive“ Innovation, die das Problem in einem Top-Down-Ansatz – das schwierige Problem zuerst und dann erst die kleineren. Das ist besser als konservativ und inkrementell von den kleinen Problemen nach oben zu arbeiten. Denn das hat uns nicht weitergebracht die letzten Jahre, das müssen wir ganz klar sagen.

Es braucht aber ein politisches Engagement, um das in Gang zu bringen. Man braucht also eine starke Regulierung, muss klare Anreize schaffen. Man muss vor allen Dingen auch ein Investitionsklima schaffen, das haben wir im Silicon Valley gesehen. Da gibt es so ein „Triangle“. Es gibt die Venture Capital Investoren, dann gibt es die Forschung an der Uni in Stanford, dann gibt es die Startups, die spielen sich alle drei gegenseitig zu. Die Uni hat eine gute Idee, dann gibt es ein Startup, dann kommen die Venture Capital-Jungs, geben Geld hinein und dann wird das ein großes Ding. Bei uns könnte man noch den Staat dazu nehmen, da sind die Kalifornier natürlich sehr zurückhaltend. Das wäre für uns noch eine gute zusätzliche Maßnahme, um so ein Quadrat aufzubauen. So etwas brauchen wir. Wir brauchen Investoren, wir brauchen Innovationen, wir brauchen Startups und wir brauchen den Staat bei uns, um das aufzubauen.

Was wir nicht tun sollten, wäre frühreif rauszugehen. Wir sehen jetzt viele Unternehmen, die sagen: hier, made in Germany, super IT-Security usw. – aber das ist nur das gleiche alte Zeug. Ich habe schon ein paar britische Kollegen getroffen, die haben gesagt, wir haben das deutsche Zeug einmal gekauft und getestet und die haben ja auch nichts auf der Pfanne. Das wollen wir nicht als Ruf im Ausland. Das ist nicht strategisch klug.

Das wäre also meine Vision, was man tun könnte und das wäre auch eine Win-Win-Win-Situation. Wir hätten einen maximalen Sicherheitsgewinn, wir hätten einen maximalen Gewinn an Freiheit und Datenschutz, und wir hätten mit Sicherheit, wenn wir das als Industrie aufbauen, als Exportindustrie, auch einen großen Gewinn an Wohlstand. Und damit vielen Dank für Ihre Aufmerksamkeit.

Digitale Bedrohungen

Alexander Geschonneck

Dem Begriff „Digitale Bedrohungen“ kann eine Vielzahl an Bedrohungen zugeordnet werden. Beispiele stellen das Ausspähen von Daten (Cyberspionage), Computersabotage und die Verletzung von Urheberrechten dar. Ein IKT-System ist hier Ziel, Werkzeug oder beides; die Bedrohungen können für Unternehmen und Behörden wie auch für Privatpersonen bestehen. Die Angriffspunkte sind entsprechend vielfältig und umfassen beispielsweise Computer, Smartphones, Industrieanlagen sowie den Bereich Connected Home.

Digitale Bedrohungen sind ebenfalls im Bereich der Wirtschaftskriminalität relevant, man spricht hier von e-Crime. Wir verstehen darunter die Ausführung von wirtschaftskriminellen Handlungen unter Einsatz von Informations- und Kommunikationstechnologien (IKT) zum Schaden einer Einzelperson, eines Unternehmens oder einer Behörde. Neben einer Schädigung von Sachwerten und einer Verletzung von Verfügungsrechten an immateriellen Gütern können diese auch aus einer Beeinträchtigung von auf den Systemen basierenden Geschäftsprozessen eines Unternehmens resultieren.

Einen Blick auf e-Crime aus kaufmännischer Unternehmensperspektive gibt die aktuelle KPMG e-Crime-Studie über Schäden in der deutschen Wirtschaft. Gemäß der Studie war ein Viertel der befragten 500 deutschen Unternehmen in den vergangenen zwei Jahren von e-Crime betroffen, wobei in der Risikowahrnehmung der befragten Unternehmen eher die anderen Unternehmen und nicht das eigene von e-Crime betroffen sind. Computerbetrug und das Ausspähen oder Abfangen von Daten werden von Betroffenen als häufigste Deliktstypen genannt. Die Bedrohungen werden zunehmend länderspezifisch gesehen.

Prävention als umfassende Maßnahme gegen interne und externe Bedrohungen

Es darf jedoch nicht außer Acht gelassen werden, dass die überführten Täter oft im unmittelbaren Umfeld der Unternehmen zu finden sind. Im Rahmen der Prävention müssen folglich Bedrohungen von innen wie außen berücksichtigt werden.

Die Absicherung gegen Innentäter muss dabei einem zunehmend komplexen und vernetzten Umfeld der Unternehmen Rechnung tragen und auch Personen des mittelbaren Umfeldes berücksichtigen, wie Mitarbeiter eines beauftragten Cloud Computing- oder sonstigen Outsourcing-Dienstleisters oder von Lieferanten. Neben der Vergabe und regelmäßigen Prüfung adäquater Zugriffsberechtigungen muss hierbei auf eine sorgfältige Auswahl und Vertragsgestaltung von Dienstleistern und Mitarbeitern geachtet werden.

Unachtsamkeit als größte Schwachstelle

Es gilt zudem zu beachten, dass nicht immer eine kompliziert auszunutzende Schwachstelle als Ursache zu sehen ist. Vielmehr sehen Unternehmen nach wie vor die Unachtsamkeit von Mitarbeitern als größte Schwachstelle im Bereich e-Crime an. Präventionsmaßnahmen sollten daher auch regelmäßige Schulungs- und Sensibilisierungsmaßnahmen umfassen, die die Wahrscheinlichkeit unabsichtlich durch Mitarbeiter hervorgerufener Schwächen im Bereich der IT-Sicherheit deutlich reduzieren können. Schulungs-Umfang und -Taktung müssen hierbei der Rolle der Person angepasst werden. Weiterhin müssen im Rahmen der Präventionsmaßnahmen neue Technologien berücksichtigt werden; so sollte geprüft werden, ob hinsichtlich der Nutzung sozialer Netzwerke in angemessenem Umfang formelle Regelungen getroffen werden sollen. Wichtig ist auch die Verbesserung der Meldung und Eskalation von Sicherheitsvorfällen innerhalb der Unternehmen, da „Kommissar Zufall“ immer noch die häufigste Meldequelle darstellt.

Verschiedene Faktoren können (Cyber-)Kriminalität begünstigen

Faktoren, die (Cyber-)Kriminalität begünstigen, zeigt das sogenannte „Fraud Triangle“ des US-amerikanischen Soziologen und Kriminologen Donald R. Cressey auf. Es umfasst die Faktoren Gelegenheit, Motivation und Rechtfertigung.
Der Faktor Gelegenheit wird dabei auf der Organisationsebene verortet. Schwächen interner Kontrollsysteme führen zu fehlenden oder unzureichenden Kontrollen, die von Tätern als Gelegenheit wahr genommen werden. Motivation und Rechtfertigung hingegen ordnet Cressey der Personenebene zu. Beeinflussend wirkt hier das Wertesystem des Unternehmens und der sogenannte „Tone from the top“.
Der Faktor Motivation kann dabei durch die Persönlichkeit sowie finanzielle und tätigkeitsbezogene Gegebenheiten beeinflusst werden. So kann eine problematische finanzielle Situation eines Mitarbeiters Motivation sein, kriminelle Taten zu begehen. Der Faktor Rechtfertigung wird durch die Persönlichkeit, aber auch unternehmenskulturell beeinflusst. So kann eine als problematisch empfundene Unternehmenskultur als Rechtfertigung krimineller Taten dienen.

Beispiele aus dem Innenleben eines Unternehmens

In der forensischen Praxis trifft man auf eine Vielzahl von Beispielen im Kontext digitaler Bedrohungen. Ein Beispiel stellt die Manipulation von Warenwirtschaftssystemen dar. Gewähren die eingerichteten Benutzerrechte in Warenwirtschaftssystemen für Nutzer zu umfangreiche Rechte, können diese beispielsweise unbemerkt Lagerbestände manipulieren oder eine Zahlung an einen fiktiven Lieferanten ohne Lieferung durchführen.
Eine Detektion kann anhand einer Überprüfung von Massendaten mittels Datenanalysen erfolgen. Ebenso können Analysen des Berechtigungssystems Schwächen aufzeigen, die beispielweise die vollumfängliche Durchführung von Transaktionen durch eine Person, aufgrund einer fehlenden Funktionstrennung, ermöglichen.

Als weiteres Beispiel können externe Callcenter oder andere externe Dienstleister genannt werden, die aufgrund der vorhandenen umfangreichen vertraulichen Daten ein potentielles Ziel von Datendieben darstellen. Neben einem Diebstahl durch externe Personen ist hier insbesondere auch an einen Diebstahl von Datensätzen durch Mitarbeiter zu denken. Die Daten werden dann zum Beispiel weiterverkauft oder vom Täter im Kontext eines Identitätsmissbrauchs selbst genutzt.
Im Rahmen der Detektion ist zu beachten, dass ein Zugriff auf die vertraulichen Daten für bestimmte Mitarbeitergruppen zur Arbeitserledigung erforderlich ist. Der Zugriff auf vertrauliche Daten muss entsprechend der gegebenen Erfordernisse definierten Personengruppen grundsätzlich erlaubt sein. Es ist jedoch zielführend, dass Systeme zum Zugriff auf diese Daten einen unbegründeten Zugriff auf eine hohe Anzahl von Datensätzen verhindern oder diesen zumindest melden.
Es gibt zahlreiche weitere Beispiele. So seien hier noch das Rogue Trading, das heißt die Manipulation von Handelsplattformen im Bereich des Investment- oder auch Commodity-Tradings sowie Angriffe auf Zahlungsverkehrssysteme genannt.

Evolution von Bedrohungen

Ist mittels geeigneter Präventionsmaßnahmen ein angestrebtes Schutzniveau erreicht, darf dieses nicht als abschließende Zielerreichung angesehen werden. Perspektivisch kann das Schutzniveau vielmehr durch die Weiterentwicklung bestehender Bedrohungen und die Entstehung neuer Bedrohungen sinken.
So ist eine Professionalisierung der Angriffe und der hierfür genutzten Werkzeuge zu beobachten. Ein Geschäftsmodell stellt es beispielsweise dar, hochentwickelte Angriffswerkzeuge zu erstellen und Dritten gegen eine Gebühr zur Verfügung zu stellen. Dies geht so weit, dass „betriebsfertige“ Lösungen als Cracking-as-a-Service angeboten werden. Ein Beispiel stellt das Malware-Toolkit „Blackhole“ dar.
Mittels dieser Lösung können Dritte auf gehackten oder für diesen Zweck extra erstellten Webseiten Malware einbringen und so Webseitenbesucher mit dieser Malware infizieren. Hierzu prüft „Blackhole“ das System des Besuchers auf Sicherheitslücken und nutzt gefundene Lücken aus. Der Angreifer kann bei Erfolg beispielsweise Daten auf dem Rechner des Opfers ausspähen oder die Rechner in Form eines Botnetzes zusammenfassen. „Blackhole“ verfügt über eine grafische Bedienoberfläche, die Nutzern unter anderem diverse Konfigurationsmöglichkeiten sowie eine Auswertung hinsichtlich erfolgreicher Angriffe zur Verfügung stellt.Die Detektion eines solchen Angriffs kann (etwas) verbessert werden, wenn Unternehmen mehrere Malware-Scanner kombinieren, um die Erkennungsrate zu steigern.

Botnetze

Beispielsweise als Resultat eines gezielten Angriffs mittels des vorgenannten „Blackhole“-Toolkits kann ein Angreifer Zugriff auf eine Vielzahl infizierter Rechner erhalten und diese zu einem sogenannten Botnet zusammenführen. Bei Botnetzen handelt es sich um zentral gesteuerte, mit Malware infizierte Rechner.
Botnetzbetreiber vermieten Ihre Botnetze oftmals an Dritte, die damit bspw. andere Rechner oder Rechnernetze überlasten können (DDoS) oder SPAM versenden. Mittels der Drohung mit einem DDoS-Angriff kann digitale Erpressung ein Geschäftsmodell darstellen. Eine Detektion ist erst zum Zeitpunkt eines Angriffs möglich, sollte es nicht zur Androhung eines Angriffs im Rahmen einer Erpressung kommen. Gegenmaßnahmen sind aufgrund der hohen Zahl angreifender Rechner aufwändig und betreffen insbesondere die Filterung unerwünschter Anfragen. Es verbleibt so primär die normale Detektion der befallenen Bot-Systeme.

Gezielte Angriffe auf Unternehmen und Datenbestände

Neben ungezielten Angriffen ist eine steigende Zahl gezielter Angriffe auf Unternehmen und Datenbestände zu beobachten. Bei diesen sogenannten „Targeted Attacks“ werden ausgesuchte Ziele angegriffen und ausgesuchte Informationen erbeutet. Hierbei kommt es zum Teil zu sogenannten „Advanced Persistent Threats“ (APTs), das heißt zu anhaltenden Angriffen. Üblicherweise gehen APTs nicht von einzelnen Tätern, sondern von Tätergruppen aus. Es wird nicht während eines kurzen Angriffs so viel wie möglich erbeutet, sondern der Zugriff auf das Ziel möglichst lang aufrecht erhalten.
Als Beispiele für gezielte Angriffe können u. a. der Angriff auf das belgische Telekommunikationsunternehmen Belgacom ab dem Jahr 2010 sowie der Angriff auf die Sicherheitsfirma Bit9 durch die Hackgruppe „Hidden Lynx“ genannt werden. Letzterer diente als Vorbereitung für Angriffe auf Kunden von Bit9 in der Rüstungsindustrie. Es wird jedoch nicht allein auf die Methoden des Crackings zurückgegriffen. Zusätzlich wurden bekannte Angriffsmethoden in Richtung gezielter Angriffe modifiziert.

So wird beispielsweise das bekannte Phishing als „Spear Phishing“ zu einer gezielten Angriffsmethode. Hierbei werden Methoden des Social Engineering gegen ausgesuchte Personen wie Mitarbeiter mit Administrationsrechten oder Mitglieder der Führungsebene eines Unternehmens (sog. „Whaling“) eingesetzt. Für Angreifer verspricht dieses Vorgehen eine höhere Erfolgsquote, ein Profiling ist oft recht einfach mittels beruflicher und privater sozialer Netzwerke möglich. Angreifer können durch diese minimal invasiven Angriffe länger unentdeckt bleiben, als wenn Sie mit tausenden Phishingmails an den Sicherheitssystemen abprallen. So konnten mittels Zugangsdaten, die durch Phishing erlangt wurden, Angreifer im Jahr 2011 in den Handel mit Emissionszertifikaten eingreifen.
Eine automatisierte Detektion dieser Angriffe ist aufgrund wechselnder Texte und gefälschter Absender schwierig. Es ist daher eine Sensibilisierung der Mitarbeiter hinsichtlich der Methoden des Social Engineering zu empfehlen.

Ein Angriffziel stellen zudem Industriesteuerungsanlagen dar. Diese verfügen oftmals über einen Anschluss an das Internet, bspw. zur Fernwartung. Erhält ein Angreifer Zugriff auf eine Industriesteuerungsanlage, kann dieser genutzt werden, um Informationen zu erlangen und die Anlagen zu manipulieren, zu beschädigen oder zu zerstören. Für diese Anlagen sollte daher genau geprüft werden, ob ein Anschluss an das Internet oder damit verbundene Netzwerke erforderlich ist.

Eine Sicherheitslücke kann schnell eine hohe Anzahl dieser Systeme verwundbar machen. So wies die Steuerungssoftware eines Hersteller im Jahr 2012 eine Sicherheitslücke auf, mittels derer eine Manipulation der Steuerung zugehöriger Systeme möglich war. Allein diese Steuerungssoftware wurde von über 250 Geräteherstellern genutzt, die u. a. Firmen im Energie- und Militärbereich beliefern.

Eine Suche mittels der auf Server spezialisierten Suchmaschine „Shodan“ nach Systemen, deren Statusmeldungen unter anderem den für Steuerungstechnik charakteristischen Term „SCADA“ (Supervisory Control and Data Acquisition) zurückliefern, listet eine Vielzahl von Systemen auf. Wenngleich bereits länger bekannt ist, dass eine solche Suche einfach möglich ist, finden sich unter diesen Systemen auch heute einige Systeme, die diverse Informationen ohne Anmeldung zur Verfügung stellen. Wenngleich diese Informationen keine Steuerung der Systeme ermöglichen, können beispielsweise Informationen zu vorhandenen Benutzerkonten Angriffe auf die Systeme erleichtern.

Entstehung neuer Bedrohungen durch neue Technologien

Die zunehmende Nutzung neuer Technologien hat auch zur Entstehung neuer Bedrohungen geführt. So haben sich beispielsweise die Infektionswege von Malware im Zeitverlauf geändert. Zu Anfang stellten oftmals externe Datenträger das Transportmedium für Malware dar. Kam es zuerst zu einer Installation von Bootsektor-Viren durch infizierte Floppydisks, folgte eine hohe Zahl von Infektionen mittels des Anschlusses von externen Datenspeichern wie externen Festplatten und USB-Sticks. Die zunehmende Verbreitung von E-Mail hatte später auch zu einem massenhaften Versand von Malware als Anhang von E-Mails zu Folge, die zu einer Infektion durch Ausführung von E-Mail-Anhängen führte.

Inzwischen stellen Drive-By-Downloads und eine Ansprache durch soziale Netzwerke ein Einfallstor für Infektionen dar. Es kommt dabei zu einer unbemerkten Installation von Malware, die lediglich den Besuch einer infizierten Webseite erfordert und Sicherheitslücken bspw. im Microsoft Internet Explorer und Adobe Flash ausnutzt. Als Verbreitungsmedium dienen gehackte Webseiten oder Accounts in Social Networks; da es sich oftmals um gehackte seriöse Accounts und Webseiten handelt, ist die Gefahr einer Infektion besonders hoch.

Sicherheitsmaßnahmen wie Malware- und Webfilter reichen bei dieser Bedrohung oftmals nicht aus, da die URLs und Signaturen der Malware sich sehr häufig ändern. Es ist daher auch hier sehr wichtig, Mitarbeiter zu sensibilisieren. Weiterhin werden mobile Endgeräte mit steigender Leistungsfähigkeit zu interessanten Zielen. Funktionalitäten wie GPS-Ortung ermöglichen neue Angriffsszenarien wie beispielsweise eine heimliche Verfolgung der Nutzer; die Installation von Apps birgt das Potential der Installation unerwünschter Funktionalitäten. Es gibt Smartphoneplattformen, bei denen davon ausgegangen werden kann, dass die Mehrheit der auf dem Markt befindlichen Geräte erfolgreich kompromittiert wurden.
Für Unternehmen entsteht in diesem Fall insbesondere dann eine Bedrohung, wenn sie dem Trend zu „Bring-Your-Own-Device“ (BYOD) folgen und als Folge auch privat genutzte Endgeräte im Unternehmensnetzwerk aktiv sind und Zugriff auf sensible Daten damit erfolgen soll. Fehlt ein adäquates Sicherheitskonzept, können Schädlinge durch Bring-Your-Own-Device ihren Weg in das Firmennetzwerk finden.

Die mobile Telekommunikation wird als risikobehaftetste IT-Anwendung für Unternehmen angesehen. Allein für das erste Quartal 2013 meldet F-Secure 149 neue Malwares für mobile Endgeräte; 136 davon zielen auf das von Google entwickelte Betriebssystem Android ab.

Cloud Computing

Auch die zunehmende (private und geschäftliche) Nutzung von Public und Private Clouds bringt Bedrohungen mit sich. Problematisch ist hierbei, dass das Sicherheitsniveau der Cloud-Dienste nicht immer feststellbar ist. Weiterhin wird eine Detektion von Angriffen in vielen Fällen durch den Cloud-Dienstleister erfolgen müssen. Auffälligkeiten sollten folglich dem Dienstleister gemeldet werden, um die Detektion eines Angriffs zu unterstützen.

Beispiele für erfolgreiche Angriffe stellen der Zugriff auf Dropbox-Konten durch Dritte nach der Kompromittierung eines Mitarbeiter-Accounts im Jahr 2012 sowie der Zugriff auf Evernote-Passwort-Hashes von 50 Millionen Nutzern durch Dritte im Jahr 2013 dar. Das Cloud Computing kann neben einem Ziel auch ein Werkzeug für Cyberkriminelle darstellen. Sie können die schnell verfügbare hohe Rechenleistung von Cloud-Diensten beispielsweise nutzen, um Passwörter zu „knacken“.

Adäquate Prävention als Wettbewerbsvorteil

Es kann festgehalten werden, dass die Zahl und Intensität digitaler Bedrohungen weiter zunimmt. Neben der Evolution bestehender Bedrohungen entstehen neue Bedrohungen, deren Wirkung aufgrund der Neuheit der damit verbundenen Technologien noch nicht ausreichend abgeschätzt werden kann. Die Täter, deren kommerzielles Interesse sehr groß ist, werden immer weiter versuchen, lange unerkannt zu bleiben. Die zunehmende Professionalisierung digitaler Bedrohungen führt zu einer Ausweitung der Gruppe potentieller Täter sowie einer zunehmend schwierigen Erkennung von Angriffen.

Die zunehmende Nutzung sozialer Netzwerke, die Internetnutzung mit mobilen Endgeräten sowie das Cloud Computing eröffnen neue Möglichkeiten für Angreifer. Neue Technologien sollten daher nicht unvoreingenommen genutzt und ggf. reguliert werden. Zunehmend gezielte Angriffe führen zu höheren Erfolgsquoten für Angreifer und erfordern eine stärkere Sensibilisierung von Mitarbeitern.

Für Unternehmen wird eine umfangreiche Prävention daher zunehmend einen Wettbewerbsvorteil darstellen. Unverzichtbar ist jedoch auch eine Zusammenarbeit von Unternehmen, beispielsweise bei der Erkennung branchenspezifischer Angriffe. Erfolgreiche Angriffe können zu erheblichen Kosten führen, bei denen auch Reputationsschäden nicht außer Acht gelassen werden dürfen.

Die Prävention darf dabei nicht auf die Umsetzung von Maßnahmen zur Erkennung von Angriffen beschränkt werden. Zusätzlich muss bereits vor einem Schadensfall geklärt werden, ob ein Unternehmen gewappnet ist, im Fall der Erkennung eines aktiven Angriffs diesen einzudämmen und aufzuklären. Da Angriffe (auch erfolgreiche) nicht unvermeidlich sein werden, werden die Unternehmen auf Dauer erfolgreich sein, die angemessen reagieren können.

Rechtliche Herausforderungen bei der Bekämpfung von Cybercrime

Dr. Wolfgang Bär

1. Einleitung

Digitale Techniken aller Art bestimmen mehr und mehr unser Leben. Das Internet ist schon heute aus unserem Alltag nicht mehr wegzudenken. Das Einkaufen im Netz, die Informationssuche, das Anschauen von Filmen und Videos, das Chatten mit Freunden ist für viele zur Selbstverständlichkeit geworden. Dies gilt noch verstärkt für die junge Generation, die sich oft täglich in sozialen Netzwerken wie Facebook und Google+ bewegt. Nicht umsonst gelten die jungen Leute als "digital natives", während wir uns mit der etwas geringschätzigen Bezeichnung der "digital immigrants" abfinden müssen.

Dabei erfasst das Internet immer weitere Lebensbereiche. Die Netze und Anwendungen werden ständig schneller. Die Halbwertszeit des Stands der Technik wird zunehmend kürzer. Fortlaufend kommen neue Geräte wie Smartphones oder Tablet-PC auf den Markt und ersetzen zunehmend bisherige Personalcomputer. Die mobile Erreichbarkeit über das Netz und der mobile Zugriff auf das Internet von überall aus werden immer wichtiger.

Dabei darf das Internet aber kein rechtsfreier Raum sein – und ist es selbstverständlich auch nicht. Das Recht der analogen Welt wird im Cyberspace nicht außer Kraft gesetzt. Die große Herausforderung besteht allerdings darin, es an die digitalen Besonderheiten anzupassen und seine tatsächliche Durchsetzbarkeit zu gewährleisten. Das Internet eröffnet jedem von uns unendliche Möglichkeiten für alles, was wir uns nur vorstellen können. Leider aber auch dem Straftäter für seine kriminellen Interessen. Es verwundert daher nicht, dass es in den letzten fünf Jahren hier zu einer Verdoppelung der in der Kriminalstatistik registrierten Verfahren gekommen ist. Dabei ist die Dunkelziffer aber sehr hoch, da in der Statistik viele Fälle - etwa Straftaten mit Auslandsbezug - gar nicht erfasst sind. Kennzeichnend ist dabei die Tendenz zu immer gefährlicheren und häufigeren Großangriffen auf Informationssysteme im öffentlichen und privaten Sektor. Gleichzeitig sind die Angriffe mit immer ausgefeilteren Methoden verbunden, bei denen kriminelle Handlungen in verschiedenen Stufen erfolgen.

In Bayern sieht das Konzept zur Bekämpfung von Internetkriminalität eine Zentralstellenfunktion mit meinem Referat für Internetkriminalität innerhalb der Abteilung E für Strafrecht und Internetkriminalität vor. In organisatorischer Hinsicht wurden bei allen 22 Staatsanwaltschaften und bei den drei Generalstaatsanwaltschaften in Bayern Sonderdezernate bzw. IT-Ansprechpartner eingerichtet, die Verfahren in diesem Deliktsbereich grundsätzlich vor Ort bearbeiten. In speziellen Verfahren besteht jedoch nach § 145 GVG die Möglichkeit, Einzelzuweisungen an eine Staatsanwaltschaft mit Wirtschaftsabteilung pro Bezirk der Generalstaatsanwaltschaften München, Nürnberg und Bamberg vorzunehmen. In den letzten Jahren wurde eine zielgruppenorientierte Aus- und Fortbildung von Staatsanwälten und Richtern umgesetzt und weiter fortgeführt. Im Rahmen des Wissensmanagements erfolgt derzeit die Überarbeitung und Verbesserung der zentralen Informationsplattform im Intranet der Justiz.

Im Folgenden sollen die wichtigsten strafrechtlichen Problemstellungen dieser neuen digitalen Welt aufgegriffen werden, um aufzuzeigen, ob zum einen alle neuen Begehungsformen durch das materielle Strafrecht erfasst werden und ob zum anderen die Strafverfolgungsbehörden mit ausreichenden Mitteln ausgestattet sind, um Straftaten mit den neuen Technologien aufdecken und angemessen verfolgen zu können. Dabei werden vor allem auch die Ergebnisse des unter meiner Leitung von der Unterarbeitsgruppe "Cybercrime" erarbeiteten Abschlussberichts berücksichtigt, die von der gemeinsamen Arbeitsgruppe Polizei/Justiz (GAG) eingesetzt wurde.

2. Materielles Strafrecht

Die rasante technische Entwicklung bei modernen IT-Systemen eröffnet den Straftätern immer neue Möglichkeiten für Straftaten. So haben sich in den letzten Jahren etwa mit den Schlagwörtern Phishing, Pharming, Skimming, Ransomware und den Bot-Netzen zahlreiche neue strafrechtliche Begehungsformen ergeben.

Dies wirft zunächst die Frage auf, welche Delikte überhaupt vom Begriff Cybercrime erfasst werden sollten. In Übereinstimmung mit der Bund-Länder-Arbeitsgruppe und den Beschlüssen der AG Kripo und des AK II bezieht sich Cybercrime auf alle Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten sowie auf solche Straftaten, die mittels dieser Informationstechnik begangen werden. Cybercrime umfasst damit auf der einen Seite "altbekannte" Straftaten, die anstelle in der realen Welt nun in der digitalen begangen werden, aber auf der anderen Seite auch eine Vielzahl von neuen Begehungsweisen, die durch die Informationstechnik erst möglich geworden sind.

Auf diese neuen Herausforderungen hat der Gesetzgeber auf nationaler Ebene mit dem 41. Strafrechtsänderungsgesetz vom 07.08.2007 reagiert und eine Reihe von Straftatbeständen, die seit der ersten Reform durch das 2. WiKG von 1986 quasi den Kernbereich des Computerstrafrechts bildeten, novelliert und ergänzt.

Im Folgenden sollen daher die einzelnen Schutzgegenstände dieser Strafnormen kurz dargestellt und etwaige Schutzlücken im materiellen Recht aufgezeigt werden. Dabei ist auch bereits zu berücksichtigen, inwieweit sich durch die im Juli 2013 verabschiedete Richtlinie 2013/40/EU des Europäischen Parlaments und des Rats über Angriffe auf Informationssysteme und zur Ersetzung des bisherigen Rahmenbeschlusses 2005/222/JI gesetzgeberischer Handlungsbedarf besteht. Die am 12.08.2013 im Amtsblatt der EU verkündete Richtlinie ist bis 04. September 2015 in nationales Recht umzusetzen.

a) Aktueller strafrechtlicher Schutz bei Cybercrime

Insgesamt muss im Blick auf die jeweiligen Schutzgüter der einzelnen denkbaren Angriffsformen zwischen folgenden Strafnormen unterschieden werden:

- Schutz der Geheimhaltung von Daten (§§ 202a - 202c StGB)
- Schutz der Datenintegrität (§§ 303a, 303b StGB)
- Schutz vermögens- und rechtserheblicher Vorgänge mit Daten (§§ 263a, 269 StGB)
- Schutz des bargeldlosen Zahlungsverkehrs (§§ 152a, 152b StGB)
- Schutz von Geschäfts- und Betriebsgeheimnissen (§ 17 Abs. 2 UWG)
- Schutz des geistigen Eigentums (§§ 106 ff. UrhG)
- Schutz von personenbezogenen Daten (§§ 43, 44 BDSG)

aa) Schutz der Geheimhaltung von Daten

Nach der alten Fassung des **§ 202a StGB** war eine Strafbarkeit durch das bloße „Knacken“ eines Computersystems unter Überwindung von Sicherungseinrichtungen noch nicht eingetreten. Vielmehr musste sich der Täter zur Tatbestandsverwirklichung erst Daten „verschafft“ haben. Damit galt bisher das Überwinden des Schlosses als straflos, das Öffnen der Tür aber nicht mehr. Diese Lücken wurden beseitigt. Zur Tatvollendung genügt nun bereits das Verschaffen des Zugangs zu den Daten. Damit erfasst § 202a StGB als „elektronischer Hausfriedensbruch“ - auch das bisher überwiegend als straflos angesehene reine „Hacking“. Der Tatbestand ist bereits bei einer konkreten Gefährdung der Vertraulichkeit von Daten erfüllt, wenn der Täter die Möglichkeit hat, auf Daten zuzugreifen, was durch die Zugangssicherung gerade verhindert werden soll. Damit wurde hier eine aus Sicht der Praxis wünschenswerte Klarstellung erreicht. Der Tatbestand deckt auch aktuelle Angriffsszenarien ab. Dies gilt etwa für unbemerkt in das angegriffene DV-System eingeschleuste sog. Trojaner aller Art, mit deren Hilfe Zugangsdaten auf dem Rechner ausgespäht werden oder der Täter sich Zugang zu Daten verschaffen kann (z.B. Keylogger) ebenso wie für den Zugriff auf das fremde System durch eine „Umgehung“ der Zugangssicherung etwa durch Trapdoor, Backdoor, Exploits.

Vor der 2007 war ein Zugriff auf Daten während der Übermittlungsphase nur dann strafbewehrt, wenn Daten – etwa durch Verschlüsselung - besonders gesichert waren. Durch **§ 202b StGB** wird nun mit der 1. Alternative das unbefugte Sichverschaffen von nicht für den Täter bestimmten Daten aus einer nichtöffentlichen, also nicht für einen größeren Personenkreis gedachten Datenübermittlung oder in der 2. Alternative aus einer elektromagnetischen Abstrahlung einer DV-Anlage unter Anwendung technischer Mittel sanktioniert. Damit richtet sich die Norm klar gegen alle Formen des Abfangens von Daten durch "Sniffing" oder "Man-in-the-middle"-Angriffe bei der Online-Kommunikation. Die Beschränkung der Tatbegehung auf technische Mittel hat praktisch keine Bedeutung, da ein Zugriff auf Informationen während der Übermittlungsphase anders nicht vorstellbar ist. Als lex specialis dazu ist die nebenstrafrechtliche Regelung des §§ 148 Abs. 1 Nr. 1 i.V.m. 89 Satz 1 TKG mit einer eigenen Strafnorm beim Abhören von Funkanlagen zu beachten. Dazu zählt auch die kabellose Datenübertragung über WLAN, die zwischen Client und Access-Point (Router) stattfindet. Das Einwählen in ein offenes WLAN ist aber kein Abhören i.S.d. § 148 TKG.[1]

[1] Vgl. LG Wuppertal, K&R 2010, 838.

Mit der umstrittenen Regelung des **§ 202c StGB** werden in der Form eines abstrakten Gefährdungsdelikts bestimmte besonders gefährliche Vorbereitungshandlungen zu Straftaten nach §§ 202a und 202b StGB sanktioniert. Die Regelung entspricht den Vorgaben des bisherigen EU-Rahmenbeschlusses sowie Art. 7 der neuen EU-RL über Angriffe auf Informationssysteme. Durch den Verweis in § 303a Abs. 3 und § 303b Abs. 5 StGB auf § 202c StGB werden auch Vorbereitungshandlungen zur Datenveränderung und Computersabotage in den Anwendungsbereich dieser Norm einbezogen. Der Tatbestand beinhaltet zwei sehr unterschiedliche Tatbestandsalternativen:

§ 202c Nr. 1 StGB erfasst Passwörter oder sonstige Zugangscodes, die den Zugang zu Daten ermöglichen. Die Regelung gilt damit für das erfolgreiche Offline-Ausspähen von Passwörtern ebenso wie für die Weitergabe von Zugangskennungen an Dritte (z.B. durch Veröffentlichung auf einer Webseite), denn die Vorbereitung setzt - anders wie die eigentliche Haupttat - gerade keinen Einsatz technischer Mittel voraus. Insoweit nicht strafbar sind aber etwa Hinweise im Internet über Sicherheitslücken in fremden Computersystemen. Die Regelung erfasst aber auch eine Weitergabe oder einen Handel mit entsprechenden Zugangskennungen nur teilweise, so dass es hier einer neuen Strafnorm für die "Datenhehlerei" bedarf.

Demgegenüber sanktioniert **§ 202c Nr. 2 StGB** die Weitergabe sog. „Hackertools“, deren eigentliches Ziel die Begehung einer Straftat nach §§ 202a, b oder 303a, b StGB ist. Die Regelung gilt nicht nur für professionelle Täter, die für gezielte Attacken gegen Rechner eine spezielle Software entwickeln und verbreiten, sondern auch für alle frei erhältlichen Hacker-Tools, die ohne große PC-Kenntnisse eingesetzt, leicht bedient und für Angriffe auf ungeschützte Rechner eingesetzt werden können. Maßgeblich für die Tatbestandsmäßigkeit ist allein die objektive Zweckbestimmung solcher Programme und nicht deren Eignung oder spezifische Eignung. Erfasst werden damit nur Programme, die mit der Absicht entwickelt oder modifiziert worden sind, um sie zur Begehung der genannten Straftaten einzusetzen. Diese Absicht muss sich auch objektiv manifestiert haben.[2] Sog. Dual-Use-Programme, die sich neben dem Einsatz für schädliche Zwecke auch für Sicherheitstests im eigenen Netz einsetzen lassen, um Schwachstellen zu erkennen und so die Abwehr von Angriffen zu verstärken, werden regelmäßig bereits vom objektiven Tatbestand nicht erfasst. Im Übrigen ist hier im Einzelfall der subjektive Tatbestand als weiteres Korrektiv zu berücksichtigen.

bb) Schutz der Datenintegrität

Der Straftatbestand der Datenveränderung in § 303a StGB, der in Abs. 3 um die Vorbereitungshandlungen nach § 202c StGB erweitert wurde, erfasst alle Manipulationen an unkörperlichen Daten. Ein Datenbestand soll durch diese der Sachbeschädigung nachgebildete Strafnorm vor Veränderungen jeglicher Art bewahrt werden. Obwohl bei § 303a StGB ein einschränkendes Kriterium - wie bei § 303 StGB durch "fremd" - zur Kennzeichnung der rechtlichen Beziehungen des Täters zum Tatobjekt fehlt, besteht Einigkeit darüber, dass der weite Tatbestand einer Präzisierung bedarf. Da eine zivilrechtliche Zuordnung von Informationen zu bestimmten Berechtigten nicht existiert und man von keinem „Dateneigentum“ ausgehen kann, lässt sich eine Datenveränderung nur bejahen, wenn die Daten als Tatobjekt einer fremden Verfügungsbefugnis unterliegen. Dies kann im Einzelfall nur durch entsprechende Fallgruppen beurteilt werden, die Rückschlüsse auf die Datenzuordnung zulassen. Die Tathandlungen des § 303a StGB erfassen mit dem Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten alle relevanten Manipulationsmöglichkeiten zur Datenveränderung, die sowohl durch individuelle

[2] Vgl. BVerfG CR 2009, 673.

Manipulationen oder automatisiert durch Programme begangen werden können. Tatbestandsmäßig ist daher etwa jede Form der Verwendung von Schadsoftware in Form von Viren, Trojanern oder auch durch (Distributed) Denial ofService-Attacken (DoS oder DDoS) ebenso wie durch die Infektion eines Rechners zur weiteren Fernsteuerung im Rahmen eines Bot-Netzes.

Gegenüber § 303a StGB mit den "Daten" ist bei der Computersabotage in § 303b StGB Schutzgegenstand eine Datenverarbeitung. Geschützt ist vom eigentlichen Grundtatbestand des § 303b Abs. 1 StGB nicht mehr nur eine Datenverarbeitung, die für ein Unternehmen, einen Betrieb, sondern nun auch jede Datenverarbeitung, die „für einen anderen von wesentlicher Bedeutung“ ist. Die liegt vor, wenn die jeweilige Aufgabenstellung von der Funktionsfähigkeit der EDV ganz oder überwiegend abhängig ist und dem Computer damit eine zentrale Funktion bei der Lebensgestaltung zukommt. Mit der Tathandlung des § 303b Abs. 1 Nr. 2 StGB, einer Eingabe oder Übermittlung von Daten in der Absicht, einem anderen einen Nachteil zuzufügen, lassen sich auch sogenannte DoS- oder DDoS- Attacken erfassen, mit dem Ziel, einen oder eine Vielzahl von Servern in einem Datennetz arbeitsunfähig zu machen.[3] Wie von Art. 7 der EU-RL zu Angriffen auf Informationsdienste gefordert, sind in § 303b Abs. 2 und 4 StGB bereits zusätzliche Qualifizierungen für die Angriffe gegen die Datenverarbeitung von Unternehmen und in weiteren besonders schweren Fällen vorgesehen. Über § 303b Abs. 5 i.V.m. § 202c StGB können auch Vorbereitungshandlungen dazu sanktioniert werden.

b) Gesetzgeberischer Handlungsbedarf

Durch die derzeitigen materiellen Strafnormen für Cybercrime lassen sich inzwischen die Mehrzahl der aufgetretenen aktuellen Angriffsformen auf Daten und Informationssysteme erfassen. Ein gesetzlicher Handlungsbedarf wird aber - in Übereinstimmung mit dem Abschlussbericht der GAG-Unterarbeitsgruppe Cybercrime - in den folgenden drei Bereichen gesehen:

aa) Datenhehlerei als neuer Straftatbestand (§ 202d-E StGB)

Im Internet hat sich inzwischen ein Schwarzmarkt für rechtswidrig erlangte Daten entwickelt. So können etwa über entsprechende Webportale oder Verkaufsforen der sog. "Underground Economy", die überwiegend auf Servern im asiatischen oder pazifischen Raum gehostet sind, gegen Bezahlung entsprechende Daten erworben werden. Für derartige Fälle besteht bisher kein umfassender strafrechtlicher Schutz. Die Regelung des § 202c Abs. 1 Nr. 1 StGB erfasst zwar grundsätzlich eine Vielzahl von Fallkonstellationen, aber vom Tatobjekt nur digitale Identitäten in Form von Passwörtern und Sicherungscodes. Vor allem aber ist die Regelung nur bei Vorbereitungshandlungen zu §§ 202a, 202b, 303a und 303b StGB anwendbar, nicht aber etwa bei den vermögensrelevanten Taten des Computerbetrugs. Auch die Datenschutzdelikte der §§ 43, 44 BDSG sowie § 17 Abs. 2 Nr. 2 UWG bei Geschäfts- oder Betriebsgeheimnisse greifen hier nur in Einzelfällen.

Vor diesem Hintergrund erscheint es geboten, in der Praxis aufgetretene Strafbarkeitslücken bei der Weitergabe rechtswidrig erlangter Daten und digitaler Identitäten zu schließen. Der Bundesrat hat deshalb einen entsprechenden Gesetzentwurf[4] zur Schaffung eines neuen § 202d StGB beschlossen. Dieser orientiert sich - zurückgehend auf das verfassungsrechtlich

[3] Vgl. LG Düsseldorf, MMR 2011, 624 m. Anm. *Bär*; anders noch vor der Gesetzesreform: OLG Frankfurt, MMR 2006, 547 mit Anm. *Gerke*.

[4] Vgl. BR-Drs. 284/13.

verankerte Recht auf informationelle Selbstbestimmung - am Schutzgut der formellen Verfügungsbefugnis bzw. dem formellen Datengeheimnis desjenigen, der aufgrund seines Rechts an dem gedanklichen Inhalt der Daten über deren Weitergabe oder Übermittlung entscheidet. Gegenüber dem zunächst allein an § 259 StGB angelehnten ersten Arbeitsentwurf ist im aktuellen Gesetzentwurf eine systematische Verortung der Neuregelung im Bereich der Delikte des persönlichen Lebens- und Geheimbereichs vorgesehen und eine enge Orientierung am Datenbegriff des § 202a Abs. 2 StGB.

Tatobjekt sind - in Übereinstimmung mit den §§ 202a ff. StGB - alle nicht unmittelbar wahrnehmbaren Daten gemäß § 202a Abs. 2 StGB. Dieser weite Datenbegriff bedarf aber weiterer Einschränkungen auf allein strafwürdige Fälle. Ausgeklammert bleiben nach § 202d Abs. 2 StGB-E daher solche Daten, die bereits aus allgemein zugänglichen Quellen entnommen werden können (sog. "Alltagsdaten") sowie Daten, an deren Nichtweiterverwendung der Berechtigte kein schutzwürdiges Interesse hat. Als Vortaten der Datenhehlerei kommen neben dem Ausspähen oder Abfangen von Daten auch alle rechtswidrigen Taten wie Diebstahl, Betrug oder Nötigung in Betracht, die der Erlangung von Daten dienen. Damit wird ein umfassender Schutz der formellen Verfügungsbefugnis des Einzelnen über seine Daten sowie des allgemeinen Rechts auf Nichtöffentlichkeit der Kommunikation erreicht. Allein vertragswidrige oder ordnungswidrige Handlungen sind gemäß § 11 Abs. 1 Nr. 5 StGB vom Tatbestand ausgenommen. Die eigentlichen Tathandlungen, die eine abgeschlossene Vortat erfordern, knüpfen an § 202c StGB an. In subjektiver Hinsicht bedarf es neben dem Vorsatz hinsichtlich des objektiven Tatbestandes zur Tatbestandsverwirklichung einer Bereicherungs- oder Schädigungsabsicht als weiterem subjektiven Element, die der Regelung des § 44 Abs. 1 BDSG entspricht. Durch die Schädigungsabsicht werden auch kriminelle Tätergruppierungen mit politischen Zielen erfasst, die regelmäßig keine Bereicherungsabsicht haben dürften. Es ist zu hoffen, dass es hier zu einem zügigen Abschluss des Gesetzgebungsverfahrens kommt, damit die bestehenden Lücken bei der Strafverfolgung alsbald geschlossen werden.

bb) Versuchsstrafbarkeit und Qualifizierungen bei §§ 202a, 202b und 303a StGB

Bisher nicht vorgesehen im Tatbestand der §§ 202a, 202b und 303a StGB sind Qualifikationen für schwerwiegende und breitflächige Angriffe. Wie die Erfahrungen der Praxis zeigen, bestehen hier aber erhebliche Unterschiede beim Unrechtsgehalt der Taten. So können gerade die Rekrutierung von Computersystemen mittels Schadsoftware zu Bot-Netzen sowie das Eindringen in Rechner von großen Firmen und kritischen Infrastrukturen zu einem erheblichen Gefahrenpotenzial oder zu hohen Schäden im Einzelfall führen. Entsprechend dem Wortlaut des § 303b Abs. 3 StGB sollten daher auch hier qualifizierende Tatbegehungen aufgenommen werden, sofern ein Vermögensverlust großen Ausmaßes herbeigeführt wird, die Täter gewerbsmäßig oder als Mitglied einer Bande handeln oder bei der Tat wichtige Einrichtungen der Daseinsvorsorge oder der Infrastruktur betroffen sind. Für solche erhöhten Strafandrohungen hatte sich auch die strafrechtliche Abteilung des 69. DJT[5] im vergangenen Jahr ausgesprochen. Entsprechende Regelungen sind auch zur Umsetzung von Artikel 9 Abs. 5 der neuen EU-Richtlinie 2013/40/EU über Angriffe auf Informationssysteme erforderlich, soweit ein breit angelegter Cyber-Angriff vorliegt und eine beträchtliche Anzahl von Informationssystemen geschädigt wird. Der vom Bundesrat beschlossene Entwurf eines Gesetzes zur Strafbarkeit der Datenhehlerei sieht bereits entsprechende Änderungen durch qualifizierende Tatbestände sowohl bei § 202a als auch bei § 202b StGB vor.[6] Über diesen

[5] Vgl. http://www.djt.de/fileadmin/downloads/69/120921_djt_69_beschluesse_web_rz.pdf.
[6] Vgl. BT-Drs. 17/14362 und BR-Drs. 284/13 jeweils Art. 1 Nr. 2 und 3.

Gesetzentwurf hinaus erscheint auch in § 303a StGB eine entsprechende Ergänzung um Qualifizierungen für besonders schwere Delikte notwendig.

Während bisher nur in § 303a Abs. 2 StGB die Sanktionierung eines Versuchs vorgesehen ist, fehlt beim Ausspähen und Abfangen von Daten bisher eine solche Versuchsstrafbarkeit. Ein virtueller Einbruchsversuch bleibt damit straflos, gleichgültig ob aus Unfähigkeit des Täters oder im Blick auf die hohe Qualität bzw. Suffizienz der Zugangssicherung. Insoweit ist daher in § 202a und § 202b StGB - ebenso wie im neuen § 202d StGB - ein Ahndungsmöglichkeit für nicht vollendete Delikte vorzusehen. Entsprechende Vorschläge sind im vorliegenden Gesetzentwurf zur Datenhehlerei bereits enthalten.[7]

cc) Erweiterter Schriftenbegriff i.S.d. § 11 Abs. 3 StGB

Ein Änderungsbedarf besteht daneben auch in Bezug auf den körperlichen Schriftenbegriff des § 11 Abs. 3 StGB. Dies hat vor allem Auswirkungen auf die Verfolgung des Besitzes von Kinderpornografie. Beim Pornografiestrafrecht stand anfangs der Verkauf von Fotos unter dem Ladentisch im Vordergrund, später die Verbreitung von Videofilmen. Kaum ein pädophiler Täter agiert aber heute noch mit solchen althergebrachten Foto- oder Videosammlungen. Bezogen wird Kinderpornografie nur noch aus dem Internet. Auf diese Veränderungen hatte der Gesetzgeber einerseits 1993 dadurch reagiert, dass er neben der Verbreitung auch den bloßen Besitz des Materials unter Strafe gestellt hat sowie 1997, indem bei den Tatobjekten durch § 11 Abs. 3 StGB den Schriften auch "Datenspeicher" gleichgestellt wurden. Mit dieser Änderung sollten alle modernen EDV-Sachverhalte einbezogen werden. Gelangen aber kinderpornografisches Material oder andere inkriminierte "Schriften" nicht mehr auf physischen Trägermaterialien in die Wohnung des Täters, sondern nur über ein Datennetz, ergeben sich neue Problemstellungen, wenn diese Daten nicht mehr auf der Festplatte oder CD des Nutzers gespeichert, sondern in jedem Bedarfsfall einfach über das Netz abgerufen werden können, ohne dass man am Monitor sichtbare Daten "besitzen" und damit gegenständliche Verfügungsmacht darüber ausüben kann.

