Fall 2017

St.Gallen Business Review

Zukunft der Luft- und Raumfahrt

Dirk Hoke
CEO Airbus Defence and Space

Security Policy: Rules for Cyberspace

Wolfgang Ischinger
Chairman of the Munich Security Conference

The Digital Transformation of the Bundeswehr

Dr. Ursula von der Leyen
German Minister of Defence

SECURITY

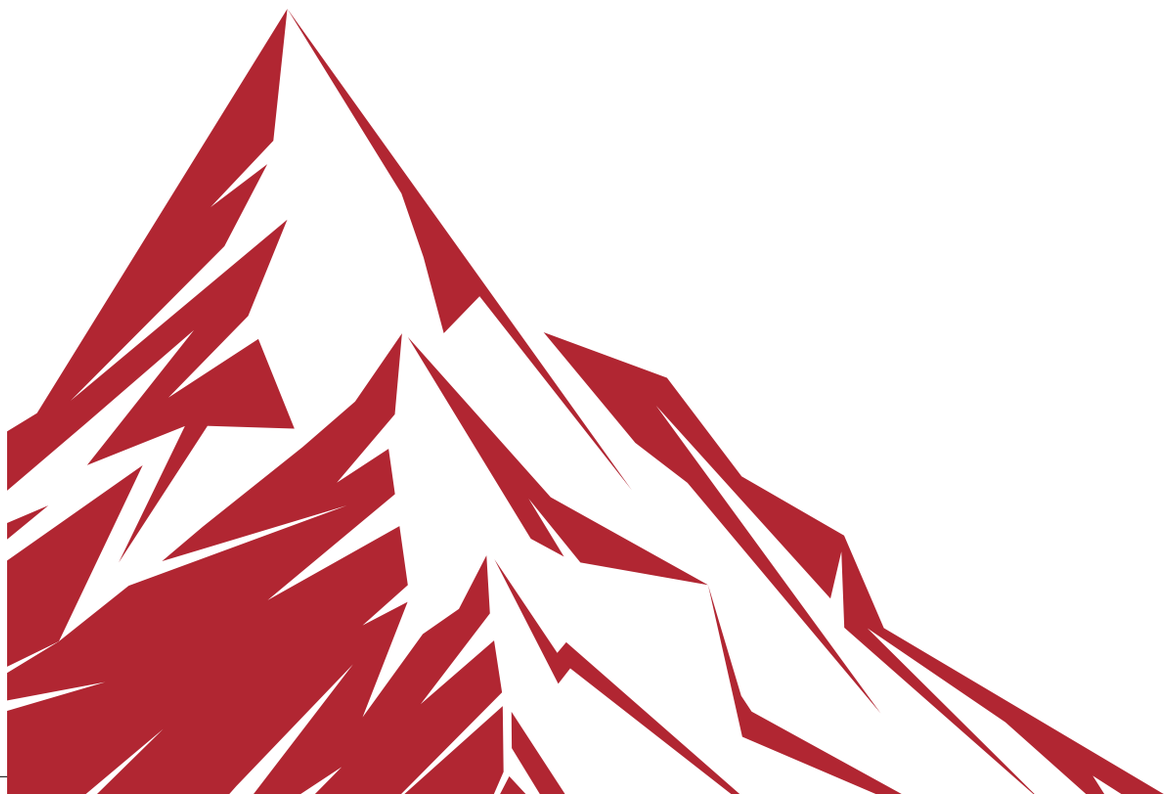
Defense_v6.indd 1 28.11.17 01:57

Gehen Sie den nächsten Schritt mit uns. ESPRIT St.Gallen Seit 1988.

ESPRIT St.Gallen - Die studentische Unternehmensberatung an der HSG.

Seit 1988 haben wir über **350 Beratungsprojekte** erfolgreich abgeschlossen. Unsere massgeschneiderten Lösungen reichen von **Marketingkonzepten** über Umfragen bis hin zu **Wettbewerbsanalysen** für eine neue **Wachstumsstrategie**.

www.espritsg.ch • info@espritsg.ch • +41 71 220 14 01



St.Gallen esprit

Defense_v6.indd 2 28.11.17 01:57

Beloved readers,

Security affects every single individual on this planet. It belongs to one of the most fundamental and basic needs of the human being. However, this desire of safety cannot always be granted. Especially over the past few years, in the wake of increased terrorist threats, the importance and demand of security in our society has increased immensely.

Meanwhile the rapid development of technology not only entails countless opportunities, however, new and yet undiscovered risks come along with it as well. Never before has access to computers been easier and as we start using the worldwide web, we begin to develop an irreversible dependency on it. In this state of permanent connection, attackers use the complexity of IT systems to their favour and put individual users, companies as well as whole economies in distress. This phenomenon leads to the emergence of a complete separate branch of industry, focussing on cybersecurity and offering expertise in all pertinent areas around this hot topic.

