Sicherheit in einer offenen und digitalen Gesellschaft

Lage – Herausforderungen – mit einem Bericht zur 64. Herbsttagung des Bundeskriminalamtes

Von LKD a.D. Ralph Berthel, Frankenberg/Sa.[1]

Die 64. Herbsttagung des Bundeskriminalamtes (BKA) kehrte nach vier Jahren des Ausweichens nach Mainz bzw. Ingelheim am 21. und 22. November 2018 an altbekannte Stätte nach Wiesbaden zurück.[2] Das BKA hatte die Veranstaltung unter das Leitthema „Sicherheit in einer offenen und digitalen Gesellschaft“ gestellt. Neben den Vorträgen renommierten Rednerinnen und Redner aus Politik, Polizei, Wissenschaft und Wirtschaft war die Veranstaltung auch im vergangenen Jahr Treffpunkt für den Austausch von Praktikern aus dem Feld der inneren Sicherheit. Der Beitrag will eine Auswahl der wichtigsten Themen der Tagung widerspiegeln und dem Leser gleichzeitig Anregung sein, sich noch tiefgründiger mit den Dokumenten der Veranstaltung zu befassen.[3]

1 Vorbemerkungen

1.1 Sicherheit in der digitalen Welt

Das erste Element der BKA-Tagung bildete die sicherheitsrelevanten gesellschaftlichen Herausforderungen in der digitalen Welt ab. Im Bericht zur Lage in der IT-Sicherheit in Deutschland für das Jahr 2018[4] analysiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Bedrohungen Deutschlands, seiner Bürgerinnen und Bürger, sog. Kritischer Infrastrukturen[5] und seiner Wirtschaft im Cyber-Raum. Das BSI hebt dabei hervor, dass das Funktionieren empfindlicher Informationstechnologien und Kommunikationssysteme von einer leistungsfähigen Infrastruktur sowie von einer sicheren Energieversorgung abhängt. Diese Systeme seien die Basis für technischen Fortschritt und wirtschaftliche Entwicklung in der Bundesrepublik. Mit wachsender Komplexität der Systeme und fortschreitender Vernetzung aller Bereiche der Informationsgesellschaft nähmen allerdings auch die Risiken von Störungen und Angriffen sowohl von innen als auch außen zu.[6]

Das BSI kommt in seiner Analyse der IT-Sicherheitslage zu dem Schluss, dass die Gefährdungen im Berichtszeitraum im Vergleich zum Vorjahr vielfältiger geworden seien. Ein Beispiel dafür seien die Hardware-Sicherheitslücken wie Spectre/Meltdown und Spectre NG, die zu Beginn 2018 bekannt geworden waren. Im Jahr 2018 seien neue große Ransomware-Wellen ausgeblieben. Gleichwohl müsse Ransomware weiterhin als massive Gefährdung eingestuft werden. Dies zeigten die Angriffe in der zweiten Jahreshälfte 2017 mit der Ransomware Petya/NotPetya: Sie verursachten allein in der deutschen Wirtschaft Schäden in Millionenhöhe. Auch würden immer neue Ransomware-Familien bekannt wie z.B. Bad Rabbit. In diesem Bereich bestehe also kein Anlass für eine Entwarnung. Insgesamt sei die Anzahl an Schadprogrammen weiter auf mittlerweile ca. 800 Millionen gestiegen. Pro Tag kämen rund 390.000 neue Varianten hinzu. Im Mobil-Umfeld existierten bereits mehr als 27 Millionen Schadprogramme allein für Google Android. Weiter heißt es im IT-Sicherheitslagebild, dass nach wie vor eine hohe Dynamik der Angreifer bei der Weiterentwicklung von Schadprogrammen und Angriffswegen zu verzeichnen sei, was hohe Aufmerksamkeit und Flexibilität zur Gewährleistung der Informationssicherheit erfordere. Und man habe eine neue Qualität von Schwachstellen in Hardware festgestellt, die ohne einen Austausch der Hardware nicht vollständig geschlossen werden könnten. Gleichzeitig, so das BSI weiter, befände man sich erst am Anfang einer Ära der Digitalisierung, die den Alltag der Menschen und der Gesellschaft insgesamt umfassend beeinflussen werde.[7]