Unser Strafrecht wird streng begrenzt durch den Wortlaut seiner Tatbestände. Ein Täter mag noch so direkten Zugriff auf Pornografie oder andere strafrechtlich relevante "Schriften" erlangen - solange das nicht mit dem Besitz an einem Datenspeicher einhergeht, bleibt er derzeit straflos. Zwar haben die deutschen Gerichte versucht, schon die automatische Festplattenspeicherung von Internetseiten durch den Browser-Cache und sogar den Datendurchlauf im Arbeitsspeicher dem Begriff des "Datenspeichers" unterzuordnen. Ein Tatnachweis kann aber nur geführt werden, wenn der Täter gewusst hat, was beim Surfen in den Speichern seines PC geschieht. Dies wird aber immer schwieriger, da die zunehmende Medienkonvergenz schon heute eine klare Trennung zwischen echten Streaming-Angeboten und zwischengespeicherten Daten im Arbeitsspeicher oder Cache des Rechners kaum mehr zulässt. Es ist daher notwendig, die "Besitzstraftaten" und damit insbesondere das Pornografiestrafrecht internetfähig machen, indem diese technikneutral auch moderne Begehungsweisen im Internet erfassen. Das Pornografiestrafrecht - und dies gilt in gleicher Weise auch für alle anderen Inhaltsdelikte des StGB - sollte daher nicht mehr an einen für körperliche Gegenstände entwickelten Schriftenbegriff und der Verbreitung von Schriften anknüpfen, sondern in allgemeiner Form an das Zugänglichmachen von Medien oder Medieninhalten mit entsprechenden strafbewehrten Inhalten. Nur so lassen sich hier Strafbarkeitslücken durch die moderne Internetnutzung vermeiden.

---

[7] Vgl. BT-Drs. 17/14362 und BR-Drs. 284/13 jeweils Art. 1 Nr. 2 und 3.

3. Strafverfahrensrecht

So wie sich Straftaten in die digitale Welt verlagern, so müssen auch die Werkzeuge zur Strafverfolgung in die Virtual Reality transferiert werden. Früher wurde ein Brief beschlagnahmt - heute interessiert der Inhalt der E-Mail. Vor 50 Jahren wurde der Bücherschank nach Heften mit Kinderpornographie durchsucht, heute der PC oder die Cloud, in der die Daten gespeichert werden. Wer hat wann mit wem Kontakt? - nicht selten eine der zentralen Fragen im Ermittlungsverfahren, kann heute häufig nur noch durch eine Auswertung der Internet- oder der Facebook-Kommunikation aufgeklärt werden. Diese Beispiele machen deutlich, dass alle neuen Formen der Cyberkriminalität nur dann effektiv bekämpft werden können, wenn auf legislativer Ebene das notwendige gesetzliche Instrumentarium für die Strafverfolgungsbehörden zur Verfügung steht, um dem hohen Gefahrenpotential der Internetkriminalität angemessen Rechnung tragen zu können. Wie das BVerfG in seinen Entscheidungen zur Online-Durchsuchung und zur Vorratsdatenspeicherung[8] ausdrücklich hervorhebt, handelt es sich bei der Effektivierung der Strafverfolgung um einen legitimen Zweck, der Eingriffe in Grundrechte grundsätzlich rechtfertigen kann. Um dem Rechtsstaatsprinzip und dem Schutzauftrag des Staates für seine Bürger Rechnung zu tragen, dürfen deshalb den Ermittlungsbehörden die rechtlichen und technischen Möglichkeiten nicht vorenthalten werden, die sie für eine solche effektive Strafverfolgung benötigen. Dabei lassen sich hier vier große Bereiche unterscheiden, in denen ein besonderer Handlungsbedarf besteht und die daher im Folgenden näher zu vertiefen sind: Neben dem weiten Feld der Eingriffe in die Telekommunikation gilt dies für Ermittlungen in sozialen Netzwerken vor allem für Beweiserhebungen in der Cloud sowie für eine Verbesserung der internationalen Zusammenarbeit.

a.) Eingriffe in die Telekommunikation

Da die meisten Straftaten mittels Telekommunikation begangen werden, sind für die Strafverfolgungsbehörden vor allem dem Stand der Technik entsprechende Befugnisse für Eingriffe in die Telekommunikation notwendig, ohne die in vielen Verfahren ein Ermittlungsansatz fehlt und eine weitere Tataufklärung gar nicht möglich ist. Hier hat der Gesetzgeber ein abgestuftes System von Eingriffsbefugnissen geschaffen, das sich an der Art der zu übermittelnden Daten und der Eingriffsintensität orientiert. Ein Zugriff auf Inhaltsdaten der Telekommunikation ist nur unter den engen Voraussetzungen des § 100a StPO zulässig, Verkehrsdaten können retrograd oder in Echtzeit nach § 100g StPO erhoben werden, weil diese Maßnahmen mit einem Eingriff in das Fernmeldegeheimnis des Art. 10 GG verbunden sind. Diese engen Voraussetzungen bestehen bei einem Zugriff auf Bestandsdaten der Telekommunikation i.S.d. §§ 95, 111 TKG nicht, da es hier nur zu einem Eingriff in das Recht auf informationelle Selbstbestimmung i.S.d. Art. 2 GG kommt.

aa) Personenauskunft zu dynamischer IP-Adresse

Für die Aufklärung von Straftaten im Bereich Cybercrime ist zunächst vor allem eine Identifizierung von Internetnutzern über ihre IP-Adresse von besonderer praktischer Relevanz. Hier hat der Gesetzgeber für den Zugriff auf Bestandsdaten der Telekommunikation und für die Personenauskunft zu einer dynamischen IP-Adresse entsprechend den Vorgaben des BVerfG im Urteil vom 24.1.2012[9] mit dem am 01.07.2013 neu geschaffenen § 100j StPO eine neue bereichsspezifische Eingriffsermächtigung als

[8] Vgl. BVerfG NJW 2008, 822 und NJW 2010, 833.

[9] Vgl. BVerfG NJW 2010, 833 [836] Rn. 195 und 261 f und BVerfG NJW 2012, 1419 mit Anm. Schnabel, CR 2012, 253; Roth, K&R 2012, 278 und ZD 2012, 228; Meinicke, MMR 2012, 416; Bertermann, ZD 2012, 282 sowie Hey, ZD 2012, 455

"zweite Tür" ergänzend zur Berechtigung zur Datenübermittlung in § 113 TKG ("erste Tür") geschaffen. Danach kann über § 100j Abs. 1 Satz 1 StPO zunächst Auskunft über die hinter einer Telefonnummer oder E-Mail-Adresse stehenden Bestandsdaten des Kunden verlangt werden. Über § 100j Abs. 1 Satz 2 StPO ergibt sich die Befugnis für den Zugriff auf Zugangssicherungscodes der Telekommunikation. Zulässig ist danach ein Auskunftsverlagen beim TK-Provider bzgl. aller Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen möglich ist, die in diesen Endgeräten oder räumlich getrennt davon eingesetzt werden. Solche Zugangsdaten als "Schlüssel" zu weiteren Informationen sind aber nur dann herauszugeben, wenn i.S.d. "dritten Tür" die strafprozessualen Voraussetzungen für die Nutzung der Daten erfüllt sind. Davon ist auszugehen, wenn als gesetzliche Befugnis für die Voraussetzungen einer Beschlagnahme oder formlosen Sicherstellung des entsprechenden Endgeräts gem. §§ 94, 98 StPO oder bei externen Speichermedien ein Abruf von Daten eines E-Mail-Accounts oder beim Cloud-Provider die Voraussetzungen der §§ 99 bzw. 102, 103 und 110 Abs. 3 StPO vorliegen.[10] Nur für diese Auskunft gilt gemäß § 100j Abs. 3 StPO grundsätzlich ein Richtervorbehalt, der jedoch dann entfällt, wenn der Betroffene vom Auskunftsverlagen bereits Kenntnis hat oder haben muss oder die Nutzung des Zugangssicherungscodes bereits durch eine gerichtliche Entscheidung gestattet wurde. Die ermittlungsrichterliche Anordnung für die Folgemaßnahme deckt damit quasi auch die vorrangige Abfrage der Zugangsdaten ab.

In § 100j Abs. 1 Satz 1 i.V.m. Abs. 2 StPO findet sich nun erstmals eine ausreichende gesetzliche Befugnis für die Personenauskunft zu einer dynamischen IP-Adresse. Diese führt nach Auffassung des BVerfG zu einem Eingriff in Art. 10 GG, da die Brücke zwischen der bekannten IP-Adresse und den als Auskunft zu übermittelnden Bestandsdaten nur durch eine Auswertung von Verkehrsdaten beim Provider hergestellt werden kann. Eines Richtervorbehalts und eines begrenzenden Rechtsgüter- oder Straftatenkatalogs bedarf es aber nicht. Durch das Erfordernis eines konkreten Zeitstempels der verwendeten IP-Adresse wird aber klargestellt, dass eine generelle Abfrage zur Verwendung einer IP-Adresse ausgeschlossen ist, da sonst die Grenze zur Verkehrsdatenabfrage nach § 100g StPO überschritten wäre.[11] Mit dem Wortlaut der Regelung vereinbar ist auch eine umgekehrte Abfrage, welche dynamischen IP-Adressen zu einem bestimmten Zeitpunkt einer bestimmten Person zugeordnet waren, da es hier zu keiner Änderung der Eingriffstiefe kommt und die Qualität der Information gleich bleibt.[12] Sowohl für die Auskunft über Zugangssicherungscodes als auch für die Personenauskunft sind die Pflichten zur nachträglichen Benachrichtigung des Betroffenen nach § 100j Abs. 4 StPO zu beachten.

bb) Anlassunabhängige Speicherung von Verkehrsdaten

Eine Zuordnung von IP-Adressen über § 100j Abs. 1 Satz 1 i.V.m. Abs. 2 StPO und eine Auskunft über Verkehrsdaten nach § 100g StPO sind aber nur dann möglich, wenn bei den jeweiligen Providern entsprechende Informationen erhoben und für einen bestimmten Zeitraum gespeichert werden. Dazu bedarf es einer gesetzlichen Verpflichtung zur anlasslosen Speicherung von Verkehrsdaten, die seit der Entscheidung des BVerfG vom 2.3.2010 mit der Folge einer Verfassungswidrigkeit der bisherigen Regelungen in §§ 113a, 113b TKG a.F. und damit seit mehr als 3 Jahren aber nicht mehr besteht.
Eine verfassungskonforme Ausgestaltung einer solchen Vorratsdatenspeicherung ist entsprechend den Vorgaben des BVerfG jederzeit möglich, wenn angemessene Regelungen zur Datensicherheit, zum Umfang der Datenverwendung, zur Transparenz und zum

[10] Vgl. näher die Kommentierung: KMR-StPO/Bär, § 100j Rn. 8 ff. (Stand: Oktober 2013).
[11] Vgl. auch BT-Drs. 17/12879, S. 15.
[12] So im Ergebnis auch: KMR-StPO/Bär, § 100j Rn. 18 (Stand: Oktober 2013); *Dalby* CR 2013, 365; *Gercke/Brunst* Praxishandbuch Internetstrafrecht Rn. 670 f.

Rechtsschutz geschaffen werden. Nur mit einer solchen Neuregelung wird auch den europarechtlichen Verpflichtungen zur Umsetzung der entsprechenden EU-RL Rechnung getragen und eine Verurteilung durch den EuGH im Vertragsverletzungsverfahren mit hohen Strafzahlungen vermieden. Erforderlich ist es daher, eine Neureglung zur anlasslosen Speicherung von Verkehrsdaten im TK-Recht zu schaffen, die vor allem einen hohen Sicherheitsstandard für die auf Vorrat zu speichernden Daten verbunden mit einer engen Zweckbindung für die Verwendung der Daten durch auskunftsberechtigte Stellen vorsieht. Die bisherige Zugriffsbefugnis auf Verkehrsdaten in § 100g StPO ist ergänzend dazu mit einer abgestuften Regelung zu versehen, die danach differenziert, auf welche Verkehrsdaten zugegriffen werden soll: Für eine Abfrage von zu Abrechnungszwecken sowie zu Zwecken der Störungsbeseitigung gespeicherten Verkehrsdaten kann die bisherige Regelung des § 100g Abs. 1 StPO unverändert übernommen werden. Für den Zugriff auf anlasslos gespeicherte Verkehrsdaten ist demgegenüber eine neue Zugriffsregelung zu schaffen, die eine Auskunft über solche Vorratsdaten entsprechend den Vorgaben des BVerfG nur unter den Voraussetzungen einer schweren Straftat zulässt.

cc) Straftatenkatalog in § 100a StPO

Um auch bei schwerwiegenden Straftaten der §§ 202a, 202b, 303a und 303b StGB eine Überwachung der Telekommunikation anordnen zu können, erscheint - wie im Gesetzentwurf zur Datenhehlerei bereits vorgesehen - eine Aufnahme der qualifizierten Tatbestände dieser Delikte in den Katalog der schweren Straftaten des § 100a Abs. 2 StPO erforderlich, soweit sie im Einzelfall schwer wiegen (§ 100a Abs. 1 Nr. 2 StPO). Dort ist auch in § 100a Abs. 2 Nr. 1 n) der qualifizierte Computerbetrug nach § 263a Abs. 3 StPO bereits enthalten. Das Ausspähen von Daten im Rahmen der Rekrutierung von Computersystemen - etwa mittels Schadsoftware zu Bot-Netzen (§§ 202a - 202c StGB) sowie die Durchführung von DDoS-Angriffen zum Nachteil von Firmen und kritischen Infrastrukturen (§§ 303a, 303b StGB) weisen ein besonders hohes Gefahren- und Schadenspotenzial auf. Bot-Netze stellen regelmäßig die technische Voraussetzung für das massenhafte Infiltrieren der Computerendsysteme mit Schadsoftware dar. Da diese Straftaten nur mit Mitteln der Telekommunikation begangen werden können, besteht meist nur bei einer TK-Überwachung ein erfolgversprechender Ermittlungsansatz. Damit wird auch der Beurteilungsspielraum des Gesetzgebers bei der Bestimmung des Unrechtsgehalts eines Delikts und bei der Entscheidung darüber sowie der Verhältnismäßigkeitsgrundsatz gewahrt, welche Straftaten er zum Anlass für bestimmte strafprozessuale Ermittlungsmaßnahmen machen will.[13]

dd) Quellen-TKÜ

Zahlreiche über das Internet nutzbare Telekommunikationsdienste (z.B. der Messenger-Dienst Skype) und Webseiten mit Datenübermittlungen im HTTPS-Standard[14] übertragen ihre Inhaltsdaten ausschließlich verschlüsselt. Aufgrund der Verschlüsselung der Kommunikationsinhalte kann diese Form der Telekommunikation nicht mittels einer „konventionellen“ TKÜ überwacht werden. Da technisch keine Möglichkeit besteht, die Kommunikationsinhalte zu entschlüsseln, ist eine Überwachung und Aufzeichnung der Inhalte nur dann möglich, wenn die Daten aus einem laufenden Telekommunikationsvorgang noch vor ihrer Verschlüsselung bzw. nach ihrer Entschlüsselung erhoben werden.
Hierzu ist die verdeckte Einbringung einer Überwachungssoftware in das Zielsystem (der „Quelle“) erforderlich. Durch technische und rechtliche Maßnahmen ist dabei sicherzustellen, dass eine Aufzeichnung von Bildschirminhalten oder anderen Inhalten außerhalb eines

[13] Vgl. BVerfG NJW 2012, 833 Rz. 203.
[14] Bei HTTPS = Hyper Text Transfer Protocol Secure handelt es sich um ein Kommunikationsprotokoll im World Wide Web, um Daten abhörsicher zu übertragen.

konkreten Kommunikationsvorgangs ausgeschlossen bleibt. Auch wenn in der Rechtsprechung der Einsatz der Quellen-TKÜ auf der Grundlage des § 100a StPO überwiegend für zulässig erachtet wird, erscheint es zur Klarstellung sinnvoll, die Quellen-TKÜ als eine besondere Form der TK-Überwachung durch eine spezielle Eingriffsermächtigung in einem gesonderten Absatz in § 100a StPO - vergleichbar der Normierung in § 20l Abs. 2 BKAG - mit aufzunehmen. Durch diese Anbindung der Regelung an § 100a StPO wird gleichzeitig sichergestellt, dass Gegenstand einer solchen Überwachungsmaßnahme - wie nach bisherigem Recht auch - nur ein laufender Telekommunikationsvorgang sein kann.

b) Ermittlungen in sozialen Netzwerken

Neben verdeckten technischen Eingriffsmaßnahmen werden zur Tataufklärung verdeckte personale Ermittlungen in sozialen Netzwerken immer wichtiger. Soziale Netzwerke wie Facebook, Wer-kennt-wen, MySpace, Twitter werden von Millionen von Menschen in weiten Teilen der Bevölkerung genutzt. Sie sind deshalb für die Strafverfolgungsbehörden aufgrund ihrer hohen Attraktivität und der stetig steigenden Verwendung eine wichtige Erkenntnisquelle. Dabei müssen aus Sicht der Strafverfolgung aber bei der Nutzung sozialer Netzwerke durch Ermittlungsbehörden zwei Bereiche unterschieden werden, die von der Art der Tätigkeit und den zu Grunde liegenden Rechtsgrundlagen nicht miteinander vermengt werden dürfen und die es im Folgenden zu unterscheiden gilt: Nutzung sozialer Netzwerke zur Aufklärung von Straftaten sowie zur Öffentlichkeitsfahndung. Geht es beim ersten Bereich allein um die Frage, in welchen Grenzen und unter welchen gesetzlichen Voraussetzungen Strafverfolgungsbehörden Informationen für Zwecke des Ermittlungsverfahrens in sozialen Netzwerken erheben dürfen, betrifft der zweite Punkt eine aktive Tätigkeit in Form des Einsatz sozialer Netzwerke für die Fahndung nach Tätern.

aa) Nutzung sozialer Netzwerke zur Aufklärung von Straftaten

Die denkbaren Ermittlungsmöglichkeiten in sozialen Netzwerken reichen hier etwa vom Aufruf entsprechender Angebote über die Beobachtung eines offenen Chats bis hin zur Teilnahme von Polizeibeamten an Kommunikationsvorgängen unter einem Pseudonym (sog. Fake-Account) und dem Einsatz "virtueller verdeckter Ermittler". Für die rechtliche Zulässigkeit solcher Ermittlungsmaßnahmen ist dabei deren jeweilige Grundrechtsrelevanz von entscheidender Bedeutung. Danach bestimmt sich letztlich, ob es mangels einer Grundrechtsrelevanz einer speziellen gesetzlichen Ermächtigungsgrundlage bedarf oder nicht bzw. falls eine solche für erforderlich gehalten wird, welche Ermächtigungsgrundlage für den Grundrechtseingriff heranzuziehen ist. Die in Betracht kommenden Rechtsgrundlagen für ein solches Vorgehen reichen dabei - je nach Eingriffsintensität - von der Ermittlungsgeneralklausel bis hin zur Spezialermächtigung zum Einsatz verdeckter Ermittler. Ausgangspunkt für die Beurteilung der Grundrechtsrelevanz von Ermittlungen staatlicher Stellen im Internet ist das Urteil des BVerfG vom 27.2.2008[15] zur Online-Durchsuchung.

So hat das BVerfG die Grundrechtsrelevanz von Ermittlungen bei der Teilnahme an einer öffentlich zugänglichen Kommunikation verneint. Es liegt hier gerade kein Eingriff in ein spezielles Grundrecht eines Kommunikationsteilnehmers - wie das Fernmeldegeheimnis (Art. 10 GG) oder das Recht auf informationelle Selbstbestimmung (Art. 2 i.V.m. Art. 1) - vor, wenn die staatliche Stelle die Inhalte der Internetkommunikation auf dem dafür technisch vorgesehenen Weg zur Kenntnis nimmt, sofern diese sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten. Das gilt selbst dann, wenn auf diese

[15] BVerfG NJW 2008, 822 = CR 2008, 306 = BVerfGE 120, 274.

Weise im Einzelfall personenbezogene Informationen erhoben werden. Grundsätzlich ist es dem Staat – hier durch die Ermittlungspersonen der Polizei bzw. die ermittelnde Staatsanwaltschaft – mithin möglich, zu Zwecken der Erkenntnisgewinnung öffentlich zugängliche Kommunikationsinhalte aufzurufen.[16] Hierbei ist es unerheblich, ob für die Nutzung eines Angebotes eine erforderliche Registrierung erfolgen muss, sofern durch den Betreiber der Internetseite eine Kontrolle der Identität nicht erfolgt.

Sofern in denjenigen Fallgestaltungen eine Grundrechtsrelevanz jedenfalls bejaht wird, weil etwa die Wahrnehmung der Daten eine Anmeldung voraussetzt,[17] kommt als Ermächtigungsgrundlage die allgemeine Ermittlungsgeneralklausel der §§ 161 Abs. 1, S. 1, 163 Abs. 1 S. 2 Alt. 3 StPO in Betracht. Diese Norm ist einschlägig für Ermittlungshandlungen, die in ihrer verfassungsrechtlichen und strafprozessualen Bedeutung (unter Berücksichtigung der Eingriffstiefe bei dem Betroffenen) unterhalb der Schwelle von „Standardermittlungsmaßnahmen“ wie z.B. einer Durchsuchung oder einer Beschlagnahme liegen. Sie kommt auch für den Einsatz eines nicht offen ermittelnden Polizeibeamten (noeP) zu Anwendung. Unter diesen Voraussetzungen ist es einer staatlichen Stelle etwa möglich, sich ohne weitergehenden Grundrechtseingriff an öffentlich zugänglichen Kommunikationsvorgängen - auch unter falschen Namen mit einem sog. "Fake-Account" - zu beteiligen. Weder das Telekommunikationsgeheimnis (Art. 10 GG) noch das Recht auf informationelle Selbstbestimmung bzw. das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG) schützen das personengebundene Vertrauen der Kommunikationsbeteiligten hinsichtlich der Identität und Wahrhaftigkeit derselben. Ein derartiges Interesse ist von Verfassung wegen nicht schutzwürdig, soweit im Internet keinerlei Mechanismen bestehen, um die Identität und die Wahrhaftigkeit zu überprüfen. Den Teilnehmern auch an einer länger bestehenden virtuellen Gemeinschaft (z.B. im Rahmen eines Diskussionsforums) ist jederzeit bewusst, dass sie die (wahre) Identität des Gegenübers nicht kennen oder dessen Angaben über sich jedenfalls nicht überprüfen können.[18]

Nur in den Fällen einer hinreichend sicheren Identifikation bei der Kommunikation im Internet kommt es auf die Kriterien an, die für eine Abgrenzung des Einsatzes einer Ermittlungsperson als nicht offen ermittelnder Polizeibeamter (noeP) oder verdeckter Ermittler (VE) von Bedeutung sind. Dazu gehören etwa die Häufigkeit des verdeckten Auftretens, die Anzahl der Ermittlungshandlungen, der Umfang der Identitätstäuschung, die Erforderlichkeit der Geheimhaltung der (wahren) Identität des Ermittlers oder die Erforderlichkeit des Betretens der Wohnung des Täters. Bei der hier erforderlichen Bewertung der Gesamtsituation wird neben dem Aufwand der Legendierung (wie etwaiger erforderlicher Maßnahmen gemäß § 110a Abs. 3 StPO) insbesondere auf die Zeitdauer der Teilnahme an geschlossenen Benutzergruppen und der damit verbundenen Vielzahl der Ermittlungshandlungen gegenüber den Teilnehmern der Gruppe abzustellen sein.[19] Entscheidend ist letztlich, ob der Ermittlungsauftrag über einzelne wenige, konkret bestimmte Ermittlungshandlungen hinausgeht oder ob es erforderlich werden wird, eine unbestimmte Vielzahl von Personen über die wahre Identität des verdeckt operierenden Polizeibeamten zu täuschen. Sofern auf das Kriterium der hinreichend sicheren Identifikation innerhalb eines internetbasierten Kommunikationsverhältnisses nicht verzichtet wird, dürften der allgemeine Rechtsverkehr oder die Beschuldigtenrechte in künftigen Strafverfahren eine mehr als nur unerhebliche Beeinträchtigung durch den Einsatz des verdeckt operierenden Polizeibeamten

---

[16] Dieses ist als h.M. anzusehen; vgl. zum Meinungsstand m.w.N.: Rosengarten/Römer, Der „virtuelle verdeckte Ermittler“ in sozialen Netzwerken und Internetboards, NJW 2012, 1764, 1766 f.

[17] Vgl. etwa Schulz/Hoffmann, Grundrechtsrelevanz staatlicher Beobachtung im Internet, CR 2010, 131.

[18] BVerfG NJW 2008, 822.

[19] So auch Rosengarten/Römer, NJW 2012, 1764, 1767; Henrichs, Kriminalistik 2012, 632.

erfahren. Als problematisch sind die in der Praxis häufiger auftretenden Fallkonstellationen zu bewerten, in denen eine eindeutige Identifizierung einer Person (im vorgenannten Sinne) nicht erfolgt, sondern eine Zutrittsberechtigung zu einem geschlossenen Forum unter Ausnutzung der (ausschließlich) einer „virtuellen Person“ zugeschriebenen Reputation gewährt wird.[20] Ob in derartigen Fällen der Einsatz eines verdeckten Ermittlers zwingend zu erfolgen hat, ist hier letztlich von den Umständen des Einzelfalles abhängig.[21] Vor diesem Hintergrund ist auch die Entscheidung des BGH[22] zu bewerten, wonach der Einsatz eines noeP im Falle eines (bloßen) E-Mail-Verkehrs ohne einen persönlichen Kontakt zwischen den Kommunikationspartners ausreichend ist, weil schützenswertes Vertrauen darauf besteht, dass hinter der zur Kommunikation verwendeten E-Mail-Adresse eine bestimmte Person steht.

Ausgehend von den grundlegenden Ausführungen des BVerfG in der Entscheidung zur Online-Durchsuchung muss an Hand der jeweiligen konkreten Maßnahme im Einzelfall die Grundrechtsrelevanz von Ermittlungen im Internet beurteilt und darauf aufbauend eine Prüfung hinsichtlich der in Betracht kommenden Eingriffsermächtigung vorgenommen werden. Eine gesetzliche Fixierung aller als Ermittlungshandlungen denkbarer Fallgestaltungen wäre gar nicht möglich. Vielmehr sind die Gerichte dazu aufgerufen, eine Abgrenzung zwischen nicht offen ermittelnden Polizeibeamten (§§ 161, 163 StPO) und verdeckten Ermittlern (§§ 110a - 110c StPO) und eine Konkretisierung hinsichtlich der im jeweiligen Einzelfall zu beachtenden Grenzen vorzunehmen.

bb) Nutzung sozialer Netzwerke zur Öffentlichkeitsfahndung

Da sich über soziale Netzwerke innerhalb kürzester Zeit ein großer Adressatenkreis erreichen lässt, können hier im Einzelfall die Erfolgsaussichten polizeilicher Fahndungsmaßnahmen gegenüber einer herkömmlichen Fahndung wesentlich erhöht sein. Bei der Nutzung sozialer Netzwerke als Fahndungshilfsmittel handelt es sich um eine Form der Öffentlichkeitsfahndung. Als Rechtsgrundlagen kommen die allgemeinen Vorschriften für eine Öffentlichkeitsfahndung in Betracht. Dies sind vor allem § 131 Abs. 3 i.V.m. Abs. 1 und 2 sowie §§ 131a Abs. 3, 131b, 131c Abs.1 Satz 1, Abs. 2 StPO. Darüber hinaus sind die Richtlinien für das Straf- und Bußgeldverfahren (Ziffer 39 ff RiStBV, Ziffer 40 Abs. 2 RiStBV i.V.m. Anlage B zur RiStBV) zu beachten. Danach setzt eine solche Öffentlichkeitsfahndung zur Strafverfolgung immer eine Straftat von erheblicher Bedeutung voraus. Auf Grund der großen Breitenwirkung einer Fahndung im Internet ist im jeweiligen Einzelfall stets eine besonders strenge Abwägung erforderlich, ob der beabsichtigte Fahndungserfolg nicht auch durch Maßnahmen erreicht werden kann, die den Tatverdächtigen oder andere Betroffene weniger beeinträchtigen. Daneben werden bei der Nutzung sozialer Netzwerke für Fahndungen im Internet spezifische datenschutzrechtliche Fragen aufgeworfen. Insbesondere ist darauf zu achten, dass bei der Umsetzung personenbezogene Daten (wie Lichtbilder oder Videos) nicht Bestandteil des Angebots eines privaten Anbieters werden, sondern durch geeignete technische Maßnahmen sichergestellt wird, dass die zur Fahndung benötigten personenbezogenen Daten ausschließlich auf Servern im Verantwortungsbereich der Strafverfolgungsbehörden gespeichert, gesichert und nicht an private Diensteanbieter übermittelt werden.

Dies kann etwa durch Link- oder I-Frame-Technologie gewährleistet werden. Nur so haben die Ermittlungsbehörden in jeder Lage des Verfahrens die Möglichkeit, die sofortige Löschung oder Änderung der Fahndung zu veranlassen und ungehindert auf die Daten der

---

[20] Vgl. hierzu die zutreffenden Ausführungen von Rosengarten/Römer, NJW 2012, 1765, 1766 f.
[21] Vgl. etwa BGH StV 2012, 539 zu Boards zum Tausch kinderpornographischer Schriften.
[22] Vgl. BGH StB 15/10, B. v. 24.06.2010 (unveröffentlicht).

Fahndung zuzugreifen. Vor diesem Hintergrund hat daher auch eine Arbeitsgruppe des RiStBV-Ausschusses derzeit Vorschläge für eine Änderung der Anlage B der RiStBV erarbeitet, die diesen Vorgaben Rechnung trägt.

c) Ermittlungen in der Cloud

Da Cloud Computing inzwischen zu den wachstumsstärksten Bereichen der Informationstechnologie zählt, hat die Auslagerung von Daten in die Cloud auch zunehmend Auswirkungen auf die Sicherung beweisrelevanter Daten im Ermittlungsverfahren. Befinden sich entsprechende Daten in der Cloud, müssen aus strafprozessualer Sicht unterschiedliche Vorgehensweisen zur Sicherung der Daten differenziert werden, je nachdem ob die Zugangsdaten zu der Cloud-Anwendung bekannt sind, wo sich die beweisrelevanten Daten befinden und ob ein Zugriff auf diese Daten im Rahmen einer Durchsuchung beim Betroffenen möglich ist oder nicht. Mit der bestehenden Regelung des § 110 Abs. 3 StPO zum Zugriff auf externe Datenspeicher im Rahmen einer Durchsuchung vor Ort nach §§ 102, 103 StPO lassen sich beweisrelevante Daten in der Cloud nur teilweise angemessen sichern. Befinden sich diese Daten im Ausland oder ist der Zugriff auf gespeicherte Daten außerhalb einer Durchsuchung nicht möglich, bestehen entsprechende Lücken bei der Beweissicherung.

Die bisherigen gesetzlichen Eingriffsbefugnisse zur Sicherstellung von Informationen gehen vom Konzept einer geographischen Verortung von Daten und der damit verbundenen Territorialität aus. Dieser Standpunkt lässt sich aber im Zeitalter von Cloud Computing nicht mehr aufrechterhalten, da hier Daten innerhalb kürzester Zeit ihren Speicherort verändern können und dem Anbieter vielfach der aktuelle Speicherort der Daten selbst nicht bekannt ist. Ebenso ist derzeit gesetzlich nicht geklärt, wie ein Abruf von Daten aus der Cloud - außerhalb einer Durchsuchungsmaßnahme - mit bekannten Zugangsdaten rechtlich zu qualifizieren ist. Die bestehenden Eingriffsbefugnisse zur Durchsuchung und zur Überwachung der Telekommunikation werden diesen Fallgestaltungen nicht gerecht. Dies hat zur Folge, dass es für den Zugriff auf beweisrelevante Daten in der Cloud dann keine sicheren rechtlichen Grundlagen gibt, wenn dieser zum einen außerhalb einer Durchsuchungsmaßnahme erfolgt und zum anderen die genaue geographische Lokalisierung der Daten nicht bekannt ist. Insoweit muss hier eine rechtliche Klarstellung zunächst im nationalen Recht geschaffen werden, die im Einzelnen die Voraussetzungen für einen Zugriff auf extern gespeicherte Daten mit Mitteln der Telekommunikation festlegt.

Zusätzlich bedarf es aber auch einer Regelung zum grenzüberschreitenden Datenabruf über die bisherige Regelung des Art. 32 der Cybercrime-Konvention hinaus, die gerade nicht eingreift, wenn der konkrete Speicherort der Daten unbekannt ist.[23] In Nr. 293 des erläuternden Berichts zur Cybercrime-Konvention[24] findet sich zu Art. 32 bereits ausdrücklich der Hinweis der Konventions-Verfasser, dass dort nur solche Situationen aufgeführt wurden, bezüglich derer eine einseitige Vorgehensweise akzeptierbar sei. Im Übrigen sei es nicht möglich gewesen, eine umfassende, rechtsverbindliche Regelung für den grenzüberschreitenden Zugriff auf gespeicherte Computerdaten zu schaffen. Es wurde aber vereinbart, andere Fälle dann zu regeln, wenn weitergehende Erfahrungen gesammelt worden seien, in Anbetracht derer man erneut diskutieren könnte. Da die in der Cloud gespeicherten Daten heute aber nicht mehr an Ländergrenzen gebunden und kaum zu lokalisieren sind, sollte insoweit eine adäquate Anpassung der rechtlichen Grundlagen in Art. 32 der

[23] Vgl. http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2013_7E_GN3_transborder_V2public.pdf

[24] Vgl. BT-Drs. 16/7218, S. 95.

Cybercrime-Konvention an die neuen technischen Entwicklungen beim Cloud Computing für einen transnationalen Zugriff auf Datenspeicher auf der Ebene der EU, des Europarats oder der Vereinten Nationen erfolgen. Nur durch solche Anpassungen kann den Bedürfnissen der effektiven Strafverfolgung bei physikalisch nicht bestimmten Hoheitsgebieten zuzurechnenden Daten Rechnung getragen werden.

d) Internationale Zusammenarbeit

Das Internet kennt keine Grenzen. Die Notwendigkeit für weitere gesetzliche Regelungen oder völkerrechtliche Vereinbarungen ergibt sich im Strafverfahrensrecht daneben vor allem mit Blick auf die Internationalisierung der strafprozessualen Ermittlungen. Wenn hier in Sekundenbruchteilen beweisrelevante Datenbestände den Ermittlungsbehörden durch Speicherungen im Ausland vorenthalten werden können, werden sehr schnell die Grenzen für die nationalen Rechtsordnungen deutlich. Hier ergeben sich durch die vom Europarat verabschiedete Cyber-Crime-Konvention aus dem Jahr 2001 zur grenzüberschreitenden Zusammenarbeit auf internationaler Ebene zwar erste entsprechende Ansätze für transnationale Ermittlungen, doch ist der Geltungsbereich dieses Übereinkommens einerseits noch beschränkt[25] und bedarf andererseits - wie bereits dargestellt - im Hinblick auf die neuen technischen Entwicklungen der letzten Jahr einer inhaltlichen Anpassung.

4. Zusammenfassung

Die modernen Informations- und Kommunikationstechnologien haben heute alle Lebensbereiche erfasst und zählen für viele bereits zu den unverzichtbaren Gütern. Dadurch steigt aber in gleicher Weise auch die Abhängigkeit der Informationsgesellschaft von der Computertechnik. Bei der Strafverfolgung im EDV-Bereich wird deshalb einerseits die Gewinnung unkörperlicher Informationen statt verkörperten Gegenstände immer wichtiger. Andererseits lösen sich die Ermittlungsmöglichkeiten vielfach von einer geographischen Verortung von beweisrelevanten Informationen, da Informationen - etwa beim Cloud-Computing - innerhalb kürzester Zeit von einem Ort zum anderen verlagert werden können.

Eine effektive Strafverfolgung in diesem Bereich setzt daher voraus, dass die Strafverfolgungsbehörden über entsprechende Straftatbestände und Eingriffsermächtigungen verfügen, die dem heutigen Stand der Technik entsprechen. Vor allem dürfen bei der Schaffung zusätzlicher Strafnormen für neue Erscheinungsformen der Kriminalität im materiellen Recht die auftretenden Aufklärungs- und Nachweisschwierigkeiten nicht unberücksichtigt bleiben.

Auf diesem Weg zu effektiven Rechtsgrundlagen zur Verfolgung von Cybercrime war das Strafverfahrensänderungsgesetz (StVÄG) 1999[26] ein erster Schritt. Ein weiterer erfolgte durch das zum 1.1.2008 in Kraft getretene Gesetz zur Neuregelung der TK-Überwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung. Vor dem Hintergrund der Entscheidung des BVerfG ist aber hier ein wesentlicher Teil dieser Neuregelung wieder weggefallen, ohne dass es bisher zu einer Nachfolgeregelung gekommen ist.

Dem hohen Gefahrenpotential der Internetkriminalität kann aber dann nicht angemessen Rechnung getragen werden, wenn den Strafverfolgungsbehörden die für eine effektive

---

[25] Vgl. Kugelmann, TMR 2002, 14 sowie Gercke, MMR 2004, 801.

[26] StVÄG 1999 vom 2. 8. 2000, BGBl. 2000, 1253. Vgl. zu den Inhalten auch BR-Drucksache 65/99.

Strafverfolgung notwendigen Ermittlungsmaßnahmen in technischer und rechtlicher Hinsicht nicht zur Verfügung stehen.

Vor allem bedarf es zur grenzüberschreitenden Bekämpfung von Cybercrime einer noch viel stärkeren Zusammenarbeit der jeweiligen nationalen Strafverfolgungsbehörden, um hier die Möglichkeiten zum Zugriff auf exterritorial gespeicherte Informationen sowie auf TK-Daten zu verbessern und eine Möglichkeit zur Zurückverfolgung von Tatbegehungen im Internet zu schaffen. Damit hier nicht innerhalb kürzester Zeit vorhandene Ermittlungsansätze durch die Löschung vorhandener Daten zunichte gemacht werden, muss hier ein computerspezifisches Kooperationsrecht geschaffen werden und durch völkerrechtliche Verträge die Möglichkeiten zu transnationalen Eigenermittlungen verbessert werden.

Kriminalistik 2.0 - effektive Strafverfolgung im Zeitalter des Internet aus Sicht des BKA

Jörg Ziercke

Nach erfolgreichen Hackingangriffen hoben Kriminelle mit gefälschten Kreditkarten innerhalb von zwei Tagen in insgesamt 23 Staaten weltweit rund 40 Millionen US-Dollar ab. Ein Trojaner ermöglichte den Zugriff auf Prozess- und Produktionsdaten und somit den Angriff auf Prozessleittechniken Kritischer Infrastrukturen – 60 % der Unternehmen der Versorgungssektoren Strom, Öl, Gas, Wasser in Deutschland entdeckten den Trojaner auch in ihren Netzen. Ein abgewehrter Angriffsversuch auf ein deutsches Telekommunikationsunternehmen hatte das Potenzial, das Internet in Deutschland außer Betrieb zu setzen.

Cybercrime hat grenzenloses Wachstums- und Schadenspotenzial

Cybercrime ist eine neue Dimension der Kriminalität. Weltweit bieten sich den Tätern unzählige potenzielle Opfer und Angriffspunkte. Das Gefahrenpotenzial für den einzelnen Bürger, für Wirtschafts- und Finanzunternehmen, für den Staat und seine Einrichtungen ist erheblich und allgegenwärtig.

Die wesentlichen Vorzüge von Cybercrime aus der Sicht Krimineller:

- Cyberstraftaten sind profitabel und verlangen wenig eigene Infrastruktur.
- Über das Internet werden Hacking-Tools angeboten, die sofort angewandt werden können.
- Die Anonymität des Internet ermöglicht eine Trennung von realer und digitaler Identität.
- Das Internet ermöglicht kriminellen Gruppen die Vernetzung über Ländergrenzen hinweg.
- Das Entdeckungsrisiko für Täter ist im Vergleich zur analogen Welt gering.

Die weite Verbreitung informationstechnischer Systeme und die zunehmende Nutzung IT-gestützter Infrastrukturen steigern die Abhängigkeit von IT-Systemen und erhöhen die Verwundbarkeit von Staaten, Unternehmen, jedes Einzelnen. Hochgradig vernetzte und sensible Systeme werden gestört und manipuliert, Straftaten werden online vorbereitet und offline umgesetzt. Wir sprechen hier von „Hybridverbrechen".
Das Internet ist ein praktisches Mittel der Kommunikation und Interaktion: Informationen, Propaganda und Absprachen sind weltweit in Echtzeit teilbar. Das Internet ist die Fernuniversität des religiös motivierten Terrorismus und dient der Vorbereitung realer Straftaten, wie den sogenannten „flashrobs", bei denen sich einander unbekannte Personen im Internet verabreden, um gemeinsam Geschäfte zu überfallen.

Nicht die Kriminalitätsphänomene, die Tatbegehungsweisen verändern sich

Die aktuelle Kriminalitätslage zeigt, dass sich nicht die Kriminalitätsphänomene, sondern die Tatbegehungsweisen verändern. Die auf Basis der Polizeilichen Kriminalstatistik (PKS) des Jahres 2012 gewonnenen Lagedaten sind nur begrenzt aussagekräftig: 64.000 Fälle von Cybercrime, 230.000 Fälle mit Tatmittel Internet, die Fallzahlen steigen seit Jahren. Wir müssen jedoch davon ausgehen, dass die Dunkelziffer weit höher liegt. Nicht alle Vorfälle werden der Polizei gemeldet, viele werden gar nicht erst erkannt. Zudem gehen Taten, die vom Ausland aus verübt werden oder bei denen Täter einen Server im Ausland nutzen, nicht in die deutsche Kriminalstatistik ein. Es ist auch kaum möglich, die wirtschaftlichen Schäden abzuschätzen, da die Angaben zu Schadenshöhen stark variieren.

Gemäß Bundeslagebild Cybercrime betrug die durch Cybercrime im engeren Sinne verursachte Schadenssumme im Jahr 2012 rund 43 Millionen Euro. Hinzu kamen Schäden in Höhe von ca. 14 Millionen Euro durch Phishing und ca. 30 Millionen Euro durch die mit Hilfe des Tatmittels Internet verübte Wirtschaftskriminalität. Die von der Internetwirtschaft verzeichneten Schäden sind deutlich höher: Die jährlich weltweit durch Kriminalität und Spionage im Internet verursachten finanziellen Schäden werden auf mindestens 100 Milliarden US-Dollar geschätzt.

Dass die tatsächlichen Fallzahlen und die Kosten, die durch Cyberangriffe entstehen, schwer abschätzbar sind, zeigt eine Unternehmensbefragung der Industrie- und Handelskammer Nord. Demnach melden nur 6 % der Unternehmen erfolgte Cyberattacken der Polizei.[1] Das größte Schadenspotenzial haben Kritische Infrastrukturen, denn Infrastruktursysteme vernetzen Europa und die Welt und bilden neuralgische Knotenpunkte. Es stellt sich heute nicht mehr die Frage, ob Angriffe auf Kritische Infrastrukturen erfolgen, sondern ob diese Angriffe erfolgreich abgewehrt werden können. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) zählt allein bis zu 2.000 Angriffe täglich auf die Computersysteme des Regierungsnetzwerks.

Eine Symantec-Studie[2] zeigt, dass insbesondere kleine und mittelständische Unternehmen im Fokus der Cyberkriminellen stehen: 50 Prozent aller Cyberangriffe zielen auf Unternehmen mit weniger als 2.500 Mitarbeitern, ein Drittel auf Unternehmen mit weniger als 250 Mitarbeitern ab. Gerade weil diese Unternehmen glauben, uninteressant für Cyberkriminelle zu sein, stoßen die Täter hier auf unzureichende Sicherheitsvorkehrungen.

1 IHK Nord: Unternehmensbefragung zur Betroffenheit der norddeutschen Wirtschaft von Cybercrime. 2013.
2 Vgl. Symantec Corporation, Internet Security Threat Report 18/2013.

Die Täter und ihre Motivationen

Die Tätertypen sind höchst unterschiedlich, dementsprechend sind auch ihre Motive und ihr technisches Können äußerst different. Vom Einsteiger bis zum Profi sind alle vertreten: Jugendliche Hacker, die ihr Potenzial testen wollen, Extremisten, Erpresser, Terroristen, lose kriminelle Strukturen und Banden, international organisierte Kriminelle, Nachrichtendienste anderer Staaten. Dabei ist die Motivation der Täter nicht immer erkennbar.

Beim Tätertyp des Finanzagenten ist die Motivation dagegen eindeutig. Als Finanzagenten lassen sich Menschen anwerben, die ihr privates Konto gegen eine Prämie zur Verfügung stellen und sich dabei in der Regel der Geldwäsche leichtfertig schuldig machen. In einem Ermittlungsverfahren des BKA konnten über 18.000 Finanzagenten identifiziert werden, davon 12.000 aus den USA, 6.000 aus Großbritannien, 160 aus Australien und 111 aus Deutschland. Den internationalen Aktionskreis in diesem Verfahren bildeten die Staaten Ukraine, Moldawien, Russland und Litauen.

Cyberkriminelle mit IT-Grundkenntnissen oder auch sogenannte Script Kiddies sehen wir als Einsteiger. Mit vorprogrammierten Software-Toolkits beschäftigen sie sich überwiegend mit Phishing im Bereich Social Engineering und Defacement, also dem Verändern von Webseiten. Dieser Gruppe geht es vor allem darum, Erfahrungen zu sammeln und die breiten Möglichkeiten des Internet zu erproben.

Fortgeschrittene Hacker mit einer hohen Affinität zur Technik sind deutlich gefährlicher. Von ihnen gehen strukturierte Attacken, wie DDoS, Drive-by-exploits oder SQL-injections aus. Die Akteure sind organisierte Gruppen, Hobby-Hacker oder ideologische Hacker. Diese Gruppe verfügt über gute IT-Kenntnisse, die es ihnen ermöglichen, an persönliche Daten, betriebsinterne Informationen oder vertrauliche Regierungsdokumente zu gelangen.