Since 2014, attacks and assassinations in public places have been mounting in Europe. For many, this raises the question to what extent public safety can be granted. Furthermore, discussions on the dilemma between the duty of governmental protection of its population and the restriction of individual freedom have ignited. Nations often reach their limits when dealing with this challenge and already had to face harsh criticism due to some of their measures that were classified as unconstitutional and violating human rights.

The topic of security as a highly complex topic cannot be widely examined and covered in one single issue. Nevertheless, with our selection of articles, we can provide a comprehensive and multifaceted insight into the most recent and exciting areas of this topic.

As always much energy and passion have driven the new edition of the St.Gallen Business Review and we hope the given insights will excite and inspire. Enjoy reading!

Milan Schéda, Philipp Kreiner, Isabel Hoffet, Lars Decker, Niklas Zeller

Defense_v6.indd 3 28.11.17 01:57

6 **Zukunft der Luft- und Raumfahrt**

Dirk Hoke
CEO Airbus Defence and Space

11 **Enkeltrick am Telefon**

KOK Kratzer
Kriminalpolizeidirektion Freiburg im Breisgau

14 **Rules for Cyberspace**

Wolfgang Ischinger
Chairman of the Munich Security Conference

22 **Die Digitale Transformation**

Kai Grunwitz
Senior Vice President EMEA bei NTT Security

28 **The Digital Transformation of the Bundeswehr**

Dr. Ursula von der Leyen
German Minister of Defence

33 **Herausforderungen des polizeilichen Alltages**

Max Hofmann
Generalsekretär für den Verband
Schweizerischer Polizei-Beamter VSPB

Defense_v6.indd 4 28.11.17 01:57

A good governance 37

Jean-Michel Rousseau
Programme Manager at the Geneva Centre for the Democratic Control of Armed Forces (DCAF)

Die OSZE: Ein Champion der «Soft Security» 40

Hans Lüber
Botschaftsrat und Militärberater bei der Ständigen Vertretung der Schweiz bei der OSZE

Zukunftsmusik am Zürcher Flughafen 44

Ueli Zoelly, lic. iur.
Chef der Flughafenpolizei Zürich

Cyberrisiken ganzheitlich angehen 48

Rolf Thomas Jufer
Partner und Mitglied der Geschäftsleitung der Funk Insurance Brokers AG

Cyber risk is the «new normal» 54

Mark Carter
Managing Partner Risk Advisory, Deloitte in Switzerland
Klaus Julisch
Partner, Cyber Risk Services, Deloitte Switzerland

Mitarbeiter als Risikofaktor 58

Raphael Blatter
Information Security Officer bei Glencore International

Defense_v6.indd 5 28.11.17 01:57

Dirk Hoke
CEO Airbus Defence and Space

Zukunft der Luft- und Raumfahrt

Der traditionelle Markt für Luft- und Raumfahrt ist grossen Veränderungen unterworfen. Neben neuen Technologien treten Konkurrenten aus Asien oder dem Silicon Valley in den Markt ein und fordern die grossen Hersteller heraus. Im Interview spricht Dirk Hoke, CEO von Airbus Defence und Space über die neuen Anforderungen an die Produkte, Cyber-Bedrohungen und den Schwierigkeiten multinationaler Rüstungsprojekte.

Defense_v6.indd 6 28.11.17 01:57

In den letzten Jahren hat sich die Bedrohungslage stark verändert. Der Ukraine-Konflikt mit den Spannungen zwischen der NATO und Russland, aber auch die Bedrohung durch terroristische Gruppen haben zu Forderungen nach höheren Verteidigungsausgaben geführt. Wie wird sich die Nachfrage nach Ihren Produkten in den nächsten Jahren ändern und welches Anforderungsprofil müssen diese in Zukunft erfüllen?

Dirk Hoke: Das Sicherheitsbewusstsein ebenso wie das gefühlte Bedürfnis nach Sicherheit wird zunehmen. Wir befinden uns heute in einer Situation, in der mehr als ein Jahrzehnt in vielen Ländern zu wenig in das Thema Sicherheit investiert wurde und somit ein starker Nachholbedarf bei der Beschaffung und Instandsetzung im Verteidigungsbereich entstanden ist. Einer der Indikatoren ist das bekannte Zwei-Prozent-Ziel der NATO, das von 28 Mitgliedsstaaten derzeit lediglich fünf Nationen erfüllen. Die Ausgaben werden steigen, sie werden sich aber auch verändern. Zum einen wird es aufgrund der kleineren Armeen einen erhöhten Bedarf im Service- und Dienstleistungsbereich geben. Darunter fällt zum Beispiel die Wartung militärischer Flugzeuge. Zum anderen spielt die Digitalisierung auch in unserer Branche eine wichtige Rolle. Unsere Produkte werden intelligenter und vernetzungsfähiger werden, um sich auf schnell verändernde Bedrohungslagen optimal einstellen zu können.