1.2 Attacken auf deutsche Industrie verursachten 43 Milliarden Euro Schaden

In einer Studie kommt der Digitalverband Bitkom zu dem Ergebnis, dass Industrieunternehmen von IT-Attacken besonders stark betroffen seien. Durch Sabotage, Datendiebstahl oder Spionage sei der deutschen Industrie in den vergangenen beiden Jahren ein Gesamtschaden von insgesamt 43,[4] Milliarden Euro entstanden. Sieben von zehn Industrieunternehmen ([68] Prozent) seien in diesem Zeitraum Opfer entsprechender Angriffe geworden. *„Mit ihren Weltmarktführern ist die deutsche Industrie besonders interessant für Kriminelle*“, erklärte Bitkom-Präsident Achim Berg bei der Vorstellung dieser Studie in Berlin. *„Wer nicht in IT-Sicherheit investiert, handelt fahrlässig und gefährdet sein Unternehmen.“* So wurden in den vergangenen zwei Jahren bei einem Drittel der Unternehmen ([32]%) IT- oder Telekommunikationsgeräte gestohlen, bei fast einem Viertel ([23]%) seien sensible digitale Daten abgeflossen. *„Illegaler Wissens- und Technologietransfer, Social Engineering und auch Wirtschaftssabotage seien keine seltenen Einzelfälle, sondern ein Massenphänomen“,* betonte der damalige Vizepräsident des Bundesamtes für Verfassungsschutz (BfV), Thomas Haldenwang.[8] Fragen der IT-Sicherheit und der Vorbeugung und Bekämpfung entsprechender Angriffe auf die IT-Infrastruktur haben daher seit geraumer Zeit den Charakter einer Herausforderung von gesellschaftlichem Rang erlangt, die einerseits die Sicherheit in der Wirtschaft und deren internationale Konkurrenzfähigkeit unmittelbar betreffen und andererseits die innere Stabilität der Bundesrepublik nicht unmaßgeblich betrifft, denkt man nur auf IT-Angriffe auf kritische Infrastrukturen.

1.3 Sicherheit und offene Gesellschaften

Das zweite Element der Tagung bildeten, die bereits 1945 von dem Philosophen Karl Popper in seinem Buch *„Die offene Gesellschaft und ihre Feinde“* (Original: *„The Open Society and Its Enemies“*) beschriebenen sog. offenen Gesellschaften. Diese hatte Popper als Gegenentwurf zu geschlossenen Gesellschaften, die ideologisch festgelegt seien und einen für alle verbindlichen Heilsplan verfolgten, entworfen. Sie seien nach seiner Überzeugung dadurch gekennzeichnet, dass willensfreie Individuen, den Lauf der eigenen Geschichte in einem pluralistischen und fortwährenden Prozess von Verbesserungsversuchen und Irrtumskorrekturen selbst bestimmen würden. Ohne an dieser Stelle einen philosophischen Exkurs anstrengen zu wollen, sei allerdings angemerkt, dass das Konstrukt des *„selbst bestimmt agierenden Menschen“* gerade im digitalen Zeitalter, dem wir u.a. Begriffe wie *„Fake News“* und *„postfaktische Politik“* verdanken und die handlungsleitend für Massen von Menschen wurden, wohl mehr denn je hinterfragt werden kann und muss. Wie manipulativ gerade soziale Medien wirken und wie *„selbstbestimmt“* wir Menschen noch sind, wurde an verschiedener Stelle der Tagung deutlich.[9] Die Verknüpfung beider gedanklichen Säulen der Tagung erfolgte allerdings nur bedingt; wäre vielleicht auch nicht zielgruppenadäquat gewesen.

2 Die digitale Welt und wie (panisch) die Menschen reagieren

Yvonne Hofstetter, Geschäftsführerin der Teramark Technologies GmbH, griff in ihren Ausführungen zu Beginn der Tagung genau den Teil der Digitalisierung auf, der die Manipulierbarkeit der Menschen und die Wirkzusammenhänge zwischen sozialen Medien und menschlichen Verhaltensmustern betrifft. Sie bezog sich dabei auf eine Amoklage vom 22. Juli 2016 in einem Münchner Einkaufszentrum und die sich daran anschließende Auswertung der Münchner Polizei zu den Reaktionen der Menschen in den sog. sozialen Medien. Dabei wurde konstatiert, dass 4.310 Notrufe eingegangen waren, davon waren 310 Mitteilungen über Terroranschläge an 71 verschiedenen Tatorten, an Phantomtatorten. Der Begriff *„Phantomtatort“* sei eine Wortschöpfung der Münchner Polizei. Er bezeichne Angaben und Hinweise zu Tat- bzw. Ereignisorten, an denen tatsächlich keine Tathandlungen stattgefunden hatten, über die die Mitteilenden gleichwohl mehr oder weniger detailliert und glaubwürdig berichtet hatten. Diese Mitteilungen waren zumindest geeignet, polizeiliche Maßnahmen nach sich zu ziehen. Schwarmverhalten und Massendynamik hätten, so Frau Hofstetter, damals in München zu einer Massenpanik geführt. Einen ganz wesentlichen Anteil daran hätten die sozialen Netzwerke gehabt, betonte die Rednerin. Und eigentlich hätte es dafür weder aus der konkreten Lage noch aus der Sicherheitssituation in Deutschland insgesamt einen Grund für derartiges Verhalten gegeben. In der Folge ging die Rednerin der Frage nach, was mit unserer Gesellschaft geschehen sei, dass Menschen so emotional geworden seien und sich immer unsicherer fühlten.