Die dritte Gruppe sind die Profis. Hier finden sich sowohl staatlich gelenkte Hacker als auch terroristische Gruppen und Hacktivisten. Hacktivisten verstehen sich als Kämpfer gegen Ungerechtigkeit, verstehen ihr Handeln als zivilen Ungehorsam gegen bestimmte politische Richtungen – ein virtueller Gang auf die Straße, um Unternehmen, Regierungsbehörden, Parteien, andere Gruppen oder Initiativen von ihrem – in den Augen von Gruppen wie Anonymous oder Lulz-Security falschen – Weg abzubringen. Mittels DDoS-Attacken legen die Profis Internet-Portale lahm oder hacken Datenbanken, um im Anschluss „sensible“ Informationen zu veröffentlichen. Dies ist eine andere Qualität von Internetangriffen: Das Ziel ist es, einen möglichst großen Schaden anzurichten, wobei der Profit ideeller Natur ist.
Welche Ausmaße solche Taten haben können, zeigen die Angriffe auf die Südkoreanische Hauptstadt Seoul im März dieses Jahres. Den Angreifern mit dem Namen „Dark Seoul Gang“ gelang es, einen Virus auf mehreren tausend Firmen- und Bankcomputern zu installieren. Der Virus löschte Daten von Festplatten, die Rechner konnten nicht mehr hochgefahren werden. Zusätzlich legte die Gruppe zahlreiche Geldautomaten der Stadt lahm. In der Konsequenz darf also nicht nur gelten, dass wir uns vor Tätern schützen, die Betriebsgeheimnisse, persönliche Daten oder digitale Identitäten für ihre Zwecke nutzen wollen, sondern wir müssen uns auch auf Täter konzentrieren, deren Ziel es ist, maximalen Schaden anzurichten.

Cybercrime – neue Kriminalitätsphänomene?

Soweit zur allgemeinen Lage. Mit welchen Phänomenen haben wir es konkret zu tun?
Technologische Entwicklungen beeinflussen nahezu jede Art von Kriminalität. Straftaten werden heute in einer Art und Weise begangen, wie sie noch vor 10 Jahren oder gar 1949, als unser Grundgesetz formuliert und verabschiedet wurde, unvorstellbar waren.

Wie sehen kriminelle Geschäftsmodelle im Bereich der Betrugsdelikte und Erpressungen heute aus? Der Online-Betrüger ist vorrangig auf der Suche nach fremden Identitäten und übernimmt fremde Accounts. Fremde Identitäten werden für den freien Einkauf im Internet genutzt, mit Daten von Onlinebanking-Kontos werden Barabhebungen durchgeführt. Eine weitere Methode ist, im Online- und Auktionshaushandel nach Vorkasse keine, minderwertige oder gefälschte Ware zu versenden.

Herausragend ist derzeit ein Ermittlungsverfahren wegen gewerbsmäßigen Betrugs an älteren Menschen – begangen aus Call-Centern in der Türkei. Eine Identifizierung der Anrufer ist in diesen Fällen häufig nicht möglich: Durch sogenanntes Call-ID-Spoofing wird die Rufnummer des Anrufers abgewandelt und verschleiert. Die tatsächliche Rufnummer des Anrufers wird dabei durch eine frei wählbare Nummer ersetzt. Die bislang festgestellten Schäden belaufen sich auf rund 23 Millionen Euro. Die Anzahl der bereits festgestellten Opfer umfasst allein in Deutschland derzeit 37.000, belastbare Schätzungen weisen aber auf über 100.000 Personen hin.

Auch Erpressungen finden heute digital in unterschiedlichen Varianten statt. Den meisten wird der sogenannte BKA-Trojaner noch erinnerlich sein, Schadsoftware, die dem Nutzer vorgaukelt, auf seinem Rechner seien illegale Inhalte, das BKA habe den Rechner aus diesem Grund gesperrt. Nach Zahlung einer Strafe sei dieser wieder nutzbar – ein Modus Operandi, der erst dieses Jahr neu aufgelegt wurde, diesmal unter Verwendung eines Bildes der Bundeskanzlerin sowie der Logos der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU), der Bundespolizei und des BKA.

Ein weiteres Beispiel sind die seit April des Jahres 2012 unter Nutzung eines Botnetzes mittels DDoS-Attacken erfolgten Angriffe auf die Webseiten von Online-Shops. Nach den ersten Angriffen erhielten die Opfer erpresserische E-Mails mit einer Zahlungsaufforderung über 10.000 US-Dollar. Im Falle der Zahlung des geforderten Schutzgeldes würde von weiteren DDoS-Angriffen abgesehen und die Firma auf eine sogenannte „Whitelist“ gesetzt, womit sie weitere, durch die Nichterreichbarkeit ihrer Online-Präsenz entstehende Verluste, abwenden könnte.

Der das Botnetz steuernde Command&Control-Server konnte von den Ermittlern lokalisiert werden. Der physikalische Standort des Servers befand sich in Litauen, so dass eine Serverüberwachung gemäß §100a StPO bei einem deutschen Internetprovider nicht in Betracht kam. Die ausländische Partnerbehörde übermittelte zwar Logdaten für administrative Serverzugriffe, die übermittelten IP-Adressen waren jedoch schon älter als sieben Tage. Die entsprechenden Anschlüsse konnten wegen fehlender Mindestspeicherfristen in Deutschland nicht mehr ermittelt werden. Die verschlüsselte Kommunikation der Täter führte dazu, dass aktuell lediglich Verdachtsmomente vorhanden sind.

Sogenannte Ransomware verfolgt ein ähnliches Prinzip: Nach der Infektion des Rechners bewirkt sie, dass der Computer für den Nutzer „gesperrt“ wird. Die Sperrung wird nur gegen Zahlung einer Gebühr wieder aufgehoben. In einem konkreten Verfahren haben die

Ermittlungen ergeben, dass ein einzelner Täter innerhalb von sechs Tagen mehr als 200.000 Infektionen versucht hat und über 32.000 erfolgreich durchführen konnte.

Hinter diesen kriminellen Geschäftsmodellen stehen professionelle und global vernetzte Täter: Dieses Modell der Ransomware wird mittlerweile in Form von sogenannten „Affiliate-Systemen“, vergleichbar den aus der realen Geschäftswelt bekannten Franchise-Modellen, vertrieben. Eine beliebige Anzahl „krimineller Kunden“ kauft diese „Pakete“ ein und betreibt die konkrete Begehung der Einzelstraftaten sozusagen „eigenverantwortlich“.

Für diese Art der Erpressungen müssen die Täter nicht zwingend programmieren können und über umfassende technische Kenntnisse verfügen. Die erforderlichen Werkzeuge, sogenannte „Exploit Kits“, können über einschlägige Internetplattformen in der „Underground Economy“ erworben werden. Weit verbreitet ist beispielsweise das sogenannte „Blackhole Exploit Kit“: Eine Nutzungslizenz kostet 700 Dollar im Quartal oder 1.500 Dollar im Jahr. Für den Angriff aktueller Systeme bietet derselbe Anbieter parallel das sogenannte „Cool Kit“ an. Für 10.000 Dollar im Monat erhalten die kriminellen Kunden Exploits für Sicherheitslücken, die noch nicht allgemein bekannt sind und für die noch keine Sicherheitsupdates existieren.

Wie wird das Ausmaß digitaler Erpressungen eingeschätzt? Anhaltspunkte geben die Zahlen der IT-Sicherheitsdienstleister Kaspersky und Symantec: Gemäß der Firma Kaspersky verwendeten Kriminelle im Jahr 2012 zur Durchführung von 1,5 Mrd. Cyberangriffen 6,5 Mio. Domains. Im Vergleich zum Vorjahr stellt dies eine Steigerung um eine halbe Million Domains dar. Symantec berichtete für das Jahr 2011 von 5,5 Milliarden geblockten Schadsoftwareangriffen. Allein in diesem Jahr wurden über 400 Millionen neue Varianten von Schadsoftware festgestellt.

Wie werden Eigentums- und Diebstahlsdelikte heute begangen?

Nicht nur Sachen und Gegenstände, auch Daten und Identitäten sind Werte, für die sich Kriminelle interessieren. Im September 2013 erhielt das BKA die Information, dass ein großes deutsches Telekommunikationsunternehmen Schadsoftware auf seinen Systemen gefunden habe. Die Software war geeignet, Kundendaten auszuspähen, indem die Daten identifiziert, vervielfältigt und anschließend ausgeleitet wurden. Dabei wurden Name, Anschrift, Bankverbindung und in bestimmten Fällen auch Kreditkartendaten der Kunden ausgespäht. Gemäß den Analysen des Unternehmens wurden die Daten nach der Ausleitung auf dem Server eines schweizerischen Providers gespeichert. Das Unternehmen geht davon aus, dass ca. zwei Millionen Kundendatensätze durch den oder die Täter kopiert und ausgeleitet wurden.

Im Februar dieses Jahres erbeuteten Kriminelle in einer konzertierten weltweiten Aktion innerhalb von zwei Tagen 40 Millionen US Dollar! Die Tat war akribisch vorbereitet worden: Zunächst brachen die Täter in die Abrechnungssysteme der Kreditkartenabwickler Bank of Muscat im Oman und Rakbank in den Vereinigten Arabischen Emiraten ein und setzten die Limits von aufladbaren Kreditkarten nach oben. Anschließend benutzten sie die Daten von einigen wenigen Prepaid-Kreditkarten der Banken und übermittelten diese an weltweit verteilte Helfer, die damit wiederum Blankokarten codierten und dann Abhebungen an Geldautomaten durchführten.

Am 20. und 21. Februar 2013 wurden nahezu zeitgleich in mindestens 23 Staaten mit diesen gefälschten Karten bei weltweit über 17.000 Transaktionen an Automaten Geld abgehoben. Allein in Deutschland betrug der Schaden bei knapp 1.000 Abhebungen in Essen, Hamburg, Dortmund, Koblenz, Bremen und Frankfurt/Main ca. 2,5 Millionen Euro.

Nicht nur gewöhnliche Cyber-Kriminelle sind an Daten interessiert

Um möglichst umfassende Informationen aus den Bereichen Politik, Wirtschaft und Militär sowie über hier aufhältige Oppositionelle zu erlangen, nutzen ausländische Nachrichtendienste die Möglichkeiten des Internet. Sie versuchen, mittels Hacking und Malware illegal in fremde Rechnersysteme einzudringen oder direkt Informationsknotenpunkte anzuzapfen. Nachrichtendienstlich betriebene IT-Angriffe sind dem äußeren Anschein nach kaum von allgemeinkriminellen Angriffen zu unterscheiden. Vordergründig weisen sie eher auf andere Straftaten hin, wie zum Beispiel Konkurrenzausspähung, Exportverstöße, Diebstahl oder eben Cybercrime. Dies mag ein Grund dafür sei, dass es zur Einleitung und Führung von strafrechtlichen Ermittlungsverfahren wegen klassischer Spionagedelikte im Zusammenhang mit Cybercrime bislang nicht gekommen ist. Erschwerend kommt hinzu:

Viele Opfer bemerken den unerlaubten Informationsabfluss nicht, oder sie zeigen diese Fälle aus Angst vor Imageverlust nicht an.

Das Internet bietet zahlreiche Nutzungsmöglichkeiten für den illegalen Handel insbesondere mit Drogen und mit Kinderpornografie. Die Vorteile des Internet für den Handel mit diesen illegalen Gütern sind offensichtlich: Der Handel ist anonym für Anbieter und Abnehmer und in Sekundenschnelle rund um die Uhr von jedem Ort der Welt aus möglich. Das Internet ist aktuell das wesentliche Medium für die Verbreitung und den Konsum von Kinderpornografie. Im Juli dieses Jahres gelang es, eine der zentralen, international tätigen Plattformen zur Verbreitung von Kinderpornografie abzuschalten. Auf der Plattform waren insgesamt zwei Millionen kinderpornografische Bilder.

Nach Einschätzung der beteiligten Strafverfolgungsbehörden ist der Verantwortliche der Plattform weltweit die zentrale Figur im Bereich des Besitzverschaffens, Verbreitens und Drittbesitzverschaffens von kinderpornografischen Inhalten. Mit Abschalten der Plattform wurden die Online-Aktivitäten von ca. 25.000 Pädophilen unterbrochen, die Szene konnte deutlich verunsichert werden. Über die retrograde Sichtung der verschiedenen Boards der Plattform konnten ca. 200 weitere mutmaßliche deutsche Nutzer festgestellt werden. Zu diesen Usern liegen lediglich Nick-Name und E-Mail-Adressen, keine IP-Adressen vor, eine Identifizierung ist so nur noch in wenigen Ausnahmefällen möglich. Für die Polizei besteht bei dieser Art von Foren ein zusätzliches Problem: Viele Inhalte werden ausschließlich in geschlossenen Foren kommuniziert. Neue Mitglieder werden nur aufgenommen, wenn sie selbst kinderpornografisches Material bereitstellen. Spezielle Bereiche werden exklusiv für Mitglieder eingerichtet, die nachweislich selbst Kinder sexuell missbrauchen.

Ein besonderes Beispiel für den digitalen Handel inkriminierter Waren ist die Webseite „Silkroad“. Silkroad war eine Webseite im sogenannten „Deep Web“, jenem Teil des Internet, der nicht über normale Suchmaschinen auffindbar ist. Silkroad war eine Art Online-Schwarzmarkt im Stil eines gewöhnlichen Onlineshops, über den nahezu alles käuflich erworben werden konnte. Die Bezahlung erfolgte anonym über Bitcoins, der geschätzte bisherige Umsatz beläuft sich auf 1,2 Milliarden US-Dollar. Als versteckter Dienst im

sogenannten „TOR-Netzwerk“[3] wurde die Anonymität der Nutzer durch Verschleierung der Verbindungsdaten gewahrt. Erschwerend kommt hinzu, dass die Onlinebezahlungen allein über die virtuelle Währung Bitcoins[4] abgewickelt wurden. Die Bitcoins wurden von Kunden an ein Treuhandkonto überwiesen, der Betrag erst dann an den Verkäufer ausgezahlt, wenn die Ware geliefert wurde. Die Auslieferung der bestellten Waren von Kleidung über Waffen bis hin zu illegalen Drogen erfolgte per Post.

Im Rahmen eines Ermittlungsverfahrens des Bayerischen Landeskriminalamtes gelang es, mehrere Tatverdächtige zu identifizieren, die über die anonymisierte Plattform verschiedene Betäubungsmittel weltweit vertrieben. Dabei gingen die Täter äußerst konspirativ vor, jegliche Kommunikation erfolgte verschlüsselt. Die Umsätze beliefen sich im Tatzeitraum von acht bis vierzehn Monaten auf über 300 Kilogramm Betäubungsmittel und über 500.000 Ecstasy-Tabletten, bei einem geschätzten Gewinn von ca. 8,7 Millionen Euro. Anfang Oktober dieses Jahres konnte der mutmaßliche Betreiber des Onlineportals Silkroad festgenommen und die Internetseite durch die US-Behörden abgeschaltet werden. Neuesten Meldungen ist zu entnehmen, dass Silkroad 2.0, eine Art Klon der Ursprungsseite, bereits online ist.

Kriminelle nutzen die Anonymität digitaler Währungen

Im Cyberspace existieren unterschiedliche Währungen, wobei das System ähnlich wie bei "normalen" Währungen funktioniert. Euro, Dollar und andere Währungen werden gegen virtuelle Zahlungsmittel eingetauscht, die dann als verschlüsselte Codes auf der Festplatte des Computers existieren. Mittlerweile akzeptieren nicht mehr nur Online-Anbieter digitale Zahlungsmittel. In der relativen Anonymität dieser Währungen liegt deren Attraktivität für kriminelle Machenschaften, insbesondere für Geldwäscheaktivitäten, begründet.

International bekannt ist der Fall der Liberty Reserve, ein weltweites Geschäftsmodell: Internetnutzer konnten bei Liberty-Reserve ein Konto eröffnen, auf das sie bei Drittanbietern "echtes" Geld einzahlten, welche daraufhin die von ihnen erkauften Liberty Reserve-Geldeinheiten auf den Nutzerkonten zur Verfügung stellten. Transaktionen der Liberty Reserve erfolgten ebenfalls über Drittanbieter, wobei das Unternehmen jeweils ein Prozent der Transaktionssumme einbehielt. Da bei diesen Dienstleistungen die Angabe falscher persönlicher Daten möglich ist und keine Authentifizierung verlangt wird, bot sich Liberty Reserve für Geldwäsche im großen Stil geradezu an. Da die Überweisungen über Wechseldienste erfolgten, waren die Zahlungsvorgänge nicht nachvollziehbar.
Über eine Million Anwender sollen das Angebot genutzt haben. Seit 2006 sollen insgesamt 55 Millionen Transaktionen mit einem Gesamtvolumen von rund sechs Milliarden US-Dollar durchgeführt worden sein. Im Mai 2013 wurde Liberty Reserve mit Sitz in Costa Rica von den US-Behörden geschlossen – ein Erfolg für die Strafverfolgungsbehörden? Nur für den Moment, denn vergleichbare Angebote haben sich bereits etabliert und werden von Kriminellen rege genutzt.

In Deutschland sind E-Geldinstitute zur Identifizierung ihrer Kunden verpflichtet, sofern der gespeicherte E-Geld-Betrag 100 Euro pro Monat übersteigt. Da die Anbieter von

[3] TOR war ursprünglich ein Akronym für „The Onion Routing“ oder „The Onion Router“ (englisch onion = Zwiebel).

[4] Bitcoins sind eine virtuelle Peer-to-Peer Währung, die internationale Überweisungen unter ihren Nutzern ermöglicht. Dabei werden reale Währungen in Bitcoins getauscht. Die Finanzwelt der Bitcoins ist unabhängig von klassischen Banken oder Finanzinstituten und kann daher staatlich bisher nicht reguliert werden.

Zahlungsdiensten ihren Geschäftssitz jedoch meist nicht in Deutschland haben, unterliegen sie weder der Aufsicht der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) noch dem deutschen Geldwäschegesetz. Nationales Recht stößt hier an seine Grenzen. Geldwäscher nutzen gezielt aus, dass Rechtshilfeersuchen langwierig sind, dass in anderen Ländern andere Bank- und Berufsgeheimnisse gelten und die Kontroll- und Strafverfolgungsintensität unterschiedlich ausgeprägt ist. E-money, Bitcoins, financial agents vereinfachen Geldwäsche und verringern gleichzeitig das Entdeckungsrisiko für Kriminelle. Digitale Zahlungsmittel anonymisieren kriminelle Finanzströme.

Straftaten im Bereich Cybercrime werden auch aus einer ideologischen Motivation heraus verübt

Bei Delikten wie Diebstahl, Betrug, Erpressung, Drogenhandel oder Geldwäsche sind die finanziellen Interessen der Täter offensichtlich. Es ist allgemein bekannt, dass das Internet inzwischen das wichtigste Mittel zur Verbreitung von Propaganda und Veröffentlichungen religiös motivierter terroristischer Organisationen und Gruppierungen ist. Die Zeiten, in denen Ideologieschulungen im Hinterzimmer stattfanden, Fanzines und Schriften zur ideologischen Schulung unter dem Ladentisch vertrieben wurden, sind vorbei.

In den vergangenen Jahren stellten wir vor allem Internetveröffentlichungen der großen und bekannten Terrororganisationen wie Al Qaida, Islamische Bewegung Usbekistan (IBU), Kaukasisches Emirat und Taliban fest. Seit einiger Zeit beobachten wir, dass auch kleinere Organisationen die Vorteile des „medialen Jihad“ erkannt haben und mit verschiedenen neuen Medienprodukten auf den jihadistischen Medienmarkt drängen. Auch radikale Gruppen in Deutschland nutzen das Internet für Propaganda und Rekrutierung. Was bedeutet das alles konkret für die Strafverfolgungsbehörden? Wie sieht die effektive Strafverfolgung im Zeitalter des Internet aus? Was kennzeichnet die Kriminalistik 2.0?

Ergebnisse des Szenario-Projektes „Always on 2018“

Zunächst möchte ich einen Blick in die Zukunft werfen, den das BKA-Zukunftsteam mit dem Szenario-Projekt „Always On 2018“ für uns vorgenommen hat. Die wesentlichen Ergebnisse sind: Immer höhere Anforderungen an Recherche- und Analyseverfahren im BKA sind zu erwarten. Da schnellere Übertragungstechnologien höhere Datentransfers bei der Verübung von Straftaten nach sich ziehen, werden die im Strafverfahren sichergestellten Datenmengen insgesamt zunehmen.

Die neuen Schwerpunkte krimineller Internet-Aktivitäten werden vor allem in den Bereichen des virtuellen Handels, der virtuellen Währungen und im Cyber-Terrorismus gesehen. Aber auch die Organisierte Kriminalität in Kombination mit „crime on demand“, bei der ohne Fachkenntnisse am eigenen PC Malware und Infrastruktur aus dem Angebot eines qualifizierten Unternehmens krimineller Prägung zusammengestellt und für den eigenen „Raubzug“ gemietet werden können, wird zunehmen. In naher Zukunft wird sich nicht allein für die öffentliche Infrastruktur, sondern durch neue Gebäudetechnologien (Stichwort: Smart Home) auch für Privatpersonen die Gefährdung durch Internetkriminalität erhöhen. Die Nutzung moderner Technologien und Kommunikationsmittel an einer Vielzahl von Geräten bzw. Schnittstellen führt nicht nur zu größeren Verwundbarkeiten, sondern auch zur vermehrten Preisgabe personenbezogener Daten.

Das BKA muss sich auf neue Bedrohungsszenarien einstellen, die Früherkennung stärken und ein abteilungsübergreifendes Wissensmanagement einführen. Dazu gehört auch ein internes Social Network für dienstliche Zwecke. Das BKA soll sich zum Cloud-Anbieter für die Bundesländer entwickeln, um eine kostensparende Harmonisierung der polizeilichen Produkte und eine Homogenisierung der Standards zu erreichen. Das BKA soll ein Ausbildungsmodul „Digitale Ermittlungen“ in der Fachhochschulausbildung verankern und die zielgerichtete Fortbildung aller Mitarbeiter in Richtung Schlüsselkompetenzen intensivieren.

Herausforderungen für die Kriminalistik 2.0

Die genannten Punkte betreffen die mittelfristige Zukunft. Aktuell liegen folgende Aufgaben vor uns: Die effektive Bekämpfung von Cybercrime setzt ein möglichst präzises Bild des Phänomens voraus. Sehr verdienstvoll ist in diesem Zusammenhang die Dunkelfelduntersuchung des LKA Niedersachsen, deren erste Ergebnisse der Innenminister Niedersachsens Ende Oktober dieses Jahres der Öffentlichkeit präsentiert hat. Fast 20.000 Niedersachsen im Alter ab 16 Jahre haben sich an der Umfrage beteiligt. Das niederschmetternde, aber zu erwartende Ergebnis: Nur 8,5 % aller computerbezogenen Straftaten werden angezeigt.

Die Anzahl der Fälle im Bereich Phishing über das Internet soll beim Zehnfachen der amtlich gemeldeten Zahlen, der Datenverlust durch Computer-Viren oder Trojaner sogar beim Zwanzigfachen liegen. Die tatsächlichen Zahlen auf Bundesebene liegen demnach nicht bei 250.000, sondern eher bei 2,5 Millionen Geschädigten. Aber auch diese Zahl halten wir für zu gering, da häufig der strafbare Versuch einer Infiltration gar nicht bemerkt wird. Das Bedrohungspotenzial ist daher sehr viel höher. Das unterstreichen auch die vom BSI im August 2013 veröffentlichten Zahlen des Identitätsdiebstahls: Innerhalb nur eines Vierteljahres waren es stattliche 250.000 Fälle.

Cybercrime ist eine besonders auch von deutschen Unternehmen unterschätzte Gefahr. Insider teilen die Branche in zwei Kategorien ein: In die, die schon gehackt worden sind, und die, die gerade gehackt werden. Die Sicherheitsbehörden benötigen zeitnahe Informationen über die Anzahl und die zeitliche und örtliche Verteilung von Fällen, über das genaue Vorgehen der Täter, ihre organisatorischen Zusammenhänge. Diese Informationen müssen so schnell und unmittelbar wie nur möglich vorliegen. Das gilt auch für die vom Ausland ausgehenden Angriffe auf deutsche Unternehmen und User, die bisher in der PKS nicht registriert werden. Aktuelle Vorfälle haben gezeigt, dass für die Täteridentifizierung umgehendes polizeiliches Handeln ein erfolgskritischer Faktor ist. In einem konkreten Fall hatte der Tatverdächtige bereits mit der Löschung beweisrelevanter Daten begonnen. Unternehmen sehen häufig von Anzeigen ab und auch für Privatpersonen ist der Gang zur Polizei eher die Ausnahme – teilweise aus Scham, aber auch weil Angriffe als nicht schwerwiegend genug erachtet oder einfach nicht erkannt werden. Das Vorgehen der Polizei muss sich auf die Bedürfnisse der Geschädigten einstellen. Unauffälliges und schnelles Vorgehen bei der Tatortaufnahme muss gesichert sein, um den Unternehmen die Angst vor Reputationsverlusten und Arbeitsausfall durch lange Sicherstellungen von IT-Systemen zu nehmen.

Die Bekämpfung von Cybercrime, speziell Ermittlungen in diesem Phänomenbereich, stellen hohe technische Anforderungen an die Strafverfolgungsbehörden. Die folgenden Ausführungen vermitteln einen Eindruck, mit welchen Problemen sich die Forschung und Entwicklung im Bereich Cybercrime im BKA derzeit beschäftigt.

Big Data heißt eines der Problemfelder. Wir erforschen und erproben intelligente Methoden zur computerunterstützten Auswertung großer fremdsprachiger Datenmengen. Die BKA-Eigenentwicklung ist in der Lage, 56 Sprachen in Texten zu erkennen. Hier geht es sehr exotisch zu: Derzeit wird die computergestützte Auswertung für die Sprachen Kurdisch-Sorani und Kinyarwanda[5] zum Zweck der Terrorismusbekämpfung bedarfsorientiert weiterentwickelt. Die Entwicklung umfasst eine automatisierte Extraktion von Kerninformationen wie zum Beispiel Personen-, Orts- und Organisationsnamen, Kfz-Kennzeichen, Bankdaten, Währungsbeträge usw. Diese Extraktion dient der Filterung großer Datenmengen im Sinne einer ersten Relevanzbewertung. Ein weiterer Schritt ist die automatisierte Extraktion von Beziehungen zwischen Entitäten und eine maschinelle Rohübersetzung. Erste Tests zeigen eine deutliche Einsparung von Ressourcen. Der Sachbearbeiter kann verwertbare Informationen aus fremdsprachigen Texten filtern, ohne zum Beispiel über russische oder arabische Sprachkenntnisse zu verfügen.
Die im Rahmen von Ermittlungsverfahren festgestellten Datenmengen werden immer größer. Sicherstellungen bis zu einem Datenvolumen von einem Petabyte sind bereits heute zu bewältigen. Das entspricht dem Inhalt von 500 Milliarden DINA4-Seiten oder einer Strecke von 75.000 Kilometern nebeneinander aufgestellten Aktenordnern!

Die Ermittlungs- und Auswertungsarbeit der Polizei steht vor einem Paradigmenwechsel

Was meine ich damit?

Zum Einen: Strafverfolgung ist konfrontiert mit

(1) unstrukturierten Daten in vielerlei Formaten, oft ohne zu wissen, ob und welche Beweismittel in diesen Daten liegen,
(2) kryptierten Datencontainern auf inkriminierten Datenträgern sowie
(3) einer hohen Komplexität in der mobilen IT-Forensik.

Zum anderen sehen wir uns stetig wachsenden Datenmengen gegenüber, die eine intelligente Datenselektion statt einer allumfassenden Auswertung erfordern. Diese Feststellung könnte auch rechtlichen Anpassungsbedarf auslösen und zur Neudefinition der Zukunft der Ermittlungsgrundlagen führen.

Ein weiteres Problem sind kontaminierte Daten, sogenannte „Schmutzdaten“, die in einer sicheren Umgebung ausgewertet werden müssen. Dies ist unabdingbar auch für die Qualität der Ermittlungsarbeit. Unser Ziel ist der Aufbau einer zentralen internetverbundenen Infrastruktur- und Schmutzdatenumgebung, kurz IVIS, die gegenüber den hausinternen Netzwerken und gegenüber dem IT-gestützten Bund-Länder-Informationsaustausch besonders abgeschirmt ist.

Nicht nur gespeicherte Daten, auch Kommunikation und Interaktion im Internet können heute mit einfachen Mitteln anonymisiert und kryptiert werden. Zahlreiche Anbieter bieten dazu kostengünstige Produkte an, worauf immer mehr Täter zurückgreifen. Das mobile Internet führt zu einem nomadisierenden Nutzerverhalten. Der Markt wird sich auch in Zukunft weiter hin zu mobiler und ultramobiler Internet-Kommunikation bewegen.

Die Verlagerung von Daten in die Cloud wird erhebliche Auswirkungen auf die investigativen Möglichkeiten der Gefahrenabwehr und Strafverfolgung haben. Die Cloud wird nicht nur

[5] Eine unter anderem in Ruanda verbreitete Sprache.

Tatort sein, zum Beispiel bei der Ausspähung gespeicherter Kreditkarteninformationen, sondern auch Tatmittel, zum Beispiel im Rahmen einer Spam-Infrastruktur oder in Form von Rechenleistung zur Überwindung von Passwortsperren. Infolge der Beliebigkeit des Netzzuganges steigen sowohl der operative Vorermittlungsaufwand im Hinblick auf den jeweils genutzten physikalischen Anschluss, als auch die Wahrscheinlichkeit von Überwachungslücken bei schwerer Kriminalität.

Interne Auswertungen bei bedeutenden Verfahren des Terrorismus und der Schwerkriminalität zeigen, bei einer Stichprobe von 85 TKÜ-Maßnahmen, folgendes Bild: In drei von vier TKÜ-Maßnahmen (75 %) werden Verschlüsselungs-, Kryptierungs- und/oder Anonymisierungsdienste genutzt! Bei der Untergruppe von DSL-TKÜ-Maßnahmen sind zwei von drei Maßnahmen (68 %) verschlüsselt, bei Mobilfunk-TKÜ-Maßnahmen sind es acht von zehn (81 %). Die Überwachung der Telekommunikationsinhalte ist in diesen Fällen so gut wie nicht möglich. Derzeit ist es technisch unmöglich, einen laufenden kryptierten Kommunikationsvorgang zu entschlüsseln.

Vor die Lage zu kommen wird immer schwieriger, zum Teil sogar unmöglich!

Das wirkt sich unmittelbar auf die Bekämpfung der Schwerstkriminalität in Deutschland aus. Im Frühjahr 2014 wird das BKA ein spezielles Fachsymposium zum Thema „Organisierte Kriminalität und Schwerstkriminalität“ durchführen, um die Lage der OK insgesamt, insbesondere der italienischen Mafia und der russisch-eurasischen Kriminalität mit Bezügen zu Deutschland sowie der aktuellen Rockerkriminalität zu beleuchten. Dabei werden die zukünftigen Möglichkeiten der Beweiserhebung eine wichtige Rolle spielen.

Ein zweites großes Thema ist die Anonymisierung im Internet. In den Phänomenbereichen Kinderpornografie, Rauschgiftkriminalität, Waffenhandel und Cybercrime werden zunehmend TOR-Netzwerke genutzt, Anonymisierungsnetzwerke, die aus vielen voneinander unabhängigen Servern bestehen. Jeder kann weltweit dieses Netzwerk mit eigenen Servern unterstützen. Dazu bedarf es lediglich einer im Internet kostenlos erhältlichen Software, die auf einem eigenen Server installiert und gestartet werden muss. Weltweit gibt es mehrere tausend TOR-Server. Der Kommunikationskanal wird über mindestens drei ausgewählte Server verschleiert, wobei innerhalb des TOR-Netzwerkes jeder Server nur den Vorgängerserver und den Nachfolgeserver kennt. Sämtliche Kommunikation der TOR-Server untereinander, wie auch zur Nutzersoftware, ist verschlüsselt. Keine Kommunikationsinstanz hat Kenntnis darüber, welcher Benutzer mit welcher Webseite Kontakt aufgenommen hat. In einem Ermittlungsverfahren ist es ausländischen Partnern gelungen, in ein TOR-Netzwerk einzudringen und – wie schon erwähnt – den bislang weltweit größten Ring von über 25.000 Pädophilen mit zwei Millionen kinderpornografischen Abbildungen zu detektieren. Mit dieser Herausforderung setzen wir uns derzeit auch in der Forschung auseinander.

Gefahrenabwehr und Strafverfolgung erfordern Gesetze, die sich an den Formen heutiger Kommunikation und Interaktion orientieren. In der virtuellen Welt kann mit den Instrumenten der analogen Welt nicht erfolgreich ermittelt werden.

Ich kann nur immer wieder betonen: Nicht die Polizei speichert zum Beispiel Verkehrsdaten, sondern dies erfolgt bei einer Vielzahl von Providern. Deshalb kann der Staat auch nicht willkürlich auf diese Daten zugreifen oder in Unmengen von Daten eigenmächtig recherchieren. Nur wenn ein Richter anordnet, dass zur Bekämpfung schwerer Kriminalität der Zugriff erlaubt ist, werden bestimmte Daten für die Strafverfolgung extrahiert und nutzbar gemacht.

Zu einem ganzheitlichen kriminalistischen Bekämpfungsansatz gehört auch, althergebrachte, bewährte Methoden nicht zu vernachlässigen. Mittel wie Fahndung, Observation, Wohnraumüberwachung und der Einsatz verdeckter Ermittler zählen nach wie vor zum Repertoire polizeilicher Ermittlungen in Fällen schwerer und schwerster Kriminalität.

Im Bereich der klassischen Fahndung eröffnet uns das Internet neue Möglichkeiten

Der Anschlag während des Boston-Marathons hat die US-amerikanischen Behörden mit der Auswertung von Massendaten in Form von Videofilmen und elektronisch übermittelten Fotos konfrontiert. Zukünftig wird das öffentliche Werben um solche Hinweise aus der Bevölkerung bei spektakulären Verbrechen zum Standard der Tatrekonstruktion und Täterermittlung gehören. Der abgelegte Sprengsatz in einer Tasche auf dem Bonner Hauptbahnhof Ende letzten Jahres wäre der klassische Anwendungsfall gewesen.
Auch die klassische Öffentlichkeitsfahndung verändert sich. Die Zielgruppe der jüngeren Bevölkerung informiert sich weniger durch Fernsehen, Rundfunk und Printmedien, sondern stärker über soziale Netzwerke wie zum Beispiel Facebook.
In Verbindung mit der enormen Verbreitung mobiler Endgeräte ist es möglich, weite Teile der Bevölkerung nach schwerwiegenden Straftaten zeitnah und zielgerichtet auf lokaler oder regionaler Ebene anzusprechen und um Hinweise zu bitten. Im Hinblick auf die Nutzung von Facebook sind jedoch nach wie vor datenschutzrechtliche Fragen zu klären.
Wir gehen davon aus, dass die verdeckte Informationsgewinnung und der Einsatz von verdeckt arbeitenden Polizeibeamten und Vertrauenspersonen angesichts der Abschottung der Täter im Internet eine größere Bedeutung bekommen wird.

IuK-Kompetenz ist heute eine der Schlüsselqualifikationen für Kriminalisten

Die Strafverfolgungsbehörden brauchen Mitarbeiterinnen und Mitarbeiter, die in der Lage sind, die digitalen Spuren der Kriminellen aufzunehmen, die Täter zu identifizieren und ihnen ihre Taten nachzuweisen. Spezialdienststellen sollen Erkenntnisse liefern, was im Netz, im „Dark Web“ und in der „Underground Economy“ vor sich geht und wie wir darauf reagieren können, hier benötigen wir Experten wie Informatiker und Cyberanalysten.

Gleichwohl sind Spezialdienststellen und Experten allein keine ausreichende Antwort auf Cybercrime. Zukünftig – das ist meine feste Überzeugung – werden wir die Bekämpfung von Cybercrime nicht allein den Spezialisten überlassen können. Unser gesamtes Personal muss bei der Bekämpfung entsprechender Straftaten mitarbeiten können. Im Bundeskriminalamt sind inzwischen in nahezu allen Abteilungen Informatiker beschäftigt. Diesen Ansatz werden wir weiter ausbauen. Cybercrime wird sich als eigenständige Deliktsform und als Tatmittel in vielen Phänomenbereichen zu einer Querschnittskriminalität entwickeln.

IuK-Kompetenz ist heute eine der Schlüsselkompetenzen, über die Kriminalisten verfügen müssen, um Straftaten zukünftig erfolgreich aufzuklären. Was heute die Aufgabe von Spezialisten ist, muss morgen das Handwerkszeug jedes Kriminalisten sein. Die Curricula unserer Ausbildungseinrichtungen müssen dazu neu justiert werden. Das gilt für die Ausbildung zum höheren Dienst an der Deutschen Hochschule der Polizei ebenso wie für die Fachhochschulausbildung an den Fachhochschulen der Polizei für den gehobenen Dienst.

Effektive Bekämpfung der Cybercrime in Kooperation mit Wirtschaft und Wissenschaft

Wenn wir von Fachkompetenz sprechen, dürfen wir uns nicht nur auf die Sicherheitsbehörden konzentrieren. Eine Vielzahl von Fachleuten wird zur Netzwerkforensik, zum Umgang mit großen Datenmengen, zur Kryptoanalyse oder Dekryptierung benötigt. Viele Fachleute sind in der Wirtschaft und Wissenschaft tätig. Ich möchte Ihnen anhand eines echten Szenarios darstellen, welcher Mehrwert für alle Beteiligten zu erzielen wäre, wenn die Sicherheitsbehörden die Expertise von Wirtschaft und Wissenschaft stärker nutzen könnten:
Ein Wirtschaftsunternehmen mit Kernkompetenz in IT-Dienstleistungen unterhält ein Rechenzentrum, um seinen Kunden verschiedene serverbasierte Produkte zur Verfügung zu stellen. Dabei haben die Kunden Administratoren-Zugriff auf die von ihnen gemieteten Produkte. Durch interne Monitoring-Sicherheitsmechanismen wird festgestellt, dass die Netzwerkinfrastruktur langsamer agiert als normal. Das Unternehmen stellt fest, dass sich Unbekannte Zugriff auf die komplette Netzwerkinfrastruktur verschafft haben und die vollumfängliche Kontrolle über sämtliche Server – über 1.000 – des Unternehmens übernommen haben. Das IT-Unternehmen wendet sich an die Strafverfolgungsbehörden.

Je nach der von Täterseite gewählten Angriffsstruktur kann es erforderlich sein, externe Spezialisten heranzuziehen, zum Beispiel in den Bereichen Entschlüsselung von Programmcodes oder Netzwerkforensik. Im Rahmen des ‚ersten Zugriffs' wird unter Einbeziehung von externen „Mitarbeitern" (zum Beispiel eines Netzwerkingenieurs) eine Datensicherung betroffener Serversysteme durch die IuK-Forensik des BKA erstellt. Dies gewährleistet die Beweissicherung zum Zeitpunkt des Angriffs. Cyberanalysten und Softwareanalytiker des BKA sowie von IT-Sicherheitsunternehmen versuchen, die Daten bzw. den Datenverkehr zu analysieren und die Wirk- und Vorgehensweise des Angriffs bzw. der Schadsoftware zu bestimmen. Anschließend wird der Zugriff auf das Netzwerk des Datenzentrums durch den Angreifer unterbunden und weiterer Schaden (zum Beispiel das Abgreifen von Kundendaten, Betriebsgeheimnissen etc.) abgewendet.

Zu guter Letzt muss die Sicherheitslücke in der IT-Infrastruktur versiegelt werden. Hierzu werden externe Partner aus IT-Security-Unternehmen benötigt. Über diese externen Partner können eventuell Informationen über bereits erfolgte Angriffe derselben Tätergruppierung gewonnen werden, wodurch gegebenenfalls neue Ermittlungsansätze generiert werden können. Begleitend erhebt das BKA über seine internationalen Kontakte Informationen zu ähnlich gelagerten Vorfällen im Ausland. Schließlich wird durch das BSI ein Warnhinweis für potenziell gefährdete Einrichtungen herausgegeben.

Der Mehrwert einer solchen Zusammenarbeit liegt auf der Hand: Die Reaktionszeit bei Eintritt eines Einsatzfalles ist kurz, da bereits bei Beginn der Ermittlungen die benötigte Expertise zur Verfügung steht. Wir wollen im BKA das Modell einer Aufrufeinheit, einer sogenannten „Quick Reaction Force Cybercrime", bestehend aus Experten der Sicherheitsbehörden von Bund und Ländern und Spezialisten aus Wirtschaft und Wissenschaft einrichten.

Die in Unternehmen, Forschungsinstituten, Wirtschaft und Wissenschaft vorhandene Fachkompetenz muss aber noch viel umfassender in die Bekämpfung der Cyber-Kriminalität einbezogen werden.Als ersten Schritt in diese Richtung haben wir mit zentralen Akteuren aus dem Bankensektor für den Bereich Cybercrime eine Kooperation in Form einer institutionalisierten Private Public Partnership (iPPP) geschlossen, weitere Partner sollen folgen. Der Vorteil einer solchen Partnerschaft liegt in erster Linie in der strukturierten und vertrauensvollen Zusammenarbeit.

Wie wichtig die Zusammenarbeit ist, zeigt die aktuelle Entwicklung bei den Sicherheitsverfahren im Online-Banking. Aktuell wird das sogenannte mobile TAN-Verfahren angegriffen, indem auf einem bereits mit Schadsoftware infizierten Rechner eines Onlinebanking-Kunden bei der Anmeldung ein „Pop-up"-Fenster eingeblendet wird. Dem Kunden wird über ein angebliches Sicherheitsupdate der Bank geraten, ein Update des mobilen TAN-Verfahrens auf seinem Handy vorzunehmen. Führt der Onlinebanking-Kunde das vermeintliche Sicherheitsupdate (es handelt sich um eine vom Täter gesendete Datei) aus, infiziert er sein Handy jedoch unwissentlich mit Schadsoftware. Die auf dem Handy installierte Schadsoftware bietet dem Täter die Möglichkeit, eingehende Nachrichten ohne Wissen des Besitzers an eine andere Rufnummer weiterzuleiten. Über diese Methode gelangt der Täter an die für die Autorisierung einer Transaktion erforderliche mobile TAN. Nicht nur in Fällen wie diesem ist der zeitnahe Austausch über neue Modi Operandi zwischen Ermittlern und Unternehmen entscheidend, um Täter möglichst schnell an weiteren Straftaten zu hindern.

Cybercrime ist international – die enge Zusammenarbeit auf internationaler Ebene ein zentraler Punkt

Europol und Interpol kommen in der internationalen Kooperation Schlüsselpositionen zu.
Beide Institutionen verfolgen zur Bekämpfung der Cybercrime einen globalen, koordinierten und kooperativen Ansatz unter Beteiligung öffentlicher und privater Partner. Hierzu wurde bei Europol in Den Haag das „European Cybercrime Center" (EC3) gegründet. Der „Interpol Global Complex for Innovation", dessen Eröffnung für September 2014 in Singapur – auch mit Unterstützung des BKA – geplant ist, soll: Möglichkeiten der digitalen Forensik vorhalten, Aus- und Fortbildung weltweit leisten, Bindeglied zwischen den Polizeibehörden und der Wirtschaft sein, um gemeinsam die Risiken von Cybercrime einzudämmen und neue Technologien im Hinblick auf sicherheitsrelevante Aspekte beobachten und entwickelte Tools allen Mitgliedsstaaten zur Verfügung stellen.

Fazit

Ich fasse die Ergebnisse meiner Analyse für die Kriminalistik 2.0 zusammen:

Das Internet ist die perfekte Plattform zur Begehung von Straftaten: schnell, anonym, weltweit vernetzt.

Cybercrime hat das Potenzial zum Massendelikt: Spezifische Kenntnisse der Täter sind nicht zwingend notwendig, Zugänge und Tatgelegenheiten sind nahezu unbegrenzt und jeder kann Opfer werden: Bürgerinnen und Bürger, Unternehmen und Staaten.

Die Innovationszyklen krimineller Tatbegehungsweisen werden immer kürzer: Täter sind höchst flexibel, suchen nach immer neuen Einfallstoren und nutzen jede technische Möglichkeit für ihre Zwecke.

Kommunikation und Interaktion im Internet werden anonymer: Verschlüsselung, Kryptierung und Anonymisierung nehmen zu.

Nationale Grenzen sind irrelevant: Tatorte, Taterfolgsorte und Aufenthaltsorte der Täter sind unabhängig voneinander. Beweismittel finden sich nicht mehr durchgängig am Tatort, sondern ausgelagert in einer Cloud.

Es gibt kein eindeutiges Profil von Cyberkriminellen: Vom Amateur bis zum Profi sind alle technischen Fähigkeiten vertreten, die Motivlagen sind höchst unterschiedlich: Monetäre, ideologische und politische Ziele treten unabhängig voneinander auf oder vermischen sich.

Die Sicherheitsakteure sind gefordert, auf der Höhe der Zeit zu bleiben: Technische Voraussetzungen, geschultes Personal, rechtlich geeignete Rahmenbedingungen und eine hohe Anpassungsfähigkeit der Strafverfolgungsbehörden sind national und international durchgängig notwendig.

Sicherheit im Internet kann nur durch Kooperationen gewährleistet werden: Schulterschlüsse zwischen Nationen, enge Kooperationen mit Wirtschaft und Wissenschaft sowie das Vertrauen der Bürgerinnen und Bürger in die Sicherheitsbehörden sind die Schlüssel einer effektiven Bekämpfung und sind zentral, um das notwendige Vertrauen ins Internet zu bewahren.

Technik und Technologien spielen in allen Lebensbereichen eine nicht mehr wegzudenkende Rolle. Großen Chancen und Möglichkeiten stehen Abhängigkeiten, Risiken und Verletzbarkeiten gegenüber.

Es ist die Aufgabe aller Akteure, diese Chancen zu gestalten, Missbrauch zu verhindern und zu bekämpfen, und im Schadensfall effektiv strafbare Handlungen zu verfolgen, um die Legitimität unserer Rechtsordnung, die auf Rechtsetzung und Rechtsdurchsetzung gründet, zu bewahren.

Das Strafrecht gilt auch im Cyberspace, auch in einer digitalisierten und hochgradig vernetzten Gesellschaft. Die justiziellen Ermittlungsinstrumente müssen – insbesondere mit Blick auf technische Entwicklungen – angemessen an die Lebenswirklichkeit angepasst werden. Dazu gibt es in einem Rechtsstaat keine Alternative. Die notwendigen Instrumentarien zur Rechtsdurchsetzung müssen geschaffen werden. Sonst verliert die staatliche Ordnung mittel- bis langfristig an Legitimität. Die Gerechtigkeitslücke darf sich nicht vergrößern.

Cybersecurity - strategisch-politische Aspekte dieser globalen Herausforderung

Michael Daniel

Eingangsbemerkungen

Guten Morgen allerseits! Vielen Dank für die freundlichen einführenden Worte. Ich freue mich, heute mit Ihnen hier in Wiesbaden zu sein und an der alljährlichen BKA-Tagung teilzunehmen - vor allem, da ihr Thema **"Cybercrime: Bedrohung, Intervention, Abwehr"** lautet. Dabei möchte ich unseren deutschen Gastgebern ein Kompliment für die Ausrichtung einer solch großartigen Veranstaltung aussprechen.

Ich heiße Michael Daniel und bin gegenwärtig Special Assistant des Präsidenten sowie Koordinator für Cybersicherheit im Weißen Haus.

In dieser Funktion leite ich die Erarbeitung einer nationalen Cybersicherheits-Strategie und -Politik der US-amerikanischen Regierung und überwache deren Umsetzung im Auftrag von Präsident Obama.

