„Digitalisierung: Herausforderung und Chance für Sicherheit, Lagebeurteilung und Resilienz"

von Dr. Markus Hellenthal

Senior Vice President
Geschäftsleiter Öffentlicher Sektor
Capgemini Deutschland
Gustav-Heinemann-Ufer 72a
D-50968 Köln
E-Mail: markus.hellenthal@capgemini.com

Vortrag anlässlich der Berliner Sicherheitskonferenz, dem Kongress zur Europäischen Sicherheit und Verteidigung am 29./30. November 2016 in Berlin (Vortragsslot: 30. November 2016, 10:25 Uhr)

„Perception is reality“ – Wahrnehmung kreiert Wirklichkeit. Diese beschreibt sehr gut, in welchem Umfeld wir heute sicherheitspolitische Herausforderungen diskutieren müssen.

Warum ist das so?

1. Sicher geglaubte Realitäten sind ins Taumeln geraten; denken wir an den Brexit, den Wahlsieg von Trump, den Ukraine-Konflikt, die Entwicklungen in der Türkei, die Infragestellung internationaler Bündnisse und massive geopolitische Verschiebungen im asiatisch-pazifischen Raum.
2. Gleichzeitig werden Wahrheiten gezielt interpretiert und manipuliert und parallele Scheinwirklichkeiten über die sozialen Medien geschaffen. Bürgerinnen und Bürger ein und derselben Nation - denken wir an die Spaltung der USA während des US Wahlkampfes oder die Wahrnehmung der Zuwanderung in Deutschland – oder ganze Regionen – zum Beispiel der Russland Ukraine Konflikt – scheinen in völlig unterschiedlichen Wirklichkeiten zu leben, gefüttert über gezielte Desinformationen. Untersuchungen zeigen, dass viele Nutzer von sozialen Medien gar nicht in der Lage sind, echte Informationen von falschen zu trennen.

3. Und nicht zuletzt werden wir mit grausamen Wirklichkeiten konfrontiert, die wir lange relativ gut ausblenden konnten: der mit Hilfe von verschlüsselter Kommunikation befeuerte internationale Terrorismus und der Cyber-Terrorismus bedrohen uns und sind im sicher geglaubten Europa angekommen; die gewaltigen Migrationsbewegungen nach und in Europa zeigen uns die Folgen von Globalisierung, Klimawandel, gescheiterten Nationenbildungen in der arabischen Welt, Krieg und Flucht direkt vor unserer Haustür.

Angesichts dieser Herausforderungen gilt es, die freiheitlich-demokratischen und rechtstaatlichen Grundlagen der Europäischen Union, ihrer Mitgliedstaaten und deren Gesellschaften wieder zu stärken und auszubauen, und dem elementaren Anspruch eines Rechtstaates gerecht zu werden: Innere und Äußere Sicherheit als genuinen Wert zu schaffen und zu erhalten und dabei die legitimen objektiven und subjektiven Sicherheitsbedürfnisse der Menschen wirksam und nachhaltig zu adressieren.

Die im wahrsten Sinne des Wortes notwendige Wirkungsorientierung staatlichen Handelns, wie sie auch prominent im neuen Weißbuch der Bundeswehr gefordert

wird, muss folglich beide Aspekte berücksichtigen, ebenso wie die bekannte Tatsache, dass einzelne Akteure der Inneren und Äußeren Sicherheit die angestrebte Wirkung nicht alleine erzielen können. Sicherheit ist ein nur gemeinsam zu schaffender Wert aller in einem Staat oder einer Staatengemeinschaft tätigen Beteiligten.

Für Deutschland kommt sozusagen erschwerend hinzu (auch wenn ich es persönlich als einen unglaublichen Reichtum empfinde), dass nur Russland und China mit jeweils 14 mehr Anrainerstaaten haben, als Deutschland; wir haben neun (9). Dazu kommen noch beträchtliche Meeresküsten. Ein bestimmendes Element unseres staatlichen, gesellschafts- wie wirtschaftspolitischen Selbstverständnisses sind daher unser guten Beziehungen zu unseren Nachbarn. Dies hat aber wiederum Relevanz in allen drei Perspektiven für die notwendig gemeinsamen Anstrengungen für Sicherheit im Innern wie im Äußeren.