2.1 Verunsicherung als Ursache jeglicher Sicherheitsdebatten?

Diese Verunsicherungen seien letztlich dafür verantwortlich, dass es überhaupt Auseinandersetzungen mit dem Thema Sicherheit in einer Gesellschaft gebe. Die Verunsicherungsthese von Frau Hofstetter darf bei nüchterner Betrachtung aktueller Forschungsergebnisse nicht unwidersprochen bleiben, wenngleich sicher der eine oder andere Besucher der Tagung und vielleicht auch Leser ihr beipflichten würde; aber da wären wir schon wieder beim Postfaktischen und nicht beim Bewiesenen.[10] Neben wissenschaftlichen Erkenntnissen zum Sicherheitsgefühl in Deutschland widerlegt auch der Umstand, dass da die Lageeinschätzungen der deutschen Sicherheitsbehörden natürlich auch und insbesondere die objektive Kriminalitätslage und nicht vordergründig das Sicherheitsgefühl der Bürger abbilden, gleichwohl jedoch zu dem Ergebnis gelangen, dass die Sicherheitslage angespannter als noch vor Jahren sei. Auch wenn man der Problemdarstellung der Rednerin nicht

uneingeschränkt folgen muss, waren ihre Erklärungsansätze für Verunsicherungen und Ängste der Menschen durchaus bemerkenswert.
Mit dem Internet of Everything steige, so Hofstetter, nicht nur die Zahl der Interaktionen zwischen den vernetzten Teilchen exponentiell an. Menschen interagierten mit noch mehr Menschen und mit Sachen. Und mittlerweile kommunizierten Sachen zudem mit anderen Sachen. Diese Wechselbeziehungen machten eine Gesellschaft hochkomplex. Als Merkmale solcher komplexer dynamischer Systeme führte die Rednerin folgende auf:

> Das Verhalten der Systeme sei nicht vorhersehbar und deshalb auch unsicher in Bezug auf die Zukunft. Der menschliche Wunsch nach Planbarkeit werde durch eine digitalisierte Gesellschaft also nicht erfüllt; vielmehr käme es zur Vervielfachung von Verunsicherungen.
>
> Komplexe dynamische Systeme tendierten gegen das Chaos. Chaos sei ein Systemzustand, in dem keine Ordnung, keine Strukturen und keine Verlässlichkeit herrschten. Je stärker eine Gesellschaft vernetzt sei, desto mehr systemische Unsicherheit entstünde und desto näher bewege sie sich in Grenzbereichen zum Chaos.

2.2 Demokratie braucht in der digitalen Welt Vertrauen

Frau Hofstetter schloss ihre Ausführungen mit der These, dass Sicherheit nicht im Gegensatz zur Freiheit stehe, Sicherheit nicht zu denken sei, ohne das Gefühl von Angst und sein Pendant Vertrauen. Kritisch äußerte sich die Rednerin zum Einsatz Künstlicher Intelligenz und/oder Big Data Analytics für die Polizeiarbeit. Sinnvoller sei es hingegen, auf gut ausgebildete und gut bezahlte polizeiliche Fachkräfte zu setzen. Die Erklärung, warum das eine nur alternativ zum anderen zu denken sei, blieb die Rednerin allerdings schuldig.