Was großartig an dieser Aufgabe ist, ist die Möglichkeit, mit einer großen Bandbreite von Vertretern aus allen Bereichen der Regierung, der Privatwirtschaft und der Wissenschaft in Kontakt zu treten und diese anzuhören. Ich habe mich ganz besonders auf diese Konferenz gefreut; dies ist meine erste Reise nach Europa in meiner Funktion als Koordinator für Cybersicherheit.

Ich möchte Ihnen heute einen Überblick über einige aktuelle Ansichten der US-amerikanischen Regierung zum Thema Cybersicherheit geben - einschließlich unserer Prioritäten, Bereiche potentieller Herausforderungen und Möglichkeiten sowie der Frage, wie die Vereinigten Staaten und Deutschland zusammenarbeiten können, um unsere kollektive Sicherheit im Cyberspace zu verbessern.

Die "NEUE NORMALITÄT"

Doch zunächst möchte ich kurz über die Herausforderungen sprechen, vor die uns das Thema Cyberspace stellt. Wie wir alle wissen, stellen Cyberbedrohungen für Staaten und die Wirtschaft gleichermaßen ein bedeutsames Problem dar. Aus Sicht des Weißen Hauses machen drei Entwicklungen die Cyberbedrohung zu etwas besonders Besorgniserregendem:

- Erstens: Die Bedrohung nimmt immer mehr Raum ein und wird vielfältiger - parallel zur Anzahl der Dinge, die wir mit dem Internet verbinden, wachsen die potentiellen Angriffsvektoren exponentiell, wodurch der Raum, den es zu verteidigen gilt, noch größer wird. Und wir verbinden stetig neue und unterschiedliche Dinge mit dem Internet - von Autos über Kaffeemaschinen bis hin zu verbreiteten Sensoren. Das Problem der Abwehr ist also eine noch größere Herausforderung als "einfach nur" der Schutz von Computern, die über Kabel miteinander verbunden sind.

- Zweitens: Die Bedrohung wird immer differenzierter - es wird immer schwieriger, Schadsoftware zu entdecken; und diese ist in der Lage, eine größere Vielfalt von Schäden anzurichten. Gleichzeitig muss man nicht mehr Programmierer sein, um Schadsoftware nutzen zu können. Es ist nicht nur so, dass böswillige Entwickler Schadsoftware leichter handhabbar gestalten, sondern Cyberkriminelle in einigen Fällen sogar Online-Helpdesks eingerichtet haben. Wenn also eine Schadsoftware nicht funktioniert, kann man dort anrufen und Hilfe bekommen.

- Drittens: Die Bedrohung wird gefährlicher – böswillige Akteure zeigen immer stärker, dass sie willens sind, durch ihre Aktivitäten mehr Zerstörung hervorzurufen, wie die Angriffe gegen Saudi Aramco letztes Jahr und gegen südkoreanische Banken zu Beginn dieses Jahres gezeigt haben.

Was jedoch letztendlich noch beunruhigender ist, ist die Tatsache, wie "normal" diese Bedrohungen werden. Die neue Normalität bedeutet nicht massive Stromausfälle oder die Lahmlegung des Zugverkehrs im ganzen Land - so etwas ist nicht "normal". Bisher jedenfalls noch nicht. Vielmehr ist es so, dass diese Entwicklungen zu einer "neuen Normalität" führen, die zwar weniger spektakulär als ein Action-Film aus Hollywood, aber dennoch sehr besorgniserregend ist: ständige Eingriffe, Verletzungen der Privatsphäre, Diebstahl von Geschäftsinformationen sowie die Verschlechterung oder Verweigerung von Diensten für legale Instanzen, die versuchen, Geschäfte zu machen oder ihre Botschaft im Internet zu verbreiten.

Kein innerer Raum im Cyberspace

Wenn wir überlegen, wie wir mit diesen Bedrohungen umgehen, müssen wir ein einzigartiges Merkmal des Cyberspace berücksichtigen. Traditionell wird argumentiert, dass es im Cyberspace keine Grenzen gibt und dass dies sowohl Vorteile (Generierung riesiger Gewinne durch den freien Informationsfluss) als auch Nachteile (großes Maß an Freizügigkeit für böswillige Akteure) hat.

Ich würde jedoch behaupten, dass solche Argumente nicht gänzlich stimmen. Überall im Cyberspace gibt es Grenzen und Grenzlinien. Überall, wo es eine Firewall oder einen Verbindungspunkt gibt, existiert eine Grenze. Stattdessen hat der Cyberspace keinen inneren Raum - es gibt kein "Inneres" in unseren Netzwerken. Tatsächlich "lebt" jeder an einer

Grenze. Wir sind alle über den Cyberspace verbunden; und diese Vernetzung bedeutet, dass alles und jeder auf die ein oder andere Art und Weise einen Rand oder eine Grenze berührt.

Und diese Tatsache hat einige tiefgreifende Auswirkungen darauf, wie wir selbst eine Gesellschaft gestalten, um uns im Cyberspace zu schützen - und auch dahingehend, wie ich versuche, meine Aufgabe im Bereich Cybersicherheit zu erfüllen. In der realen Welt beispielsweise übertragen wir die Aufgabe des "Grenzschutzes" der Regierung. Doch wenn im Cyberspace jeder direkt an einer Grenze lebt, ist es physisch nicht möglich, die Aufgabe des "Grenzschutzes" an nur eine Gruppierung oder ein Element in unserer Gesellschaft zu übertragen - nicht einmal an die Regierung. Diese Aufgabe wird zu einer Gemeinschaftsaufgabe, bei der jeder Mensch in einem Land oder einer Gesellschaft eine Rolle ausfüllt. Und das bedeutet auch, dass konventionelle Denkweisen zu Bedrohungen sich ebenfalls ändern müssen. Zum Beispiel erwarten die Bürgerinnen und Bürger in vielen Ländern, dass sich die jeweilige Regierung mit "externen" Bedrohungen befasst und lokale Behörden begrenzte "interne" Bedrohungen wie Kriminalität bekämpfen. Wir haben jedoch erlebt, wie Staaten mittels lokaler Server böswillige Handlungen vornehmen und Kleinkriminelle Geld aus dem Ausland stehlen; wir können als Grundlage für die Zuordnung von Verantwortlichkeiten für Maßnahmen nicht mehr nur einfach zwischen "extern" und "intern" unterscheiden.

Leitprinzipien

Wie verbessern wir also unsere kollektive Sicherheit in dieser "neuen Normalität" der täglichen Eingriffe zum Nachteil von Einzelpersonen, Unternehmen und Staaten? Wenn Sie gehofft haben, dass ich diese Fragen jetzt beantworten werde, fürchte ich, dass ich Sie leider enttäuschen muss. Ich habe noch nicht alle Antworten darauf und auch niemand anderes, denke ich. Allerdings möchte ich gern einige der Prinzipien herausstreichen, an die wir uns in den Vereinigten Staaten halten, um dieser Herausforderung zu begegnen.

Kompromisse sind unvermeidbar; stellen Sie sich darauf ein. Da wir in dieser "neuen Normalität" leben, dürfen wir nicht überrascht sein, wenn Eingriffe und Ausfälle vorkommen. Stattdessen müssen wir darauf vorbereitet sein. Sowohl die Wirtschaft als auch Staaten sollten Cybersicherheits-Notfallpläne ausarbeiten und testen; sie sollten die besten Vorgehensweisen und Technologien zum modernen Netzwerkschutz nutzen und ihre Netzwerke - unter der Annahme, dass sie angegriffen worden sind - stetig überwachen. Für den Fall, dass alles andere versagt, sollte außerdem jeder über mit Service-Providern abgestimmte, gültige Notfall- und Sicherungspläne verfügen.

Informationen müssen ausgetauscht werden - und zwar häufig und schnell. Das Thema Cybersicherheit ist eine gemeinsame Herausforderung und es ist die gemeinsame Verantwortung der internationalen Gemeinschaft, zusammenzuarbeiten, um sie anzugehen. Zu diesem Zweck müssen wir alle willens und in der Lage sein, Informationen zu den jeweiligen Bedrohungen, denen wir gegenüberstehen, auszutauschen. Dies erfordert Zusammenarbeit auf allen Ebenen: die Zusammenarbeit von Staaten, von Staaten und der Wirtschaft sowie von Unternehmen in der Privatwirtschaft. Immerhin könnten Bedrohungen, denen sich eine Stelle heute gegenübersieht, Bedrohungen sein, die morgen eine andere Stelle betreffen.

Teamarbeit ist erforderlich. Wenn ich in meiner Heimat eine Rede halte, sage ich oft: "Cybersicherheit ist ein Mannschaftssport“. Damit meine ich, dass keine einzelne Stelle in unserem Land dieses Thema allein angehen kann. Jede Stelle hat eine Aufgabe, die es zu erfüllen gilt - von der Privatwirtschaft über Strafverfolgungsbehörden bis hin zum Heimatschutz und der Zivilgesellschaft. Das trifft auf die Vereinigten Staaten zu und gilt meiner Meinung nach auch auf internationaler Ebene - wenn wir nur so stark wie das schwächste Glied in unseren untereinander verbundenen Netzwerken sind, sind wir alle zusammen für unsere gemeinsame Sicherheit verantwortlich.

Priorität Nummer Eins: Netzwerkschutz. Im Cyberspace ist das Risiko der Fehlzuschreibung, Fehlberechnung und Eskalation sehr real. Als Regierung prüfen wir all unsere Aktivitäten in Sachen Cybersicherheit und Netzwerkschutz auf ihre möglichen Auswirkungen auf die Außenpolitik und unseren Wunsch, internationale Normen eines akzeptablen Verhaltens im Cyberspace zu etablieren. Wir wollen nicht, dass unsere Reaktion auf einen kleinen Zwischenfall im Cyberspace unsere Beziehungen zu anderen Nationen schädigt oder - schlimmer noch - eine physische Auseinandersetzung nach sich zieht. Deshalb werden wir zunächst Maßnahmen zum Netzwerkschutz ergreifen und hart daran arbeiten, diese Lösungen wirkungsvoll zu gestalten, bevor wir andere Maßnahmen gegen böswillige Handlungen einleiten.

Es gilt, die Privatsphäre und bürgerliche Freiheiten zu schützen. Die Vereinigten Staaten glauben fest daran, dass Cybersicherheit und die Privatsphäre sich gegenseitig stärken und nicht in Konkurrenz zueinander stehen. Wenn sie gut gemacht ist, schützt die Cybersicherheit die Privatsphäre und bürgerliche Freiheiten durch die Stärkung von Netzwerken und Systemen, welche persönliche Daten enthalten; und wir ergreifen Schritte, um diese Vorstellung in die Realität umzusetzen. Wir bauen den Schutz persönlicher Daten in unser Cybersicherheits-Rahmenkonzept für kritische Infrastrukturen mit ein. Gleichzeitig stellen wir sicher, dass unsere Maßnahmen im Bereich Netzwerkschutz unser Engagement für den Schutz der Privatsphäre und der bürgerlichen Freiheiten der Nutzerinnen und Nutzer dieser Netzwerke widerspiegeln und dass Verfechter des Schutzes der Privatsphäre sowie weitere Hauptinteressensvertreter in diese Diskussioneingebunden werden und gleichzeitig Unternehmen unterstützt und die Sicherheit verstärkt werden Wir bestehen auch auf wirksamen Regelungen zum Schutz der Privatsphäre bei jeder Art von Gesetz im Bereich Cybersicherheit, das unser Kongress prüft. All unsere Partner - sowohl in den Vereinigten Staaten als auch auf internationaler Ebene - müssen auf unsere Fähigkeit vertrauen, die Informationen, die sie mit uns teilen, zu schützen.

Internationale Umsetzung der Prinzipien

Wir setzen diese Prinzipien im Rahmen all unserer Anstrengungen in Sachen Cybersicherheit um - und zwar sowohl auf nationaler als auch auf internationaler Ebene.

Schutz von kritischen Infrastrukturen

Zunächst arbeiten wir daran, die Cybersicherheits-Standards und -Praktiken im Bereich unserer kritischen Infrastrukturen auszubauen. Ein wesentlicher Schritt war dabei die Unterzeichnung eines Erlasses durch Präsident Obama zu Beginn dieses Jahres, durch den verschiedene Aktivitäten angeordnet wurden, die auf genau dieses Ziel ausgerichtet sind. Der Erlass stärkt vor allem die Partnerschaft der US-amerikanischen Regierung mit Besitzern und Betreibern kritischer Infrastrukturen zwecks Bekämpfung von Cyberbedrohungen durch den Austausch von Informationen, den Schutz der Privatsphäre und bürgerlicher Freiheiten sowie

die Entwicklung eines Rahmens von besten Vorgehensweisen und Standards im Bereich Cybersicherheit.

Wir glauben, dass die Regierung eindeutig die Aufgabe hat, Unternehmen der Privatwirtschaft Hilfe zur Selbsthilfe zu leisten - insbesondere was die Besitzer und Betreiber kritischer Infrastrukturen betrifft. Zu diesem Zweck verpflichtet der Erlass die US-amerikanische Regierung, sich verstärkt darum zu bemühen, Erkenntnisse mit den Stellen auszutauschen, die sie am dringendsten benötigen: Netzwerkschützer, Unternehmen und andere Staaten. Wir haben bereits damit begonnen, wollen jedoch noch weiter gehen. Beispielsweise haben wir allein in den letzten sechs Monaten hunderttausende Signaturen und Informationen, die auf böswillige Cyberaktivitäten hinweisen, mit der Privatwirtschaft und mehr als einhundert Staaten ausgetauscht. Dazu gehören auch wirksame Regelungen zum Schutz der Privatsphäre, indem Bundesbehörden dazu verpflichtet werden, sich bei der Umsetzung ihrer Cybersicherheits-Aktivitäten an die Prinzipien zum fairen Informationsaustausch (Fair Information Practice Principles, FIPPs) zu halten.

Wir haben jedoch erkannt, dass der Austausch von Informationen allein nicht ausreicht; wir mussten außerdem die Messlatte für die Cybersicherheit in den Vereinigten Staaten höher ansetzen. Durch den Erlass wurde deshalb auch die Schaffung eines Rahmens von besten Vorgehensweisen und Standards der Cybersicherheit im Bereich der kritischen Infrastrukturen angewiesen. In den letzten neun Monaten hat die US-amerikanische Regierung mit der Privatwirtschaft zusammengearbeitet, um diesen Rahmen auszuarbeiten. Verstehen Sie mich bitte nicht falsch: Der Rahmen stellt keinen wissenschaftlichen Durchbruch in Sachen Cybersicherheit dar. Es handelt sich tatsächlich um etwas Grundlegenderes, das die besten Vorgehensweisen, die viele Unternehmen bereits anwenden, skizziert. Allerdings stellt der Rahmen Unternehmen eine strukturierte Möglichkeit zur Verfügung, ihre Cybersicherheitsrisiken zu überdenken, ihr gegenwärtiges Niveau an Cybersicherheit zu bestimmen und dann zu entscheiden, wie hoch dieses Niveau sein soll. Der Rahmen verweist schließlich auf die Standards und Vorgehensweisen, durch deren Umsetzung Unternehmen ihr gewünschtes Niveau an Cybersicherheit erreichen.

Vor Kurzem ist der Vorentwurf dieses Rahmens fertig gestellt worden. Unserer Meinung nach ist dies ein exzellenter Anfang, doch wir wissen, dass er künftig verbessert werden kann und wird. Im Prozess der Fertigstellung des Vorentwurfs haben wir Unternehmen, Industriezweige - tatsächlich quasi jeden - gebeten, den Rahmen umzusetzen und uns eine Rückmeldung darüber zu geben, was gut und was schlecht ist. Die Anfrage ist auch international ausgerichtet - wir freuen uns über jede Rückmeldung von Staaten oder internationalen Firmen, die sich dazu entschließen, eine Rückmeldung zu geben. Wie bereits gesagt: Die Vereinigten Staaten haben nicht die Antwort auf alle Fragen - wir wissen, dass wir durch die Zusammenarbeit mit unseren Partnern gemeinsam mehr erreichen können als jeder für sich allein.

Entwicklung von Normen und Außenpolitik

Zweitens arbeiten wir daran, das Thema Cybersicherheit als Kernelement in unsere außenpolitischen Beziehungen zu anderen Staaten zu integrieren. Cybersicherheit geht mit gemeinsamer Verantwortung einher; deshalb handelt es sich nicht um ein ausschließlich nationales Thema.

Wie in allen Bereichen tragen Staaten auch im Cyberspace eine besondere Verantwortung zum Schutz ihrer eigenen nationalen Sicherheit sowie zur Förderung von Frieden und Stabilität mit anderen Nationen. Folglich bemühen wir uns weiter, unsere Verbündeten und

Partner weltweit dazu zu bringen, Verhaltensnormen für den Cyberspace festzulegen - was also Staaten und andere Akteure im Cyberspace tun bzw. nicht tun sollten - und sicherzustellen, dass das Internet offen, dialogfähig, sicher, zuverlässig und stabil bleibt, indem die in der US-amerikanischen Internationalen Cyberspace-Strategie (International Strategy for Cyberspace) dargestellten Prinzipien befolgt werden. Dabei streben wir danach, ein Umfeld zu schaffen, in dem jeder vom Cyberspace profitieren kann, Zusammenarbeit gefördert wird und es nur wenig Anreiz für Staaten gibt, sich gegenseitig zu stören oder anzugreifen.

Es ist jedoch so, dass Taten mehr zählen als Worte. Um also die Normen, die wir uns wünschen, zu fördern, müssen wir Maßnahmen ergreifen, um sie umzusetzen. Wir müssen auf ein Umfeld hinarbeiten, in dem alle Länder routinemäßig und schnell auf Unterstützungsersuchen zur Eindämmung der Cyberkriminalität und anderer böswilliger Cyberaktivitäten antworten, die von ihrem Staatsgebiet ausgehen. Die Vereinigten Staaten setzen sich für die Zusammenarbeit mit der internationalen Gemeinschaft zum Aufbau der Verfahrensweisen und Kapazitäten ein, die vonnöten sind, um durch solch kollektives Handeln auf böswillige Aktivitäten zu reagieren.

Die Verwaltung des Internets

Drittens befürworten die Vereinigten Staaten weiter das Konzept einer Internet-Verwaltung, welches den internationalen Handel und das internationale Gewerbe unterstützt, die Sicherheit auf internationaler Ebene stärkt sowie die freie Meinungsäußerung und Innovation fördert. Wir glauben fest daran, dass Vorschläge zugunsten einer internationalen Regulierung zur Einschränkung des offenen und freien Wesens des Internets die Innovation und wirtschaftliche Entwicklung verlangsamen würden und zu einer noch nie da gewesenen Kontrolle dessen, was Menschen online sagen und tun, führen könnten. Solche Vorschläge spielen repressiven Regimes in die Hände, welche die unangebrachte Kontrolle von Inhalten durch den Staat legitimieren wollen. Stattdessen glauben wir, dass die Staaten, die Privatwirtschaft und die Zivilgesellschaft ein bedeutsames Mitspracherecht haben, was die Zukunft des Internets betrifft. Wenn wir tatsächlich glauben, dass der Weg hin zu wirtschaftlichem Wachstum und Wohlstand über eine offene, vernetzte Welt führt, müssen wir die Institutionen der vielen Interessensvertreter, die für die Verwaltung des Internets selbst entscheidend sind, stärken - und nicht schwächen.

Die Zusammenarbeit von Strafverfolgungsbehörden

Als Viertes glauben wir, dass wir unsere Fähigkeit, böswillige Aktivitäten im Cyberspace zu unterbinden, ausbauen müssen. Zur Erreichung dieses Ziels müssen wir die Zusammenarbeit von Strafverfolgungsbehörden innerhalb der internationalen Gemeinschaft vertiefen - und zwar vor allem mit Deutschland und anderen europäischen Bündnispartnern. In den letzten Jahren haben die Vereinigten Staaten und Europa mehrfach Erfolge verzeichnet:

- Wir richteten eine EU-US-Arbeitsgruppe zum Thema Cybersicherheit und Cyberkriminalität zur Feststellung gemeinsamer Ziele und Maßnahmen zur Erreichung dieser Ziele ein.

- Es gab Erfolge hinsichtlich der Ratifizierung der Cybercrime-Konvention des Europarates durch weitere Länder und dabei, diese zu einem wahrhaft globalen Instrumentarium zur Bekämpfung der Cyberkriminalität zu machen.

- Außerdem initiierten die Vereinigten Staaten und die EU letztes Jahr das globale Bündnis gegen den sexuellen Missbrauch von Kindern im Internet (Global Alliance Against Child Sexual Abuse Online).

All diese Erfolge stellen eine bemerkenswerte Leistung dar. Doch da sich die Technologie weiterentwickelt, müssen sich die entsprechenden rechtlichen Konsequenzen gleichermaßen weiterentwickeln. Themen wie Datenschutz, der grenzüberschreitende Zugang von Strafverfolgungsbehörden zu Daten oder der Informationsaustausch zwischen Staat und Privatwirtschaft schaffen neue Herausforderungen für die Zusammenarbeit unserer Strafverfolgungsbehörden. Wir können und müssen sicherstellen, dass unsere Zusammenarbeit diesen Herausforderungen gerecht wird, um die sich ständig weiterentwickelnde Bedrohung durch Cyberkriminelle und nicht-staatliche Akteure anzugehen.

Aufbau von Kapazitäten

Ich habe ausführlich über die Anstrengungen der Vereinigten Staaten in Sachen Cybersicherheit gesprochen; indessen sind wir uns der Tatsache bewusst, dass viele Länder noch daran arbeiten, Industriezweige, Technologien und die für die wirtschaftliche Entwicklung im 21. Jahrhundert notwendige Konnektivität aufzubauen. Um diese Lücke zu schließen, sind wir bestrebt, mehr Menschen überall auf der Welt mit der digitalen Zukunft zu verbinden. Die Vereinigten Staaten glauben, dass ein erweiterter globaler Zugang zur Telekommunikation und Breitband-Diensten - in Kombination mit einem integrativen, von mehreren Interessensvertretern getriebenem Konzept zur Internet-Verwaltung - weiterhin der beste Weg in Richtung Wirtschaftswachstum darstellt, von dem alle profitieren..

Und schließlich setzen wir uns dafür ein, sich entwickelnde Nationen überall auf der Welt dabei zu unterstützen, ihre Cybersicherheits-Kapazitäten aufzubauen. In der US-Regierung haben wir Programme eingerichtet, um Staaten zu helfen, Cybersicherheits-Strategien und -Programme von Grund auf zu entwickeln. Diese Programme tragen dazu bei, allen möglichen Erfordernissen, wie der Entwicklung der Rechtstaatlichkeit im Cyberspace, der Ausarbeitung nationaler Cybersicherheits-Strategien und der Bildung von Computer-Notfall-Teams, gerecht zu werden. Um nur ein Beispiel zu nennen: Das US-Außenministerium hat beträchtlich viel Zeit und Kraft in die Zusammenarbeit mit dem Senegal und Ghana investiert, um langfristige Cybersicherheits-Partnerschaften zwischen den Vereinigten Staaten und 14 Staaten in West- und Zentralafrika aufzubauen.

Wir sind jedoch nur ein Land und verfügen nicht unbegrenzt über Ressourcen. Aus diesem Grunde sind wir bestrebt und willens, mit anderen Nationen im Bereich der Bewusstseinsschaffung, der rechtlichen und technischen Ausbildung und weiterer Initiativen zusammenzuarbeiten, die unser kollektives Bestreben nach einem offenen, dialogfähigen, sicheren und zuverlässigen Cyberspace stützen.

US-Europäische Zusammenarbeit Im Bereich Cyberspace

Es wäre nachlässig von mir, diese Rede zu halten und nicht zu betonen, wie sehr die Vereinigten Staaten die Cybersicherheits-Partnerschaft mit Europa - und insbesondere Deutschland - wertschätzen. Was den Aufbau eines sichereren Cyberspace betrifft, so war und ist Deutschland ein wesentlicher Partner und wird dies weiterhin sein.

Wie ich bereits gerade zum Thema Cyberkriminalität sagte: Unsere Strafverfolgungsbehörden blicken auf eine lang währende und intensive Zusammenarbeit zurück und arbeiten bei Ermittlungen und Fällen von Strafverfolgung weiter zusammen. Unsere Computer-Notfall-Teams arbeiten regelmäßig im Bereich der Reaktion auf Ereignisse zusammen, um Informationen zu Bedrohungen auszutauschen und böswillige Cyberaktivitäten zu bekämpfen. Wir waren vor allem sehr dankbar für die schnelle und sofortige Unterstützung von Seiten der deutschen Regierung zu Beginn dieses Jahres, als wir wegen anhaltender Denial-of-Service-Angriffe auf unsere Banken und den Finanzsektor um Hilfe baten.

Was die Außenpolitik angeht, so sind unsere Diplomaten weiter die zuverlässigsten Verfechter unserer übereinstimmenden Ansichten zur Anwendbarkeit des Völkerrechts auf den Cyberspace sowie Verhaltensnormen für Staaten im Cyberspace.

Wir setzen uns für diese Partnerschaft ein. Was die am besten geeignete Vorgehensweise zum Aufbau eines sichereren Cyberspace anbelangt, vertreten die Vereinigten Staaten und Deutschland zuweilen unterschiedliche Meinungen; doch wir sind uns einig, was die Bedeutung dieser Aufgabe angeht. Wir können und dürfen nicht vergessen, dass unsere Zusammenarbeit und unser fortgesetzter Dialog der Stärkung und Sicherung des Cyberspace zugunsten unserer beiden Völker dienen.

Fazit

Ich möchte den Vortrag mit einigen letzten Gedanken beschließen:

- Erstens: Wir müssen uns der Bedrohungen, denen wir gegenüber stehen, weiter bewusst sein. Gleichzeitig müssen wir alle unsere Kapazitäten im Bereich der kollektiven Cybersicherheit durch Zusammenarbeit und Partnerschaften verbessern.

- Zweitens: Die Herausforderungen in Sachen Cybersicherheit zu meistern, wird nicht leicht sein und uns allen Beharrlichkeit abverlangen. Doch wie Präsident Obama in seiner Rede zur Lage der Nation zu Beginn dieses Jahres sagte: "Wir dürfen nicht in einigen Jahren zurückblicken und uns fragen, warum wir angesichts realer Bedrohungen für unsere Sicherheit und Wirtschaft nichts unternommen haben."

- Und schließlich: Das Informationszeitalter hat gerade erst begonnen. Die Probleme, vor denen wir stehen, sind komplex und schwierig. Doch wir haben jetzt die Möglichkeit, die Grundlagen für eine sicherere Zukunft zu schaffen. Ich jedenfalls freue mich auf diese Herausforderung.

Ich möchte unseren Gastgebern nochmals für die Ausrichtung einer solch großartigen Tagung danken. Ich bedanke mich für die Möglichkeit, zu Ihnen sprechen zu dürfen, und freue mich auf die Weiterführung unserer Arbeit zur Bewältigung dieser Herausforderungen.

Vielen Dank.

Präsentation zu Sicherheitsrisiken

Carsten Schulz
Markus Blasl

Es wurde demonstriert, wie ein Angreifer das Vertrauen eines Benutzers in die Integrität seiner Internetverbindung in einem alltäglichen Szenario missbraucht, um in krimineller Absicht Daten abzufangen.

Das Opfer würde sich hierzu mit seinem firmeneigenen mobilen Endgerät (Tablet, Smartphone, Laptop) während eines simulierten "Hotelaufenthaltes" mit dem Firmennetzwerk über das Internet verbinden, um beispielsweise per Email zu kommunizieren oder eine Datensynchronisation durchzuführen.

Die Verbindung mit dem Internet sollte dabei über das hoteleigene WLAN erfolgen.
Demonstriert wurde, wie ein Angreifer (vom Opfer unbemerkt) den hoteleigenen Internetzugang verdrängt und stattdessen einen eigenen Zugang etabliert, welchen das Opfer nun irrtümlich benutzte.

Der Angreifer würde diese Situation in krimineller Absicht von nun an ausnutzen, um beispielsweise die Zugangsdaten des Opfers in Erfahrung zu bringen, bzw. unerlaubt Emails und Geschäftsdaten auszulesen.

Digitale Bedrohungen und Gegenmaßnahmen aus Sicht der Wirtschaft

Dr. Thomas Kremer

Meine Damen und Herren,

Internetsicherheit oder in neudeutsch „Cyber Security“ ist heute ein Thema, das für die Wirtschaft von hohem Interesse ist. Das hat nicht zuletzt die Resonanz des Cyber Security Summit am 11. November 2013 in Bonn gezeigt.

Zunächst möchte ich Ihnen einen kurzen Überblick über die Cyber-Sicherheitslage, insbesondere die laufenden Angriffe auch auf das Netz der Deutschen Telekom aufzeigen., Schwachstellen und Gegenmaßnahmen benennen sowie einen Ausblick auf das weitere Vorgehen geben.

Zur Bedrohungslage in der Wirtschaft

Cyber-Security ist kein Medienhype. Fast jeden Tag können wir in der Presse über neue Cyber Attacken lesen. Allein im Oktober standen mehrere Vorfälle im Fokus des öffentlichen Interesses. Schon am 4. Oktober wurde über einen massiven Cyber-Angriff auf Belgacom mit hochentwickelter Malware auf „Heise.de“ berichtet. Es entstand der Verdacht eines neuen

GCHQ Skandals[1]. Am 07. Oktober 2013 berichtete CIO.de davon, dass gerade deutsche Webserver häufig Schadsoftware verbreiten. Diese Meldung beruhte auf Angaben des russischen Cyber Security Spezialisten Kaspersky-Lab. Der TecChannel berichtete am 15. Oktober 2013 darüber, dass IT-Angriffe immer raffinierter und die Zugriffsmethoden von IT-Kriminellen auf Business Applications zur Datenbeschaffung immer ausgefeilter werden. Auch eine Häufung von Betrugsfällen beim mTAN-Verfahren durch Bankbetrüger wurde am 24. Oktober 2013 u. a. auf „Zeit Online“ öffentlich. Dies nur als ein kurzer Überblick.

Die Angriffsziele

Die Veröffentlichungen zeigen auch, dass alle Branchen von Cyber Attacken betroffen sind. Betroffen waren Rüstungskonzerne wie Lockeed Martin oder EADS, aber auch Industriegüter-Hersteller wie ThyssenKrupp oder Medienunternehmen wie die Washington Post oder die New York Times. Auch soziale Medien wie LinkedIn oder Facebook und Twitter waren von Cyber Attacken betroffen. Gleiches gilt für Internetunternehmen wie Apple und Microsoft, die Opfer erfolgreicher Angriffe waren. Die Liste ließe sich unschwer weiter fortsetzen.
Der jüngste in der Presse berichtete Fall betrifft ein Datenleck bei Sky Deutschland. Hier berichtete der „Spiegel“ noch Ende letzter Woche von einem mutmaßlichen Datendiebstahl.

Zur Identität der Angreifer

Bei dieser Vielzahl von Fällen stellt sich sofort die Frage: Wer sind eigentlich die Angreifer? Hier zeigt uns die Analyse, dass sich mehrere Typen von Angreifern identifizieren lassen. Wir unterscheiden insoweit vier Kategorien, die klassischen „Hacker“, organisierte Kriminalität, Hacktivisten und selbstverständlich auch Nachrichtendienste. Was sie alle gemeinsam haben, sind ähnliche Methoden des Vorgehens, aber natürlich ganz andere Ziele.

Bei den klassischen Hackern geht es in erster Linie um das Thema Ruhm und Ehre. Sie wollen zeigen, was technisch machbar ist. Es handelt sich zumeist um Einzelpersonen, die z. B. Internetseiten verunstalten oder von ihnen entdeckte Schwachstellen in Webseiten an die Presse weitergeben oder im Rahmen von sogenannten BugBounty-Programmen den Unternehmen offen legen.

Die organisierte Kriminalität im Internet fokussiert sich auf Betrug, Erpressung und Geldwäsche. Es handelt sich in der Regel um Gruppen, die hoch arbeitsteilig vorgehen. Sie sind über die ganze Welt verteilt und verfügen über hohe Finanzmittel. Ihre Tools sind z. B. Phishing Emails, DDoS auf Onlineshops bzw. Anbieter von Onlinewetten, die Spam-Versendung oder ähnliches.

Ziel und Motivation von Hacktivisten sind die politische Meinungsäußerung und deren Verbreitung. Es sind in der Regel gut organisierte Gruppen, die hoch arbeitsteilig vorgehen und zum Teil weltweit organisiert sind. Als Beispiele für die Aktivitäten von Hacktivisten lassen sich nennen: Anonyme Angriffe auf Unternehmen sowie die DDoS-Angriffe gegen Banken, die Wikileaks Konten gesperrt hatten.
Gerade in der jüngsten Zeit sind Aktivitäten von Nachrichtendiensten besonders bekannt geworden. Ihr Ziel sind Spionage und Sabotage, sie sind staatlich gelenkt und haben sehr hohe Finanzmittel zur Verfügung. In der Presse werden als Aktivitäten von Nachrichtendiensten die Programme „Stuxnet“ und „Red October“ genannt.

[1] GCHQ (Government Communications Headquarter) ist ein britischer Geheimdienst.

Professionelles Vorgehen

Bei einer Gesamtbetrachtung der Angriffe lässt sich inzwischen feststellen, dass die Angreifer immer professioneller vorgehen. Das lässt sich anhand der organisierten Kriminalität im Internet beispielhaft erläutern. Die kriminellen Gruppen gehen oft nach demselben Muster vor: zunächst werden sogenannte Bots[2] eingeschleust, um den PC eines Opfers fernsteuern zu können. Die Verteilung dieser Bots erfolgt zumeist per Spam Mail oder durch „Drive-by-Attacken". Der mit Bots infizierte Rechner wird dann für DDoS-Angriffe, Phishing von Zugangsdaten z. B. für Online-Banking oder für die Spam-Versendung missbraucht. Auf diese Weise können kriminelle Gruppen 10.000-fach ein und dieselbe Schadsoftware nutzen

Insbesondere „PRISM" und „Tempora" und die Folgen

Wie unsicher und angreifbar das Internet heutzutage ist, haben auch die Vorgänge um „PRISM" und „Tempora" deutlich gemacht. In diesem Zusammenhang ist immer wieder die Frage gestellt worden, wie ein solches Abhören machbar ist. Wie sich Abhören technisch realisieren ließe, lässt sich klar beantworten: Bei der strategischen Fernmeldeaufklärung werden nach den Ausführungen von Edward Snowden heutzutage überwiegend Glasfaserleitungen überwacht, da die Satellitenkommunikation nur eine untergeordnete Rolle spielt. Aufgrund geologischer Gegebenheiten wie z. B. unterseeische Gebirgszüge laufen interkontinentale Glasfaserleitungen an wenigen Knotenpunkten weltweit zusammen. Eine zentrale Überwachung ist damit technisch leicht realisierbar. Die Überwachung von Glasfaser erfolgt nach Angaben von Edward Snowden überwiegend mit optischen Splittern, die eine 1:1-Kopie der gesamten übertragenen Inhalte einer Glasfaserleitung passiv ausleiten. All das ist technisch aufwendig und erfordert ein hohes Maß an Professionalität.

Meine Damen und Herren,
dies alles sind technische Details. Erforderlich ist aber auch eine Bewertung der Vorgänge unter den Gesichtspunkten Datensicherheit und Datenschutz. Hierzu lässt sich fraglos feststellen, dass die vielfach geforderte Aufklärung der Sachverhalte bis heute noch aussteht. Insbesondere die Bundesregierung darf bei diesem Thema nicht locker lassen und muss von den amerikanischen und britischen Partnern Aufklärung verlangen. Transparenz ist die wichtigste Maßnahme, um verloren gegangenes Vertrauen zurück zu gewinnen. Auch der Schutz der deutschen Wirtschaft für Industriespionage gehört in diesen Zusammenhang. So genannte No-Spy-Abkommen können diesen Schutz verstärken und sind deshalb zu begrüßen. Aber nicht nur die Unternehmen, auch jeder einzelne Internetnutzer muss vor unangemessenen Abhörmaßnahmen geschützt werden. So lange die Spielregeln nicht klar sind und die Internetsicherheit nicht gewährleistet werden kann, besteht aller Anlass, über andere Schutzmaßnahmen für die Bürger in Deutschland und Europa nachzudenken. Ganz eng damit verbunden sind Themen wie nationales Routing oder europäisches Schengen-Routing. Darüber hinaus sind einheitliche und strenge Regeln für den Datenschutz erforderlich, an die Unternehmen aus Europa und aus Übersee in gleicher Weise gebunden sind. Die seit Jahren diskutierte europäische Datenschutzgrundverordnung sollte so schnell wie möglich finalisiert und verabschiedet werden. Auch bei dem Safe-Harbour besteht deutlicher Nachholbedarf.
Werfen wir nun einen Blick auf einen weiteren sehr relevanten Aspekt zum Thema Cyber-Sicherheit und das ist das immer wieder anzutreffende Problem veralteter Software.

[2] Ableitung von „Roboter".

Schwachstelle: veraltete Software

Es gibt relativ einfache Möglichkeiten, Internetangriffe zu gestalten. Angriffspunkte sind z. B. bekannt gewordene Sicherheits-Schwachstellen. Es besteht generell ein hohes Risiko, dass Software Fehler enthält. Einige Softwarefehler haben Auswirkungen auf die Sicherheit und können durch Angreifer ausgenutzt werden. Pro Monat werden durchschnittlich 400 solcher Schwachstellen bekannt. Ca. 10 % der Schwachstellen sind kritisch. Natürlich gibt es neben den bekannten Schwachstellen auch andere, die unbekannt sind, da der Hersteller noch kein Software Update - also einen Sicherheitspatch - zur Verfügung gestellt hat. Und es gibt natürlich die sogenannten „Zero-Day-Exploits“, die erst durch einen gelungenen Angriff bekannt werden. Als Beispiele für Angriffe auf Basis von bekannten Sicherheitsschwachstellen lassen sich die Fälle New York Times, Washington Post, Microsoft und Apple nennen.

Vorbeugende Sicherheitsmaßnahmen

Aber was kann man tun? Was können gerade Unternehmen tun, um aus den erfolgten Angriffen zu lernen und die eigenen Systeme zu härten?

Honeypots

Bei der Telekom setzen wir dazu sogenannte Honeypots ein. Das sind Systeme, die im Internet Schwachstellen simulieren und auf diese Weise Angriffe auf sich ziehen. Die Angriffe werden dann analysiert und die gewonnenen Erkenntnisse werden zur Härtung der eigenen Systeme eingesetzt. Die Deutsche Telekom verfügt weltweit über 180 Honeypot-Sensoren. Diese haben innerhalb der letzten drei Jahre rund 8,7 Millionen neue Angriffsmuster identifiziert. Pro Tag erkennen wir bis zu 800.000 Angriffe auf die Honeypots. Eine weitere Zahl ist aus meiner Sicht sehr bemerkenswert. Ein simuliertes Smartphone wurde innerhalb eines Jahres mehr als 300.000 Mal attackiert. Durchschnittlich ein Angriff pro Tag war erfolgreich. Weltweit werden derzeit fast eine Milliarde Smartphones genutzt. Das ist eine große Zahl und das damit verbundene Risiko ist nicht unerheblich. Viele Smartphone Nutzer haben sich angewöhnt, Software Updates nicht wie bei ihren PCs zu Hause oder im Unternehmen regelmäßig aufzuspielen sondern die Smartphones eher wie Telefone zu behandeln und keine Updates vorzunehmen. Von dieser Vorgehensweise müssen wir dringend abraten, denn Smartphones sind Hochleistungsrechner, die genauso geschützt werden müssten wie unsere PCs. Andernfalls sind sie leichte Angriffsziele.

Der Sicherheitstacho

Mit den Honeypots hat die Deutsche Telekom die Möglichkeit, ein Gesamtbild der Angriffe auf ihre Systeme in Echtzeit transparent zu machen. Das Lagebild ist für jedermann frei zugänglich über das Internet. Unter „www.sicherheitstacho.eu“ können Sie die aktuellen Cyberangriffe verfolgen. Im Monat Oktober kamen die meisten Angriffe aus den USA, aus Großbritannien und aus Deutschland. In diesen Ländern standen die Server, von denen die Angriffe ausgehen. Das Echtzeit-Lagebild gibt aber keine Auskunft darüber, ob die Server Teil von Botnetzen sind und von wo aus das Botnetz gesteuert wird. Um dies heraus zu bekommen, sind weitere Ermittlungen notwendig.

Trendbeobachtung und strategisches Bedrohungsradar

Die Erkenntnisse der Honeypots lassen sich zu einem strategischen Bedrohungsradar weiterentwickeln, das aktuelle Trends bei den Cyber-Angriffen aufzeigt. Das strategische Bedrohungsradar der Deutschen Telekom weist drei Risikofelder auf. Die Risikofelder sind

(1) bekannte Schwachstellen, die aktiv ausgenutzt werden,
(2) vorhandene Schwachstellen deren Ausnutzung nachgewiesen ist sowie als schwächste Gruppe
(3) Bereiche, in denen Schwachstellen vorhanden und jedenfalls theoretisch ausnutzbar sind.

Die Analyse der Schwachstellen wird dann kombiniert mit einer Betrachtung von Eintrittswahrscheinlichkeit und möglichem Schaden. Daraus ergibt sich z. B., dass bei der Deutschen Telekom größtes Risiko bei Advanced persistent threats besteht.

CERT-Teams

Um mit den Cyber Risiken umzugehen, hat die Telekom ein sogenanntes Cyber Emergency Response Team oder kurz „CERT“ gebildet. Das CERT ist für die Bearbeitung von Cyber Security Incidents wie z. B. Hackerangriffe oder kritische Schwachstellen sowie deren Prävention zuständig. Das CERT pflegt das strategische Bedrohungsradar und bildet die Schnittstelle zu Behörden, politischen Institutionen und zu internationalen Security Community.

Abuse-Management

Um die Sicherheit im Internet zu erhöhen, ist auch das Verhalten der Internetnutzer, aus Sicht der Telekom der Kunden, besonders wichtig.

Deshalb hat die Telekom ein sogenanntes Abuse-Management eingerichtet. Aufgabe des Abuse-Managements ist es, eingegangene Hinweise auf Schwachstellen zu überprüfen und gegebenenfalls die Kunden darüber zu unterrichten. Die Telekom schickt monatlich bis zu 40.000 Warnschreiben an die Kunden und bittet sie, Passwörter zu ändern, Softwareupdates einzuspielen oder ähnliches.

Verbesserte Sicherheit durch verstärkte Zusammenarbeit

Die genannten Beispiele stammen aus dem Bereich der Deutschen Telekom, die beim Thema Cyberangriffe sehr transparent ist. Viele andere Unternehmen sind deutlich zurückhaltender, weil sie z. B. Reputationsverluste beim Bekanntwerden von erfolgreichen Angriffen fürchten. Daher fehlt uns heute ein Gesamtbild der Sicherheitslage für Deutschland, aber auch für ganz Europa. Hinzu kommt, dass das Know-how für die Abwehr von Cyber-Angriffen ebenfalls ungleich verteilt ist. Unternehmen wie die Deutsche Telekom haben das Know-how, aber gerade im mittelständischen Bereich fehlt es vielfach. Daher brauchen wir insgesamt mehr Transparenz und die „Mauer des Schweigens“, die viele Unternehmen um sich errichtet haben, muss in Sachen Cyber.Sicherheit eingerissen werden. Unternehmensübergreifende Kooperationen auch unter Einbeziehung der öffentlichen Hand, insbesondere des Bundesamtes für Sicherheit und der Informationstechnik, sind dringend erforderlich. Die effiziente Zusammenarbeit ist ein Schlüsselfaktor für einen sicheren Cyber-Standort Deutschland. Daher ist z. B. die vom BSI und Bitkom gegründete „Allianz für Cyber Sicherheit“ sehr zu begrüßen. Diese Allianz umfasst heute schon mehr als 340 teilnehmende Institutionen und bietet eine Plattform zum Pooling von Informationen, zum Erfahrungsaustausch und zur Fort- und Weiterbildung. All das ist sehr hilfreich. Darüber hinaus ist wichtig, dass in den Unternehmen das Thema Cyber-Sicherheit nicht mehr nur IT-

Spezialisten überlassen wird. Angesichts der erläuterten Risiken muss klar sein, dass Cyber-Security heute ein Thema für Geschäftsführungen und Vorstände der Unternehmen aus allen Branchen ist. Erforderlich ist für jedes Unternehmen eine Einschätzung der eigenen Risikolage, der Definition von daraus abgeleiteten Maßnahmen und selbstverständlich die zu Verfügung Stellung von sachlichen und personellen Ressourcen. In diesem Zusammenhang muss auch betont werden, dass die IT-Sicherheit auch ein Kriterium bei der Auswahl von Lieferanten sein muss.

Zusammenfassung

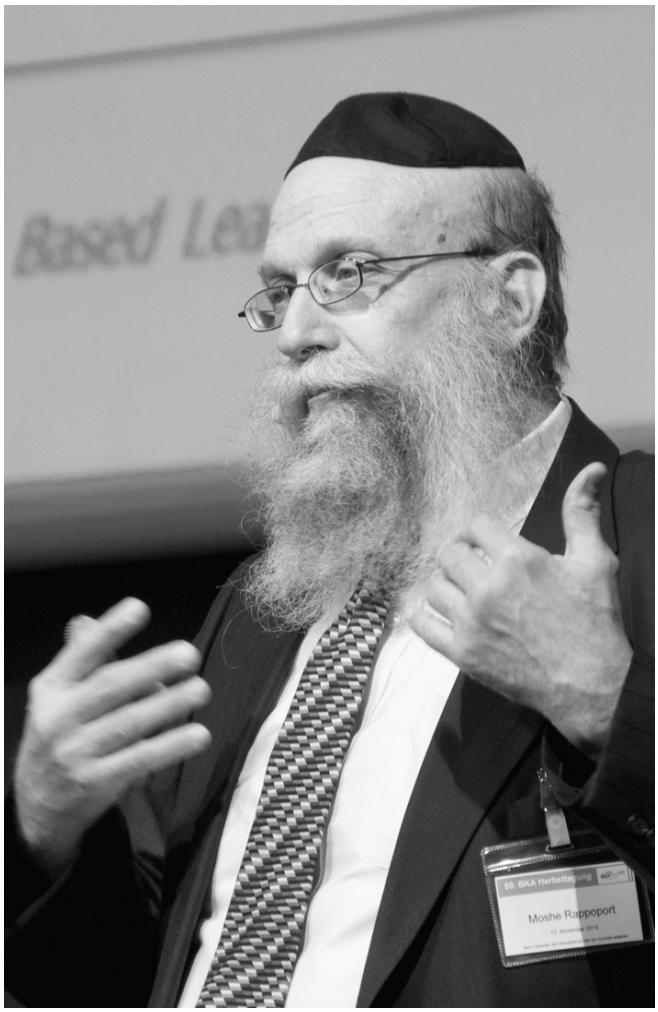
Cyberangriffe sind eine reale Bedrohung nicht nur für Netzwerkbetreiber, sondern für alle Unternehmen in allen Branchen.

Die Angreifer werden immer professioneller. Das gilt insbesondere für den Bereich der organisierten Kriminalität. Risiken entstehen z. B. durch veraltete Software auf Smartphones.

Die Deutsche Telekom hat Instrumente zur Früherkennung von Angriffen entwickelt (Honeypots, Sicherheitstacho, strategisches Bedrohungsradar, CERT), deren Erkenntnisse zur Härtung der Systeme eingesetzt werden. Über ein ABUSE werden Kunden informiert, wenn die Telekom eine Kompromittierung von Systemen des Kunden erkennt.