Sicherheit und Mobilität in einer immer stärker - real wie virtuell - vernetzten Welt zählen mehr denn je zu den zentralen Herausforderungen, denen sich Staat, Politik, Gesellschaft, Industrie und Wissenschaft stellen müssen. Es ist ein Gemeinplatz, dass insbesondere bei terroristischen Bedrohungen sowie anderen Gefahren katastrophischen

Ausmaßes genauso wie Cybercrime weder rein national noch jeweils autark durch Bundes- oder Landespolizei oder die Streitkräfte und alleine mit herkömmlichen Einsatzmitteln die Sicherheit gewährleistet werden kann.

Für die Bundes- wie die Landespolizeien ebenso wie für die Bundeswehr – als Akteur in der Äußeren Sicherheit und als Unterstützungskraft im Inneren – sind funktionierende und sichere, homogene und interoperable IT-Systeme daher eine ganz elementare Voraussetzung zur Erfüllung ihres Auftrages. Gerade die Interoperabilität stellt alle Beteiligten der Sicherheitsarchitektur vor eklatante Herausforderungen. Dies gilt insbesondere für die Gefahren und Risiken, die der Cyberraum mit sich bringt.

Die Digitalisierung ist auch für die Bundeswehr eine wesentliche Aufgabe. Sie muss nutzen- bzw. wirkungsorientiert, innovativ und effizient vorgehen, denn:

- staatliche Einrichtungen sind Hochwertziele im Cyber- und Informationsraum,
- die IT der Bundeswehr muss bei höchster Verfügbarkeit im Einsatz extremen Umweltbedingungen standhalten und zudem autark und mobil eingesetzt werden können,

- die Bundeswehr muss mit der NATO und ihren Bündnispartnern nahtlos zusammenarbeiten, und
- die Bundeswehr muss als Unterstützungskraft genauso nahtlos und integriert mit den zivilen Sicherheitsorganen des Bundes und der Länder zusammenarbeiten.

Ich möchte drei ganz praktische, fast operative Beispiele hervorheben, die zu einer positiven Wirkung auf die subjektive und objektive Sicherheit in Deutschland und Europa beitragen können. Sie sind als Forderung allesamt nicht wirklich neu und gehen m.E. über die bereits bestehenden Zusammenarbeitsplattformen wie das Gemeinsame Zentrum für Terrorismusabwehr, das Maritime Sicherheitszentrum oder auch das nationale Cybercrime Abwehrzentrum deutlich hinaus.

Mit der Digitalisierung und geeigneten IT-Plattformstrategien können durchgängige Informationsarchitekturen geschaffen werden. Damit bietet sich heute die große Chance, wesentliche Fortschritte für die Sicherheit, die Prävention, eine gemeinsame und konsistente Lagebeurteilung und Resilienz von Staat und Gesellschaft wirksam anzugehen.

Die drei Beispiele sind:

1) Eine nahtlose, integrierte praktische Zusammenarbeit der relevanten Sicherheitsorgane – sowohl in der Gefahrenvorsorge und -abwehr wie in der Strafverfolgung und militärischen Interaktion
2) Eine nahtlose, integrierte, gemeinsame relevante Lagedarstellung zur kontinuierlichen Lagebeurteilung und interdependenten Entscheidungsfindung
3) Eine wirkungsoptimierte und ressortübergreifende Interoperabilität mithilfe gesamtheitlicher Informationsarchitekturen, sicheren Cloud Services und einem Mobility First Ansatz, um das Ganze mit Leben zu erfüllen.

Vernetzte Sicherheit bedingt das Prinzip der Vernetzung von fähigkeitsorientierten, wirksamen Mitteln, die auf der Grundlage einer umfassenden relevanten Lagebeurteilung zielorientiert eingesetzt werden. Die Tatsache, dass das Grundgesetz das Instrument der Amtshilfe kennt, belegt, dass es auf die Quelle der Wirkmittel zunächst nicht ankommt.