3 Lageerkenntnisse und Herausforderungen aus der Perspektive des BKA

Der Präsident der BKA, Holger Münch, thematisierte im Rahmen seiner Ausführungen sowohl phänomenologische Entwicklungen und Herausforderungen, aber eben auch Handlungsoptionen für die Polizeien im Zeitalter von Big Data, Algorithmen und autonomen Systemen. Dabei bezog sich der Redner auch auf die durch den Bundesminister des Innern, für Bau und Heimat Horst Seehofer im Rahmen der Tagung erhobenen Forderung, dass den Polizeien in der digitalen Welt die gleichen Befugnisse zustehen müssten, wie in der analogen.
An den Beginn seiner Ausführungen stellte der BKA-Präsident die Darstellung eines Sachverhaltes, bei dem Täter durch arbeitsteiliges Agieren mittels einer sog. DDos-Attacke ein konkurrierendes Unternehmen schädigen wollten. Beim Versuch, weltweit Router illegal in ein Botnetz zu integrieren, wurden auch Router in Deutschland angegriffen. Hier gelang der Angriff allerdings nicht, da die Router der Deutschen Telekom den Angriff abwehren konnten. Allerdings schalteten sie sich aufgrund der Attacke in einen sog. *„undefinierten Zustand“* und damit aus.
Die Folge war, dass ca. eine Millionen Router ausgefallen waren und zahlreiche Privatpersonen, Firmen und öffentliche Einrichtungen keinen Internet- und Telefonzugang hatten. Neben der Verletzlichkeit von IT-Infrastrukturen machten die Ausführungen des BKA-Präsidenten auch deutlich, dass weder die Bundesrepublik als Staat noch einzelnen Unternehmen wehrlos gegen derartige Angriffe sind.

3.1 Drei Dimensionen digitaler Straftaten

Durch rasches, abgestimmtes Handeln des BKA, des BSI und des angegriffenen Unternehmens sei, so Münch, die Identifizierung des Täters innerhalb weniger Wochen und kurze Zeit später dessen Festnahme in Großbritannien möglich gewesen. Der Fall verdeutliche, dass digitale Straftaten von drei Dimensionen charakterisiert würden:

> **Räumliche Dimension:** Die Grenzen von Staaten spielten hier, wie in vielen anderen Fällen, für den Täter keine Rolle. Entsprechend waren die Ermittlungen auch international.
>
> **Digitale Dimension:** Im vorliegenden Fall verfügte der Täter selbst über die für die Begehung der Taten erforderlichen IT-Kenntnisse. Doch um Cyberangriffe begehen zu können, müsse man kein Experte mehr sein; vielmehr könne man solche *„Dienstleistungen“* auch in der Underground Economy des Word Wide Web einkaufen, betonte der BKA-Präsident.
>
> **Gesellschaftliche Dimension:** Der Cyberangriff hatte Auswirkungen auf Millionen deutscher Haushalte, die zeitweilig ohne Internetzugang waren. Der Schaden betrug rund 2 Millionen Euro. Und zu den gesellschaftlichen Dimensionen gehört sicher auch die rechtspolitische Frage, ob die verhängte Strafe von einem Jahr und acht Monaten auf Bewährung den Unwertgehalt der Tat widerspiegelt und welches Signal die Verhängung einer solchen Strafe in die Gesellschaft sendet.

3.2 Kooperationen und Zukunftsfähigkeit der deutschen Polizeien

Formen der Zusammenarbeit, wie sie Münch zu Beginn seiner Ausführungen im Zusammenhand mit der Aufklärung des Angriffes mittels einer DDos-Attacke beschrieben hatte, stellte er in den Mittelpunkt seiner weiteren Darlegungen. Dabei bezog er sich sowohl auf die Erfordernisse der Kooperation zwischen den Polizeien als auch die Ausprägung spezieller Fähigkeiten einzelner Organisationen zum Nutzen der gesamten Polizeiorganisation.
Wenn von Zukunftsfähigkeit der Polizeien in Deutschland die Rede sei, müsse man den Blick nicht nur auf die Bekämpfung von Cybercrime richten. Vielmehr sollten auch die Formen der Zusammenarbeit der Polizeien im föderalen Rechtsstaat neu gedacht werden. Um einen modernen, intelligenten und damit auch erfolgreichen Föderalismus in der Polizei zu leben, müsse zu einer sinnvollen Arbeitsteilung und effektiveren Zusammenarbeit gefunden werden. Die tradierte föderale Arbeitsweise der Polizei, sei noch zu häufig geprägt vom obersten Verwaltungsgrundsatz *„§1: Jeder macht seins“* und stoße bei der Dynamik der Veränderung schnell an Grenzen.