Für eine effiziente Bekämpfung der Cyberangriffe sind Transparenz und eine enge Zusammenarbeit zwischen Unternehmen und Behörden entscheidend. Bestehende „Mauern des Schweigens“ müssen eingerissen werden.

Möglichkeiten und Herausforderungen von Big Data



Moshe Rappoport

Die Menge an digitalen Daten wächst unaufhaltsam. Mittlerweile werden pro Tag etwa 2500 Billionen Gigabytes erzeugt. 90 Prozent der Gesamtmenge an digitalen Informationen wurden allein in den letzten zwei Jahren generiert. Ursächlich für diese Informationsexplosion sind etwa die fortschreitende Vernetzung von Computern und Kommunikationssystemen jeglicher Art, die Durchdringung der Welt mit Sensorik – dem so genannten *Internet of Things* – und die rasante Ausbreitung sozialer Netzwerke. Man spricht von „Big Data“.

Um die Möglichkeiten und Herausforderungen im Zusammenhang mit „Big Data“ zu erfassen, ist es zunächst wichtig, das Phänomen im Kontext der Entwicklung und Anwendung von Informationstechnologie zu verstehen. Hier lassen sich drei Phasen erkennen. Die erste Phase zwischen ca. 1970 bis 1990 war die Einführung von IT in Unternehmen. Vor 1970 war Computertechnologie führenden Forschungsinstitutionen und wenigen großen Firmen vorbehalten. Dann allerdings begann eine rasche Ausbreitung in die Unternehmen. Der Erfolgsfaktor von IT in dieser ersten Phase war die Technologie selbst und ihr rasanter Fortschritt, der durch die Halbleiterindustrie und Firmen wie IBM angetrieben wurde. Je schneller der Prozessor, je größer der Speicher, je besser das Netzwerk, desto größer der Wettbewerbsvorteil für das Unternehmen. Um 1990 war Computertechnologie in Unternehmen etabliert und es kam zu einem ersten markanten Wendepunkt. Die IT-Bedürfnisse von Unternehmen änderten sich. Nicht die Frage nach der Schnelligkeit des

Prozessors stand nunmehr im Mittelpunkt, sondern welchen Geschäftsnutzen ein System liefern konnte, welchen Return-on-Investment und ähnliche Aspekte. Hinzu kamen die Ausbreitung des Internets, der Siegeszug des PCs in den Haushalten und der Beginn des E-Business – die Verlagerung von Geschäftstätigkeiten ins Internet. Die Kombination von PC, Internet und günstiger Datenleitungen in den späten 90ern führten zur Demokratisierung des Computings. Der durchschnittliche Bürger und Konsument wurde Teil der digitalen Welt – also nicht nur Geschäftsleute, Gamer, Buchhalter und Programmierer – und begann mit seinem Heimcomputer und dem Internet, verschiedenste neue elektronische Dienstleistungen in Anspruch zu nehmen. Diese Entwicklung schritt zügig fort und führte in der Folge zu einem weiteren Wendepunkt in der IT-Entwicklung. In dieser dritten Phase, in der wir uns noch immer befinden, rückt die Gesellschaft – die digital vernetzte Informationsgesellschaft – als Innovationstreiber ins Zentrum. Die Benutzer und gesamtgesellschaftliche Problemstellungen werden zu bestimmenden Faktoren für die Entwicklung neuer IT-Lösungen und Computertechnologien. Mittlerweile ist klar erkennbar, dass Technologien, die diesen Bedürfnissen nicht entsprechen, am Ende die falsche Sprache sprechen.

Deutlich wird dies vor allem auch am veränderten Umgang mit Technologie: Die Generationen, die heute in die Geschäftswelt einziehen und allmählich auch in den Führungsetagen aktiv werden, sind mit dem Computer aufgewachsen. Sie gehören zu den so genannten *Digital Natives*. Sie gehen spielerisch mit neuen Technologien um, nehmen alles technologisch Neue intuitiv an – Technologie ist ein Selbstverständnis. Dagegen ist der Grossteil der Personen, die vor 1970 geboren sind, erst im Erwachsenenalter mit Computertechnologie in Berührung gekommen. Sie sind *Digital Immigrants* und werden wie beim Erlernen einer Fremdsprache immer einen schwierigeren Zugang zu IT haben. Diese Kluft zwischen beiden Gruppen wird *Digital Divide* genannt. Sie stellt ein veritables Problem dar, das nicht zu unterschätzen ist, denn für die nächsten zehn bis 15 Jahre gilt, dass IT-Anwendungen beide Gruppen als mögliche Benutzer ansprechen müssen.

Digital Natives bringen zudem ganz neue Bedürfnisse hinsichtlich der Anwendung von IT mit sich. Sie müssen nicht mehr vom Potenzial neuer Technologien überzeugt werden. Im Gegenteil: Sie haben vielfältigste Vorstellungen und Anforderungen an Technologie, die wesentlich mit „Big Data“ verknüpft sind. Zum einen stehen 10 000-mal mehr Daten zur Verfügung als noch vor ein paar Jahren. Diese bestehen aus historischen Daten, die Unternehmen traditionellerweise seit Jahren gesammelt haben, wie z.B. Kundeninformationen, Transaktionsdaten, Geschäftskennzahlen, Produktinformationen usw. Diese Kategorie an Daten bildet eine wichtige Grundlage, um geschäftsrelevante Entwicklungen und Trends zu erkennen. In der Fachsprache werden diese Daten als *strukturierte* Daten bezeichnet, die sich *at rest* befinden – im Ruhezustand bzw. in einer Datenbank, wo sie sich nicht verändern. Immer wichtiger für Unternehmensentscheidungen wird andererseits die Kategorie der „bewegten“ Daten oder *data in motion*. Dies sind Daten, die fortlaufend generiert werden und die häufig auch in unstrukturierter Form wie Texte, Bilder und Videos oder als Statusmeldungen auf sozialen Netzwerken vorliegen. Zu dieser Gruppe kommen noch Millionen von Daten hinzu, die kontinuierlich durch Sensoren oder mobile Geräte, dem *internet of things*, generiert werden. Ein weiterer Aspekt ist die Geschwindigkeit. Technologisch sind wir heute in der Lage, Daten bis zu 10 000-mal schneller als noch vor wenigen Jahren zu verarbeiten und es entsteht eine neue Generation an Analytiktools, um Einsichten aus diesen Daten zu gewinnen. Die neue Generation von jungen Managern will diese Möglichkeiten ausschöpfen und dies jederzeit und überall – ob am PC, am Mobiltelefon oder auf dem Tablet. Festzuhalten ist, dass „Big Data“ und „Analytik“ wie zwei Seiten einer Medaille zusammengehören. Die Herausforderungen, die „Big Data Analytik“ mit sich bringt, bezeichnen wir bei IBM als die 4 V-s:

- Das Volumen an Daten – der Umgang mit einer immer größer werdenden Datenmenge und damit einhergehend Problemstellungen wie: Welche Daten sollen wie gespeichert und verarbeitet werden? Wie werden sie angemessen gesichert? Hierbei spielen nicht nur technische, sondern vor allem auch rechtliche und gesellschaftliche Aspekte eine immer wichtigere Rolle.
- Die Varietät der Daten – die unterschiedlichen Datenformate und wie bringt man strukturierte und unstrukturierte Daten zusammen?
- Die Geschwindigkeit (englisch velocity), mit der Daten entstehen und damit mitunter auch verarbeitet werden müssen. Im Finanzbereich zählen zum Teil bereits Millisekunden, um Entscheidungen zu treffen. Welche neuen Technologien braucht es, um Echtzeit-Verarbeitung selbst bei großen Datenströmen zu ermöglichen?
- Unsichere Daten (englisch data veracity): Welchen Daten kann man trauen? Welche Unsicherheiten oder Fehleranfälligkeiten (wie bei Sensordaten beispielsweise) haften einigen Daten an? Wie können IT-Systeme damit bei der Auswertung solcher Daten umgehen?

Diese Herausforderungen anzugehen, bietet große Chancen für Organisationen und Unternehmen, aus „Big Data“ Wert zu generieren. In Zukunft werden sehr viele Geschäftsinnovationen und –erfolge auf „Big Data“ und entsprechender Analytik aufbauen. Man kann „Big Data“ tatsächlich als nächste natürliche Ressource bezeichnen, die darauf wartet, erschlossen zu werden. Ein entscheidender Punkt hierbei ist der Einbezug von Kontext und Personalisierung. Als Kunde bin ich beispielsweise eher geneigt, auf eine auf mich persönlich abgestimmte Empfehlung oder Angebot zu reagieren, als auf ein Angebot an die breite Masse. Tante Emma im Laden an der Ecke kannte meine Vorlieben und gab mir entsprechende Hinweise und Empfehlungen. Mit Big Data und Analytik wird es nun möglich, den einzelnen Kunden in seinem individuellen Kontext zu betrachten und entsprechend auf seine Vorlieben einzugehen. Ich bezeichne dies als *Tante-Emma-Effekt*. Er eröffnet eine riesige Chance, wieder viel näher an die individuellen Bedürfnisse des Kunden heranzurücken.

Technologisch erfordert dies fundamental neue Ansätze. Das wohl zukunftsweisendste Beispiel ist die Watson-Technologie, welche die IBM Forschung in 2011 vorgestellt hat. Watsons Architektur ist spezifisch dafür entworfen, die natürliche menschliche Sprache zu „verstehen“ sowie Wörter und deren Bedeutung im Kontext mit Hochgeschwindigkeit zu analysieren, um in kürzester Zeit präzise Antworten auf Fragen zu geben. In der US-amerikanischen Quizshow *Jeopardy!* hat das neuartige System in 2011 seine Fähigkeiten eindrücklich unter Beweis gestellt. Es war selbst den beiden weltbesten menschlichen Champions überlegen. In der Show geht es darum, anspruchsvoll formulierte Wissensfragen mit versteckten und mehrdeutigen Hinweisen zu beantworten und Rätsel zu entschlüsseln. Watson markiert den Beginn einer neuen Entwicklungslinie von so genannten lernenden oder kognitiven Computersystemen. Mittlerweile ist das Watson-System für den Einsatz in der Praxis etwa im Gesundheitswesen oder in der Kundenberatung weiterentwickelt worden. Das System ist dort besonders wertvoll, wo die Fülle des verfügbaren Wissens nicht in nützlicher Frist von Menschen aufgenommen und verarbeitet werden kann. Watson kann die menschlichen Fähigkeiten erweitern. Der *Watson Engagement Advisor* ermöglicht es etwa, Personalisierung und Qualität in der Kundenberatung zu steigern. Kunden können mit Watson interagieren – direkt oder über einen Mitarbeiter – um personalisierte Antworten auf ihre Fragen zu erhalten. Im Gesundheitswesen unterstützt Watson in einem Pilotprojekt Ärzte bei der Diagnose und bei der Auswahl passender Therapien. Dafür greift das System auf Informationen aus medizinischen Datenbanken und Publikationen zu und wird mit Patientendaten, Symptomen und Befunden gefüttert. Ausgegeben werden etwa Vorschläge

mit wahrscheinlichen Diagnosen und Empfehlungen zur Behandlung. Kognitive Systeme wie Watson basieren auf einem fundamental neuen Ansatz. Sie lernen aus der Interaktion mit Daten und Benutzern und können sich so in einem gegebenen Rahmen an neue Gegebenheiten oder veränderte Aufgabenstellungen anpassen, ohne neu programmiert zu werden. Sie werden uns künftig als „smarte Assistenten“ oder in Form von *cognitive apps* auf unseren Mobilgeräten bei unseren Entscheidungen unterstützen und in der Lage sein, mit uns in Dialog und Interaktion zu treten. Damit können sie uns in einer ganz neuen Qualität dabei unterstützen, die digitale Datenflut besser und effizienter zu nutzen und neue Erkenntnisse aus grossen, polystrukturierten und mehrdeutigen Informationsmengen zu ziehen.

Situative Prävention von Cybercrime: ein chancenreicher Bekämpfungsansatz

Prof. Dr. Pieter Hartel

Vielen Dank, Herr Prof. Dr. Kerner, für die gelungene Einführung, die ich selbst nicht besser hätte machen können. Ich danke auch dem Bundeskriminalamt für meine Einladung als Vortragsredner. Ich bin überwältigt in Anbetracht der großen Zahl von Zuhörern, die sich hier eingefunden haben, um meinem Vortrag zuzuhören. Ich werde versuchen, dem gerecht zu werden.

Das Thema meines Vortrags ist, wie Sie sehen können, die „Situative Prävention von Cybercrime“ und ich werde versuchen, Ihnen im Verlauf meiner Ausführungen zu erklären, was damit gemeint ist. Aber bevor ich beginne, seien noch folgende Anmerkungen gestattet: Es geht hier nicht um die Art von Cybercrime, über die am Vormittag gesprochen wurde. Es geht hier nicht um Cyberspionage. Es geht auch nicht um all die Großereignisse, die jeden Tag Schlagzeilen machen, sondern es geht um das Alltagsgeschäft. Da dies so allgegenwärtig ist, lohnt sich eine nähere Betrachtung, denn eine Vielzahl kleiner Vorfälle besitzt in der Summe auch ein großes Schadenspotenzial. Deshalb ist es auch lohnend, die Aufmerksamkeit auf einfache Erscheinungsformen der Kriminalität zu richten. Lassen Sie mich dies anhand einiger Beispiele beschreiben, die wir bisher noch nicht behandelt haben:

Der folgende Fall ereignete sich im Jahr 2000 in Australien: Ein Angestellter ärgerte sich über seinen Chef, weil dieser ihm einen unbefristeten Arbeitsvertrag verweigerte. Er wurde daraufhin entlassen, was ihn sehr verärgerte. Zuständig war er für die Kläranlage in Queensland. Ausgelöst durch seinen Ärger, begann er, die Einrichtungen zu manipulieren. Man hatte vergessen, seine Zugangsberechtigungen zu widerrufen mit der Folge, dass er immer noch seinen Benutzernamen und sein Passwort besaß. Natürlich war das ein großer Fehler, aber Menschen machen nun einmal Fehler. Die betreffende Person hat dann Millionen Liter ungeklärtes Wasser auf die städtischen Parkanlagen geleitet, und das nicht nur einmal, sondern 46 Mal, und zwar über einen Zeitraum von mehreren Monaten, in denen er nicht gefasst werden konnte. Letztlich gelang es, ihn dingfest zu machen, aber zunächst einmal war man ganz offensichtlich gezwungen, knietief durch Klärschlamm zu waten, ohne dass der

Verursacher gestoppt werden konnte. Bei diesem Fall handelt es sich nach meiner Auffassung um eine Form von Cybercrime. Ein weiterer, m. E. interessanter Beispielsfall liegt bereits einige Jahre zurück und ereignete sich in Moskau. Ein gelangweilter russischer Hacker wollte seine Muskeln spielen lassen und seine Fähigkeiten an einer großformatigen digitalen Werbetafel im Zentrum der Hauptstadt erproben. So hackte er sich in das entsprechende Programm, um auf der Videotafel Pornos abzuspielen und zu testen, was dann mit dem Verkehr passiert. Sie können sich vorstellen, dass das Ganze sehr unerfreulich war, denn selbst zu den besten Zeiten ist das Verkehrsaufkommen in Moskau nicht gerade angenehm, und diese Aktion machte das Ganze noch viel schlimmer. Für sein kleines Abenteuer wurde der Hacker verurteilt und für eineinhalb Jahre aus dem Verkehr gezogen.

Ein weiterer Fall beschäftigte die europäische Polizei, insbesondere die niederländischen Kollegen, die sich vor einigen Jahren sehr lange mit dem Betreiber eines Bot-Netzes, dem sogenannten Bredolab-Bot-Net, befassen mussten, um dieses unschädlich zu machen. Dabei handelt es sich zugleich um den ersten Cyber-Kriminellen, der in Armenien, seinem Geburtsland, hinter Schloss und Riegel sitzt, was als großer Erfolg zu werten ist. Wir haben es mit einer großen Bandbreite von Cyberkriminalität zu tun; einige Fälle machen große Schlagzeilen und verursachen große Schäden, und andere sind etwas weniger einschneidend.

Meine Hypothese lautet, dass dies etwas mit Gelegenheiten zu tun hat. Betrachtet man das Beispiel des russischen Hackers, so hat dieser für sich eine Gelegenheit entdeckt und sie genutzt, und es gab nichts, was ihn davon abgehalten hätte. Für diesen großen Spaß rechnete er mit einem geringen Risiko und sah somit keinen Grund, von seinem Vorhaben abzulassen. Meine Hypothese lautet also, dass der Cyberspace einfach viele Tatgelegenheiten bietet.

Herr Prof. Dr. Kerner hat gerade die Theorie der Routineaktivität erwähnt. Es braucht nur einen motivierten Straftäter und ein geeignetes Angriffsziel, und derer gibt es viele im Cyberspace. Der zur Tat entschlossene Straftäter glaubt, dass er sich einem geringen Risiko aussetzt, wenn er seine Taten aus der sicheren und geschützten Umgebung seiner eigenen vier Wände heraus verübt. Die angegriffenen Personen kennen das Risiko nicht; viele benutzen schwache Passwörter oder verhalten sich so, wie es eigentlich nicht sein sollte, oder beides. Und als professionelle Sicherheitsdienstleister geben wir Verhaltensempfehlungen, aber niemand kann für die Missachtung unserer Warnungen belangt werden. Und sowohl auf Seiten der Täter als auch auf Seiten der angegriffenen Personen stellt sich die Frage der Risikobewertung, die nicht immer so beantwortet wird, wie sie sollte. Es gibt in unserer Welt eine Vielzahl von Tatgelegenheiten, die uns Anlass zur Sorge geben sollten. Und aus Erfahrung wissen wir, dass Gelegenheit Diebe macht. Auch ein ansonsten braves Kind bedient sich eigenmächtig an der Keksdose, wenn es hierzu die Gelegenheit erhält. Und vielleicht waren wir als Kinder auch nicht anders. Ich zumindest kann mich da nicht ausnehmen. Das ist keineswegs schön, entspricht aber der menschlichen Natur. Man mag dies in Abrede stellen, aber ist es besser, dies zur Kenntnis zu nehmen und in Bezug auf die Tatgelegenheiten Maßnahmen zu ergreifen. Versuchen wir einmal, von der Annahme auszugehen, dass sich Menschen ihren Gewohnheiten entsprechend verhalten, und lassen Sie uns dann versuchen, ihnen das Ergreifen von Gelegenheiten einfach zu erschweren. Zu diesem Zweck müssen wir uns die Theorie der Tatgelegenheiten anschauen.

Es gibt 5 Prinzipien der Reduzierung von Tatgelegenheiten:

1. Erhöhung des Aufwandes; das klassische Beispiel hierfür ist die Verwendung besserer Türschlösser, was in der Regel funktioniert, sofern die Tür tatsächlich verriegelt wird.

2. Erhöhung des Entdeckungsrisikos; Überwachungskameras können hierfür als offenkundiges Beispiel dienen und deren Nutzen konnte in einigen Fällen belegt werden.

3. Reduzierung des Nutzens; wenn der ungünstige Fall eintritt und privates Eigentum gestohlen wird, wird dies im Falle der eindeutigen Kennzeichnung als Privateigentum - z. B. durch Eingravieren des Kfz-Kennzeichens in die Fenster Ihres Fahrzeugs - zu einem weniger attraktiven Angriffsziel, weil es auf diese Weise schwerer ist, das Diebesgut weiter zu veräußern, wodurch die Tatgelegenheit eingeschränkt wird.

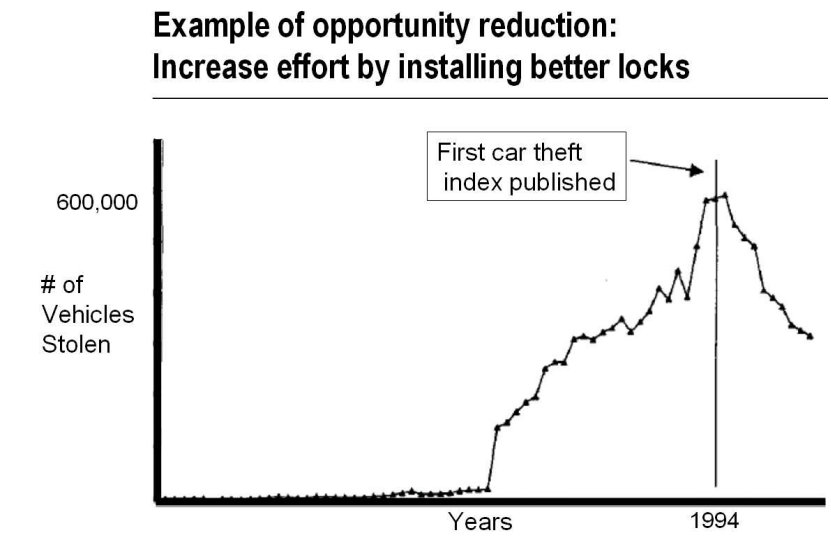
4. Reduzierung des Anreizes für die Tatbegehung.

5. Reduzierung von Entschuldigungsgründen.

Somit steht eine Reihe von Möglichkeiten zur Reduzierung von Tatgelegenheiten zur Verfügung.Bemerkenswert ist, dass die Tauglichkeit dieser fünf Prinzipien in einer Vielzahl von Fällen nachgewiesen wurde und viele Forschungsarbeiten belegen, dass die Beachtung dieser Prinzipien in der Tat die Gelegenheiten zur Begehung einer Straftat reduziert.

Im Bereich des US-Justizministeriums gibt es das Center for Problem-Oriented Policing (Zentralstelle für Problemorientierte Polizeiarbeit), das eine Sammlung von Eingriffsmaßnahmen vorhält, die auf den genannten Prinzipien basieren und die nachweislich erfolgreich zur Reduzierung von Tatgelegenheiten beigetragen haben.

Wenn wir das Gesagte als Grundannahme betrachten, dann könnten wir uns jetzt die Frage stellen, warum wir einen so erfolgreichen Ansatz nicht auf den Bereich Cybercrime übertragen? Das ist eine Frage, die ich mir selbst vor einigen Jahren gestellt habe. Zuvor sei aber noch ein weiteres Beispiel für die Wirksamkeit dieses Ansatzes angeführt.



Die obige Graphik zeigt die Anzahl der zum Ende des letzten Jahrhunderts im Vereinigten Königreich gestohlenen Fahrzeuge. Dieser Graphik lässt sich entnehmen, dass bis zu einem bestimmten Zeitpunkt ein Anstieg der Anzahl gestohlener Fahrzeuge verzeichnet wurde. Verantwortlich hierfür waren zum einen gestiegene Zulassungszahlen, zum anderen aber auch eine wachsende Zahl von Diebstahlsfällen. In den achtziger Jahren ließ sich mit dem Schlüssel eines Ford Taunus wahrscheinlich auch jeder andere Fort Taunus auf der Straße öffnen. Dieses Beispiel einer außerordentlich schwachen Sicherung, aus der sich ein Übermaß an Tatgelegenheiten ergab und bei denen Täter der Versuchung nachgegeben haben, ist ein Beleg für unsere Feststellungen. Unter dem Eindruck des damaligen Sicherheitsdefizits im Bereich der Kraftfahrzeuge erkannte die Regierung des Vereinigten Königreichs Handlungsbedarf und fasste einen sehr interessanten Beschluss. Dieser bestand in der Veröffentlichung eines Index' gestohlener Kraftfahrzeuge. Wenn Fahrzeughersteller dann feststellen mussten, dass die eigene Marke und das Vorzeigemodell ganz oben auf diesem Index standen, dann war das keine gute Werbung in der Öffentlichkeit. Man wollte nicht auf dieser Liste sein, weil die eigene Kundschaft dann geneigt war, zu denken: „Wenn ich dieses Marke und dieses Modell kaufe, dann wird es umgehend gestohlen, weshalb ich mich besser für ein anderes entscheide."

Das war ein sehr starker Handlungsanreiz für die Fahrzeughersteller, ihre Fahrzeuge in der Folge mit besseren Sicherungsvorrichtungen auszustatten. Und siehe da, nach Veröffentlichung dieses Index' gestohlener Fahrzeuge zeigte sich, dass die Diebstahlszahlen zurückgingen. Für den Rückgang der Zahlen könnte es natürlich auch andere Gründe geben. Es könnte mit dem Ölpreis zusammenhängen oder mit sinkenden Verkaufszahlen, aber die Wissenschaftler, die in diesem Bereich geforscht haben, haben sich sehr darum bemüht, die Lage umfassend zu berücksichtigen und sind zu dem Schluss gekommen, dass der Rückgang der Kfz-Diebstahlszahlen mit hoher Wahrscheinlichkeit auf die Installation besserer Sicherungstechnik zurückzuführen ist. Das sind Maßnahmen, die funktionieren - vielleicht auch im Bereich Cybercrime. Betrachten wir nun die von uns durchgeführten Untersuchungen.

Die selbst gestellte Aufgabe bestand in der Beantwortung der Frage, wie viele der Maßnahmen zur Reduzierung von Tatgelegenheiten tatsächlich im Cyberbereich ausprobiert worden sind und wie wirksam sie waren. Zunächst wurde, wie in der Wissenschaft üblich, eine Auswertung der vorhandenen Literatur durchgeführt, d.h. eine Auswertung der gesamten Literatur in den Bereichen Informatik und Verhaltensforschung, um entsprechende Belege zu finden. Das Resultat war im Grunde gleich null - ein sehr ernüchterndes Ergebnis. Auf der einen Seite gibt es einen Schatz vielversprechender Forschungsergebnisse und auf der anderen Seite das zu lösende Problem, und keiner hat beides bisher miteinander in Verbindung gebracht. Es gibt nur eine kleine Ausnahme, und zwar Forschung in Bezug auf die Bekämpfung von Phishing; hier gibt es Belege für die Wirksamkeit der in Rede stehenden Maßnahmen. Aber da wir alle täglich Phishing-E-Mails erhalten und dies gewiss keine Einzelfälle sind, kann dieses Problem gewiss noch nicht als gelöst gelten, sondern besteht ohne Zweifel größtenteils fort. Die wesentliche Folgerung lautet unbestreitbar, dass dies noch Terra incognita ist und genau deren Erforschung haben sich meine Kollegen und ich verschrieben.

Ich möchte Ihnen daher kurz über drei Versuche berichten, mit denen wir versucht haben, mehr über Tatgelegenheiten und deren Reduzierung herauszufinden.

Der erste Teil ist eine klassische Kriminalaktenauswertung mit dem Ziel, herauszufinden, wie viel Cybercrime es tatsächlich gibt. Das ist zum Einstieg stets ein guter Ansatz, der auch ein sehr interessantes Ergebnis erbracht hat.

Bei dem zweiten Experiment handelt es sich um ein Musterbeispiel für die Schaffung von Tatgelegenheiten. Gemeint sind soziale Netzwerke für Sporttreibende im Internet. Das Experiment offenbarte deren teilweise sehr naive Nutzung, wozu im weiteren Verlauf ergänzende Ausführungen folgen.

Bei dem dritten Experiment ging es darum, mit Hilfe des "social engineering" in den Besitz fremder Büroschlüssel zu gelangen, was erstaunlicher Weise sehr gut gelang. Dies sollte ohne Zweifel vermieden werden, da hierdurch jede noch so gute Sicherheitsstrategie ausgehebelt wird.

Die erste Fallstudie bestand in der Analyse von 809 Kriminalakten der fünf niederländischen Polizeiregionen mit einer Grenze zu Deutschland. Der Grund für die Auswahl dieser Polizeien liegt darin, dass sich unsere Einrichtung dort befindet. Dies erleichterte den Zugang zu den kriminalpolizeilichen Akten. Die so zu untersuchende Fragestellung lautete: Wie groß ist der Cyberanteil in diesen Vorgangsakten? Berichten anderer Forscher zufolge macht Cybercrime ein Prozent der Kriminalität aus. Das ist die in offiziellen Polizeistatistiken genannte Zahl, die aus der Anfangszeit der hier beschriebenen Forschungsarbeit stammt. Es bestand jedoch die Auffassung, dass ein Prozent nicht zutreffend sein kann; 96 Prozent der Bevölkerung in den Niederlanden nutzen heute ständig das Internet. Wie kann es nun sein, dass eine Sache, die so umfassend Bestandteil des täglichen Lebens ist, keinen Niederschlag in der Kriminalstatistik findet? Der Schluss liegt nahe, dass hier eine Unstimmigkeit besteht. Und es galt herauszufinden, womit das zusammenhing.

Wie bereits gesagt ging es um die Betrachtung von Allgemeinkriminalität, d.h. mit Einbruchdiebstahl in zwei Ausprägungsformen - Wohnungseinbruch und Einbruch in Geschäftsräume. Außerdem wurden Fälle von Bedrohung und Betrug ausgewertet. Bezogen auf jede Kriminalitätskategorie wurden etwa 300 Fallakten analysiert, also insgesamt 900 Fallakten. Die Analyse erfolgte mit größtmöglicher Sorgfalt. Jede Akte wurde sehr genau studiert und anhand einer langen Liste von Kriterien ausgewertet. Dies erbrachte folgendes Ergebnis: Es gab 135 Fälle von Einbruchdiebstahl und nur in 3 Prozent der Fälle wurde in irgendeiner Form Informations- und Kommunikations-(IuK-)Technologie eingesetzt. Dabei handelte es sich um E-Mails oder Mobiltelefone etc., wie sie im Arbeitsalltag genutzt werden. Dies galt dann in dem jeweiligen Fall von Einbruchdiebstahl als Teil des Modus Operandi (M.O.). Der prozentuale Anteil ist also gering. Was den Einbruchdiebstahl zum Nachteil von Geschäften angeht, so gab es hier keinerlei Hinweis auf die Nutzung von ICT im Modus Operandi. Ergänzend ist jedoch festzuhalten, dass es aufgrund vieler Überwachungskameras durchaus einen hohen IuK-Anteil gab. So konnten die meisten Einbrüche in Geschäftsräume aufgeklärt werden, weil es dank der Überwachungskameras Beweismaterial gab. Aber da Überwachungskameras nicht Bestandteil des M.O. ist, wurden diese Fälle für die Auswertung nicht gezählt.

Bei den Bedrohungsfällen kam IuK mit einem Anteil von 16 Prozent zum Einsatz. Häufig kommt es gerade zwischen Familienmitgliedern oder Geschäftspartnern oder generell im Kontext zwischenmenschlicher Beziehungen zu Bedrohungen, also etwa dem Versenden von E-Mails mit bösartigem Inhalt, so dass der Anteil von vornherein schon sehr hoch ist.

Bei Betrugstaten ist es so, dass in fast der Hälfte aller Fälle IuK Teil des M.O. war. Dabei geht es um Betrug bei Online-Auktionen, wo jemand etwas bestellt, bezahlt und keine Ware erhält oder umgekehrt, sowie Betrug im Zusammenhang mit Online-Banking und dergleichen.

Wenn man einen aggregierten Anteil von IuK an allen Fällen betrachtet, liegt dieser IuK-Anteil bei 20 Prozent, und das ist deutlich mehr als ein Prozent. Das hängt natürlich damit zusammen, wie gemessen wird. Wir sind aber der Auffassung, dass wir eine bessere Messmethode gefunden haben, unabhängig von der örtlichen Gesetzgebung, denn bei der Messung von Cybercrime nach der klassischen Methode schlägt man die im Strafgesetzbuch enthaltene Definition von Cybercrime nach und zählt dann die Fälle in der Kriminalstatistik.

Das ist allerdings nicht die hier angewandte Methode. Wir haben uns die tatsächliche Auswirkung der Technik angeschaut und gelangten so zu der ersten überraschenden Erkenntnis. Die zweite Überraschung ergab sich aus Zeitungsberichten, denen zufolge Cybercrime einen hohen Organisationsgrad aufweisen soll. Es gibt einen Bericht der UNODC, demzufolge 90 % von Cybercrime Organisierte Kriminalität ist.

Hierzu wurden Fälle von Alltagskriminalität betrachtet sowie bei den Betrugsfällen Verdächtige, die festgenommen wurden und bei denen entsprechende Informationen in den Fallakten zu finden waren. Dabei wurde festgestellt, dass im Falle der Nutzung von IuK 95 Prozent der Täter alleine arbeiten, die Taten mithin keineswegs Fälle von organisierter Kriminalität sind. Es kann sich dabei um Fälle handeln, in denen jemand vielleicht seine ehemalige Freundin mit einer E-Mail bedroht oder auch eine schwerwiegendere Tat begeht, was jedoch keineswegs organisierte Kriminalität darstellt. Viele der Täter haben keine kriminalpolizeilichen Erkenntnisse, was als ergänzender Hinweis dafür dienen mag, dass Organisierte Kriminalität nicht vorliegt. Alle Täter gehen einem regulären Beruf nach und agieren auch nicht weltweit, sondern an ihrem Heimatort. Somit ergibt sich ein ganz anderes Bild als das, das man bei der Betrachtung hochkarätiger Fälle erhält. Und auch das ist Teil der

Realität von Cybercrime. Wir sind der Auffassung, dass es sich dabei um eine recht interessante Feststellung handelt. Soll dieses Phänomen nun reduziert werden, dann muss man dieser Feststellung Rechnung tragen.

Lassen Sie mich nun zu der zweiten Fallstudie kommen. Sie wissen alle, was ein soziales Netzwerk im Internet ist, also Facebook, Linked-In etc., aber es gibt auch spezialisierte soziale Netwerke im Internet für Leute, die einen bestimmten Sport treiben. Dabei geht es etwa um Läufer, die ein GPS-fähiges Aufzeichnungsgerät haben und nach Beendigung eines Laufs diesen automatisch hoch laden. Benutzt wurden hier die Daten eines Studenten, der diese freundlicherweise zur Auswertung und für Präsentationszwecke zur Verfügung stellte.

Anhand der Daten lässt sich herausfinden, wo dieser Student wohnt. Das GPS-Gerät wird eingeschaltet, wenn man die Haustür passiert. Anschließend wird der Lauf absolviert und das Gerät ausgeschaltet, wenn der Läufer wieder zuhause ankommt oder, um es noch ein wenig interessanter zu machen, das Gerät wird schon ein wenig früher ausgeschaltet, weil man verhindern will, dass Aufwärm- und Auslaufphase die Laufstatistik verzerren.

Es lässt sich nun aber herausfinden, wo jemand wohnt, und das ist die frohe Botschaft für Straftäter. Dieser muss nur die Website aufrufen, auf der die Läufe aufgezeichnet werden; zum einen weiß der Täter dann, wo das Opfer wohnt, und zum anderen, wann es sich außer Haus befindet. Das sind ideale Voraussetzungen für einen Wohnungseinbruch. Es gibt einen Slogan, der lautet "auch Diebe haben Facebook" und ich würde ergänzen "Diebe kennen auch die Seite RunKeeper".

Untersucht wurden insgesamt 513 Profile, wobei folgendes festgestellt wurde: Die Analyse der Ergebnisse männlicher Läufer (313 von 513) ermöglichte in 36 Prozent der Fälle die Feststellung des Wohnorts. Bei den weiblichen Läuferinnen ergab sich sogar noch ein höherer Prozentsatz. Wenn man das vergleicht mit der Prozentzahl, die bei den weiter verbreiteten sozialen Netzwerken ermittelt wurde, dann liegt diese deutlich niedriger, weil Leute bei Facebook sehr viel zurückhaltender mit der Offenlegung ihrer Namen und Anschriften sind als im Falle der Nutzer spezialisierter Netzwerke. Die meisten Leute sind sich dieser Risiken einfach nicht bewusst und ich denke, dies erzeugt eine große Zahl von Gelegenheiten, über die wir nachdenken sollten.

Bei der letzten Fallstudie sind wir selbst aktiv geworden und wollten herausfinden, inwieweit Menschen Sicherheitsvorkehrungen befolgen, die ihnen von einer Hausgemeinschaft vorgegeben sind. Wir haben für unsere Büros elektronische Schlüssel, die keinesfalls in fremde Hände gelangen dürfen. Wir haben hierzu der Hälfte der Bewohner eines Mehrparteienhauses spezielle Schlüsselanhänger ausgehändigt, auf denen geschrieben stand „Gib mich nicht an einen Fremden weiter“. Zwei Wochen später entsandten wir eine Gruppe von Studenten eines Masterstudiengangs in das Wohnhaus. Die Studenten sollten mit einer erfundenen Geschichte versuchen, in den Besitz möglichst vieler Schlüssel zu gelangen. Der Vorwand hierfür war recht einfach konzipiert: Wir benutzten hierzu ein Kästchen mit einer Batterie und einem Schalter verbunden mit einer eingebauten LED, also eine wenig komplizierte Vorrichtung. Wenn der Schlüssel nun in das Kästchen eingeführt wird, leuchtet die LED auf.

Die Studenten hatten die Vorgabe, zu behaupten, dass es bedauerlicherweise Probleme mit den elektronischen Schlüsseln gebe – zur Erinnerung: das rechtfertigt den IuK-Bezug – und dass die Funktionalität des Schlüssels überprüft werden müsse. Die Stundenten sollten dann sagen, dass der Schlüssel defekt sei und repariert werden müsse. Teil der fingierten Geschichte war zudem, dass die Schlüssel jeden Tag von neuem aktiviert werden müssen, da sie ein digitales Zertifikat beinhalten, dessen Gültigkeit vermeintlich nach 24 Stunden abläuft. Wenn man morgens zur Arbeit geht und das Büro betritt, wird der Schlüssel aktiviert. Nach der Versuchsanordnung sollten die Studenten die Schlüssel dann an sich nehmen, um sie im Erdgeschoss wieder zu aktivieren. Das stand im Widerspruch zu den Sicherheitsvorschriften der Bewohnergemeinschaft, denn die Bewohner sollten den Schlüssel ja nicht aus der Hand geben, sondern die erneute Aktivierung persönlich vornehmen. Sie können sich vorstellen, dass unsere Masterstudenten von dieser Art der Versuchsgestaltung begeistert waren. Zudem erhielten sie Credits für ihren Einsatz. Mittels „Social Engineering“ die Schlüssel anderer Leute entwenden und hierfür obendrein Credits erhalten, ist natürlich eine feine Sache.

Die Ergebnisse sind wie folgt: Es gab 74 Zielpersonen, die angesprochen wurden. Die Hälfte der Zielpersonen gab ihren Schlüssel heraus, die andere Hälfte nicht. Dabei handelt es sich nicht um einen Auswertefehler. Tatsächlich hat sich eine Pattsituation von 50 zu 50 ergeben. Das kommt nicht sehr häufig vor, dieses Ergebnis ist aber korrekt.

Noch interessanter ist der Umstand, dass die Personen gewarnt wurden, indem sie den Schlüsselanhänger mit der Aufschrift erhielten "Don't give this key away", denn dies hatte signifikante Auswirkungen auf das Verhalten: 38 Prozent gaben ihren Schlüssel heraus, während in der Kontrollgruppe, die den Schlüsselanhänger *nicht* erhielt, 62 Prozent den Schlüssel herausgaben. Es ist also tatsächlich möglich, aktiv zur Reduzierung von Tatgelegenheiten beizutragen. Bei den Personen, mit denen dieser Versuch durchgeführt wurde und die tatsächlich auf diese unglaubliche Geschichte hereinfielen, handelte es sich um Elektroingenieure. Man stelle sich einmal vor, wie sich Nicht-Ingenieure in einer solchen Situation verhalten. Wie dem auch sei, dieser Versuch war zwar hilfreich, aber nicht hilfreich genug, denn das Problem ließ sich zwar halbieren, aber ein Großteil blieb bestehen. Das bedeutet, dass noch viel zu tun ist.

Damit bin ich bei meinen Schlussfolgerungen angelangt. Eine der wesentlichen Schlussfolgerungen, die sich festhalten lassen, lautet: Cybercrime speist sich aus Gelegenheiten, und da sie alle Lebensbereiche durchdringt, hat Cybercrime gewissermaßen den Charakter von Alltagskriminalität.

Festgestellt wurde auch, dass Frauen kriminell wesentlich aktiver sind, wenn der Cyberraum eine Rolle spielt, und wir sind der Auffassung, dass dies damit zu tun hat, dass sie sich sicherer fühlen, wenn sie aus der sicheren Umgebung ihrer eigenen vier Wände agieren können. Sie sind z.B. bereit, jemanden bei einer Online-Auktion zu betrügen, während es in der realen Welt größere Risiken gibt, weshalb sie hier möglicherweise weniger geneigt sind, eine solche Tat zu begehen. Das bedeutet wiederum, dass wesentlich mehr Leute kriminell werden, und das ist ein Alarmsignal. Dies zeigt aber auch, in welche Richtung wir uns begeben müssen, wenn wir uns um Vorbeugung bemühen. Einer der Schlüsselaspekte ist das „Social Engineering“. Wenn man eine gute Geschichte hat, kann man fast alles erreichen. Psychologie ist ein wesentlich wichtigeres Instrument als Technologie, um dem hier in Rede stehenden Problem zu begegnen.

Um das Problem von Cybercrime zu lösen, muss man es vielleicht gar nicht als technisches Problem sehen, sondern vielmehr als psychologisches. Und das ist ein Aspekt, den Techniker nur schwer zu akzeptieren bereit sind, aber meiner Auffassung zufolge handelt es sich hierbei um eine Tatsache.

Hier wurde der Versuch unternommen, der Frage nachzugehen, ob die Reduzierung von Gelegenheiten auch im Cyberraum funktioniert. Endgültige Antworten sind noch nicht gefunden und wie bereits gesagt war auch die einschlägige Literatur nicht ergiebig. Meiner Auffassung nach liegt hier aber ein großes Potenzial und es ist zu hoffen, dass ein oder zwei der hier Anwesenden bereit sind, mit anzupacken und diese Forschung weiter voranzutreiben.

Vielen Dank für Ihre Aufmerksamkeit. Vielen Dank nochmals an das Bundeskriminalamt für die Einladung. Und ich hoffe, Sie haben mir gerne zugehört.

Cybersicherheit und Abwehr von Cybercrime - aktuelle Initiativen und strategische Ansätze

Andreas Könen

Die Lage im Cyberraum spitzt sich weiter zu. Das BSI detektiert eine Vielzahl von Angriffen, die hinsichtlich der Zielsetzung, des Vorgehens, der Angriffsmethoden und der technischen Qualität ein großes Spektrum aufweisen. Unternehmen berichten beispielsweise über zunehmende Erpressungsversuche in einem der Felder, in dem das BKA und das BSI zusammenarbeiten: der Cybersabotage. Dabei werden zunächst Identitätsdaten erbeutet, um diese dann für Sabotageangriffe zu nutzen. Denial of Service-Angriffe, wie wir sie etwa Anfang des Jahres gegen US-Banken gesehen haben, stützen diese Erkenntnis. Hinzu kommen ausgefeilte, zielgerichtete Angriffe auf Behörden und Unternehmen mit dem Ziel der Cyberspionage.

Aktuelle Herausforderungen

Cyberspionage und Cybersabotage, das sind die großen Felder, in denen wir akut gefordert sind.
Dem allgemeinen Trend folgend breiten sich diese Angriffe nunmehr auch auf mobile Geräte aus, die ja in Bezug auf ihre Sicherheit immer wieder für Diskussionen sorgen. Sorge bereitet uns auch der Bereich der industriellen Steuerungssysteme. Diese Systeme werden heutzutage über einen sehr langen Zeitraum konstant eingesetzt. Für die Unternehmen ist dies eine Frage des Return of Investment. Wenn Sie in solche Technologien investieren, als Autobauer oder auch als Kraftwerksbetreiber, dann müssen Sie über einen langen Zeitraum mit Bedrohungen leben, die beim Kauf dieser Technologie und bei deren Entwicklung noch lange nicht absehbar waren. Hier müssen Betreiber einen riesigen Spagat zwischen betrieblichen Anforderungen und den Profitanforderungen auf der einen und dem notwendigen Schutz dieser Komponenten, insbesondere für Netze und Prozesse, auf der anderen Seite leisten. Besonders wichtig ist dies für den Bereich der kritischen Infrastrukturen, auf den ich später noch einmal zurückkommen werde.

Eine der größten Herausforderungen in Bezug auf Cybersicherheit ist aber die technologische Entwicklung. Sie geht hin zu einer immer höheren Integration in Netze, zu immer höheren Geschwindigkeiten. Das heißt, die Verteidiger müssen permanent Schritt halten mit einer hohen Agilität der Angreifer. Es gibt einen schönen Satz, der sagt: „Ein Verteidiger muss tausendmal erfolgreich verteidigen, aber ein Angreifer braucht nur ein einziges Mal unter tausend Angriffen Erfolg zu haben." Insofern ist es wichtig, all die neu entdeckten Schwachstellen, die selbst oft nur für kurze Zeit als Zero-Day-Exploits nutzbar sind, zu bekämpfen. Das ganze Spektrum der Exploit-Kits, der Trojaner, der vielen Möglichkeiten von Schadprogrammen, zeigt das auf. Als Verteidiger wie das BSI und als Strafverfolger wie das BKA müssen wir mit all diesen neuen Spektren und Geschwindigkeiten umgehen.

Prävention und Kooperation

BSI und BKA sind sich dabei einig, dass der Schlüssel zu mehr Cybersicherheit natürlich die Prävention ist. Kriminalprävention oder Informationssicherheitsprävention, das ist der gute Ansatz, den wir uns alle wünschen würden. In diesem Moment ist nämlich noch nichts passiert und wir beugen gemeinsam vor. Aber man kann einfach nicht übersehen, dass in einer Welt der unperfekten Software, in einer Welt, in der IT eben nicht wirklich bis zum Ende sicher durchdacht ist, uns nichts anderes übrig bleiben wird, als die Angriffe, um die es geht, zu detektieren und schließlich und endlich auch abzuwehren. Diese Abwehr äußert sich nun zwischen BKA und BSI in zwei Weisen. Auf der einen Seite durch die Strafverfolgung, durch die Methoden der Repression, die Täter zu entdecken und dingfest zu machen. Auf der anderen Seite die Detektion in einem weitergehenden Sinne, wie sie etwa das BSI-Lagezentrum betreibt, und damit die Erfüllung der Forderung, die sich aus der Cybersicherheitsstrategie ergibt: ein gemeinsames Aufstellen gegen jede Form von Kriminalität, Spionage oder Sabotage. Dafür benötigen wir einen Informationsaustausch.

Denn das BKA sieht natürlich andere Fakten, andere Erscheinungsformen aus dem Bild der Kriminalität. Wir als BSI müssen vom BKA vor allen Dingen über Modi Operandi erfahren, die von den Tätern eingesetzt werden, um uns dann darauf in unserer Konzeption von Sicherheitsmechanismen und von neuen IT-Sicherheitsformen in Software und Hardware einzustellen. Auf der anderen Seite können wir Ihnen aber zu diesen Modi Operandi entgegenkommen durch technische Analyse, durch das Erstellen von Signaturen, die Sie wiederum in die Lage versetzen, Täter dingfest zu machen und in die Infrastrukturen der Täter einzudringen. Der Informationsaustausch zwischen BKA und BSI findet, abgesehen von dem wirklich sehr guten Austausch über unsere Verbindungsbeamten hinweg, auch im Nationalen Cyberabwehrzentrum statt. Dies ist schon deswegen eine notwendige Einrichtung, weil wir uns über unsere beiden Häuser hinaus natürlich auch mit den anderen Sicherheitsbehörden zu deren Erkenntnissen über die Infrastrukturen austauschen müssen, um schließlich ein gemeinsames Lagebild auch schlüssig erstellen zu können.