Vernetzte Einsatzführung verfolgt vielmehr das Ziel, gerade durch eine als notwendig erkannte Vernetzung von Sensoren, Effektoren, Entscheidern und Akteuren die angestrebte Wirkung zu erzielen. Voraussetzung dafür sind

Vernetzbarkeit und Interoperabilität sowie die effektive und variable Nutzung gemeinsamer relevanter Informationen, um angemessene Entscheidungen in geeignet kurzen Zeiträumen treffen und zur Wirkung bringen zu können. Die Stichworte sind hier Big Data bzw. Data Analytics in Echtzeit.

Zudem hängt die Leistungsfähigkeit einer vernetzten Einsatzführung sowohl der militärischen wie der nicht-militärischen Sicherheitsorgane von der Vollständigkeit und Güte des Inputs aus Nachrichtengewinnung und Aufklärung ab. Das allein reicht aber nicht aus, sondern es gehören ausreichend leistungsfähige, zuverlässige und rund-um-die-Uhr verfügbare sichere IT-Services dazu. Diese wiederum müssen auf der Grundlage einheitlicher Standards und ganzheitlicher IT- bzw. Informationsarchitekturen möglichst vollständig interoperabel sein.

Und da Einsätze selten stationär und in der Regel mit verteilten Kräften ablaufen, ist es aus Gründen der Produktivität und Effizienz nur folgerichtig, die relevanten IT-Fähigkeiten über sichere Cloud Services und konsequent in erster Linie über mobile Endgeräte anzubieten.

Damit verbinde ich die Hoffnung, dass möglichst bald auch sichere Messenger-Dienste für Polizeivollzugsbeamte und

Soldaten verfügbar sein werden, ebenso wie eine wirkliche Breitbandkommunikation in der Fläche: Damit Informationen as a Service dann ressortübergreifend zur Verfügung stehen und abgerufen werden können, wenn sie benötigt werden.

Das muss alles nicht im Widerspruch zu einem effektiven Datenschutz sein. Herr Bundesinnenminister Dr. de Maiziere hat auf der BKA-Herbsttagung in der vorvergangenen Woche dargelegt, wie auch der Datenschutz sich angesichts der einerseits technischen Weiterentwicklung und andererseits aktueller Gefahren für Staat und Gesellschaft ebenfalls weiterentwickeln muss. Die Sicherheitsorgane müssen in die Lage versetzt werden, Sicherheit auch in Zeiten der Digitalisierung zu gewährleisten.

Dafür kann die schon angesprochene Plattform Informationsarchitektur Lageanalysten und Einsatzkräften in Fällen unmittelbarer Gefahr, wie z.B. im Falle des Amoklaufs in München, effizient unterstützen, indem sie beispielsweise eine zeitlich und örtlich beschränkte Nutzung aller beliebigen Sensordaten, wie z.B. Videokameras, zur Lagebeurteilung und Entscheidungsfindung erlauben könnte.

In dem Zuge hoffe ich auch sehr, dass die Initiative des Bundesinnenministers zu einer durchgängigen Plattformstrategie

und einheitlichen Informationsarchitektur bei den polizeilichen Fall- bzw. Vorgangsbearbeitungssystemen und Datensammlungen schnell erfolgreich umgesetzt wird.

Mit den heutigen Systemfragmenten und einer in Teilen immer noch erforderlichen händischen Synchronisierung wird es immer schwieriger, IT zuverlässig und sicher zu steuern. Zugleich wird es immer schwieriger, die personellen und finanziellen Mittel freizuschaufeln für die Erfüllung der eigenen Kernaufgaben, nämlich die Gewährleistung der objektiven und subjektiven Sicherheit der Bevölkerung.

Ähnlich ausbaufähig ist die Interoperabilität zwischen den Teilstreitkräften und ganz besonders zwischen militärischen und nicht-militärischen Sicherheitsorganen, wie die jüngsten Einsatzerfahrungen z.B. in München gezeigt haben.

In diesem Zusammenhang möchte ich allerdings auch die alte Erkenntnis in Erinnerung rufen, dass solche Einsätze ohne regelmäßige praktische Übungen nicht zuverlässig funktionieren. Das gilt verstärkt dann, wenn sie organisationsübergreifend erfolgen müssen, wie in der notwendig vernetzten Sicherheit.