3.3 BKA will Kompetenzen im Bereich Cyber-Gefahrenabwehr übernehmen

Globalen, digital vernetzen Gefahren könne man nicht mit lokalen Maßnahmen der Gefahrenabwehr begegnen. Münch forderte daher, dass Cyberabwehrbefugnisse nicht nur bei den Polizeien der Länder, sondern künftig auch beim Bund liegen müssten. Das BKA sei bereit und in der Lage, Verantwortung für die Gefahrenabwehr im Cyberraum zu übernehmen. Dabei könnten sich präventive Zuständigkeiten des BKA am Erfolgsmodell *„Präventivbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus“* und an den schon bestehenden Strafverfolgungskompetenzen des BKA im Bereich Cybercrime orientieren.
Münch sah daher eventuelle Zuständigkeiten BKA dann gegeben, wenn

- eine Bundeseinrichtung oder Kritische Infrastrukturen betroffen seien,
- eine länderübergreifende Gefahr bestehe
- oder wenn die Zuständigkeit einer Landespolizei nicht erkennbar sei bzw. ein Land das BKA um Übernahme des Falls ersuche.

3.4 Cyberkompetenzen des BKA werden ausgebaut

Unabhängig von der etwaigen Zuweisung von Gefahrenabwehrkompetenzen habe das BKA Weichen gestellt, um den dynamischen Entwicklungen im Cyberraum entsprechen zu können. Aufbauend auf den bereits vorhandenen Kompetenzen beabsichtige das BKA noch stärker in eigene Fähigkeiten, die technische Infrastruktur, Methodenkompetenz und das Personal zu investieren. Dazu stelle man sich organisatorisch neu auf. Im BKA werde eine eigene Abteilung zur Bekämpfung und – unter Vorbehalt der zu schaffenden rechtlichen Befugnisse – Abwehr von Cybercrime einrichten. In dieser Abteilung sollten künftig Ermittlungsverfahren der Cybercrime im engeren Sinne geführt werden, so Münch. Das war mehr als nur die Ankündigung einer neuen Organisationseinheit. Es war die Unterlegung der Forderung nach Kompetenzen im Gefahrenabwehrbereich mit Ressourcen, was den Ländern eine Teilaufgabe ihrer alleinigen Gefahrenabwehrzuständigkeiten in diesem Bereich schmackhaft machen sollte.
Abschließend erhob der BKA-Präsident die Forderung nach einer grundsätzlichen Neugestaltung der föderalen Polizei-Strukturen in der Bundesrepublik. Erforderlich seien in diesem Kontext,

- die Entwicklung einer gemeinsamen digitalen Plattform der deutschen Polizeien,
- eine neue Form von Arbeitsteilung bei der Entwicklung von Fähigkeiten sowie
- eine Bund-Länder-Zusammenarbeit, die Themenführerschaften festlege und damit schneller und agiler agieren könne.

4 Straf- und Strafprozessrecht müssen Schritt halten!

Der Frage, wie das deutsche Straf- und Strafprozessrecht weiterentwickelt werden muss, um mit den Entwicklungen im Cyberraum Schritt halten zu können, widmete sich der Stellvertretende Leiter der Strafrechtsabteilung beim Hessischen Ministerium der Justiz, Rainer Franosch. Aus seiner Sicht seien insbesondere die folgenden vier Merkmale des digitalen Wandels für das Straf- und Strafprozessrecht von Bedeutung:

- Unkörperlichkeit,

Allgegenwärtigkeit,
Vernetzung und
Grenzenlosigkeit.

Im Rahmen seines prononcierten Redebeitrages stellte er sowohl den Ist-Stand und damit eine Reihe von Regelungslücken als auch Handlungsoptionen des Gesetzgerbers dar. Beispielhaft seien seine Ausführungen zu aktuellen Cybercrime-Erscheinungsformen und den lückenhaften Schutz vor diesen im Kernstrafrecht kurz dargestellt:

Zunächst bezog sich Franosch auf eine Entscheidung des BVerfG aus dem Jahr 2008[11]. Darin heißt es: *„Der Einzelne kann […] Zugriffe zum Teil gar nicht wahrnehmen, jedenfalls aber nur begrenzt abwehren. Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann. Ein technischer Selbstschutz kann zudem mit einem hohen Aufwand oder mit Funktionseinbußen des geschützten Systems verbunden sein. Viele Selbstschutz-möglichkeiten – etwa die Verschlüsselung oder die Verschleierung sensibler Daten – werden überdies weitgehend wirkungslos, wenn Dritten die Infiltration des Systems, auf dem die Daten abgelegt worden sind, einmal gelungen ist. Schließlich kann angesichts der Geschwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognostiziert werden, welche Möglichkeiten dem Nutzer in Zukunft verbleiben, sich technisch selbst zu schützen.“* Fransoch leitete daraus die Forderung ab, dass das Strafrecht den lückenlosen Schutz auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sicherzustellen habe. Dieser Schutz werde im Kernstrafrecht derzeit im Wesentlichen durch die §§ 202a (Ausspähen von Daten), 303a (Datenveränderung) und 303b (Computersabotage) StGB gewährt: Das geschehe allerdings nur lückenhaft. So betreffe § 202a StGB nur das Ausspähen solcher Daten, die durch eine besondere Zugangssicherung geschützt sind. Zudem greife diese Norm nur dann, wenn der Täter unter Überwindung der Zugangssicherung handele. Datenausleitung über voreingebaute Hardwarebauteile sei von § 202a StGB jedoch nicht erfasst, da von Anfang an keine Zugangssicherung gegeben sei. Aktuelle Modi Operandi von Cybercrime-Delikten wie z.B. der Einsatz von Hardwaretrojanern oder von vorinstallierter Malware sowie die unbefugte Benutzung von Computern mittels Java-Script zum Erzeugen von Kryptowährungseinheiten würden durch die bestehenden Strafnormen nur unvollständig erfasst.
Auch mit aus seiner Sicht dringend gebotenen Gesetzesänderungen im Bereich des Strafprozessrechts setzte sich der Redner auseinander. Dabei forderte er insbesondere, den Straftatenkatalog des § 100a Abs. 2 StPO um – überwiegend noch zu schaffende – qualifizierte Begehungsweisen der §§ 202a, 202b, 202c, 202d und 303a, 303b StGB zu erweitern.
Nicht zuletzt verwies Franosch darauf, dass im Zusammenhang mit der Problematik der Flüchtigkeit von Daten die Vorgaben von Art. 16 (Umgehende Sicherung gespeicherter Computerdaten) und 17 (Umgehende Sicherung und teilweise Weitergabe von Verkehrsdaten) der Cybercrime Convention[12] zur umgehenden Sicherung von Computerdaten umzusetzen sei und das Instrument einer Sicherungsanordnung in der Strafprozessordnung verankert werden müsse.

5 Perspektiven unterschiedlicher Akteure auf das Themenfeld IT-Sicherheit in einer Gesellschaft

Diese Perspektiven beleuchteten auch weitere Referenten. Zu ihnen gehörten die Exekutivdirektorin von EUROPOL, Catherine De Bolle, der Leiter der Abteilung Zentrales Informationsmanagement des BKA, Jürgen Ebner sowie für externe Partner der Vorstand für Datenschutz, Recht und Compliance bei der Deutschen Telekom AG, Dr. Thomas Kremer, Stephan Micklitz, Director of Enginieering Google Germany gmbH und der Präsident des BSI, Arne Schönbohm.

6 Der Mensch wird auch im digitalen Zeitalter die Basis für den Erfolg bleiben“[13]

6.1 Die VUCA-Welt

Digitalisierung bedeutet Veränderung; Veränderung in einem bisher nicht gekannten Ausmaß und mit rasanter Geschwindigkeit. Die Redner im letzten Teil der Tagungsabfolge setzten sich insbesondere mit dem Managen von Veränderungsprozessen und dem Faktor Mensch[14] auseinander.
Der Organisations- und Managementberater Dr. Klaus Doppler kennzeichnete zu Beginn seiner Ausführungen die aktuelle Entwicklung mit dem Begriff der sog. VUCA-Welt. Diese sei geprägt durch die Faktoren

volatility (Volatilität), d.h. Instabilität, Flüchtigkeit,
uncertainty (Unsicherheit),
complexity (Komplexität) und

ambiguity (Ambiguität), also Mehr- bzw. Doppeldeutigkeit.

Alle Menschen seien mit nicht kalkulierbaren Entwicklungen, ob technologischer, wirtschaftlicher, gesellschaftlicher und/oder politischer Natur, konfrontiert. Das Gelingen von Veränderungsprozessen sei von erfolgskritischen Faktoren abhängig, die Absolventen polizeilicher Studiengänge aus der Befassung mit Projektmanagement durchaus bekannt sein dürften:

Abklären bzw. Festlegen der Ziele

Ganzheitliche Projektarchitektur

Beteiligung der Betroffenen

Widerstands- und Konfliktmanagement

Von der einseitigen Information zur echten Kommunikation im Dialog

Emotionale Wetterkarte parallel zur sachlichen Entwicklung.