Die Kooperation darf allerdings an dieser Stelle nicht einfach bei den Behörden enden. Wie Sie wissen, haben wir mit der Allianz für Cybersicherheit eine Kooperation mit der Privatwirtschaft eröffnet, vor allen Dingen zugunsten der kleinen und mittleren Unternehmen, die sich in Bezug auf IT-Sicherheit allein nicht optimal aufstellen können. Das BSI hat daher gemeinsam mit dem BITKOM auf der CeBIT 2012 die Allianz gegründet, die zwischen professionellen Anwendern, Herstellern, Dienstleistern, Forschungseinrichtungen, Behörden und weiteren Beteiligten in Wirtschaft und Verwaltung vermittelt. Mittlerweile reden wir von ca. 500 freiwilligen Teilnehmern, Anbietern und Multiplikatoren, was eine sehr erfolgreiche Zahl ist.

Darüber hinaus ist der UP KRITIS zu erwähnen, eine seit 2005 bestehende öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen. Wir haben seitdem verschiedene Arbeitsgruppen gemeinsam mit der Wirtschaft gegründet, mit den Energieversorgern, mit den Banken, mit vielen anderen kritischen Infrastrukturen, in denen operativ zusammengearbeitet wird. Hier werden bei Gefährdungen Informationen ausgetauscht, aber auch in Übungen der Umgang mit IT-Krisen geübt, evaluiert und optimiert. Im Moment stellen wir diesen UP KRITIS auf eine neue verbreiterte Arbeitsweise um, die sich nicht nach Sektoren, sondern nach Branchen ausrichtet und damit eine nochmals erweiterte Plattform der Kommunikation mit diesen kritischen Infrastrukturen bietet.

Perspektiven der Cybersicherheit

An dieser Stelle möchte ich auf das Thema Cybercrime eingehen. Die Kernfrage lautet, wie wir unsere gesamte Gesellschaft fit machen für IT-Techniken. Sieht man sich die Bedrohungslage und die Vielfalt der Angriffe an, ist an dieser Stelle sicher noch viel Arbeit zu leisten. Wenn wir alleine auf die Aufstellung zum Thema Cybercrime schauen, so wird doch ganz offensichtlich, dass uns eines fehlt und das hat Prof. Rappoport heute in seinem Vortrag schon angesprochen: „Wir müssen in die Position kommen, zu antizipieren." Er hat das so ausgedrückt: „Die neuen modernen Mitarbeiter aus dem Management kommen und fragen, was soll ich morgen tun?" Sie treffen nicht mehr Entscheidungen für heute, sie wollen wissen, wie sie sich durch die IT-Zukunft bewegen. Und das ist auch für uns ein entscheidender Faktor. Wir sind in erster Linie reaktiv aufgestellt. Das ist gut und wichtig, aber wir müssen zugleich in die Vorhand kommen. Wie kann das gehen bei moderner IT? Es ist so, dass natürlich auch der Cyberraum gewisse Gesetzmäßigkeiten aufweist. Wir müssen uns mittel- und langfristig damit auseinandersetzen, wie etwa Täter agieren. Wer wird von Tätern ins Visier genommen? Welche Schwachstellen, etwa in Software, werden gerade von Tätergruppen analysiert? Womit setzen sie sich auseinander? Wo suchen sie nach neuen Wegen? Welche Geschäftsprozesse, etwa in der Aufstellung der Täter selbst, sind zu beobachten? Wohin entwickelt sich die Underground-Economy? Aber auch: Welche Geschäftsprozesse bei den Opfern werden durch die Täter beobachtet? Wo geraten insbesondere bestimmte IT-Geschäftsvorgänge in das Visier von Cyberkriminellen und wie können wir uns entsprechend aufstellen? Letztlich gehört dazu auch die Frage: Wie können wir Täter im Netz identifizieren? Das sind entscheidende Fragestellungen, denen wir uns widmen müssen, und ein Themenfeld, das BKA und BSI nur gemeinsam bearbeiten können - im Grunde sogar nur gemeinsam mit weiteren Playern, Sicherheitsbehörden und der Forschung, die uns an dieser Stelle unterstützen.

Gemeinsames Lagebild

Grundlage für all das ist aber Informiertheit. Wir müssen informiert sein über das, was in Netzen vorgeht, über die Angriffe, die in Netzen laufen, mit dem Ziel, tatsächlich zu einem gemeinsamen Lagebild zu kommen. Dieses gemeinsame Lagebild können wir als BSI für die Behördenlandschaft, insbesondere für die Bundesbehörden, sehr genau zeichnen, weil wir dort entsprechende Befugnisse besitzen und an den Schaltstellen der Bundesnetze sitzen und sehen, was abläuft. Wir haben das sehr erfolgreich in dem Bereich der kritischen Infrastrukturen, in der Zusammenarbeit im UP KRITIS ausgeweitet, wenn auch hier die Zusammenarbeit natürlich auf Freiwilligkeit beruht. Wenn man etwa an Banken und Versicherungen denkt, kann dies sehr gut funktionieren, insbesondere bei denjenigen, die Regulierung kennen. Diese Unternehmen wissen, wie die Zusammenarbeit mit dem Staat

läuft, oder sind aus bösen Umständen heraus, die man ihnen nicht hätte wünschen wollen, in eine Zusammenarbeit mit dem BSI gekommen. In dem Moment erfahren die Unternehmen, dass diese Zusammenarbeit auf vertraulicher Basis machbar ist, dass wir sehr sorgfältig mit dem umgehen, was wir an Informationen erhalten und auch einen Return of Investment dafür leisten, indem wir Maßnahmen produzieren und Hinweise geben, wir man aus Problemen mit der Cybersicherheit herauskommt und sich für die Zukunft besser aufstellt.

Allerdings haben die Gespräche, die etwa durch den Bundesinnenminister im Laufe der vergangenen eineinhalb Jahre geführt wurden, gezeigt, dass es dieses Vertrauen leider noch nicht in allen Branchen gibt. Wir werden daher durchaus darauf angewiesen sein, in der neuen Legislaturperiode noch einmal mit dem Informationssicherheitsgesetz anzutreten. Auch dieses Gesetz stellt die Prävention in den Mittelpunkt. Dort werden Anforderungen an Infrastrukturen gestellt, wie diese in Bezug auf die Sicherheit gut aufgestellt werden können. Das muss im gemeinsamen Interesse aller liegen, allerdings brauchen wir dafür auch Informationen über Sicherheitsvorfälle. Über einen geeigneten Mechanismus dafür wird sicherlich zu reden sein, denn Vertrauenswürdigkeit und Vertraulichkeit müssen gewährleistet sein. Letztlich muss man aber festhalten, dass ein solches Vorgehen im Sinne einer Gesamtlage, in einer Fürsorge für die gesamte KRITIS-Wirtschaft und letztlich auch für unser Gemeinwesen unabdingbar ist. Dazu gehört auch, dass das BKA durch dieses Informationssicherheitsgesetz mit entsprechenden Befugnissen ausgestattet wird, um in diesen Fällen schwerer Kriminalität, die ja immer mit Sabotage einhergehen, auch tatsächlich tätig werden zu können. Diese wichtige Aufgabe wird die Kooperation zwischen Bundeskriminalamt und BSI weiter fördern. Das ist eine Zukunftsaussicht, der ich mit sehr viel Zuversicht entgegensehe.

Peter Henzler

Das Spektrum der Aufgaben, die es zur Gewährleistung von Cybersicherheit und für eine wirksame Bekämpfung von Cybercrime zu bewältigen gilt, ist gewaltig. Es macht deutlich, dass die Aufrechterhaltung von Cybersicherheit eine „res publica“ ist, eine Aufgabe für das gesamte Gemeinwesen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundeskriminalamt (BKA) stehen gemeinsam für den komplementären Ansatz, mit dem auf Bundesebene hierfür ein Beitrag erbracht werden soll. Die Maßnahmen der Bundesregierung zielen darauf ab, Deutschland als einen der sichersten Standorte für die Erbringung und Nutzung von IT-Dienstleistungen weltweit zu etablieren. Hierzu legt die Cyber-Sicherheitsstrategie für Deutschland die Grundlagen, um Cyber-Sicherheit auf einem hohen Niveau zu gewährleisten. Teil dieser Strategie ist ein enger Austausch zwischen Staat, Wirtschaft und Wissenschaft, sowie in der internationalen Staatengemeinschaft. Die Aktivitäten von BSI und BKA in den Breichen Cybersicherheit und Cybercrime sind integrale Bausteine der konsequenten Umsetzung dieser Strategie. Der Schwerpunkt des BSI liegt dabei im Bereich der Sicherheit aus technischer Perspektive, der des BKA in der Strafverfolgung. Beide Sphären, Cybersicherheit und die Bekämpfung von Cybercrime, lassen sich nicht voneinander trennen, sie sind zwei Seiten einer Medaille. Lücken in der Sicherheit sind gerade im Cyberspace die Einfallstore für Straftäter. Weil sich ihre Aufgabenbereiche nicht voneinander trennen lassen, begegnen BSI und BKA dieser Herausforderung im Schulterschluss. Bei der Identifizierung von Sicherheitslücken und von Straftätern arbeiten die Mitarbeiterinnen und Mitarbeiter von BSI und BKA Seite an Seite. Von unverzichtbarem Wert ist die Expertise des BSI beispielsweise in den Bereichen Netzwerktechnik, sicherer Serverbetrieb, Programmierung, und hier insbesondere eines sehr weiten Spektrums von Programmiersprachen, Reverse Engineering, technische Analysen, Rückmeldewege von Schadsoftware sowie seine zahlreichen wichtigen Kontakte zu AV-Herstellern, Softwareunternehmen und Computer Emergency Response Teams in Europa und der ganzen Welt - diese Aufzählung ist nicht abschließend. Diese Expertise ergänzt kriminalistische Analysen des BKA und führt zu einem umfassenderen, tieferen Verständnis des Täterhandelns. Das hilft bei der Strafverfolgung und zugleich bei der Entwicklung von Gegenmaßnahmen. Die gemeinsame Strategie von BSI und

BKA lässt sich wie folgt zusammenfassen: Das BSI sorgt mit Hilfe des BKA dafür, dass Cyberangriffe abgewehrt und Sicherheitslücken geschlossen werden; das BKA identifiziert und verfolgt die Straftäter und erhält dabei Unterstützung vom BSI.

Welche Herausforderungen bergen Straftaten im und gegen das Internet sowie gegen IT-basierte Infrastruktur-, Wirtschafts – und Finanzsysteme in Zukunft? Bei den Tätern handelt es sich zunehmend um auf Hochschulen oder in namhaften IT-Firmen ausgebildete IT-Spezialisten. Diese schließen sich, ohne ihre jeweilige wahre Identität preiszugeben, temporär, projektartig und räumlich über die ganze Welt verteilt mit ihren jeweiligen Fähigkeiten zusammen. Sie nutzen neueste Trojanertechnologien und unterlaufen damit die Gegenmaßnahmen der Anti-Viren-Hersteller. Diese benötigen im Regelfall etwa 30 Tage von der Entdeckung einer neuen Schadsoftware bis zur Erstellung einer zu ihrer Blockierung oder Beseitigung erforderlichen Anti-Viren-Signatur. Wenn erforderlich, setzen die Angreifer Innentäter ein, um Sicherheitssysteme gegen Angriffe von außen zu umgehen. Sie bedienen sich gekaperter Privatrechner, die zu Bot-Netzen, d.h. einem Verbund von mit zehntausenden oder hunderttausenden nach ihrem Willen gesteuerten und zusammengeschlossenen Fremdrechnern. Zusätzlich wird für die Tatbegehung notwendiges Know-how zunehmend als Service angeboten und vertrieben. Ihre Beute können Finanztransaktionen zu ihren Gunsten und Erlöse aus Online-Erpressungen, der Rückverkauf gestohlener Daten an den Eigentümer, der Verkauf von Firmen Know-how oder Forschungsergebnissen an Konkurrenten sein. Sie können Börsenkurse durch breit angelegte Falschinformationen künstlich in die Höhe treiben und selbst zum richtigen Zeitpunkt abkassieren. Die erlangten Gelder bzw. geldwerten elektronischen Werte werden unter Nutzung von E-Money-Diensten weltweit durchs Netz geschleust und kommen, ohne Spuren hinterlassen zu haben, bei den Tätern an. Es handelt sich um international organisiertes Cybercrime!

Die Bekämpfung von Cybercrime ist bereits heute einer der Treiber der Netzwerkbildung – zwischen Behörden und Behörden, zwischen Behörden und der Wirtschaft, innerhalb der Wirtschaft, auf Ebene der Länder, des Bundes, in Europa und darüber hinaus. Diese Kooperationen bieten neben einem optimierten Informationsaustausch auch die Entwicklung eines erhöhten Problembewusstseins bei allen Beteiligten durch umfassende Information und, - dies ist erfolgsrelevant- sie schaffen Vertrauen zwischen den Akteuren. Von einer begleitenden Steigerung der Kompetenzen aller Kooperationspartner ist dabei auszugehen.

Auf Bundesebene haben sich die Sicherheitsbehörden in einem Cyber-Abwehr-Zentrum vernetzt. Bereits der Name des Zentrums postuliert einen hohen Anspruch. Dieser Ansatz hat sehr viel Potenzial, muss allerdings konsequent weiterentwickelt werden, um dieses vollständig auszuschöpfen.

Strukturimmanent hat der deutsche Sicherheitsföderalismus von Anbeginn die Netzwerkbildung befördert. So auch im Bereich von Cybercrime.

Die rasante Entwicklung von Cybercrime und ihre Komplexität erfordern eine enge Vernetzung der Expertise in den Polizeien der Länder und beim Bundeskriminalamt. Zu diesem Zweck wurde bereits 2006 die *Leitertagung Cybercrime* ins Leben gerufen. Im Rahmen dieses wichtigen polizeilichen Gremiums stehen die Leiter der Cybercrime-Dienststellen der LKÄ und des BKA in einem ständigen fachlichen Austausch und definieren die Anforderungen und Rahmenbedingungen für die Spezialisten in ihren Bereichen. Die Leitertagung Cybercrime hat die Bündelung der Informationen über den kriminalpolizeilichen Meldedienst für Cybercrime auf ein neues Niveau befördert. Tatzusammenhänge können dadurch besser festgestellt werden; sie bilden zugleich die Bausteine für eine umfassende

Analyse von Cybercrime. Neue Erscheinungsformen und ihre Verbreitung werden heute früher erkannt und gemeinsam Bekämpfungsstrategien schneller entwickelt. Doch die Aufgabe der Leitertagung ist in einem Punkt von besonderer Bedeutung: Sie ist verantwortlich für die konzeptionellen Arbeiten zur konkreten fachlichen Ausgestaltung der nationalen Zusammenarbeit. So wurde hier die Strategie zur Bekämpfung von Cybercrime entwickelt, deren Bestandteile wie *„Optimaler Informationsaustausch"* auf allen Ebenen (Bund/Ländern, Private), *Wirksame Kriminalitätsbekämpfung*, z.B. durch die Einrichtung von Fachdienststellen und die *Sensibilisierung und Stärkung von Anbietern, Entwicklern und Anwendern* [„Verantwortungsbewusste Anbieter und Entwickler"; „Kompetente private und professionelle Anwender"] in die Praxis umgesetzt wurden. Die Leitertagung regelt unter den Fachleuten, wie mit Massendaten umgegangen und die Zusammenarbeit mit den Providern organisiert werden soll. Im Zuge eines Auftrages übergeordneter Gremien oder eigeninitiativ erarbeitet sie Lösungen für aktuell auftretende Fragestellungen auf dem Gebiet Cybercrime, beispielsweise ganz konkret zu einem Botnetz-take-down oder strategisch zur Abbildung des Phänomens Cybercrime in der Polizeilichen Kriminalstatistik.

Auf internationaler Ebene arbeitet das BKA, im Regelfall in seiner Rolle als Zentralstelle für die gesamte deutsche Polizei mit einer Vielzahl von Organisationen und Institutionen zusammen. Beispielhaft für eine Vielzahl weiterer seien an dieser Stelle *INTERPOL*, *EUROPOL* mit seinem in diesem Jahr eingerichteten Cyberarbeitsbereich *EC 3*, dem *European Cybercrime Center*, die *Hightec Crime Subgroup* der *G 8 Roma Lyon Group* mit 60 Kooperationspartnern und einem 24 /7 Kontaktstellennetzwerk sowie die *NCFTA/FBI* (die National Cyber Forensics and Training Alliance des FBI) erwähnt.

Das Bundeskriminalamt übernimmt Verantwortung, auch international. Im Projekt „Cybercrime" der *European Multidisciplinary Platform Against Criminal Threats – EMPACT* hat das BKA im August 2013 den Vorsitz übernommen.

EMPACT wurde am 8./9. November 2010 durch den Rat der EU als EU-Politikzyklus zur Bekämpfung der organisierten und schweren internationalen Kriminalität eingerichtet. Mit diesem mehrjährigen Zyklus soll in kohärenter und methodischer Weise gegen die größten Bedrohungen für die EU durch organisierte und schwere Kriminalität vorgegangen werden, und zwar durch eine optimale Zusammenarbeit zwischen den zuständigen Dienststellen der Mitgliedsstaaten, den Institutionen und Agenturen der EU sowie Drittländern und Organisationen, ggf. unter Einbeziehung des Privatsektors

Im Projekt „Cybercrime" werden die strategischen Ziele für eine gemeinsame Bekämpfung von Cybercrime innerhalb Europas festgelegt und danach durch konkrete Projekte umgesetzt. Durch diese Driver-Funktion war es dem BKA möglich, die positiven Erfahrungen, die in Deutschland mit der strategischen Neuausrichtung bei der Bekämpfung von Cybercrime gemacht wurden, in die Entwicklung einer gemeinsamen europäischen Strategie für den Zeitraum bis 2017 einzubringen. Diese Strategie beinhaltet die folgenden Ziele:

- Die Erstellung eines umfassenden Cybercrime-Lagebilds, als gemeinsame Basis für die Festlegung von Prioritäten und Zielen.

- Die gemeinsame Bekämpfung von Cybercrime durch gemeinsame Ermittlungen und koordinierte Strafverfolgung.

- Die Verbesserung der operativen und justiziellen Zusammenarbeit sowie die Koordinierung mit Drittstaaten bei der Bekämpfung priorisierter Bedrohungen.

- Eine Maximierung der Zusammenarbeit mit Akteuren außerhalb der Strafverfolgung unter Einbeziehung von Cyber Emergency Response Teams (CERTs) und privaten Unternehmen, um die Koordinierung und den Austausch von Informationen zu intensivieren sowie präventive Kompetenzen und Ermittlungsleistungen zu stärken.

- Die Einrichtung eines koordinierten multidisziplinären Reaktionsmechanismus in Fällen eines schwerwiegenden Cyber-Angriffes von internationaler Dimension mit klar definierten Rollen, Verfahrensweisen und Verantwortungen.

- Den Aufbau und die Stärkung von Kompetenzen im Cyber-Bereich durch Entwicklung geeigneter Ressourcen und Werkzeuge, sowie den Ausbau von Fachwissen und fachlichen Fähigkeiten bei den Strafverfolgungsbehörden, der Justiz sowie Schlüsselpartnern in der Forschung.

- Die Stärkung des Bewusstseins für das Thema Cybersicherheit bei den Anwendern, d.h. die Erhöhung von Verantwortungsbewusstsein, Resilienz und Flexibilität bei privaten und professionellen Nutzern, insbesondere bei Betreibern kritischer Infrastrukturen und Informationssystemen.

- Die Feststellung der Möglichkeiten zur Fortschreibung des Rechtsrahmens, um eine wirksame Prävention, Erkennung, Ermittlung, Zerschlagung und Strafverfolgung von Cyberstraftaten zu ermöglichen und aktiv an der Debatte der erkannten juristischen Probleme mitzuwirken.

Wie eingangs erwähnt, ist die Gewährleistung von Cybersicherheit eine „res publica“, eine gesamtgesellschaftliche Aufgabe. Eine herausragende Rolle haben hierbei die Akteure der Internetwirtschaft. Bereits heute gibt es eine Vielzahl von behördlich–privaten Kooperationen, die sich dem gemeinsamen Ziel verschrieben haben, Kommunikation, soziale Zusammenhänge und insbesondere wirtschaftliches Leben, soweit es mit dem Internet verbunden ist, gegen immanente Gefahren im Cyberraum zu schützen und dadurch dort ein freies und sicheres Agieren zu ermöglichen.

Stellvertretend für eine Reihe weiterer Initiativen und Kooperationen stehen beispielsweise die *Allianz für Cybersicherheit*, der Verein *Deutschland sicher im Netz e.V.*, der *Bundesverband IT-Sicherheit e.V.,* die *Sicherheitskooperation Cybercrime* zwischen den Landeskriminalämtern Nordrhein-Westfalen und Baden-Württemberg und dem BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) und der *Umsetzungsplan Kritische Infrastrukturen*.

Die Initiative „Umsetzungsplan Kritische Infrastrukturen (UP-KRITIS)“ wurde vom Bundesministerium des Innern 2007 ins Leben gerufen. Kritische Infrastrukturen sind Organisationen und Einrichtungen von erheblicher Bedeutung für das staatliche

Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere weitreichende Folgen eintreten würden. Derzeit gehören dem UP-KRITIS zahlreiche Betreiber Kritischer Infrastrukturen in Deutschland und deren Verbände an. Primäre Ziele der Zusammenarbeit sind, die KRITIS-relevanten IT-Prozesse robuster zu machen sowie IT-Krisen besser zu beherrschen. Hierzu sind bspw. geeignete Kommunikationsstrukturen geschaffen worden. Schwerpunkte der Zusammenarbeit im Rahmen des UP-KRITIS sind die Aufrechterhaltung kritischer Infrastrukturdienstleistungen, Notfall- und Krisenübungen sowie Krisenreaktion und --bewältigung. Darüber hinaus wird der Erfahrungsaustausch der Teilnehmer forciert. Single Points of Contact (SPoCs) stehen im Mittelpunkt der Kommunikationsstruktur, um die Kommunikationswege zu strukturieren und den Kommunikationsaufwand jedes Beteiligten zu minimieren.

Die *Allianz für Cyber-Sicherheit* wurde 2012 auf Initiative des BSI in Zusammenarbeit mit dem Branchenverband BITKOM e.V. gegründet. Die Federführung liegt beim BSI. Als Teilnehmer der Initiative kommen deutsche Institutionen sowohl aus dem privatwirtschaftlichen als auch aus dem öffentlichen Sektor in Frage, die durch aktive Beiträge die Cyber-Sicherheit in Deutschland gestalten, fördern und verbessern. Angesprochen sind dabei Organisationen außerhalb der Kritischen Infrastrukturen wie bspw. CERTs, Anwenderbranchen mit intensivem IT-Einsatz sowie Multiplikatoren aus Medien und Wissenschaft. Zwischen den Beteiligten besteht keine (formale) gemeinsame Kooperationsvereinbarung. Interessierte Institutionen können sich als „Teilnehmer“ oder „Partner“ registrieren lassen. Voraussetzung ist, dass sie sich bestimmten Regelungen und Verfahrensweisen unterwerfen und dies schriftlich bestätigen. Schwerpunktaktivitäten sind einerseits die zentrale Bereitstellung von Informationen durch das BSI und durch Partner der Allianz und andererseits die Unterstützung des Erfahrungsaustauschs der Teilnehmer untereinander.

Der *Verein Deutschland sicher im Netz e.V.* (DsiN e.V.) wurde 2007 unter der Schirmherrschaft des BMI gegründet. Er ist Ansprechpartner für Verbraucher und mittelständische Unternehmen zu Fragen der IT-Sicherheit. Mit dem gemeinsamen Ziel, das Sicherheitsbewusstsein von Anbietern und Verbrauchern beim Umgang mit dem Medium Internet zu erhöhen, kooperiert der Verein mit dem BMI. Als übergreifende Institution bündelt DsiN e.V. die Aktivitäten von Unternehmen, Branchenverbänden sowie Vereinen und stellt herstellerunabhängig und produktneutral einen zentralen Ansprechpartner dar.

Der *Bundesverband IT-Sicherheit* (TeleTrusT) ist ebenfalls ein eingetragener Verein und fördert Wissenschaft und Bildung auf dem Gebiet der Entwicklung einer sicheren und vertrauenswürdigen Informations- und Kommunikationstechnik. Unter Federführung des *Instituts für Internet-Sicherheit* der Westfälischen Hochschule Gelsenkirchen treffen sich seit dem Jahr 1989 mehr als 170 Mitglieder aus Industrie, Verwaltung und Wissenschaft. Neben dem BKA ist auch das BSI Mitglied dieser Initiative.

Die *Sicherheitskooperation Cybercrime* wurde 2011 erstmalig zwischen der BITKOM e.V. und dem LKA Nordrhein-Westfalen geschlossen. Das LKA Baden-Württemberg hat sich im März 2013 angeschlossen. Ziel ist die Förderung der Sicherheit bei der Nutzung von Informations- und Kommunikationstechnologien sowie zur präventiven und repressiven Bekämpfung von Cybercrime. Hierzu zählen eine Verbesserung des Bewusstseins um die Gefahren der Computerkriminalität, die Verbesserung der phänomenologischen Erkenntnisse, die Erweiterung der technischen Kompetenzen, die Fortentwicklung der Prävention sowie eine Intensivierung des Wissenstransfers zur Bekämpfung der Computerkriminalität.

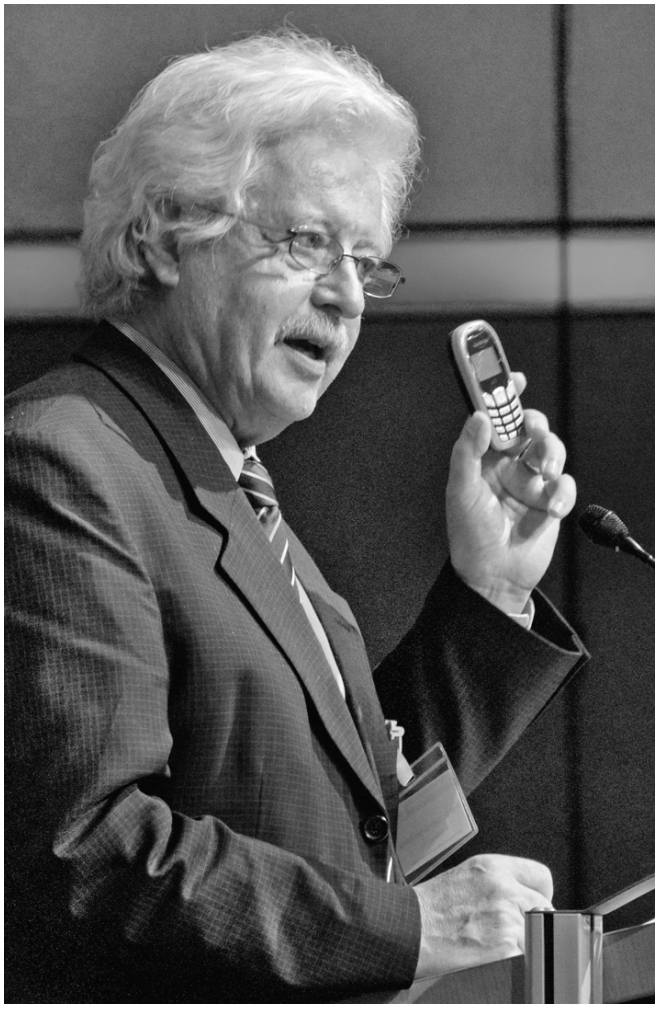
Zur Umsetzung dieser Ziele erfolgen ein Informationsaustausch und Wissenstransfer, gegenseitige Hospitationen, die Konzeption und Durchführung von Präventionsmaßnahmen und die Vermittlung von Experten in konkreten Einzelfällen.

Das jüngste „Start-up" auf diesem Sektor ist das *„ German Competence Center against Cyber Crime"*, kurz G4C, ein Verein, der Anfang November 2013 von den Vorständen dreier bedeutender deutscher Banken gegründet wurde. Satzungsgemäßer Zweck ist es, die Kriminalprävention zu fördern. Erreicht werden soll dieses Ziel durch die Förderung der Zusammenarbeit zwischen Sicherheits- und Strafverfolgungsbehörden und der Privatwirtschaft, die Schaffung und den Betrieb einer Plattform für den ganzheitlichen Austausch, die Erarbeitung von Maßnahmen zur Erkennung und Verhinderung von Schäden und die Sammlung und Korrelation relevanter Informationen sowie die zielgerichtete Weitergabe an Mitglieder zum Schutz der Öffentlichkeit.

Der Verein ist der private Teil einer institutionalisierten Public Private Partnership mit dem Bundeskriminalamt und dem Bundesamt für Sicherheit in der Informationstechnik. Beide Partner werden künftig auf der Grundlage einer Kooperationsvereinbarung agieren, die die jeweiligen Rechte und Pflichten regelt und die unter Beachtung der für eine solche Partnerschaft maßgeblichen gesetzlichen Vorschriften erarbeitet wurde, insbesondere denen des Datenschutzes. Räumlich unter einem Dach werden arbeitstäglich von Spezialisten der beteiligten Akteure Lösungen für tagesaktuelle Probleme der Cybercrime entwickelt und auch langfristige strategische Ziele abgestimmt und verfolgt. Angriffe und Angriffsmöglichkeiten auf über das Internet vermittelte Produkte und Dienstleistungen, wie beispielsweise das Online-Banking, werden aus den unterschiedlichen Perspektiven analysiert mit dem Ziel, passgenaue Schutzmechanismen zu entwickeln und parallel Wege zu finden, die Täter der Strafverfolgung zuzuführen, ihre Logistik einzuziehen und erbeutete Gelder wiederzuerlangen.

In der Anfangsphase dieser Public Private Partnership stehen auf der privaten Seite Banken, da diese zum einen eine besondere Verantwortung für den sicheren Zahlungsverkehr via Internet tragen und zum anderen bislang die durch Angriffe auf den Zahlungsverkehr verursachten Schäden regulieren, obwohl es ihre Kunden sind, bei denen die Angriffe auf das Online-Banking erfolgreich sind. Ob Banken diese Schäden auch künftig tragen werden, kann bezweifelt werden. Dann, aber bereits auch jetzt, dient die Public Private Partnership mit dem G4C jedem einzelnen Kunden, d.h. der Bevölkerung insgesamt. Bereits bei Gründung waren sich alle Partner einig, und so ist es auch in der Satzung des Vereins G4C festgehalten, dass es eine Erweiterung der Mitglieder des Vereins auf alle interessierten Unternehmen und Branchen der Internetwirtschaft geben soll, um den Marktplatz „Internet" in Deutschland sicher zu machen und damit das Wirtschaftssystem und den Zahlungsverkehr insgesamt zu schützen.

Cybercrime: *Einführende Betrachtungen zur Podiumsdiskussion über* „Freiheit im Netz und Cybersicherheit“



Seniorprofessor Dr.
Hans-Jürgen Kerner

Dieser Beitrag diente ursprünglich in verdichteter Fassung als Einleitung zur Podiumsdiskussion am Schlusstag der Herbsttagung des Bundeskriminalamts im November 2013. Für die Zuhörer sollte/konnte er als Überblicks-Resümee zum bislang erlebten Tagungsverlauf und Tagungsgeschehen dienen. Für den Leiter der Podiumsdiskussion, den Chefredakteur des WDR-Fernsehens, Jörg Schönenborn, und die Podiumsteilnehmer[1], die den Verlauf der Tagung nicht selbst erlebt hatten, sollte er als ein einführender Hintergrundbericht zur Einstimmung in das Thema der Podiumsdiskussion dienen, das spezifisch ausgerichtet war, wenngleich der eine oder andere Aspekt bereits in den Referaten angeklungen war.

Präsident **Ziercke** ging zu Beginn seiner Begrüßungsansprache[2] auf die hohe Aktualität des Themas ein, was viele (andere) Veranstaltungen im Jahr 2013 belegten, die sich mit dem Problem Cyberkriminalität beschäftigten. Auch in vielen Sondersitzungen der Polizeien des

[1] Jürgen Stock, Vizepräsident beim BKA; Markus Beckedahl, netzpolitischer Aktivist aus Berlin und Gründer des Blogs „netzpolitik.org“; Marianne Janik, als Senior Director Public Sector Mitglied der Geschäftsleitung bei der Microsoft Deutschland GmbH; Thilo Weichert, Landesbeauftragter für den Datenschutz Schleswig-Holstein.

[2] Mehr und Näheres dazu s. bei Ziercke 2013a; s.a. Ziercke 2013c mit Tagungsbericht in der Zeitschrift „Der Kriminalist“. Zu weiteren Tagungsberichten s. Bertel 2013 und Kock 2014.

Bundes und der Länder habe das Thema eine Rolle gespielt, mit dem Fokus auf der Frage, wie im digitalen Zeitalter eine effektive Verbrechensbekämpfung verwirklicht werden könne.

Mit Blick auf die anschließende Skizze zum Vortrag von Herrn Rappoport, der im Programm deutlich später angesetzt war, ist es aber nützlich, sogleich auf die „Internet-Lage in Staat, Wirtschaft und Gesellschaft“ vor möglichen Missbräuchen oder speziell krimineller Nutzung der Technologie und der Technik einzugehen. Präsident Ziercke führte aus, in Statistiken sei noch vor 10 Jahren der Prozentanteil von „Haushalten mit Internetanschluss“ bzw. die „Ausstattung von Haushalten mit PC“ erhoben worden. Solche Erhebungskriterien kämen einem heute fast anachronistisch vor, im Zeitalter von Smartphones, Tablets, WLAN-Hotspots und SmartGrid. Die digitale Revolution bringe Umwälzungen mit sich, welche mit denjenigen im Zeitalter der industriellen Revolution vor 200 Jahren verglichen werden können.

Digitale Technologien hätten alle Lebensbereiche, Kommunikationsformen und Interaktionsformen durchdrungen. Sie seien eine bedeutende Lebensader unserer Welt geworden, prägten mehr denn je alle Entwicklungen einer rasant fortschreitenden globalen Vernetzung. Ihr Potential erscheine unerschöpflich. Aber damit einher gingen auch spezifische Abhängigkeiten, Bedrohungen, Verletzlichkeiten und spezifische subjektive Unsicherheitsgefühle.[3]

Moshe **Rappoport** ist seit 28 Jahren in Zürich bei IBM beschäftigt und sein Kernanliegen, das er am IBM-Labor in Rüschlikon bei Zürich verfolgt, ist die Trendforschung im Sinne des Beginns eines neuen digitalen Zeitalters und eines Global Technology Outlook (GTO).

In den letzten 50 Jahren habe es drei größere Technologiewellen gegeben, die den Einsatz von Computern in Unternehmen bestimmt haben. Heute hätten wir einen neuen Wendepunkt erreicht und befänden uns auf dem Scheitelpunkt einer vierten Welle. Diese Welle sei durch das Zusammenwirken von sozialen, mobilen und Cloud-Technologien, das Aufkommen riesiger Datenmengen, sogenannte "Big Data", und die neuen Arten analytischer Informationssysteme gekennzeichnet, die zur Wertschöpfung in diesem Umfeld benötigt werden. Der GTO 2013 richte sein Augenmerk auf dieses Zusammenwirken, welches derzeit eine entscheidende Umgestaltung unseres Umgangs mit der digitalen Welt bewirke. Durch das Zusammenwirken der einzelnen Technologie-Treiber würden vier "Megatrends" mit entscheidenden Auswirkungen vorangetrieben:

• Wachsender Umfang - niedrigere Eintrittsschwelle;

• Wachsende Komplexität - dennoch größere Benutzerfreundlichkeit;

• Schnelllebigkeit ;

• Kontextuelle Überfrachtung.

Der weitere Vortrag widmete sich dem Thema „Big Data“ im Detail. Der Begriff meint große bis extrem mächtige Datenmengen, die unter anderem im täglichen Geschäftsbetrieb von vor allem mittleren bis großen Unternehmen anfallen, die (fast) alles (auch) elektronisch abwickeln und als Datenspuren speichern. Interessant wird es vor allem, wenn Datenmengen aus vielen, aufeinander beziehbaren, Quellen zusammentreffen oder sekundär

[3] Über aktuelle Hoffnungen und Befürchtungen der Bevölkerung geben wiederholte repräsentative Umfragen Auskunft. Hingewiesen sei auf Deutsche Telekom 2011 und 2013; Deutsches Institut für Sicherheit und Vertrauen im Internet 2013. Zur europäischen Ebene s. zuletzt das Eurobarometer 404 der European Commission 2012.

zusammengeführt werden können. Neue Technologien, neu entwickelte Datenverarbeitungsmethoden (Algorithmen) und nach und nach sozusagen gegen „Unendlich“ wachsende Datenspeicher (bereits jetzt im Exabyte-Bereich) machen vordem Ungeahntes möglich. Dazu gehört unter der Perspektive von möglichst verlustarmer gezielter Breitenwerbung, aber auch unter der Perspektive einer die Ressourcen schonenden und die Gewinnmargen erhöhenden intelligenten Logistik, das Durchsuchen, Analysieren, Visualisieren und Interpretieren von je für sich eher mäßig interessanten, aber in der Zusammenführung/komplexen Gesamtheit hoch bedeutsamen Befunden. Ein elektronischer Kassenbon eines Berufstätigen aus einer Coffee-Shop-Filiale, bezogen auf ein ganz bestimmtes Getränk, ein weiterer Kassenbon vom selben Tag über in einer Buchhandlung gekaufte Zeitschriften einer bestimmten Art, und schließlich ein abendlicher Kassenbon vom selben Tag über ein Dinner in einem gehobenen Restaurant – alles mit Kreditkarte bezahlt –, bieten ein weiteres Steinchen im marktrelevanten Mosaik des „Vorlieben-Profils“ einer bestimmten Kunden-Teilmenge.

Moshe Rappoport zog einen großen, und auf Strecken die Zuhörer merklich in den Bann ziehenden Bogen.[4] Dabei zog er seine eigene Person und Lebensgeschichte mit ein, rückblickend auf die zeitgeschichtlich erstaunlich kurz zurückliegenden Anfänge der auf „die Menschen“ und nicht im Kern auf „den Markt“ oder die „Firmen“ (der Industrie, des Bankenwesens, aber auch des Handwerks und des Konsums) konzentrierten neuen Welt von Information und Dokumentation. Was von heute aus betrachtet nach außen hin wie eine durchgehende Erfolgsgeschichte des Internets, der Personal Computer, und danach aller anderen Technologien, Instrumente und Interaktionsströme auch nach Art der Sozialen Plattformen oder Netzwerken erscheine, habe im damaligen direkten und vielfach von aktueller sowie prognostischer Unsicherheit gekennzeichneten Alltagsbetrieb selbst einer führenden Firma wie IBM wiederholt krisenhafte Züge angenommen.

Der Referent war von Anfang an entweder direkt oder indirekt an der Zurüstung der neuen elektronischen Ära beteiligt. Dennoch meinte er zum Erstaunen und hörbar zur nicht geringen verständnisvollen Heiterkeit vieler Teilnehmer im Saal, er komme mit den neuen Apparaturen oft nur schlecht und manchmal gar nicht zurande. In diesem Rahmen war die von ihm eingeführte Unterscheidung in Digital Immigrants (wozu er sich selbst zählte) und in Digital Natives aufschlussreich. Als Digital Natives gelten ihm die Jugendlichen und mehr und mehr auch schon ganz jungen Kinder, die in einer entsprechend ausgestatten Umwelt (schon der Familie) von der neuen und eben auch optisch und sonst buchstäblich „attraktiven“, also anziehenden Gerätschaft, täglich umgeben sind. Sie probieren diese, neugierig und vorbehaltlos und ggf. auch ins Spielerische verloren, einfach aus, und lernen in einer für Erwachsene verblüffend kurzen Zeit kompetent damit umzugehen. Besonders das auch mimisch untermalte Beispiel eines der noch nicht sprechenden kleinen Enkel des Referenten, der ihm einen Tablet-PC aus der Hand nahm und den richtigen Umgang damit demonstrierte, war ebenso lustig wie fundamental erhellend für die auch personale und interpersonale Wucht der schon zu Beginn der Veranstaltung von Präsident Ziercke angesprochenen Umwälzungen der fortlaufenden elektronischen Revolution.

Ergänzend sei bemerkt: Bei Big Data Mining geht es um „massenhafte“ Hintergründe und Verknüpfungen, die eine Personalisierung bzw. Individualisierung schon im Ansatz nicht benötigen, so dass bei entsprechender Programmierung ein Datenschutzproblem ausgeschlossen werden kann. So etwas ist auch für wissenschaftliche Analysen in vielen Fachdisziplinen unmittelbar attraktiv. Bei der Kriminologie ist das noch nicht so recht angekommen. Interessante Strukturen, die in ihrer ggf. sogar täglichen und mehrfach

[4] Mehr und Näheres dazu s. bei Rappoport 2013

variierenden Dynamik beobachtet werden könnten, wären beispielsweise Kriminalitätsströme bzw. Täter-Aktions-Ströme, die aus kriminalökologischer Perspektive gerade als Ströme Aufschluss über latente Attraktoren vermitteln könnten. Ein Kollege hat bei der European Society of Criminology Conference in Budapest im September dieses Jahres vorgetragen, wir seien doch sehr rückständig, jammerten mit den Strafverfolgungsorganen, dass Kriminelle Big Data ausnutzen, anstatt selbst zu probieren, was man an Erkenntnissen für die Grundlagenforschung wie für angewandte Forschung herausholen könne. Er kam aber, nebenbei gesagt, auch aus einem Land, das datenschutzrechtlich nicht so sensibel ist wie Deutschland, weswegen die Diskussion nach dem Vortrag dann auch zeitweise heftig verlief, und Befürchtungen deutlich vorgetragen wurden.

Im seiner Begrüßungsrede war Präsident Ziercke auf Derartiges eingegangen, nämlich auf subjektive Unsicherheitsgefühle, aber auch auf objektive spezifische Abhängigkeiten, Verletzbarkeiten und Bedrohungen. Dies sei auch ein noch nicht hinreichend bearbeitetes Feld der Politikberatung durch die fachkundigen Behörden. In Bezug auf die Menschen im Lande sei es notwendig, auf die über das Internet zur Verfügung gestellte digitale Infrastruktur und auf die durch sie möglich gewordenen neuartigen Modus Operandi für Straftäter, mit enormen Schadenspotentialen und auch schon aktuell Schadensausmaßen, problembewusstseinsbildend stetig hinzuweisen. Der Zugriff auf die elektronischen Quellen stehe in der Gefahr, dass die gegen Cyberkriminelle vorgehenden Ermittler mit negativen Konnotationen wahrgenommen würden, im Extrem als Totalüberwacher, Datensammelwütige oder Datenprofilneurotiker. Es sei die Frage, wie man es schaffen könne, den Bürgerinnen und Bürgern verstehbar zu erklären, dass bei der Verfolgung von schwerer Kriminalität im Internet derzeit eine Gerechtigkeitslücke entstehe. Diese bevorteile wieder einmal nur die Cleveren und Verantwortungslosen, lasse aber den rechtstreuen Bürger fassungslos zurück.

Die vielen klaren Gesetzesverstöße erschienen bis heute in keiner Statistik, so dass man den Umfang und die Details nur schwer den Nicht-Kundigen anschaulich vermitteln könne. Es gehe um Angriffe auf Internetnutzer in Deutschland, Privatpersonen, private Vereinigungen und Unternehmen. Insbesondere gehe es um Botnet-Angriffe, bei denen hunderttausende Rechner allein in Deutschland kompromittiert und sabotiert oder als kriminelles Werkzeug benutzt würden. Eine in der Vorbereitung befindliche Geschädigtenstatistik solle künftig Auskunft darüber geben, wie bzw. wie oft eine Million oder auch zwei Millionen oder noch größere Mengen von Menschen als Opfer von Cybercrime betroffen sind.[5]

Nach Präsident Ziercke wandte sich Staatsekretär Klaus-Dieter **Fritsche** vom Bundesministerium des Innern in Vertretung des durch Koalitionsverhandlungen in Berlin gebundenen Innenministers Hans-Peter Friedrich an das Plenum[6], mit der die Sicht des Bundesministeriums des Inneren erläuternden Eröffnungsansprache zum Thema „Cyberkriminalität – globale Herausforderungen weltweiter Netzwerke." Auch er wies eindringlich auf die vielfältigen Probleme hin, die sich für die polizeiliche Informationsverarbeitung in der gegenüber früher massiv verschobenen Sachlage ergäben. Betrug beim Online-Banking, Identitätsdiebstahl in Datenbanken, DDoS-Attacken auf Firmenwebsites, Cyberspionage, Angriffe auf kritische Infrastrukturen, Cyberterrorismus – das World Wide Web biete Kriminellen unzählige Angriffspunkte. Allein die polizeiliche Kriminalstatistik in Deutschland – und damit nur das Hellfeld der Kriminalität – weise für das

[5] Zur Frage der Sicherheit der digitalen Kommunikation haben BITKOM und das Bundesministerium der Justiz und für Verbraucherschutz zu Anfang 2014 einen gut besuchten „Safer Internet Day" veranstaltet, auf dem auch die Ergebnisse neuer Bevölkerungsumfragen diskutiert wurden; s. Kurzbericht dazu bei BMJV-Pressestelle 2014.

[6] Mehr und Näheres dazu s bei Fritsche 2013.

Jahr 2012 insgesamt 64.000 Fälle von Cybercrime und 230.000 Fälle mit dem Tatmittel Internet aus. Viele Cyber-Straftaten entgingen noch der statistischen Erfassung.[7] Hier müsse die internationale Zusammenarbeit über das BKA hinaus noch stärker forciert werden. Er hoffe sehr, dass das EC3-Center bei Europol ein effektives Ermittlungsinstrument werde.[8] Neben verstärkten und besseren Online-Durchsuchungen sei es wichtig, sich bei der Debatte um die Mindestspeicherfrist von Daten nicht auf die IP-Adressen zu beschränken, vielmehr eine „technikoffene Lösung" anzudenken, die zukünftige Entwicklungen mit einschließen könne.

In der Anmoderation zum Thema der Freiheit und deren daran sozusagen angepassten Gefährdungen hatte ich die moderne Form der Weltwahrnehmung und der Interkommunikation angetippt und anhand von Mobiltelefonen veranschaulicht. Ein altes Mobiltelefon „kann nicht viel, und ich kann nicht viel". Umgekehrt gelte aber dann eben: „es kann *mir* auch nicht viel antun!" Das alte Handy ist so was wie ein kleiner karg möblierter Raum im 3. Stock einer Großstadt, noch vergittert; selbst wenn ein Einbrecher dort durchkommen sollte, würde er nicht viel Wertvolles erbeuten. Ein modernes Smartphone als substantiell vollwertiger Kleincomputer entspricht demgegenüber einer großen Villa mit öfter offenen ebenerdigen Fenstern, manchmal aus Versehen auch noch offenen Türen, und innen beachtlichen Reichtümern und sensiblen Dokumenten. Bei der Nutzung sind die Besitzer sozusagen mit der ganzen Welt verbunden. Nach einem Einbruch besteht die Gefahr, dass – um im Bild zu bleiben – sich die ganze Welt beim Besitzer und ggf. seinem elektronischen Umfeld auf Dauer eingenistet hat.