Wichtig ist bei all dem, auch die Chancen von uns allen als Arbeitgeber auf einem zunehmend enger werdenden Bewerberfeld in den Blick zu nehmen. Wenn die Bundespolizei

und das BKA, die Bundeswehr und vielleicht auch die eine oder andere Landespolizei jetzt zum Teil massiv personell ausgebaut werden, begrüße ich das als Staatsbürger sehr. Personalgewinnung und -erhalt ist jedoch ein kontinuierlicher Prozess, bei dem es zu Beginn, aber auch fortlaufend darauf ankommt, als Arbeitgeber möglichst attraktiv zu sein und zu bleiben. Das ist einer der vornehmsten Führungsaufgaben.

Es ist heute aber nur noch schwer Kandidatinnen und Kandidaten oder später dann Kolleginnen und Kollegen zu vermitteln, dass die Nutzung moderner Kommunikations- und Kollaborationswerkzeuge nicht zur selbstverständlichen Grundausstattung eines attraktiven Arbeitgebers gehören sollen. Gerade Soldaten und Polizeibeamte sind i.d.R. aus persönlicher Überzeugung und ursprünglicher Begeisterung in den Polizei- beziehungsweise Soldatendienst eingetreten.

Den Slogan der Bundeswehr „Wir.Dienen.Deutschland.“ nehmen die allermeisten persönlich, das ist auch gut so. Das gilt sicherlich ebenso für die Angehörigen der Polizeien des Bundes und der Länder. Ich war selbst einer davon und fühle mich dem auch noch heute eng verbunden. Dafür schulden Staat und Gesellschaft den Sicherheitsbeamtinnen und -beamten nach meiner festen Überzeugung die bestmögliche und effektive Ausstattung.

Mein Plädoyer lautet daher: Mögen alle Akteure der vernetzten Sicherheit in derselben Lage leben und nahtlos zusammenarbeiten, so dass aus einem erweiterten Fähigkeitspotential die objektive und subjektive Sicherheit auch wirklich gewährleistet wird.

Ich möchten Vortrag schließen, indem ich meine Freunde darüber ausdrücke, dass ich hier heute als Vertreter der größten Unternehmensberatung europäischen Ursprungs sprechen darf, die mit über 180.000 Mitarbeiterinnen und Mitarbeitern für eine exzellente deutsch-französische Partnerschaft steht. Wir gehören weltweit zu den beliebtesten Arbeitgebern. In unserem östlichen Nachbarstaat Polen sind wir sogar zweitbeliebtester Arbeitgeber nach Google. Wir betreiben dort, gesteuert aus Deutschland, eigene Nearshore-Zentren für Anwendungsentwicklung, u.a. mit einem Fokus auf modernste mobile App-Entwicklungen und virtuelle Realität. Inzwischen haben wir in unseren polnischen Niederlassungen über 1.000 Mitarbeiterinnen und Mitarbeiter. Sie arbeiten in deutscher Sprache, auf einer deutschen IT-Infrastruktur und erfüllen deutsche Sicherheitsanforderungen. Über 100 Mitarbeiterinnen und Mitarbeiter davon arbeiten bereits für deutsche Kunden aus dem öffentlichen Sektor, mit einer erfreulich steigenden Tendenz.

Diese Attraktivität von Capgemini liegt u.a. an den spannenden Kundenprojekten, die wir durchführen dürfen. Oft sind die Aufgaben ganz nahe an vorderster Front der Geschäftsthemen unserer Kunden. Als Unternehmensberatung und IT-Systemhaus sind wir auf die Wirkung unserer Arbeit für unsere Kunden fokussiert. Diese Wirkung und damit unser Erfolg hängen ganz entscheidend davon ab, unsere Kunden und ihre Herausforderungen zu verstehen. Das gilt im Kontext dieser Konferenz ganz besonders für die maßgeblichen Akteure der Inneren und Äußeren Sicherheit.

Erst dadurch, dass wir gemeinsam mit unseren Kunden die Voraussetzungen, Rahmenbedingungen und Erfolgsfaktoren verstehen, unter denen sie arbeiten, entsteht aus unserer Sicht die Chance, echten und messbaren Mehrwert zu erzeugen. Das ist unser Antrieb.