6.2 Lebzeitverbeamtung vs. modernes Personalmanagement?

Prof. Dr. Jürgen Weibler, Professor für Betriebswirtschaftslehre an der Fernuniversität Hagen, hob hervor, dass erfolgreiche Unternehmen und Institutionen nicht nur die eigene Organisation digital *„aufstellten“.* Die erfolgreichen wüssten auch, dass sie auf eine jüngere Generationen träfen, deren Zuspruch sie benötigten und deren Erwartungen sie gleichzeitig zu berücksichtigen hätten. Diese hätten also erkannt, dass sie attraktive Arbeits- und Lebensbedingungen schaffen müssten. Hier hätte sich nicht nur der Verfasser gewünscht, dass der Saal mit Leitern von Personalbereichen in den Polizeien gefüllt gewesen wäre. Wenn in einigen Amtsstuben die Innovationsbereitschaft beim Verweis auf die hergebrachten Grundsätze des Berufsbeamtentums endet und die Lebzeitverbeamtung als das *„Non plus ultra“* der Motivation postuliert wird, fällt der optimistische Blick in die Zukunft bisweilen schwer.
Elmar Vaher, Leiter der estnischen Polizei- und Grenzschutzbehörde, stellte in seinem Vortrag die Herausforderungen und Chancen des Technikeinsatzes bei der Polizeiarbeit und die dabei in Bezug auf das Management gesammelten Erfahrungen der estnischen Polizei und des Grenzschutzes dar.
Fast zum Abschluss der Tagung stellte Thomas Model, Leiter der Akademie der Polizei Hamburg, tradierten Mustern der Personalgewinnung erfrischend neue Ideen gegenüber. Er kritisierte, dass es den Polizeien gegenwärtig an validen Anforderungs- und Kompetenzprofilen fehle. Hier müsse schnell nachgearbeitet werden, um diese in die Auswahlverfahren einzubringen. In diesen wiederum müsse, so Model, neben der fachlichen und persönlichen Eignung der angehenden Nachwuchskraft vor allem die Frage beantwortet werden, wie die Passung der Person zum Unternehmen festzustellen sei.

7 Fazit

Auch die 2018-er Ausgabe der BKA-Herbsttagung griff wieder hochaktuelle Themen der gesellschaftlichen Entwicklung und deren Konsequenzen für die innere Sicherheit auf. Erneut gelang es dem BKA, renommierte Rednerinnen und Redner aus Politik, Polizei, Wissenschaft und Wirtschaft zu gewinnen, die eine Vielzahl von Perspektiven auf das Leitthema einbrachten und neben den Diskussionsbeiträgen und Fragen aus dem Auditorium für zwei interessante und sehr lebendige Tage in Wiesbaden sorgten.

Anmerkungen

1. Leitender Kriminaldirektor a.D. Ralph Berthel studierte Rechtswissenschaften an der Humboldt-Universität zu Berlin. Von 2001 bis 2005 war er Dozent für Kriminalistik an der damaligen PFA in Münster-Hiltrup (heute: DHPol). Von 2005 bis 2013 leitete er die Hochschule der Sächsischen Polizei (FH) in Rothenburg/O.L. und unterrichtete Kriminalistik im Masterstudiengang „Öffentliche Verwaltung – Polizeimanagement“. Von 2013 bis 2015 leitete er das Projekt „Die sächsische Polizei im digitalen Zeitalter - Die Nutzung von sozialen Netzwerken und von Mobilfunk-Applikationen (Polizei-App) durch die sächsische Polizei (DigiPol)“. Von 2015 bis Anfang 2019 war Ralph Berthel Abteilungsleiter im LKA Sachsen. Er ist Ehrenprofessor (Pocetnyi Professor) der Belgoroder Juristischen Hochschule des Ministeriums des Innern Russlands und Dozent im Masterstudiengang Kriminologie, Kriminalpolitik und Polizeiwissenschaft an der Ruhr-Universität Bochum. Der Autor ist Gründungsmitglied der Deutschen Gesellschaft für Kriminalistik e.V. Erreichbarkeit: ralph-berthel@web.de.
2. Die Herbsttagung 2018 fand in dem im April 2018 neu eröffneten RheinMain-CongressCenter in Wiesbaden statt. Damit stand ein Haus mit exzellenten logistischen Voraussetzungen für die Veranstaltung zur Verfügung.

3. Das Programm der Herbsttagung, alle verfügbaren Redebeiträge sowie Kurzstatements („Interviews“) der Referenten sind abrufbar (Stand: 22.12.2018) auf der Homepage des BKA (https://www.bka.de/DE/AktuelleInformationen/Publikationen/BKA-Herbsttagungen/2018/bka-herbsttagungen2018_node.html).

4. Im Bericht wird die Gefährdungslage der IT-Sicherheit in Deutschland im Zeitraum 1. Juli 2017 bis 31. Mai 2018 beschrieben.