Prof. Udo **Di Fabio**, Bundesverfassungsrichter a.D., Professor für Öffentliches Recht am Fachbereich Rechtswissenschaft der Universität Bonn, Mitglied der NRW Akademie der Wissenschaften und Künste, war als nächster Redner zu einem **Festvortrag über „Freiheit und Grenzen der digitalen Gesellschaft"** eingeladen worden.[9]

Das Thema Professor Di Fabios umfasste die inhärente Missbrauchsgefahr jeglicher Freiheit, getreu dem Dreierspruch: Alles was missbraucht werden kann, wird missbraucht, alles kann missbraucht werden, also logischer Schluss: Alles wird missbraucht werden. Daher ergibt sich aus der Wahrung der Freiheit selbst die stete Notwendigkeit einer Grenzziehung, die man in moderner juristisch politologischer Sprache die Einhegung von Gefahren nennen könnte, denn es hat seine eigenen nicht nur semantischen Schwierigkeiten, in einem genuin grenzenlosen Raum von einer Grenzsetzung zu sprechen.. Und schließlich geht es um das Ziel einer Balance von Freiheitsgewährung und Schadensvorsorge in einen demokratischen Staat, der doch letzten Endes, wie demokratietheoretisch ja immer betont, für die Bürger und die Sicherheit dieser Bürger da ist.

Dem hier angetippten Problem der Schadensvorsorge näherte sich, aus der Perspektive der mit der Kriminologie sachlich eng verbundenen Crime Science Prof. Pieter **Hartel** von der Universität Twente bei Enschede in den Niederlanden.[10] Er ist dort Professor an der Fakultät für Elektrizitätsingenieurswesen, Mathematik- und Computerwissenschaft sowie Mitglied einer in diese Fakultät eingebundenen sowie auf verschiedene Akteure und Institutionen verteilten Arbeitsgruppe Sicherheitsforschung. Das Thema seines englischsprachigen Vortrages war die **„Situative Prävention von Cybercrime: ein chancenreicher**

---

7 Zum Bundeslagebild Cybercrime 2012 s. Bundeskriminalamt 2013.

8 s. den ersten Jahresbericht des 2013 gegründeten Zentrums unter: European Cybercrime Centre 2014.

9 Mehr und Näheres dazu s. bei Di Fabio 2013.

10 Mehr und Näheres dazu s. bei Hartel 2003.

Bekämpfungsansatz“. Den Fokus in der Denkrichtung bilden die sozio-technischen Aspekte von Cybersicherheit. Prof. Hartel ist außerdem Mitherausgeber der interdisziplinären und internationalen Zeitschrift Crime Science, die den Vorteil hat, eine Opensource-Zeitschrift zu sein. „Crime Science“ könnte man wörtlich mit „Kriminalitätswissenschaft“ übersetzen. Der Redner selbst bevorzugte den Begriff „Kriminalwissenschaft“. Das Hauptziel dieser Wissenschaft bestehe in der Verringerung von Kriminalität durch Verringerung der Gelegenheiten zur Begehung von Straftaten.

Ein Kernthema für die Cybersicherheit sei die situative bzw. situationsbezogene Kriminalprävention. Etwas verkürzt dargestellt geht es dabei, mit den Worten des Moderators, um eine Trias, die dem Praktiker, der Polizei und der Strafverfolgung durchaus als solche geläufig ist, wenngleich nicht immer unter derselben Terminologie, nämlich die Trias von Tatgelegenheit, tatbereiten Individuen, und die Anwesenheit oder eben auch Abwesenheit von fähigen und einsatzbereiten Wächtern. Auch die experimentelle Kriminologie kommt ins Spiel. Sie ist in Deutschland noch unterentwickelt. Ihr Motto kann man in einer populärwissenschaftlichen Pointierung wie folgt formulieren: Gestaltet die Wirklichkeit bzw. einen genau definierten Ausschnitt davon und registriert genau, was an Befunden herauskommt, statt abstrakt nur darüber zu räsonieren, was herauskommen müsste, wenn man mal was täte!

Prof. Hartel wies dann darauf hin, dass an sich sehr gute und umfangreiche Sammlung praktischer Ratschläge für problemorientiertes Vorgehen der Polizei, das Problem Oriented Policing, die durch das POP-Center auf dem Internet bereit gestellt würden, meist für übliche Kriminalitätsformen und nicht für IuK-Kriminalität gälten, also Kriminalität im Zusammenhang mit Informations- und Kommunikationstechnik. Dazu gab es im weiteren Vortrag dann detaillierte Überlegungen.

Weitere wichtige Themengebiete im Kontext der Bedrohungen im Cyberraum sind **Cyberterrorismus, Cyberspionage und Cyberwar.** Aus der Sicht des Moderators lag es bei der Vorstellung des Themas **„Cyberterrorismus, Cyberspionage und Cyberwar – eine aktuelle Bedrohungseinschätzung aus Sicht der Wissenschaft**“ nahe, auf den vom Vortragenden Dr. Sandro Gaycken nicht verlangten Bezug zur naturwissenschaftlichen Kriminalistik hinzuweisen, die an sich bestens im Bundeskriminalamt und auch einigen Landeskriminalämtern aufgehoben ist. Weitere Bezüge wurden gesehen zu Kriminalstrategie, Kriminaltaktik, Kriminalprävention und schließlich zu Kriminologie und Strafprozesslehre, was nicht dasselbe ist wie das Strafprozessrecht.

Herr Dr. **Gaycken** ist Technik- und Sicherheitsforscher an der Freien Universität Berlin, Fachbereich Mathematik und Informatik. Dort arbeitet er im Institut für Computerwissenschaft. Seine speziellen Forschungsinteressen und Forschungstätigkeiten widmen sich dem Datenschutz, der Datensicherheit, dem Cyber Warfare, Cybercrime und Hacking.

Der Referent stieg in seinen Vortrag[11] mit der Bemerkung ein, strategisch bedeutsame Cyberspionage und Cyberwar seien heutzutage keine theoretischen Konstrukte mehr. Dafür brachte er sehr anschauliche, zum Nachdenken anregende und wahrscheinlich etliche Tagungsteilnehmer auch „aufregende“ Belege vor, vor allem mit Bezug zu China und den USA. Andere Länder seien vergleichsweise schwierig zu beobachten, seien aber nach seiner Ansicht kaum zurückhaltender, so Großbritannien und Frankreich. Ein ergänzender Trend sei

[11] Mehr und Näheres dazu s. bei Gaycken 2013.

das epidemische Anwachsen von Cyber-Söldnerfirmen, die im internationalen Markt hochwertige Exploits anböten. Gerade die rapide voranschreitende Evolution der Aktivitäten und Budgets, verbunden mit einer Kommerzialisierung der Offensive, machten eine Kontrolle der immer zahlreicher entstehenden Cyberwaffen immer schwieriger. Die Cybersicherheit sei derzeit nicht gewährleistet, weil es keine tragfähigen Schutzkonzepte gebe. Eine der Optionen für eine bessere Zukunft liege in der Entwicklung von „Hochsicherheits-IT", wozu in Deutschland an sich – näher dargelegte – beste Voraussetzungen gegeben seien.

Im Vortrag Dr. Gayckens waren erstmals auf der Herbsttagung, von der speziellen Themenstellung fast „naturgemäß" induziert, zahlreiche Verbindungen zu einer anderen mächtigen Cyberbedrohung deutlich angetippt worden. Dabei geht es um die Aktivitäten staatlicher Institutionen bzw. „Dienste" zur Ausspähung anderer Staaten. Diese Materie blieb bei der Tagungsgestaltung insgesamt außen vor, in gut nachvollziehbarer Selbstbeschränkung schon deshalb, weil sie bereits nach den jetzt ans Licht der Öffentlichkeit kommenden Dimensionen eine eigene mehrtägige Konferenz, wenn nicht sogar mehrere Tagungen in Anspruch nehmen würde. Soweit in der bisherigen Diskussion oder auch Debatte von „befreundeten Staaten" oder ähnlichem die Rede ist, wird man bezweifeln dürfen, dass dies jemals mehr als eine auf moralischer oder emotionaler Ebene angesiedelte und insoweit durchaus ehrenwerte Motivation zu einer vertrauensvollen Kooperation war. Es erscheint heilsam, gerade was die Zukunft angeht, sich einen Satz in Erinnerung zu rufen, der aus Zeiten einer offener von ggf. „nackter" Staatsräson geleiteten Politik stammt, und verschiedenen Personen zugeschrieben wird. Im Netz finden sich bei Recherchen insoweit besonders häufige Nennungen des ehemaligen französischen Staatspräsidenten Charles de Gaulle und des ehemaligen britischen Premierministers William Ewart Gladstone. Wie dem auch genau sei: der Satz lautet, mit geringen Variationen der Überlieferung: „Staaten haben keine Freunde, nur Interessen!"

Wenn vielleicht nicht erst geweckt, aber doch durch den Vortrag Dr. Gayckens erheblich gefördert, war aus der Sicht des Moderators und dem Auffangen der „Stimmung" im Saal das besondere Interesse der Zuhörerschaft am englischsprachigen Vortrag von Special Assistant Michael **Daniel** aus Washington, D.C., Vereinigte Staaten von Amerika. Mr. Daniel ist Berater und Sonderbeauftragter des Präsidenten der USA. Seine zentralen Aufgaben sind dreifach. Zum einen die Leitung der Nationalen Strategie der Cybersicherheit. Zum anderen die Überwachung der Implementation dieser Strategie (vorwiegend) in den Bundesbehörden der USA. Und schließlich die Arbeit an dem großen Plan, Behörden der Einzelstaaten und der großen Cities in eine zielführende Partnerschaft einzubinden, ergänzt durch enge Verbindungen zu Wirtschaftsunternehmen und privaten Institutionen bzw. Vereinigungen (sogenannten NGOs oder Non-Government Organisations).[12]

Der Referent bezeichnete es als sein Anliegen, mit dem Vortragsthema „Cybersecurity – strategisch-politische Aspekte dieser globalen Herausforderung" einen Überblick über einige („some") Denkansätze der amerikanischen Bundesregierung zur Cybersecurity zu vermitteln. Dies umfasse die amerikanischen Prioritäten, die Bereiche von potentiellen Herausforderungen und Gelegenheiten, sowie schließlich die Frage, wie die USA und Deutschland künftig zusammenarbeiten könnten, um die *kollektive Sicherheit* im Cyberspace zu verbessern. Es gebe eine „neue Normalität" in der Cyberbedrohung für Politik und Wirtschaft gleichermaßen; diese steige an und diversifiziere sich zunehmend, und die

[12] Aus Moderatorsicht wurde, pleonastisch formuliert, die „reale Verwirklichung" gerade dies als besonders schweißtreibende und Kopfweh erzeugende Mammutaufgabe bezeichnet, die nach organisationssoziologisch und verwaltungswissenschaftlich vielfach belegten Erkenntnissen auch weitere amerikanische Regierungen noch hinreichend behelligen werde.

Angriffe würden zunehmend mehr „sophisticated“ sowie technisch hochgefährlich bis destruktiv. Im Weiteren zweifelte der Referent an, dass die übliche Redeweise vom grenzenlosen Cyberspace ganz zutreffend sei. Es gebe überall Grenzen und Einschränkungen; als Beispiel dienten die Firewalls bzw. Connection Points. „Guiding Principles“ für künftiges kollektives Handeln seien die folgenden: „Compromises are inevitable: plan for them“; „information must be shared, frequently and rapidly“;„teamwork is a requirement“; „networked defense first“ und „protect privacy an civil liberties“. Internationale Kooperation sei wichtig, es müsse ein „Internet Governance“ entwickelt werden, die internationale „Law Enforcement Cooperation“ müsse vertieft werden, und es geht um vermehrte Investitionen im Sinne eines „Capacity Building“.[13]

Die tatsächliche Angreifbarkeit öffentlicher Netze wurde den Tagungsteilnehmern im Anschluss von Herrn Carsten **Schulz** und Herrn Markus **Blasl** demonstriert. Beide Referenten sind Mitarbeiter des Bundesamts für Sicherheit in der Informationstechnik. Ihr Anliegen war es, den Tagungsteilnehmern in einer dynamisch interaktiven Live-Präsentation an zwei PCs professionell zu demonstrieren und dabei doch weitestmöglich anschaulich für sozusagen Normalnutzer des Internets und der auf dieses zugreifenden Gerätschaften die aktuelle Gefährdungslage „begreifbar“ zu machen.[14] Im Kern ging es darum, einen unmittelbaren Eindruck darüber zu verschaffen, welchen Stand die Sicherheitsrisiken gegenwärtig schon erreicht haben, die enorme Schäden verursachen und unter anderem die Innere Sicherheit beeinträchtigen.

Als Demonstrationsobjekt diente die Homepage der eigenen Behörde. In laienhaften Worten umschrieben, „kaperten“ die IT-Spezialisten die Startseite und weitere Seiten dergestalt, dass ein elektronischer Besucher des Bundesamts für Sicherheit in der Informationstechnik auch bei Kenntnissen von der Materie nicht hätte merken können, einem virtuellen Fake aufzusitzen. Die „Angreifer“ hatten/hätten dann sozusagen freie Bahn, die Daten des Besuchers auf ihre Installationen umzuleiten und mit dem Besucher-PC je nach dort installierter Sicherheitshardware oder -Software ein Maximum an Eigeninteressen/Schädigungspotential zu verwirklichen. Die Komplexität von IT-Angriffen wurde im Plenum auch dadurch deutlich, dass selbst IT-Spezialisten vor Aussetzern und Systemabstürzen nicht gefeit sind. Die Referenten jedoch blieben jedenfalls nach außen hin ganz „cool“ und bemerkten, man bekomme eben hier keinen vorbereiteten Film bzw. ein nachträglich bereinigtes Video demonstriert, sondern ein Exempel genau dazu, was ad hoc mit welchen Zwischenfällen auch immer am Ende erfolgreich innerhalb weniger Minuten „angerichtet“ werden könne.

Auf der Basis dieser Präsentation und den Eindrücken aus den vorherigen Vorträgen drängte es sich für den Moderator auf, folgende Einschätzungen zu den „Charakteristika der Täterseite“ im realen virtuellen Raum zu versuchen[15]:

- Grenzenlosigkeit des Agierens im virtuellen Raum, verbunden mit transnationalen Geschäften im realen Raum der Nationen, Wirtschaftssysteme und Gesellschaften der Welt.
- Transnationale Kommunikation und Entscheidung in Echtzeit.
- A-Moralität und funktionale „Gesetzlosigkeit“ im Denken und im Arbeitsansatz.

[13] Mehr und Näheres dazu s. bei Daniel 2013.
[14] Mehr und Näheres s. bei Schulz/Blasl 2013.
[15] Zu angloamerikanischen, bereits vertieften, Einsichten und Befunden s. Kirwan & Power 2013.

- Verfügung über “großes Geld“ zum „Einkauf“ von legaler Beratung, die man eben auch hin und wieder bei grundlegend illegalen Geschäften benötigt.
- Skrupellosigkeit im Einsatz auch paralegaler und illegaler bis im besonderen Fall hoch-krimineller Methoden und Instrumente.
- Endemische Anstrengungen zur Korrumpierung von Amtsträgern und Entscheidungsträgern auf allen relevanten Ebenen, ergänzt im Weiteren nach etablierter Beziehung eher durch subtile Drohungen denn durch offene Erpressung oder gar Gewaltanwendung.
- Im Falle von aus Tätersicht unvermeidlicher Gewalttätigkeit bevorzugt der Einsatz von Formen von Gewaltmaßnahmen, die zugleich perfekt instrumentell und eine symbolische Botschaft für Dritte vermittelnd ausgestaltet sind.

Ein weiterer Aspekt des Themas Cybercrime sind Bedrohungen der Wirtschaftsunternehmen und die weitreichenden Folgen. Der Referent, Herr Geschonneck, ist Partner des weltweit tätigen Wirtschaftsprüfungs- und Beratungsunternehmens KPMG AG mit rund 8.600 Mitarbeitern an 25 Standorten. Zugleich ist er dort als Leiter des Firmenbereichs Forensic Technology tätig, mit Schwerpunkt auf digitalen Beweismitteln bei Korruptions- und Betrugsbekämpfung und E-Crime; letzteres ein Begriff zur Kennzeichnung einer ergänzenden Perspektive für den Firmenfokus auf Fraud Prävention und Forensic Investigations bei der Prävention gegen Wirtschaftskriminalität in Unternehmen.

Digitale Bedrohungen beschreibt der Referent als Oberbegriff für eine Vielzahl von Handlungsweisen gegen Unternehmen, Behörde und Privatpersonen. Dazu gehörten das Ausspähen von Daten im Wege der Cyberspionage, die Computersabotage und die Verletzung von Urheberrechten. Ein darauf bezogenes IKT-System könne je nachdem Werkzeug, Ziel oder beides sein. Bei digitalen Bedrohungen als Form von Wirtschaftskriminalität spreche man von e-Crime. Einen Blick auf diese Landschaft aus kaufmännischer Perspektive vermittle die aktuelle Studie von KPMG über Schäden in der deutschen Wirtschaft. Danach war ein Viertel der befragten 500 deutschen Unternehmen in den vergangenen zwei Jahren von e-Crime betroffen, wobei die Bedrohungen zunehmend länderspezifisch gesehen werden.[16]

Im weiteren Verlauf des Vortrages ging der Referent darauf ein, dass außer Bedrohungen von außen zunehmend auf Bedrohungen von innen geachtet werden müsse, da die überführten Täter oft im unmittelbaren Umfeld der Unternehmen zu finden seien. Eine der größten Schwachstellen in Unternehmen sei die Unachtsamkeit von Mitarbeitern, was die Notwendigkeit von steten Schulungen und Sensibilisierungsmaßnahmen deutlich mache. Die Evolution von Bedrohungen durch Professionalisierung der Angriffe beschleunige sich. Ein bedeutsames Beispiel für das Anbieten von sozusagen betriebsfertigen Lösungen als „Cracking-as-a-Service“ stelle das Malware-Toolkit „Blackhole“ dar, auf das auch schon der Referent Gaycken hingewiesen hatte. Den gezielten und näher beleuchteten Angriffen auf Unternehmen und Datenbestände, die sich durch die Nutzung neuer Technologien stetig verschärften, gelte es, adäquate Präventionsstrategien und –maßnahmen entgegenzusetzen. Diese stellten für gut ausgerüstete und unablässig wachsame Firmen inzwischen schon, und künftig noch stärker, einen Wettbewerbsvorteil dar.[17]

[16] Zu einer aktualisierten Auflage der Studie s. KPMG 2014.
[17] Mehr und Näheres dazu s. bei Geschonneck 2013.

Fortgesetzt wurde die Betrachtung aus Sicht der Wirtschaft mit einem Vortrag von Dr. Thomas **Kremer** über „Digitale Bedrohungen und Gegenmaßnahmen aus Sicht der Wirtschaft“. Herr Dr. Kremer ist Vorstand der Deutschen Telekom AG und dort zuständig für die Bereiche Datenschutz, Recht und Compliance. Seine letzten vorherigen Tätigkeiten ab 2003 waren die Leitung des Corporate Center Legal & Compliance bei Thyssen Krupp, zusätzlich ab 2007 die Ernennung zum Chief Compliance Officer des Thyssen Krupp-Konzerns, und 2011 die Ernennung zum Generalbevollmächtigten. Also verfügt er auch über viel Erfahrung in einem großen Industriebetrieb. Seit Oktober dieses Jahres ist er zudem Mitglied der Regierungskommission Deutscher Corporate Governance Index.[18].

Herr Dr. Kremer betonte, dass die Bedeutung von Cybersecurity nach wie vor unterschätzt werde. Auch fehle es an der notwendigen Transparenz bezüglich des Umfangs der Angriffe auf deutsche Unternehmen, wobei alle Branchen betroffen seien. Die heutigen Cyberangriffe seien vielfach zwischen verschiedenen Angreifern gut koordiniert und nutzten die oft einfachen Schwachstellen von Unternehmen nachhaltig aus. Im Rahmen der Aufgabe, sich diesen Herausforderungen buchstäblich Tag für Tag zu stellen, müssten die Firmen in zukünftige Sicherheitskonzepte stärker selbstlernende Schutzsysteme einbeziehen und moderne Prävention in Echtzeit betreiben.[19] Wie so etwas verwirklicht werden kann, war Gegenstand des weiteren Vortrags. Dabei stellte der Referent unter anderem das von der Deutschen Telekom (mit) entwickelte und in den Informationsteilen öffentlich zugängliche System „Sicherheitstacho“ vor.[20]

Sich der Bekämpfung von Cybercrime und Cybersicherheit widmend, erörterten Vertreter zweier wichtiger staatlicher Institutionen in einem Podiumsgespräch das Thema „Cybersicherheit und Abwehr von Cybercrime – aktuelle Initiativen und strategische Ansätze“.
Andreas **Könen** ist seit 1. Februar 2013 Vizepräsident des Bundesamts für Sicherheit in der Informationstechnik. Beim BSI ist er schon seit 2006, vorher war er seit 1998 in verschiedenen Bereichen der Bundesverwaltung auf dem Gebiet der Informationssicherheit tätig.
Peter **Henzler** ist Vizepräsident beim Bundeskriminalamt. Er war schon vorher, seit 1990, im BKA in verschiedenen Funktionen, in operativen Arbeitsbereichen sowie auch im Leitungsstab eingesetzt. Ab 2007 hatte er die Abteilung „Zentrale Dienste“ übernommen, ab 2010 leitete er die Abteilung „Schwere und Organisierte Kriminalität“. Sein breites Erfahrungsspektrum ergänzt das von Herrn Könen bestens.

Ihrer beider gemeinsames Thema ist für das BKA besonders bedeutsam, aber auch für die Landeskriminalämter und andere Dienste, insgesamt für die Gewährleistung und stete Stärkung der nationalen Sicherheit gegenüber der IT-Kriminalität. Die Referenten spielten sich im Verlauf des Geschehens sozusagen abwechselnd die Bälle zu, indem sie die im BKA und im BSI gegebenen Strukturen, darauf aufbauend aktuelle Initiativen zur Effizienzsteigerung und Effektivierung der Gefahrenabwehr, und schließlich mögliche

[18] Die Telekom war u.a. Auftraggeber mehrerer von IfD Allensbach durchgeführter Befragungen, die in „Sicherheitsreports“ zusammengefasst und veröffentlicht wurden. Siehe dazu Deutsche Telekom /T-Systems 2011 und 2013.

[19] Mehr und Näheres dazu bei Kremer 2013. Zu Forderungen aus der Wirtschaft s. a. Diekmann 2013.

[20] Zur Verlinkung auf die Website siehe Deutsche Telekom 2014. Zur Frage der Internationalität von Cybercrime s. noch, aus Sicht des Bundeskriminalamts, Stock 2012. Die Involvierung der Organisierten Kriminalität betont Schönbohm 2013. Die breitere Perspektive der „digitalen Schattenwirtschaft“ wird von Brodowski &Freiling 2011 erörtert. Cybercrime sozusagen auf dem Lande beschreibt praxisorientiert Burandt 2013.

Veränderungen bei mittel- bis langfristigen Bekämpfungsstrategien diskutierten.[21] Für die Teilnehmer entstand daraus eine vertiefende Ergänzung von Befunden und Einsichten aus den vorherigen Vorträgen von Jörg Ziercke, Klaus-Dieter Fritsche, Carsten Schulz und Markus Blasl.

Auch **„Rechtliche Herausforderungen bei der Bekämpfung von Cybercrime**" umschreiben eine große „Gesamt-Herausforderung" für Rechtspraxis, Rechtswissenschaft, Justiz und Polizei.

Herr Dr. Wolfgang **Bär** ist Ministerialrat im Bayerischen Staatsministerium der Justiz und für Verbraucherschutz und erläuterte dieses immanent wichtige Themenfeld für die Strafverfolgung bei der Durch- und Umsetzung von Cybersicherheit. Dr. Bär ist Leiter des Referats zur Bekämpfung von Internetkriminalität und des Missbrauchs neuer Technologien. In seiner letzten vorherigen Praxisposition vorher war er als Richter am Oberlandesgericht Bamberg tätig gewesen.

Man könnte auch von einer Querschnittsmaterie sprechen, sofern und soweit es um die Herausarbeitung übergreifender Topoi und Lösungsversuche geht. Als Praktiker wie als Theoretiker sieht man sich, vom Anforderungsprofil her beschrieben, von einer „irgendwie bunten" Mischung aus materiellem Strafrecht und Strafverfahrensrecht[22], Europarecht[23], internationalem Recht und weiteren Rechtsmaterien konfrontiert.

Der Referent legte den Schwerpunkt seines Vortrages auf das Strafrecht und das Strafverfahrensrecht. Von dem näher umschriebenen Befund ausgehend, dass das Internet immer weitere Lebensbereiche erfasse und mit bestimme, stellte er dem die These entgegen, dass das „Recht der analogen Welt" im Cyberspace nicht außer Kraft gesetzt werde. Allerdings bestehe die fortlaufend große Herausforderung darin, dieses Recht an die Bedingungen einer digitalen Welt anzupassen und vor allem seine tatsächliche Durchsetzbarkeit zu gewährleisten. Im weiteren Vortrag griff der Referent die wichtigsten einschlägigen strafrechtlichen Problemstellungen auf**.**[24] Die leitende Fragestellung dabei war, ob zum einen wirklich alle neuen Begehungsformen von Cybercrime durch das geltende materielle Strafrecht erfasst werden, und ob zum anderen die Strafverfolgungsbehörden mit ausreichenden Mitteln ausgestattet sind, um Straftaten mit den neuen Technologien aufdecken und angemessen verfolgen zu können. Phishing, Pharming, Skimming, Ransomware und Bot-Netze stellten nur Beispiele für eine Vielfalt dar, welche namentlich klassisches Strafrechtsdenken mit noch vor wenigen Jahren ungeahnten Hürden konfrontiere.

Der Referent beleuchtete detailliert die jüngere rechtspolitische und gesetzgeberische Entwicklung ab dem 41. Strafrechtsänderungsgesetz vom August 2007 und insbesondere den akuten breit gestreuten Handlungsbedarf im Gefolge der EU-Richtlinie vom Juli 2013 zum Bereich des Angriffs auf Informationssysteme. Die Gesetzgebung zur Umsetzung der Vorgaben der Entscheidung des Bundesverfassungsgerichts über Vorratsdatenspeicherung war ein weiterer Schwerpunkt. Und schließlich ging es um die notwendigen Änderungen der

---

21 Mehr und Näheres s. bei Könen & Henzler 2013.

22 Siehe dazu weiter vertiefend beispielsweise Englert & Hermstrüwer 2013; Plewka 2013; Sieber 2012; zu Sexualstraftaten s. Albrecht 2011; zum Bullying s. jüngst Kowalski u. a. 2014; vgl. auch aus rechtspsychologischer Sicht Gasch 2013.

23 Zu jüngeren EU-Initiativen und Rechtsakten s. etwa Buono 2013; Naziris 2013.

24 Mehr und Näheres dazu s. bei Bär 2013.

gesetzlichen Eingriffsbefugnisse zur Sicherstellung von Informationen, deren Grundkonzept der Territorialität durch das Aufkommen von Cloud Computing in Teilen überholt sei.

BKA-Präsident Ziercke leistete mit seinem Vortrag über „Kriminalistik 2.0 – effektive Strafverfolgung im Zeitalter des Internet aus der Sicht des BKA“ quasi einen fachlich vertiefenden „Nachstoß“ zu den in der Begrüßungsrede angerissenen allgemeinen Perspektiven moderner Polizeiarbeit und Kriminalistik im Feld von Cybercrime.[25] Bei „Kriminalistik 2.0“ handele es sich (noch) nicht um eine fertig konzipierte und für die Praxis sogleich voll umsetzbare „neue Kriminalistik“. Derzeit gehe es vielmehr darum, mit Blick auf eine solche mögliche neue Gesamtlösung die Phänomene und die daraus entstehenden Herausforderungen zu verdeutlichen und erste Schritte zu skizzieren, wovon effektive Strafverfolgung in der digitalen Welt abhängig ist.

Als wesentliche Merkmale des näher dargelegten grenzenlosen Wachstums- und damit Schadenspotentials stellte der Referent heraus

- Cyberstraftaten seien profitabel und verlangten wenig eigene Infrastruktur.
- Das Internet biete Hacking-Tools, die sofort appliziert werden könnten.
- Das Netz sei anonym. Dies ermögliche eine Trennung von realer und digitaler Identität.
- Das Netz ermögliche die Vernetzung krimineller Gruppen über Ländergrenzen hinweg.
- Das Entdeckungsrisiko für die Täter sei im Vergleich zur analogen Welt gering.

Die weite Verbreitung von informationstechnischen Systemen und die zunehmende Nutzung IT-gestützter Infrastrukturen steigerten die Abhängigkeiten von IT-Systemen und erhöhten die Verwundbarkeit von Staaten, Unternehmen und tendenziell auch jedes Einzelnen. Hochgradig vernetzte und sensible Systeme würden gestört und manipuliert. Straftaten würden online vorbereitet und offline umgesetzt. Man könne insoweit von einer neuen Art von „Hybridverbrechen“ reden. Auf dieser Basis widmete sich der Referent sodann ausführlich, und unter Heranziehung aktueller quantitativer und qualitativer Befunde aus der Ermittlungs-, Aufklärungs- und Verfolgungspraxis, der Phänomenologie des gegenwärtigen Cybercrime und den daraus folgenden Notwendigkeiten für angepasste kriminalistische und weitere „Antworten“ auf die Herausforderung.[26]

Der Titel der Podiumsdiskussion **„Freiheit im Netz und Cybersicherheit – ein unlösbarer Widerspruch?“** lässt den Betrachter in erster Annäherung an das Thema an die technische Sicherheit denken, bzw. an „Safety“ in der englischen Bedeutung. Bei weiterer Überlegung drängt sich jedoch die Alternative als bedeutsamer auf, nämlich über „Security“ zu sprechen, einen Begriff mit Bedeutungsähnlichkeit zu Safety, aber einer stärkeren Fokussierung auf die menschliche Komponente. Als Moderator nachdenkend, kann man das Thema insoweit verorten als: „Freiheit im Netz zwischen Wissenserwerb und Selbstverwirklichung“ einerseits, als „Missbrauch und kriminelle Schädigung andererseits“, nämlich Schädigung von Individuen, gesellschaftlichen Gruppen, der Wirtschaft, des Staats und der gesamten über das Rechtliche und Polizeiliche hinausreichenden positiven Inneren Sicherheit.

Dazu fügt sich ein Menschenbild, das auf eine skeptische, bioantropologische sowie subkultur- und sozialanthropologische Grundlage unserer Conditio humana aufgebaut ist. Der

[25] Zu den Herausforderungen und dem Stand ihrer Bewältigung für Kriminologie und Strafrecht siehe beispielsweise Holt & Bossler 2014; Meier 2012; Sieber 2012; Stol 2013 und Wall & Williams 2013.

[26] Mehr und Näheres dazu s. bei Ziercke 2013b.

Grund-Satz dieser Orientierung lautet: als Gattung sind „wir Menschen“ alle im Guten wie im Bösen zu allem fähig. Was den Aspekt der „Freiheit ohne Bindung“ betrifft, kann man an die Ausführungen im Festvortrag von Prof. Di Fabio anknüpfen, der das mit öffentlich-rechtlicher verfassungsrechtlicher Dignität und philosophischer Begründung vorgetragen hat. Hier kurz und pointiert gewendet: Freiheit ohne Bindung enthält *stets* einen potentiell autodynamischen Treibsatz von Beliebigkeit, von Entbindung der bösen Seite bzw., ins Extrem getrieben, von Schädigungs- und Vernichtungslust. Eine kleine Ausprägung davon ist das Cybermobbing, nicht nur, aber auch unter jungen Leuten.

Dazu kommt eine lange Erfahrung in der Geschichte der Menschheit mit Prognosecharakter für die Zukunft. Sie beruht auf dem schon einmal am ersten Tag erwähnten Dreisatz dahingehend: Erstens: alles, was missbraucht werden kann, wird missbraucht werden. Zweitens: alles kann missbraucht werden. Ergo drittens: alles wird missbraucht werden, morgen, übermorgen, in 4 Wochen, in einem Jahr, irgendwann. Irgendeiner wird es missbrauchen. Auch mit Lust am Missbrauch nach dem Motto „wenn ich schon untergehen muss, wird die Welt mit mir untergehen“. Neben vielen anderen meist eher harmlosen Zeitgenossen gibt es aggressionsgeladene Spinner und tatbereite Terroristen zuhauf. Dieser Dreisatz bildet nicht notwendigerweise eine Pflichtgrundlage für konkret integrierte oder integrale Ansätze für Risikoabschätzung in Industrie und Wirtschaft, oder etwas anders ausgedrückt, Technikfolgenabschätzung, womit sich erst seit einigen Jahren auch das Bundeskriminalamt im Verein mit Wirtschaften, wirtschaftlichen Unternehmungen sehr intensiv beschäftigt, was auch zum Teil zu sehr schönen Erfolgen geführt hat.

Was man stets bei allen Freiheitsräumen berücksichtigen muss, auch wenn man nicht wie ich an die Potentialität und Realität des Bösen glaubt, ist a) die Hinfälligkeit unserer Psyche oder anders gesagt b) die Anfälligkeit für Versuchungen dahingehend, den eigenen Vorteil zu nutzen und sich am Andern zu rächen oder einfacher ihn/sie mindestens zu täuschen und ggf. zu übervorteilen. Hatte nicht auch unter den anwesenden Teilnehmern der Tagung gelegentlich der eine oder die andere schon mal so „Gelüste“ im persönlichen Umgang, bei Gegnern und anderen? Das Entscheidende ist, das die Mehrzahl der sozial integrierten Menschen es in den meisten Anmutungs- bis Versuchungssituationen schafft, dem Drang nicht nachzugeben. Aber es gibt eben genug Menschen, die schon deswegen leicht oder gerne nachgeben, wenn und weil sie sich dran gewöhnt haben.

Pointiert zusammengefasst in dem etwas ironischen Spruch, der nach meiner Quellenlage von Kurt Schneider stammt, u. a. auch Psychiater: „Die Menschheit ist gut, wenn bloß die Leute nicht wären!“.

Bei der Kontrolle und Prävention des Missbrauchs des Cyberraums ist die Frage, was die „Akteure und Kontrolleure“ aufseiten der Gefahrenabwehr und der Strafverfolgung charakterisieren sollte bzw. wogegen stetig angekämpft werden muss. Fünf Aspekte verdienen meines Erachtens, hervorgehoben zu werden:

- Erstens: notwendig ist die Bindung an Recht und Gesetz im Inland, materiell und verfahrensmäßig.

- Zweitens: notwendig ist die Beachtung europarechtlicher und völkerrechtlicher Normen und Verträge, grenzüberschreitend.

- Drittens: notwendig ist die Beachtung von Eingriffsschwellen und ggf. des Grundsatzes der Verhältnismäßigkeit.

- Viertens: nicht notwendig sind aber, in ein Wortspiel gepackt, wiederholt noterzeugend, um nicht zu sagen Notstände hervorrufend: personelle und materielle Kapazitätsprobleme.,

- Und schließlich fünftens: das Uraltproblem von staatlicher Bürokratie aber auch von Großunternehmen oder Großvereinigungen: die Formalien und Realien der Kooperation, einschließlich der Hindernisse, die „Fallen" durch Routinen des Denkens, Routinen des Handelns, schließlich Eigenwilligkeit und Eigentümlichkeit der involvierten Personen gemäß dem leicht ironischen Spruch: „auch Beamte sind Menschen".

Wir brauchen mittelfristig eine Rechtsreform. Darauf ist Herr Di Fabio, auch mit Blick auf das Bundesverfassungsgericht und einen möglichen Spruch des Europäischen Gerichtshofs eingegangen: die Schaffung eines gerade auch für die Strafverfolgung hilfreichen und zugleich begrenzenden, aber offiziell separaten Vorermittlungsverfahrens vor dem eigentlichen Ermittlungsverfahren. Darüber haben wir nicht diskutiert, das wäre eine eigene Diskussion wert. Dieses Vorermittlungsverfahren als separater Teil des staatlichen Zugriffs ist nicht geleitet von dem durch Kritiker beschworenen Generalverdacht gegen die Gesamtbevölkerung. Vielmehr ist es geleitet durch ein belegbares Wissen über dunkle Strukturen, ich will das so einmal formulieren, aus der Organisierten Kriminalität heraus, wo ich mich ein klein bisschen auskenne, geleitet durch belegbares Wissen über dunkle Strukturen, die man im Detail noch nicht kennt, die man aber durch gezielte, von diesem Annäherungswissen geleitete, Verdachtsschöpfungsverfahren aufgehellt, schlussendlich sanktioniert bekommen kann. Zur Ausgestaltung solcher Verdachtsschöpfungsverfahren gehört, dass strenge und streng kontrollierte Regeln des Löschens von vorläufigen und dann nicht zielführenden Befunden, im Sinne eins verbindlichen staatlichen „Tilgens von Notizen und sonstigen Handlungsspuren", mithin eines auch sozial wirksamen „Vergessens von potentiell Nachteiligem".

Verzeichnis der Referenten bzw. Tagungsbeiträge sowie ausgewählter das Thema ergänzender Literaturstellen

Die Literaturdokumentation des Bundeskriminalamtes hat zur Tagung einen aktuellen Band (Nr. 35) der COD-Literatur-Reihe erstellt: „Cybercrime- Bedrohung, Intervention, Abwehr – Eine Literaturauswahl", mit einem Begleitwort von Franziska Wallraff-Unzicker. Der Band kann von der Homepage des BKA als PDF-Datei heruntergeladen werden.

Albrecht, Hans-Jörg: Grooming, das Internet und die Schließung von Sicherheits- und Strafbarkeitslücken. In: Monatsschrift für Kriminologie und Strafrechtsreform 94, 2011, Heft 2, Editorial.

Bär, Wolfgang: Rechtliche Herausforderungen bei der Bekämpfung von Cybercrime. Vortrag (des Ministerialrats im Bayerischen Staatsministerium für Justiz und Verbraucherschutz) zur Herbsttagung des Bundeskriminalamts am 12. November 2013, über das Generalthema „Cybercrime – Bedrohung, Intervention, Abwehr. [Zur redigierten Druckfassung s. den Beitrag in diesem Sammelband].

Bertel, Ralph: Cybercrime – Bedrohung, Intervention, Abwehr. Mit einem Bericht zur BKA-Herbsttagung 2013. In: Die Polizei 105, 2014, S. 29-40.

BMJV-Pressestelle: „Mailen, Surfen, Chatten – wie ist die Privatsphäre zu retten?“ Pressemitteilung vom 11.2.2014, auf der Homepage im Archiv weiterhin aufrufbar.

Brodowski, Dominik & Freiling, Felix: Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft. Berlin 2011 (auch als elektronische Ressource erhältlich).

Bundeskriminalamt (Hrsg.): Cybercrime Bundeslagebild 2012. Wiesbaden 2013.

Buono, Laviero: The Key Features of the EU Cybercrime Directive 2013: The Newly Adopted European Framework for Legislative Measures on Attacks Against Information Systems. In: Computer Law Review International 14, 2013, 4, Pp. 103-107.

Burandt, Klaus: Cybercrime – nicht nur in der Großstadt. Erfahrungen am Beispiel einer Ermittlungskommission. In: Kriminalistik 67, 2013, S. 523-525.

Crime Science. A Springer Open Journal. Edited by Marianne Junger, Gloria Laycock, Pieter Hartel, and Jerry Ratcliffe. First Volume 2012. Homepage: http://www.crimesciencejournal.com/

Daniel, Michael: Cybersecurity – strategisch-politische Aspekte dieser globalen Herausforderung. englischsprachiger Vortrag (des Special Assistant to the President of the United States, and Coordinator for Cybersecurity in the White House) zur Herbsttagung des Bundeskriminalamts am 13. November 2013, über das Generalthema „Cybercrime – Bedrohung, Intervention, Abwehr. [übersetzte Druckfassung in diesem Sammelband].

Deutsche Telekom: Sicherheitstacho. Weltweit aktives Frühwarnsystem der Deutschen Telekom über Cyberangriffe im Internet. Bonn. Zuletzt abgerufen am 15.2.2014, Hauptinformationsseite mit Überblick über die aktuellen Angriffe und sonstigen Informations-Kapiteln: http://www.sicherheitstacho.eu/?lang=de

Deutsche Telekom/T-Systems (Hrsg.): Sicherheitsreport 2011. Eine repräsentative Studie zur Sicherheit in Deutschland. Durchgeführt vom Institut für Demoskopie Allensbach. Allensbach am Bodensee 2011.

Deutsche Telekom / T-Systems (Hrsg.): Sicherheitsreport 2013. Eine repräsentative Studie zur Sicherheit in Deutschland. Durchgeführt vom Institut für Demoskopie Allensbach. Allensbach am Bodensee 2013.

Deutsches Institut für Sicherheit und Vertrauen im Internet (Hrsg.): DIVSI-Studie zu Freiheit versus Regulierung im Internet. Eine repräsentative Bevölkerungsbefragung des Instituts für Demoskopie Allensbach (IfD): Hamburg. Dezember 2013

Diekmann, Florian: Deutsche Industrie fordert Ächtung von Wirtschaftsspionage. Ausspähaffäre. Beitrag zu Spiegel-Online vom 26. Oktober 2013.

Di Fabio, Udo: Freiheit und Grenzen der digitalen Gesellschaft. Festvortrag (des ehemaligen Richters am BVerfG und jetzigen Professors für öffentliches Recht) zur Herbsttagung des Bundeskriminalamts am 12. November 2013, über das Generalthema „Cybercrime – Bedrohung, Intervention, Abwehr. [Druckfassung in diesem Sammelband].

Englert, Markus/Hermstrüwer, Yoan: Die Datenkrake als Nutztier der Strafverfolgung. Zum strafprozessualen Zugriff auf Facebook-Profile. In: Rechtswissenschaft 4, 2013, S. 326-359.

European Commission, DG Home Affairs an DG Communication (Eds.). Cyber Security Report. Special Eurobarometer 404. Brussels, November 2013.

European Cybercrime Centre: First Year Report. Den Haag 2014. PDF unter https://www.europol.europa.**eu**/ec3

Fritsche, Klaus-Dieter: Cyberkriminalität – globale Herausforderungen weltweiter Netzwerke. Eröffnungsansprache (des Staatsekretärs im Bundesministerium des Innern) zur Herbsttagung des Bundeskriminalamts am 12. November 2013, über das Generalthema „Cybercrime – Bedrohung, Intervention, Abwehr. [Druckfassung in diesem Sammelband].

Gasch, Ursula C.: Meta- und Cybercrime: Quo Vadis? Grundlegende kriminalpsychologische Gedanken im Zusammenhang mit (potenziell) strafrechtlich relevantem Verhalten in virtuellen Welten. In: Kriminalistik gestern – heute – morgen. Stuttgart 2013, S. 145-161.

Gaycken, Sandro: Cyberterrorismus, Cyberspionage und Cyberwar – eine aktuelle Bedrohungseinschätzung aus Sicht der Wissenschaft. Vortrag (des Technik- und Sicherheitsforschers an der FU Berlin) zur Herbsttagung des Bundeskriminalamts am 12. November 2013, über das Generalthema „Cybercrime – Bedrohung, Intervention, Abwehr. [Druckfassung in diesem Sammelband].

Geschonneck, Alexander: Digitale Bedrohungen. Vortrag (des Partners von KPMG AG und Leiters des dortigen Bereichs Forensic Technology) zur Herbsttagung des Bundeskriminalamts am 12. November 2013, über das Generalthema „Cybercrime – Bedrohung, Intervention, Abwehr. [Zur redigierten Druckfassung s. den Beitrag in diesem Sammelband].

Hartel, Pieter: Situative Prävention von Cybercrime: ein chancenreicher Bekämpfungsansatz. Englischsprachiger Vortrag (des Mitherausgebers der Zeitschrift Crime Science und Professor an der Universität Twente, NL) zur Herbsttagung des Bundeskriminalamts am 13. November 2013, über das Generalthema „Cybercrime – Bedrohung, Intervention, Abwehr. [Druckfassung in diesem Sammelband].

Holt, Thomas J. / Bossler, Adam M.: An Assessment of the Current State of Cybercrime Scholarship. In: Deviant Behavior 35, 2014, Pp. 20-40.

Kirwan, Grainne / Power, Andrew: Cybercrime. The Psychology of Online Offenders. Cambridge et al. 2013.

Kock, Sonja: Cybercrime – Bedrohung, Intervention, Abwehr. Ein Bericht über die Herbsttagung des Bundeskriminalamts. Kriminalistik 68, 2014, S. 3-9.

Könen, Andreas & Henzler, Peter: Cybersicherheit und Abwehr von Cybercrime – aktuelle Initiativen und strategische Ansätze. Podiumsgespräch (zwischen dem Vizepräsidenten des Bundesamtes für Sicherheit in der Informationstechnik und dem Vizepräsidenten beim Bundeskriminalamt) zur Herbsttagung des Bundeskriminalamts am 13. November 2013, über das Generalthema „Cybercrime – Bedrohung, Intervention, Abwehr. [Druckfassungen in diesem Sammelband].

Kowalski, Robin M./Giumetti, Gary W./Schroeder, Amber N./Lattaner, Micah R.: Bullying in the Digital Age. A Critical Review and Meta-Analysis of Cyberbullying Research Among Youth. In: Psychological Bulletin 137, February 10, 2014.

KPMG Deutschland (Hrsg.): KPMG-Studie Forensic e-Crime. Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und der Schweiz. Frankfurt am Main, März 2013. Aktualisierte Ausgabe vom Februar 2014. Auch als elektronische Ressource.

Kremer, Thomas: Digitale Bedrohungen und Gegenmaßnahmen aus der Sicht der Wirtschaft. Vortrag (des Vorstandsmitglieds der Deutschen Telekom AG für den Bereich Datenschutz,

Recht und Compliance) zur Herbsttagung des Bundeskriminalamts am 13. November 2013, über das Generalthema „Cybercrime – Bedrohung, Intervention, Abwehr. [Druckfassung in diesem Sammelband].

Meier, Bernd-Dieter: Sicherheit im Internet. Neue Herausforderungen für Kriminologie und Kriminalpolitik. In: Monatsschrift für Kriminologie und Strafrechtsreform 95, 2012, S. 184-204.

Naziris, Yannis: A Tale of Two Cities in three Themes: A Critique of the European Union´s Approach to Cybercrime from the „Power“ versus „Rights“ Perspective. In: European Criminal Law Review 3, 2013, Pp. 319-354.

Plewka, Ingo: Cybercrime: Bestandsaufnahme eines schwierigen Kampfes. In: Deutsche Richterzeitung 91, 2013, S. 44-47.

Rappoport, Moshe: Möglichkeiten und Herausforderungen von Big Data. Vortrag (des Executive Technology Briefer, Zürich Research Laboratory, IBM) zur Herbsttagung des Bundeskriminalamts am 13. November 2013, über das Generalthema „Cybercrime – Bedrohung, Intervention, Abwehr. [Druckfassung in diesem Sammelband].

Schönbohm, Arne: Cybercrime. Lukratives Geschäft für die Organisierte Kriminalität. In: Aus Politik und Zeitgeschichte 63, 2013, Heft 3839. S. 28-34.

Schulz, Carsten & Blasl, Markus: Präsentation zu Sicherheitsrisiken. Interaktive Online-Darstellung (der Mitarbeiter des Bundesamts für Sicherheit in der Informationstechnik) zur Herbsttagung des Bundeskriminalamts am 13. November 2013, über das Generalthema „Cybercrime – Bedrohung, Intervention, Abwehr.

Sieber, Ulrich: Cybercrime und Strafrecht in der globalen Informationsgesellschaft. In: Jahresbericht der Max-Planck-Gesellschaft zur Förderung der Wissenschaften. Band 2011, München 2012, S. 37-42

Stock, Jürgen: International Cybercrime: Results from the Annual International Forum. In: Coester, Marc & Marks, Erich (Eds.) International perspectives of crime prevention 4: Contributions from the 4th and the 5th Annual International Forum 2010 and 2011 within the German Congress on Crime Prevention. - Mönchengladbach 2012, S. 129-136.

Stol, Wouter Ph. (Ed.): Cybercrime and the Police. The Hague 2013.

Wall, David S. & Williams, Matthew L.: Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing. In: Policing and Society: An International Journal of Research and Policy 23, 2013, No. 4. Special Issue, Pp. 409-412.

Ziercke, Jörg: Begrüßung und Einführung in das Tagungsthema. Begrüßungsrede des Präsidenten des BKA zur Herbsttagung des Bundeskriminalamts am 12. November 2013a, über das Generalthema „Cybercrime – Bedrohung, Intervention, Abwehr. [Druckfassung in diesem Sammelband].

Ziercke, Jörg: Kriminalistik 2.0 – effektive Strafverfolgung im Zeitalter des Internet aus Sicht des BKA. Fachvortrag (des Präsidenten des BKA) zur Herbsttagung des Bundeskriminalamts am 13. November 2013b, über das Generalthema „Cybercrime – Bedrohung, Intervention, Abwehr. [Druckfassung in diesem Sammelband].

Ziercke, Jörg: Cybercrime – Bedrohung, Intervention, Abwehr. BKA-Herbsttagung vom 12. - 13. November 2013. In: Der Kriminalist 45, 2013c, 12, S. 17-21.

Diskussion

Teilnehmer (von links nach rechts)

Dr. Thilo Weichert, Landesbeauftragter für den Datenschutz Schleswig-Holstein

Dr. Marianne Janik, Microsoft Deutschland GmbH

Jörg Schönenborn, Chefredakteur WDR-Fernsehen

Markus Beckedahl, Netzpolitischer Aktivist aus Berlin, Gründer des Blog netzpolitik.org

Prof. Dr. Jürgen Stock, Vizepräsident beim Bundeskriminalamt

Unter der Moderation von WDR-Chefredakteur Jörg Schönenborn diskutierten Dr. Marianne Janik, Dr. Thilo Weichert, Markus Beckedahl, und Prof. Dr. Jürgen Stock, über das Thema **„Freiheit im Netz und Cybersicherheit – ein unlösbarer Widerspruch?“**

Mit dem Zitat des Bloggers Johnny Haeusler „Das Internet ist kaputt – für immer“ eröffnete Herr Schönenborn die Diskussion. Er stellte „…die Idee des Internets als Raum der Freiheit, der Entfaltung, der gesellschaftlichen und demokratischen Teilhabe…“ durch die Enthüllungen von Edward Snowden und damit verbundene Datenskandale als gefährdet dar und verband damit die Frage nach dem Vertrauen in das Internet, die Sicherheit und Freiheitsrechte**.** Herr Weichert zeigte sich von den Informationen aus der „NSA-Affäre“ nicht überrascht. Es habe ihn nicht verwundert, „…dass die Amerikaner keinen Grundrechtsschutz bei der Datenverarbeitung haben, dass auch ansonsten keine politischen Begehrlichkeiten bestehen, das irgendwie zu regeln, und dass die US-amerikanischen Firmen mit dem Thema Datenschutz sehr locker umgehen…“. Er sähe aus dem Blickwinkel des Datenschutzes in den Enthüllungen vor allem einen Aspekt „…der Augen geöffnet hat“ – bestenfalls auch den Verantwortlichen in der Politik. Frau Janik widersprach der Aussage, dass amerikanische Unternehmen den Datenschutz nicht ernst nehmen, denn „Datenschutz und Sicherheit der Privatsphäre sind längst zu einem Wettbewerbselement geworden. Wer das als Unternehmen nicht versteht, hat am Markt verloren, verliert Vertrauen“. Sie äußerte den Wunsch, dass die Enthüllungen „…die notwendige gesellschaftliche Debatte sinnvoll voranbringen […], dass wir hier Klartext sprechen, Transparenz herstellen und gleichzeitig zurückgehen auf eine faktenbasierte Diskussion.“ Frau Janik führte auf die Frage von Herrn Schönenborn zur Unterstützung der NSA durch Microsoft aus, dass sich Microsoft in jedem Land, in dem das Unternehmen tätig sei, an Recht und Gesetz halte, gesetzliche Verpflichtungen genau prüfe und in keinem Land „…Einblick in die Arbeit der Geheimdienste“ habe.

Prof. Dr. Jürgen Stock

Herr Stock zeigte sich erstaunt über „…das Ausmaß [und] über die Ressourcen, die zur Verfügung stehen“ bei Datenauswertungen in den USA. Auf Nachfrage von Herrn Schönenborn zu den rechtlichen Restriktionen in Deutschland führte Herr Stock aus, dass eine Aufgabentrennung und damit auch eine Trennung der Ermächtigungen von Polizei und Nachrichtendiensten bestehen. Das offensichtliche Vorgehen der NSA habe nach Herrn Stock „…mit polizeilicher Arbeit nichts zu tun.“ In der aktuellen Diskussion gebe es lediglich teilweise thematische Verbindungen, was u. a. „neue Ermächtigungsnormen und notwendige neue kriminalistische Möglichkeiten für die Polizei, die natürlich auch getragen sein müssen von dem Vertrauen der Bevölkerung“, betrifft. Ein (ungerechtfertigter) Vertrauensverlust in die polizeiliche Arbeit und eine abnehmende Zusammenarbeit mit dem Bürger hätten fatale Folgen für die kriminalistische Arbeit. Er betonte die Schranken der Gesetze sowie die breiten Kontrollfunktionen in Bezug auf polizeiliche Maßnahmen – sei es im Rahmen der Gefahrenabwehr oder sei es bei der Strafverfolgung. Die Sachleitungsbefugnis der Staatsanwaltschaften und die Notwendigkeit richterlicher Anordnungen in den meisten Fällen böten in Deutschland eine entsprechende Kontrolle. Herr Stock erinnerte angesichts des Spannungsverhältnisses zwischen neuer Bedrohungslage und rechtlichen Ermächtigungen an die Notwendigkeit der „Anpassung unseres rechtlichen Instrumentariums“.

Herr Beckedahl appellierte an das Verständnis der Bürgerinnen und Bürger und betonte: „…[es sollte] schon bewusst sein, dass wir auf einmal ständig und überall überwacht werden. Die Frage ist nicht mehr, ob wir überwacht werden, sondern nur noch wie oft, durch wen, wo und ob das für immer gespeichert und gegen uns verwendet wird.“ Er beschrieb dies als Problem einer Demokratie und jedes Einzelnen, da diese Überwachung einen Grundrechtseingriff darstelle. Die Tatsachen der aktuellen „NSA-Affäre“ waren für Herrn Beckedahl nicht neu. Er berief sich auf den Echelon-Skandal[1]: „Das war der Vorläufer-Skandal. Damals ist auch schon rausgekommen, dass unsere ganze Internet-Kommunikation überwacht wird, dass die NSA und der britische Geheimdienst einfach ’mal die Glasfaserkabel anzapfen.“ Dies sei in seinen Augen inakzeptabel. Man müsse „…technisch und politisch die richtigen Wege einschlagen, damit wir zukünftig wieder anonym kommunizieren können.“

[1] Europäisches Parlament/Gerhard Schmidt: BERICHT über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON), 2001/2098, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//DE (Stand: 12.03.2014))

Frau Janik unterstrich den Handlungsbedarf, forderte im Vorfeld jedoch Klarheit und Transparenz, ehe Verantwortlichkeiten und Maßnahmen bei Politik, IT-Wirtschaft und Nutzern eingefordert werden könnten.

Dr. Marianne Janik

Herr Schönenborn konkretisierte die Bedrohungs- und Überwachungslage für die Nutzer, die objektiv betrachtet von Cyberkriminellen, aber auch „…fremden staatlichen Mächten…“ ausgehen könne. Die notwendigen Konsequenzen bzw. Handlungsansätze gestalteten sich für ihn auf drei Ebenen – der persönlichen Nutzerebene, der rechtlichen und der technischen Ebene. Doch bereits die persönlichen Konsequenzen, die Nutzer aus einer solchen Enthüllung für die eigene, erhöhte „Awareness“ ziehen sollten, blieben offensichtlich aus. Aus einer Umfrage im Deutschland-Trend ergebe sich, dass 90 % der befragten Nutzer ihr Telefonieverhalten mit dem Mobiltelefon im Zuge der „NSA-Affäre“ nicht geändert haben und keine gesteigerte Vorsicht walten ließen.

Herr Weichert erklärte dies mit der fehlenden Betroffenheit der meisten von den Zielen der unterschiedlichen Angreifer: „Die Hacker in China klauen ihre Wirtschaftsgeheimnisse, der Kriminelle klaut ihnen das Geld vom Konto und die NSA sorgt dafür, dass sie nicht mehr in die USA einreisen können. Die 90 % sind in den meisten Fällen eher nicht betroffen.“ Daher zögen viele ihre eigenen Konsequenzen erst, wenn sie auch unmittelbar betroffen seien. Wirtschaftsunternehmen reagierten hier sensibler, stellte er fest: „Cloud-Computing hat nicht mehr ansatzweise diese Relevanz, insbesondere für die Wirtschaft, wie sie es vor fünf Monaten noch hatte. Die US-Anbieter verlieren massiv an Marktanteilen, die hatten teilweise 90 bis 100 % an Marktanteilen. Wenn jetzt 10, 20 % auf einmal wegbrechen, dann zeigt es, dass sich das Verhalten verändert.“ Diese Entwicklung wird nach seiner Meinung weitergehen, beschränke sich jedoch nicht ausschließlich auf die Nachfrage, sondern auch auf ein adäquates Marktangebot derartiger Dienste in Europa.

Herr Beckedahl nannte die Sorglosigkeit der Nutzer eher Naivität. Fehlendes Wissen über die Datenspuren, die man hinterlasse, mache es den abschöpfenden Institutionen leicht. Nur wer Schutzmechanismen kenne, könne sich auch schützen. Herr Beckedahl formulierte hieraus seinen Vorwurf: „Und hier hat eigentlich auch die Gesellschaft, hier hat die Politik versagt, diese Menschen mitzunehmen, ihnen zu erklären, dass man vielleicht nicht auf jeden Link draufklicken sollte, der per Mail zu einem geschickt wird.“ Insbesondere die demografische Entwicklung sei bei der zielgruppenorientierten Sensibilisierung in der Prävention nicht genügend berücksichtigt. Auch bei Politikern sei das Gefahrenbewusstsein kaum ausgeprägt. Frau Janik erweiterte diese Forderung in Richtung der Politik um den Aspekt, dass die Politik allein nicht das zu bewegen vermöge, was erwartet werde. Sie sagte: “ Wir brauchen eine

Allianz zwischen Politik, denjenigen, die die Technologie in den Markt bringen, und dem Nutzer. Wir brauchen diese breite Allianz und da sind wir noch ganz am Anfang.“ Wenn man die Themen Transparenz, Zugang, Sicherheit und Verantwortungsrahmen isoliert definiere und angehe, könne man zügig tätig werden.

Herr Beckedahl gab jedoch zu bedenken, dass das Vertrauen in Unternehmen, die in die Aktivitäten der NSA involviert seien, problematisch sein dürfte. Er fragte: „Warum wechselt das Auswärtige Amt von freier Software hin zu Microsoft? Warum gehen wir nicht den umgekehrten Weg und stellen jetzt ’mal unsere ganzen Infrastrukturen auf vertrauenswürdige, offene, freie Infrastrukturen um?“ Frau Janik sah hier jedoch unscharfe Elemente, die nicht auf Fakten basierten, und forderte erneut eine faktenbasierte Diskussion, um wirklich Fortschritte in Sachen Datenschutz, Cybersicherheit und Vertrauensbildung zu machen. Herr Weichert schloss sich der Forderung nach faktenbasierter Diskussion an. Einseitiger und voreingenommener Anti-Amerikanismus sei nicht geboten. Eine differenzierte Betrachtung der Tatsachen sei dringend notwendig – auch im Hinblick auf die beteiligten Wirtschaftsunternehmen. Dennoch blieb für Herrn Weichert festzuhalten: „Mit Daten wird Geld verdient, mit Daten wird Weltmacht abgesichert. Und deswegen sind die Amerikaner auch in Zukunft nicht bereit, jetzt hier ihre Gesetze zu ändern und Transparenz herzustellen, wenn man sie nicht dazu zwingt. Das ist ausschließlich eine politische Frage und nicht eine Frage des Verhaltens von irgendwelchen Konsumenten oder von irgendwelchen einzelnen Wirtschaftsunternehmen.“

Markus Beckedahl

Den Aspekt der politischen Handlungsnotwendigkeit griff Herr Schönenborn auf und lenkte die Diskussion auf die Frage: „ob auch im Interesse des Schutzes vor Kriminalität, vor Strafverfolgung, eigene europäische, deutsche Standards helfen…“ und zitierte den Präsidenten des Europäischen Parlaments Martin Schulz, der sinngemäß gesagt habe: „Wir müssen lernen, dass staatliche Souveränität heute nicht mehr eine Frage von Grenzsicherung ist, von Grenzkontrollen, von Truppen, die mein Land verteidigen können, sondern staatliche Souveränität ohne digitale Souveränität, ohne Beherrschung von Codes und Netzen ist eigentlich nicht mehr denkbar.“ Als Beispiel nannte Herr Schönenborn die Deutsche Telekom, die versuche, den innerdeutschen Datenverkehr sicherzustellen, um damit „…Alternativen zu den amerikanisch beherrschten Standards oder im Mobilfunk ja auch chinesisch beherrschten Standards...“ zu suchen.

Herr Stock relativierte den berechtigten Einwand notwendiger internationaler Regulierungen und stellte nationale Maßnahmen in den Vordergrund, die sich mit dem Awareness-Gedanken gegen zuviel Sorglosigkeit bei Privatnutzern, aber auch in Unternehmen richten.

Die Tatsache, dass es bei der Betroffenheit von cyberkriminellen Straftaten heute nur noch eine Kategorie gebe, nämlich Betroffene – sei es bewusst oder unbewusst – gebe, führe gesamtgesellschaftlich dazu, zuvorderst vor allem nationale Maßnahmen zu ergreifen. Herr Stock hob neben der phänomenologischen Aufklärung der Nutzer vor allem die technische Prävention und eine aussagekräftige Kriminalstatistik mit geringst möglichem Dunkelfeld als Grundlage erfolgreicher Präventions- und Strafverfolgungsarbeit hervor. Andererseits regte Herr Stock vor dem Hintergrund der extremen Schnelllebigkeit bei der Entwicklung von IT-Technologien und den entsprechenden Cybercrime-Phänomenen an, den notwendigen Diskurs über politische Entscheidungen zu Gunsten der Handlungsfähigkeit gegen Cyberkriminelle zu beschleunigen.

Herr Beckedahl griff das Beispiel der Telekom auf, um zu verdeutlichen, dass Bestrebungen, die Sicherheit zu erhöhen, immer im Detail betrachtet und untersucht werden müssten. Es gelte, zusätzliche Investitionen in die Sicherheit zu tätigen und nicht bereits standardmäßige Maßnahmen als neue Sicherheitstechnologien zu verkaufen. Insbesondere den innerdeutschen Datenverkehr zu routen, sei bereits seit Jahren technisch kein Problem, werde aber nicht gemacht, so Markus Beckedahl. An diesem Punkt lenkte er den Fokus erneut auf die Diskussion um die Abhörskandale und fragte: „…ob das beste Routing auch was bringt, wenn überall irgendwer abhört und die Daten dann im Ringaustausch mit den USA geteilt werden.“

Dr. Thilo Weichert

Die Auffassung, dass solche Maßnahmen aussichtslos seien, teilte Herr Weichert nicht und berief sich auf positive Bestrebungen seiner Behörde; „in Schleswig-Holstein gibt es nach allen meinen Informationen eine einzige Behörde [Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein], die verschlüsselte E-Mails von Bürgern annimmt. Untereinander wird schon abgesichert ausgetauscht und es gibt ein sicheres Netz.“ Im internationalen Kontext sah Herr Weichert vor allem die Notwendigkeit von validen Strukturen: „Wir müssen so etwas wie eine digitale Menschenrechtscharta entwickeln. Das ist im Prinzip heute keine Frage mehr von nationalen Staaten, sondern einer globalen Gesellschaft, weil die Bürgerrechte eines Amerikaners in Deutschland genauso verteidigt werden müssen, wie die eines Deutschen in den USA.“ Er hob hier die europäische Datenschutzverordnung hervor, denn „…dies würde Druck auf die Amerikaner, aber auch auf alle anderen Wirtschaftspartner ausüben, weil diese gezwungen würden, diese Standards irgendwann anzunehmen, wenn sie sich mit Europa austauschen wollen.“

Frau Janik, die die politische Diskussion begrüßte, führte jedoch erneut an, dass man es mit einer gesellschaftlichen Frage zu tun habe; sie sagte: „…es müssen alle Beteiligten an einen Tisch, es muss zusammen gearbeitet werden, innerdeutsch, aber auch mit internationalen Partnern. Sonst verharren wir im Stillstand. In zehn Jahren stehen wir wieder da und haben festgestellt, dass das ganze Thema komplexer geworden ist."

Herr Stock wies an dieser Stelle auf die bereits existenten weitläufigen Kooperationen, wie beispielsweise den Cybersicherheitsrat oder den Austausch im Nationalen Cyberabwehrzentrum beim BSI hin. In diesem Zusammenhang solle insbesondere der Schutz von kritischen Infrastrukturen oberste Priorität haben, bei dem es nicht mehr ausreiche, innerhalb der Kooperation langwierige Entscheidungsprozesse und Zusammenkünfte zu realisieren, sondern es erforderlich werde, sich täglich mit der Problematik und ihrer Lösung zu befassen. Herr Stock verwies auch auf die bereits vorgestellten Ideen und Maßnahmen des Bundeskriminalamts einer engeren Zusammenarbeit mit der Wirtschaft.

Jörg Schönenborn

Gefragt nach den Wünschen und Forderungen der Strafverfolgung an den Gesetzgeber erläuterte Herr Stock neben der bereits erwähnten Notwendigkeit eines bspw. aus Informationen der Wirtschaft, der Strafverfolgung, des BSI und dem Ausland zusammengeführten Lagebildes auf die Bedeutung der IP-Adresse als wichtigen Anknüpfungspunkt und damit einhergehend die Notwendigkeit der Vorratsdatenspeicherung. Außerdem „… brauchen wir klare rechtliche Grundlagen für die sog. Online-Durchsuchung, die wir im BKA im Bereich der Gefahrenabwehr haben, das ist hier angesprochen worden. Es wäre wünschenswert, das auch im Bereich der Strafprozessordnung zu haben." Des Weiteren sei eine europäische und weltweite Rechtsharmonisierung neben allen nationalen Bestrebungen unabdingbar. Herr Weichert, der Verständnis für die Bedürfnisse der Ermittlungsbehörden zeigte, bewertete jedoch die bisherige „…Grundlage [zur Vorratsdatenspeicherung], die sich Europa gegeben hat [als] nicht notwendig und nicht verhältnismäßig" und sah einen Kompromiss in kurzen Speicherfristen mit Quick-Freeze-Regelungen. Dies werde den polizeilichen Bedürfnissen gerecht, sei praktikabel und zugleich grundrechtskonform. Darüber hinaus wünsche man sich aus dem Blickwinkel der Datenschützer Anpassungen im G10-Gesetz und ausgereifte Regelungen zur Internetüberwachung.

Herr Stock wies Herrn Weichert auf die fehlende Praktikabilität von Quick-Freeze Regelungen in der Strafverfolgung hin und ergänzte, dass das Bundesverfassungsgericht in Sachen Vorratsdatenspeicherung den Rahmen für eine verfassungsgemäße Ausgestaltung einer gesetzlichen Regelung bereits festgelegt habe.

Aus Sicht von Microsoft Deutschland plädierte Frau Janik vor allem für „…die Vereinheitlichung der Datenschutzvorschriften in Europa.“ Microsoft sei aber heute schon in der Lage, den unterschiedlichen Rechtsnormen in Sachen Datenschutz und IT-Sicherheit vollständig gerecht zu werden, ergänzte sie. Persönlich sah sie einen großen Nutzen in No-Spy-Abkommen zwischen befreundeten Nationen.

Markus Beckedahl warnte mit Blick auf die Balance von Sicherheit und Freiheit im Netz vor einer anlasslosen Überwachung der Kommunikation im Sinne einer Vorratsdatenspeicherung, die einem Generalverdacht gleichkomme und unverhältnismäßig sei. Er wünsche sich ein IT-Grundrecht „…auf Integrität und Vertrauen in informationstechnische Geräte…[und] Systeme“ in gesetzlicher Form. Außerdem sei die Förderung der Kryptografie durch die Bundesregierung ein Punkt, der neben der Forderung nach mehr Möglichkeiten anonymer Nutzung und Kommunikation im Netz genannt werden müsse.

Zu den Referenten[1]:

Bär, Wolfgang, Dr.

Ministerialrat, Bayerisches Staatsministerium der Justiz und für Verbraucherschutz

1980 - 1984 Studium der Rechtswissenschaften an der Universität Bayreuth; 1984 - 1987 Rechtsreferendar beim Landgericht Bayreuth mit Abschluss 2. Staatsexamen; 1987 - 1991 Akademischer Rat am Lehrstuhl für Strafrecht, Strafprozessrecht und Informationsrecht (Prof. Dr. Sieber) an der Universität Bayreuth mit Dissertation „Zugriff auf Computerdaten im Strafverfahren“ (1991); 06/1991 - 05/2000 Richter/Staatsanwalt mit verschiedenen Aufgaben in Zivil- und Strafsachen beim Amtsgericht Bayreuth und bei der Staatsanwaltschaft Bayreuth, dabei von 1994 - 2000 zuständig für EDV-Betreuung in Wirtschaftsstrafsachen für Schwerpunktstaatsanwaltschaften in ganz Bayern; 06/2000 - 06/2007 Verantwortlicher hauptamtlicher Leiter der Arbeitsgemeinschaften für Rechtsreferendare beim LG Bayreuth; 16.08.2005 Ernennung zum Richter am Oberlandesgericht; 07/2007- 10/2011 Mitglied im 2. Strafsenat beim Oberlandesgericht Bamberg und dort zuletzt stellvertretender Vorsitzender; seit 11/2011 Leiter des Referats zur Bekämpfung von Internetkriminalität und des Missbrauchs neuer Technologien in der Strafrechtsabteilung des Bayerischen Staatsministeriums der Justiz und für Verbraucherschutz; 01.01.2013 Ernennung zum Ministerialrat.
Weitere Tätigkeiten: Referent an der Deutschen Richterakademie in Trier und Wustrau sowie bei weiteren Fortbildungsveranstaltungen der Justiz und Polizei; Mitwirkung bei internationalen Projekten im Bereich des Computerstrafrechts (EU-Twinning, TAIEX u.a.); zahlreiche Publikationen zum Bereich des Computerstrafrechts, u.a. Handbuch zur EDV-Beweissicherung im Strafverfahren, Boorberg Verlag, 2007, TK-Überwachung Kommentar Heymanns-Verlag 2010, Kommentierung §§ 100a - 101 StPO im KMR-Kommentar zur StPO mit ständigen Aktualisierungen.

80335 München, Prielmayerstraße 7

Beckedahl, Markus

Netzpolitischer Aktivist aus Berlin

Bloggt seit 2002 unter www.netzpolitik.org, einem der meist zitierten Blogs im deutschsprachigen Raum; Mitorganisator der re:publica-Konferenzen sowie Partner und Gründer der Agentur „newthinking communications GmbH“; Sachverständiger in der Enquete-Kommission „Internet und digitale Gesellschaft“ im Deutschen Bundestag; Mitglied des Medienrates der Medienanstalt Berlin-Brandenburg; ehrenamtlicher Sprecher von „Creative Commons Deutschland“.

10119 Berlin, Schönhauser Allee 6/7

[1] Stand: November 2013

Blasl, Markus

Bundesamt für Sicherheit in der Informationstechnik

1998 - 2003 Studium der „Allgemeinen Informatik“ an der Fachhochschule Karlsruhe; 2002 - 2003 Forschungszentrum Informatik (FZI) Karlsruhe; 2004 - 2005 tätig für "Schmieder it-solutions GmbH"; 2005 - heute Bundesamt für Sicherheit in der Informationstechnik, derzeit Referat C23 "Allianz für Cyber-Sicherheit, Penetrationszentrum und IS-Revision"; 2008 - 2011 Studium "Computer Science" Fernuniversität Hagen.

53175 Bonn, Godesberger Allee 185-189

Daniel, Michael

Special Assistant des Präsidenten der Vereinigten Staaten von Amerika und Koordinator für Cybersicherheit, Weißes Haus

In dieser Position leitet er die behördenübergreifende Entwicklung der nationalen Cybersicherheitsstrategie und -politik und überwacht die Umsetzung dieser Maßnahmen in den Behörden. Michael Daniel stellt auch sicher, dass die US-Regierung effektiv mit dem Privatsektor, mit Nichtregierungsorganisationen, anderen Regierungsbereichen und -ebenen und mit anderen Nationen zusammenarbeitet. Vor dem Wechsel zum *National Security Staff* (Büro für nationale Sicherheit) war Michael Daniel 17 Jahre beim *Office of Management and Budget* (OMB, Büro für Verwaltung und Haushalt) tätig. Michael Daniel spielte eine Schlüsselrolle bei der Ausgestaltung der Budgets der Nachrichtendienste, der Verbesserung der Verwaltung der *Intelligence Community* und der Lösung wichtiger Strategiefragen der *Intelligence Community*, einschließlich Cybersicherheit, Ausgaben für Terrorismus-bekämpfung sowie Informationsaustausch und -sicherung.
Michael Daniel machte den Bachelor-Abschluss in Politik (*Public Policy*) an der *Woodrow Wilson School* der Universität Princeton und den Master-Abschluss in Politik an der *Kennedy School of Government* in Harvard.

USA, Washington DC 20500, Weißes Haus

Di Fabio, Udo, Prof. Dr. Dr.

Professor für Öffentliches Recht an der Universität Bonn

1970 - 1980 Kommunalverwaltungsbeamter bei der Stadt Dinslaken; 1985 - 1986 Richter beim Sozialgericht Duisburg; 1987 Promotion Rechtswissenschaften; 1990 Promotion Sozialwissenschaften; 1993 Habilitation an der Universität Bonn; 1993 - 2003 Professor an den Universitäten Münster, Trier, München; 1999 - 2011 Richter des Bundesverfassungsgerichts; seit 2003 an der Universität Bonn; Mitglied der Nordrhein-Westfälischen Akademie der Wissenschaften und Künste.
Veröffentlichungen (Auswahl): Wachsende Wirtschaft und steuernder Staat, 2010; Gewissen, Glaube, Religion, 2. Aufl. 2009; Die Kultur der Freiheit, 2005; Die Staatsrechtslehre und der Staat, 2003; Das Recht offener Staaten, Grundlinien einer Staats- und Rechtstheorie, 1998; Risikoentscheidungen im Rechtsstaat, 1994.

53113 Bonn, Adenauerallee 44

Fritsche, Klaus-Dieter

Staatssekretär im Bundesministerium des Innern

1973 - 1974 Wehrdienst in Regensburg; 1974 - 1978 Jurastudium an der Friedrich-Alexander-Universität Erlangen, Erstes Staatsexamen in Erlangen; 1979 - 1981 Referendariat, Zweites Staatsexamen in Nürnberg; 1981 - 1984 Verwaltungsrichter am Verwaltungsgericht Ansbach; 1984 - 1986 Regierungsrat an der Regierung von Mittelfranken; 1986 - 1988 Verwaltungsrichter am Verwaltungsgericht Ansbach; 1988 - 1991 Innen- und umweltpolitischer Referent der CSU-Landesgruppe in Bonn; 1991 - 1993 Vertreter des Bayerischen Staatsministeriums des Innern bei der Bayerischen Vertretung in Bonn; 1993 - 1995 Leiter des Büros von Herrn Staatssekretär Hermann Regensburger im Bayerischen Staatsministerium des Innern; 1995 - 1996 Leiter des Büros des Bayerischen Staatsministers des Innern Dr. Günther Beckstein; 1996 - 2005 Vizepräsident des Bundesamtes für Verfassungsschutz; 2005 - 2009 Leiter der Abteilung 6 im Bundeskanzleramt; seit Dezember 2009 Staatssekretär im Bundesministerium des Innern.

10559 Berlin, Alt Moabit 101D

Gaycken, Sandro, Dr.

Technik- und Sicherheitsforscher im Fachbereich Informatik an der Freien Universität Berlin

Dr. Sandro Gaycken forscht zu dem Themenfeld Informationstechnik und Gesellschaft, genauer zu Datenschutz, Datensicherheit, Cyberwarfare, Cybercrime, Hacking sowie zu Utopien der Informationsgesellschaften. Neben seiner Forschungstätigkeit berät er Politik und Wirtschaft. Er war mehrfach zu Anhörungen im Bundestag, der NATO, der G8 sowie der EU und war als Stratege zu Cyber-Außen- und Sicherheitspolitik im Planungsstab des Auswärtigen Amtes tätig.

14195 Berlin, Fabeckstraße 15

Geschonneck, Alexander

Leiter und Partner des Bereiches Forensic Technology der KPMG AG Wirtschaftsprüfungs-gesellschaft in Berlin
Sein Tätigkeitsschwerpunkt ist die Sicherstellung und Analyse von digitalen Beweismitteln im Rahmen der Korruptions- und Betrugsbekämpfung sowie die Aufklärung von IT-Sicherheitsvorfällen. Er unterstützt private und öffentliche Organisationen im Rahmen der Erstreaktion auf Cybercrime-Vorfälle mit einem technischen Ermittlungsteam. Er ist Autor des deutschen Standardwerkes über Computer-Forensik sowie Herausgeber der regelmäßig erscheinenden Studie "eCrime in der deutschen Wirtschaft".

10785 Berlin, Klingelhöferstraße 18

Hartel, Pieter, Prof. Dr.

Ordentlicher Professor für Informatik an der Universität Twente
Pieter Hartel ist ordentlicher Professor für Informatik an der Universität Twente. Sein Forschungsinteresse gilt dem sozio-technischen Aspekt der Cybersicherheit. Er studierte Mathematik und Informatik an der Freien Universität Amsterdam und promovierte 1989 an der Universität Amsterdam in Informatik. Er war an der Forschungseinrichtung CERN in Genf/Schweiz, den Universitäten Nimwegen, Amsterdam/Niederlande sowie Southampton/Vereinigtes Königreich tätig. Er fungierte als Unternehmensberater für mehrere internationale Unternehmen wie Sun Microsystems sowie nationale Organisationen wie die Niederländische Organisation für Angewandte Naturwissenschaftliche Forschung (TNO). Er ist Mitherausgeber der Fachzeitschrift *Crime Science* und Mitglied zahlreicher Fachausschüsse internationaler Konferenzen. Er ist Koordinator eines umfangreichen Europäischen Projekts namens TREsPASS: Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security (FP7-ICT-2011-8).

NL-7500 AE Enschede, PO Box 217

Henzler, Peter

Vizepräsident beim Bundeskriminalamt
1974 - 1979 Offizier der Bundeswehr; 1980 - 1989 Studium der Rechtswissenschaften, 1. Staatsexamen, Assessorausbildung, 2. Staatsexamen; 1990 Eintritt in das Bundeskriminalamt; 1991 -1993 Stellvertretender Leiter des Referates Verdeckte Ermittler und Mobiles Einsatzkommando; 1993 - 1995 Stellvertretender Leiter des Referates „Waffenkriminalität, Proliferation, Umweltkriminalität“; 1995 - 2000 Stellvertretender Leiter und Leiter des Referates „Stabs- und Grundsatzangelegenheiten der Abteilung Organisierte und Allgemeine Kriminalität“; 2000 - 2005 Leiter des Stabes der Amtsleitung; 2005 - 2007 Leiter der Gruppe „Zentrale Angelegenheiten/Einsatz verdeckter Ermittler“; 2007 - 2010 Leiter der Abteilung „Zentrale kriminalpolizeiliche Dienste“; 2010-2013 Leiter der Abteilung „Schwere und Organisierte Kriminalität“; 01.04.2013 Berufung zum Vizepräsidenten beim Bundeskriminalamt.

65193 Wiesbaden, Thaerstraße 11

Janik, Marianne, Dr.

Microsoft Deutschland GmbH
Nach ihrem Studium der Rechtswissenschaften in Würzburg und Genf startete Marianne Janik bei der Daimler Benz AG ins Berufsleben. 1995 schloss sie ihre berufsbegleitende Promotion in Europäischem Gemeinschaftsrecht mit „magna cum laude“ ab. Nach verschiedenen Managementpositionen innerhalb des Daimler Benz-Konzerns wechselte sie im Jahr 2000 zur Plaut Consulting GmbH. Als Prokuristin, Mitglied der Geschäftsleitung und Director Sales and Marketing widmete sie sich dem Aufbau eines Zentralvertriebes und war für alle Kommunikationsaktivitäten der Plaut Gruppe verantwortlich. Im Zeitraum zwischen 2003 und 2010 war Dr. Marianne Janik Mitglied der Geschäftsleitung und Bereichsleiterin Geschäftsentwicklung bei der ESG GmbH. Zuletzt war sie als General Manager und Prokuristin Western und Eastern Europe bei der Elster GmbH tätig.
Dr. Marianne Janik ist seit Mai 2011 bei der Microsoft Deutschland GmbH und als Senior Director Public Sector Mitglied der Geschäftsleitung. Sie verantwortet das gesamte Geschäft mit der öffentlichen Verwaltung, dem Bildungsbereich und dem Gesundheitswesen. Janik berichtet an den Vorsitzenden der Geschäftsführung Microsoft Deutschland und Area Vice President International, Christian P. Illek.

85716 Unterschleißheim, Konrad-Zuse-Str. 1

Könen, Andreas

Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik
1980 - 1987 Studium der Mathematik an der Universität zu Köln, Abschluss als Diplom Mathematiker; 1987 - 1988 Wehrdienst im Programmierzentrum der Luftwaffe für Luftverteidigung; Dezember 1988 - Oktober 2006 Bundesnachrichtendienst (BND), Referent und Sachgebietsleiter, zuletzt Sachgebietsleiter im Leitungsstab des BND-Präsidenten in Berlin; Oktober 2006 Leiter des Leitungsstabes im Bundesamt für Sicherheit in der Informationstechnik (BSI); Februar 2009 Leiter des Fachbereichs „Sicherheit in Anwendungen und Kritischen Infrastrukturen“ im BSI; Juli 2011 Leiter des Fachbereichs „Koordination und Steuerung“ im BSI; November 2011 Leiter der Abteilung „Beratung und Koordination“ im BSI; seit Januar 2013 Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik.
53175 Bonn, Godesberger Allee 185-189

Kremer, Thomas, Dr.

Vorstandsmitglied Deutsche Telekom AG, Datenschutz, Recht und Compliance
Dr. Thomas Kremer ist seit Juni 2012 Vorstand für Datenschutz, Recht und Compliance bei der Deutschen Telekom AG. Vor seiner Tätigkeit für die Deutsche Telekom war Thomas Kremer für die ThyssenKrupp AG tätig. 1994 trat er in die Rechtsabteilung von Krupp ein. 2003 übernahm er die Leitung des Rechtsbereichs der ThyssenKrupp AG. Zusätzlich wurde er 2007 zum Chief Compliance Officer des ThyssenKrupp Konzerns bestellt. 2011 erfolgte die Ernennung zum Generalbevollmächtigten.
Zu den weiteren Stationen in seinem beruflichen Werdegang zählte die Tätigkeit als Rechtsanwalt in der Sozietät Schäfer, Wipprecht, Schickert in Düsseldorf (heute CMS Hasche Sigle). Nach seinem Studium der Rechtswissenschaften war Thomas Kremer wissenschaftlicher Mitarbeiter am Institut für Handels- und Wirtschaftsrecht der Rheinischen Friedrich-Wilhelms Universität in Bonn. Seine Arbeitsgebiete umfassten das GmbH-Recht sowie das Aktien- und Konzernrecht. 1994 promovierte er zum Doktor der Rechte.
Seit Oktober 2013 ist Thomas Kremer zudem Mitglied der Regierungskommission Deutscher Corporate Governance Kodex.

53113 Bonn, Friedrich-Ebert-Allee 140

Rappoport, Moshe

Executive Technology Briefer, Zurich Research Laboratory, IBM
Moshe Rappoport studierte Informatik an der City University in New York, USA. Bevor er 1986 seine Tätigkeit in der IBM Forschung aufnahm, arbeitete er zwölf Jahre an der Entwicklung von innovativen Managementinformationssystemen bei 3M Europa. Seit 28 Jahren ist er bei IBM Research, Zürich tätig. Als Executive Technology Briefer im Trend- und Innovationsforum des IBM Forschungslabors bei Zürich diskutiert er Technologietrends und den Einfluss neuer Informationstechnologien auf Unternehmen und Gesellschaft mit Meinungsträgern und IT-Führungskräften. Er verfügt über eine weitreichende Erfahrung in vielen IT-Bereichen, dies umfasst End User Computing, Collaboration, Benutzerfreundlichkeit sowie Informations- und Wissensmanagement.

Switzerland, 8803 Rueschlikon, Saeumerstraße 4

Schönenborn, Jörg

Chefredakteur Fernsehen des Westdeutschen Rundfunk (WDR)
Moderation des »ARD-Presseclub« und »ARD-Brennpunkt«; seit 1999 Präsentation von Umfrage- und Wahlergebnissen und politischen Analysen als ARD-Wahlmoderator; Autor des monatlichen »ARD-DeutschlandTrends«; 1983 - 1988 Studium der Journalistik und Politikwissenschaft; nach einem Volontariat Arbeit als Hörfunk- und Fernsehredakteur beim WDR sowie als Inlands-Korrespondent für »Tagesschau« und »Tagesthemen«; von 1997 - 2002 Leitung der WDR-Fernsehredaktionsgruppe »Zeitgeschehen aktuell«; seit 2002 Chefredakteur Fernsehen des Westdeutschen Rundfunk (WDR).
Preise/Ehrungen: 1993/1994 Telestar-Förderpreis und Axel-Springer-Preis für Fernsehjournalismus anlässlich seiner Berichterstattung vom Brandanschlag in Solingen; 2005 und 2009 Nominierung für den Deutschen Fernsehpreis als Moderator der ARD-Sendung »Wahlarena«; 2011 RIAS-Fernsehpreis als Moderator für »Die Lange Obama-Nacht - Halbzeit für den Präsidenten«.

Westdeutscher Rundfunk, 50600 Köln

Schulz, Carsten

Bundesamt für Sicherheit in der Informationstechnik
1986 - 1989 Studium an der Fachhochschule des Bundes, Mannhein; 1989 - 1993 Bundeswehr, Marinearsenal Arsenalbetrieb, Kiel; 1993 - heute Bundesamt für Sicherheit in der Informationstechnik, derzeit Referat C23 "Allianz für Cyber-Sicherheit, Penetrationszentrum und IS-Revision", Projektleiter "Übungszentrum Netzverteidigung".

53175 Bonn, Godesberger Allee 185-189

Stock, Jürgen, Prof. Dr.

Vizepräsident beim Bundeskriminalamt
1978 - 1987 Kriminalbeamter in Hessen; 1984 - 1990 Studium der Rechtswissenschaften; 1990 Erste juristische Staatsprüfung; 1990 - 1993 Forschungsassistent an der Universität Gießen, Professur für Kriminologie; 1993 - 1995 Rechtsreferendar; 1995 Zweite juristische Staatsprüfung und Promotion; 1996 Rechtsanwalt; 1996 - 1998 Referent im Bundeskriminalamt; 1998 - 2000 Ernennung zum Professor, Gründungsrektor der Fachhochschule der Polizei Sachsen-Anhalt; 2000 - 2004 Leiter der Abteilung „Kriminalistisches Institut“ im Bundeskriminalamt; 2004 Berufung zum Vizepräsident beim Bundeskriminalamt. Zusätzliche Aufgaben: 1999 - 2000 Vorsitzender der Konferenz der Rektoren/Präsidenten der Polizei-Fachhochschulen, Sprecher/Leiter der Fachbereiche „Polizei der Verwaltungsfachhochschulen“, stellvertretender Vorsitzender der Konferenz der Rektoren der Fachhochschulen für den öffentlichen Dienst; 2004 - 2007 Vorstandsmitglied der Mitteleuropäischen Polizeiakademie (MEPA); 2005 - 2006 Mitglied des European Security Research Advisory Board (ESRAB); 2005 - 2007 Delegierter für Europa im Exekutivkomitee der Internationalen Kriminalpolizeilichen Organisation (IKPO-Interpol), Vorsitzender des Finance Subcommittee; 2007 - 2009 Stellvertretender Vorsitzender des European Security Research and Innovation Forum (ESRIF); 2007 - 2010 Vizepräsident für Europa der Internationalen Kriminalpolizeilichen Organisation (IKPO-Interpol), Vorsitzender des Strategic Development Subcommittee; 2007 - 2012 Mitglied des Wissenschaftlichen Programmausschusses Sicherheitsforschung der Bundesregierung; 2010 - 2012 Mitglied des Beratungsgremiums beim Bundesministerium für Wirtschaft und Technologie zur „Industriepolitischen Strategie für innovative und international erfolgreiche Sicherheitslösungen“; seit 2000 Mitglied der Projektleitung des Programms Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK); seit 2004 Mitglied des Vorstandes der Kriminologischen Gesellschaft (KrimG), Wissenschaftliche Vereinigung deutscher, österreichischer und schweizerischer Kriminologen e.V.; seit 2006 Honorarprofessor für Kriminologie am Fachbereich Rechtswissenschaft der Justus-Liebig-Universität Gießen; seit 2008 Mitglied im Beirat aus Wissenschaft und Praxis des Studiengangs „Risiko- und Sicherheitsmanagement“ der Hochschule für Öffentliche Verwaltung Bremen; seit 2009 Mitglied des Arbeitskreises Corporate Compliance des Institute for European Affairs (INEA).

65193 Wiesbaden, Thaerstraße 11

Weichert, Thilo, Dr.

Landesbeauftragter für den Datenschutz Schleswig-Holstein
Jurist und Politologe, Studium in Freiburg und Genf/Schweiz; 1984 - 1986 Landtagsabgeordneter in Baden-Württemberg; von 1982 an Tätigkeiten als Rechtsanwalt, Politiker, Publizist, Dozent in Freiburg, Stuttgart, Dresden und Hannover; 1991 Justiziar beim Sächsischen Landtag, zugleich juristischer Berater der Bürgerkomitees zur Auflösung der Staatssicherheit; 1990 - 2004 Vorsitzender der Deutschen Vereinigung für Datenschutz (DVD); 1992 - 1998 Referent beim Landesbeauftragten für den Datenschutz in Niedersachsen; von 1998 an stellvertretender, seit 2004 Landesbeauftragter für Datenschutz Schleswig-Holstein und damit Leiter des Unabhängigen Landeszentrums für Datenschutz in Kiel (ULD).

24171 Kiel, Postfach 7116

Ziercke, Jörg

Präsident des Bundeskriminalamtes
1967 Eintritt in den Dienst der Landespolizei Schleswig-Holstein; 1968 - 1970 Ausbildung zum Kriminalbeamten, 1970 - 1975 Verwendung im operativen Bereich bei der Schutz- und Kriminalpolizei sowie beim Landeskriminalamt Kiel; 1976 - 1977 Fachlehrer Kriminalistik an der Landespolizeischule Eutin; 1977 - 1979 Aufstieg in den höheren Dienst der Kriminalpolizei, Studium an der Polizei-Führungsakademie Münster; 1979 - 1985 Leiter der Kriminalpolizei Neumünster und Vertretungsaufgaben des Leiters der Kriminalpolizeidirektion Kiel; 1981 Abordnung zur Kriminalpolizeidirektion Itzehoe; 1985 - 1990 Personalreferent, Aus- und Fortbildungsreferent der Landespolizei im Innenministerium Schleswig-Holstein; 1990 - 1992 Leiter der Landespolizeischule Schleswig-Holstein sowie Unterstützung beim Aufbau der Landespolizeischule Mecklenburg-Vorpommern; 1992 - 2004 Abteilung „Polizei“ im Innenministerium Schleswig-Holstein, ab 1995 Leiter der Abteilung; 26.02.2004 Berufung zum Präsidenten des Bundeskriminalamts.
Zusätzliche Aufgaben: 1995 - 2004 Mitglied im Kuratorium der Polizei-Führungsakademie, Mitglied im Kuratorium der Wasserschutzpolizeischule Hamburg; 1999 - 2004 Vorsitzender des Arbeitskreises II (Innere Sicherheit) der Innenministerkonferenz; 2003 - 2004 Mitglied des Forschungsbeirates des Bundeskriminalamtes; seit 2001 Mitglied des Vorstandes des Deutschen Forums für Kriminalprävention (DFK) in Bonn; seit 2012 Stellvertretender Bundesvorsitzender WEISSER RING e.V.

65193 Wiesbaden, Thaerstraße 11

Gesamtmoderation der Tagung:

Kerner, Hans-Jürgen, Prof. Dr.

Seniorprofessor der Universität Tübingen, emeritierter Ordinarius für Kriminologie, Jugendstrafrecht, Strafvollzug und Strafprozessrecht
Studium an den Universitäten München, Berlin und Tübingen; 1967 erstes juristisches Staatsexamen; 1968 - 1975 Wissenschaftlicher Angestellter, Wissenschaftlicher Assistent und Akademischer Rat; 1969 - 1972 Mitglied einer Forschungsgruppe des Europarates in Straßburg zur Organisierten Kriminalität in Europa; 1972 zweites juristisches Staatsexamen; 1973 Promotion zum Dr. jur. in Tübingen; 1975 Habilitation für die Fächer Kriminologie, Jugendstrafrecht, Strafvollzug und Strafprozessrecht, Wissenschaftlicher Rat und Professor der Universität Bielefeld; 1977 Ordentlicher Professor der Universität Hamburg; 1977 - 1980 Direktor des Seminars für Jugendrecht und Jugendhilfe der Universität Hamburg, zugleich Richter am zweiten Strafsenat des Hanseatischen Oberlandesgerichts; 1980 Ordinarius der Universität Heidelberg; 1980 - 1986 Direktor des Instituts für Kriminologie der Universität Heidelberg; 1986 - 2011 Ordinarius an der Juristischen Fakultät der Universität Tübingen und Direktor des Instituts für Kriminologie; seit 1. Oktober 2011 emeritiert.
Gastprofessuren: Southampton und Cambridge (England), Peking (VR China), Philadelphia (Pennsylvania, USA) und Melbourne (Australien); außerdem für fünf Jahre Mitglied im wissenschaftlichen Ausschuss des European Committee for Crime Problems des Europarates in Straßburg als Vertreter für die Bundesrepublik Deutschland.
Ehrenpräsident auf Lebenszeit der Internationalen Gesellschaft für Kriminologie in Paris;
Mitgliedschaften: Mitglied in verschiedenen deutschen, europäischen und internationalen Gesellschaften, z.B. Kriminologische Gesellschaft, European Society of Criminology, World Society of Victimology, International Society for Criminology; Mitglied der Forschungsgruppe Täter-Opfer-Ausgleich; Vorsitzender der Deutschen Stiftung für Verbrechensverhütung und Straffälligenhilfe.

72074 Tübingen, Melanchthonstraße 18