5. „Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das Gemeinwesen. Ihre Systeme und Dienstleistungen, wie die Versorgung mit Wasser oder Wärme, ihre Infrastruktur und Logistik sind immer stärker von einer reibungslos funktionierenden Informationstechnik abhängig. Eine Störung, Beeinträchtigung oder gar ein Ausfall durch einen Cyber-Angriff oder IT-Sicherheitsvorfall kann zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen.“ BSI, Die Lage der IT-Sicherheit in Deutschland 2018, S. 10.

6. BSI, a.a.O., S. 3.

7. BSI, a.a.O., S. 91ff.

8. www.bitkom.org/Presse/Presseinformation/Attacken-auf-deutsche-Industrie-verursachten-43-Milliarden-Euro-Schaden.html, Abruf: 22.12.2018.

9. Vgl. etwa Ausführungen von Y. Hofstetter sowie S. Vosoughi, D. Roy, S. Aral, The spread of true and false news online, Science 09 Mar 2018, science.sciencemag.org/content/359/6380/1146, Abruf: 9.12.2018. Die Autoren stellen darin die Ergebnisse von Untersuchungen zu „Gerüchtkaskaden“ auf Twitter im Zeitraum von 2006 bis 2017 dar. Folgende Feststellungen konnten sie treffen:
   • Etwa 126.000 Gerüchte wurden von 3 Millionen Menschen verbreitet.
   • Falsche Nachrichten erreichten mehr Menschen als die Wahrheit.
   • Die obersten 1% der falschen Nachrichtenkaskaden verbreiteten sich zwischen 1.000 und 100.000 Menschen, während die Wahrheit selten bei mehr als 1.000 Menschen verbreitet wurde.
   • Die Studie kommt auch zu dem Schluss, dass die Falschheit nicht nur mehr Menschen erreiche, sie verbreitete sich auch schneller als die Wahrheit.
   • Verantwortlich dafür machten die Autoren sowohl die Emotionalität der Menschen auch deren Drang nach Neuem.
   • „Der Grad der Neuheit und die emotionalen Reaktionen der Empfänger können für die beobachteten Unterschiede verantwortlich sein“, so die Hypothese der Forscher.

10. Die These von Frau Hofstetter wird durch die Ergebnisse aktueller Untersuchungen zum Sicherheitsempfinden der Deutschen nicht bzw. nur sehr eingeschränkt gestützt. Vgl. www.lebendige-stadt.de/pdf/Forsa-Umfrage.pdf. Danach fühlen sich knapp 90 % der Befragten sicher. Zu ähnlichen Ergebnissen kommt die Kriminologische Forschung und Statistik (KFS) des LKA Niedersachsen in der Befragung zu Sicherheit und Kriminalität in Niedersachsen 2017. Vgl. www.lka.polizei-nds.de/forschung/dunkelfeldstudie/dunkelfeldstudie---befragung-zu-sicherheit-und-kriminalitaet-in-niedersachsen-109236.html, Abruf: jeweils am 9.12.2018.

11. BVerfG v. 27.2.2008, 1 BvR 370/07, 1 BvR 595/07-juris.

12. Vgl. dazu Gesetz zu dem Übereinkommen des Europarats vom 23. November 2001 über Computerkriminalität vom 5. November 2008, BGBl. 2008, II S. 1254f., www.bgbl.de/xaver/bgbl/start.xav.F%2F*%5B%40attr_id%3D%27bgbl208s1242.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl208s1242.pdf%27%5D__1544693879769, Abruf: 13. Dezember 2018.

13. H. Augustin, TRANSFER, Online Magazin des Steinbeis-Verbundes, transfermagazin. steinbeis.de/? p=2836, Abruf: 13.12.2018.

14. Unter dem Begriff „Menschlicher Faktor“, „Faktor Mensch“ oder „Human Factor“ versteht man Interaktionen zwischen Menschen, technischen Komponenten, Umwelten und organisationalen Bedingungen in aufgabenbezogenen sozio-technischen Systemen. Das Wissen darum schließt Erkenntnisse der Psychologie, der Arbeitswissenschaft und der Bewegungswissenschaft einschließlich ihrer experimentellen, diagnostischen und sozialwissenschaftlichen Methoden sowie ausgewählter Gebiete der Ingenieurwissenschaften und der Informatik ein. Mittlerweile existieren Studiengänge (Etwa Master of Science [M.Sc.] Human Factors an der Technischen Universität Chemnitz), die sich den Fragen der Mensch-Technik-Interaktionen widmen. (Vgl. www.tu-chemnitz.de/hsw/studium/humanfactors/studieninhalte/index.php, Abruf: 23.12.2018).

© Verlag Deutsche Polizeiliteratur