Cyber-Angriffe werden im 21. Jahrhundert verstärkt eingesetzt und können erhebliche Schäden bei den betroffenen Staaten und Unternehmen verursachen. Airbus Defence and Space bietet Produkte und Lösungen auf dem Gebiet der Cyber-Security an. Wie können Unternehmen bei der Implementierung von Industrie 4.0 optimal unterstützt und Cyber-Bedrohungen verhindert werden?

Die Bedrohung durch Cyber-Attacken ist allgegenwärtig. Man kann nur die Schutzmauer erhöhen, aber einen vollständigen Schutz wird es nie geben. Mit den Chancen, die die «digitalen Fabriken» eröffnen, wachsen gleichzeitig auch die Risiken für die Unternehmen. Durch die starke Vernetzung werden Unternehmen, aber auch Behörden, anfällig für komplizierte Cyberattacken, die nicht – wie bisher – nur Teilbereiche infizieren, sondern sich aufgrund der Digitalisierung innerhalb der neuen, «smarten» Industrie weit ausbreiten. Das beginnt bei der Unterbrechung der Lieferkette und endet beim Diebstahl von Personaldaten oder der Manipulation von Konstruktionszeichnungen. Cybersicherheit hat sich bei Airbus somit vom reinen Selbstzweck zu einer bedeutsamen Geschäftsvoraussetzung entwickelt. Wir bieten heute massgeschneiderte Sicherheitskonzepte, die sich nahtlos in den bestehenden Produktionsprozess der Unternehmen einfügen lassen. Früher war man davon überzeugt, dass es genügt, die IT-Systeme von Verwaltung und Produktion zu trennen, um ausreichenden Schutz vor Cyberangriffen zu haben. In der Industrie 4.0 ist die Situation aber komplexer. Wichtig für unsere Kunden ist, sich darüber im Klaren zu sein, wo sie am leichtesten verwundbar sind. Nach dieser Analyse sind die Schutzmöglichkeiten dann breit gefächert. Das reicht bis zur Beobachtung der Netzwerke rund um die Uhr durch Spezialisten in unseren Cyber-Kontrollräumen.

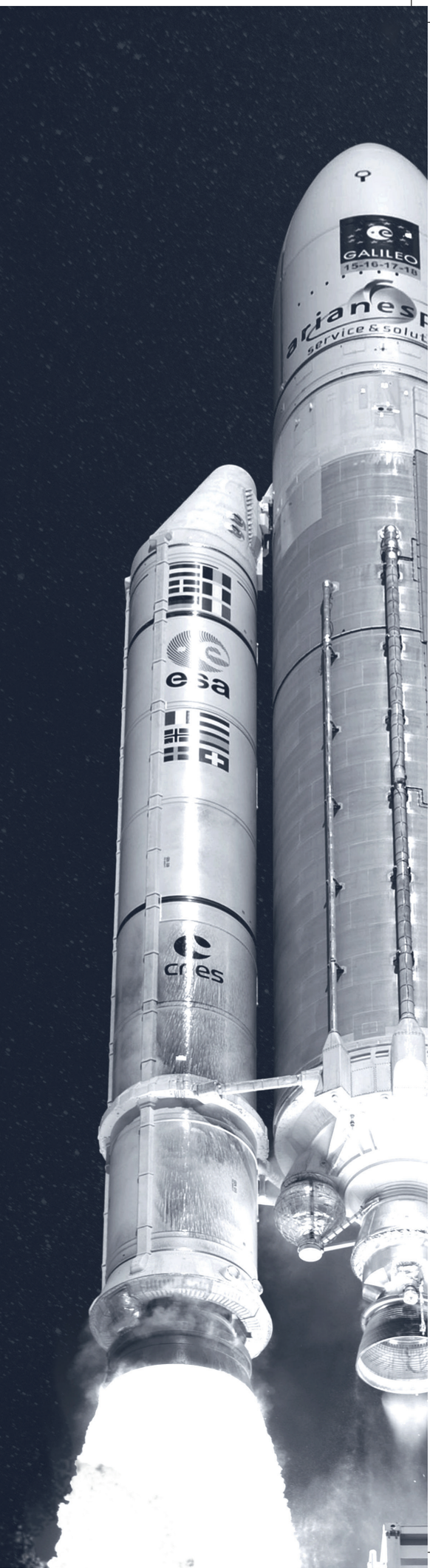
Defense_v6.indd 7 28.11.17 01:57

Die Auslieferung Ihres Militärtransporters A400M hat sich immer wieder verzögert und technische Probleme erschweren den Einsatz. Was sind die grössten Schwierigkeiten bei solchen Projekten und wie sieht der weitere Zeitplan bei der Auslieferung dieses Flugzeugtyps aus?

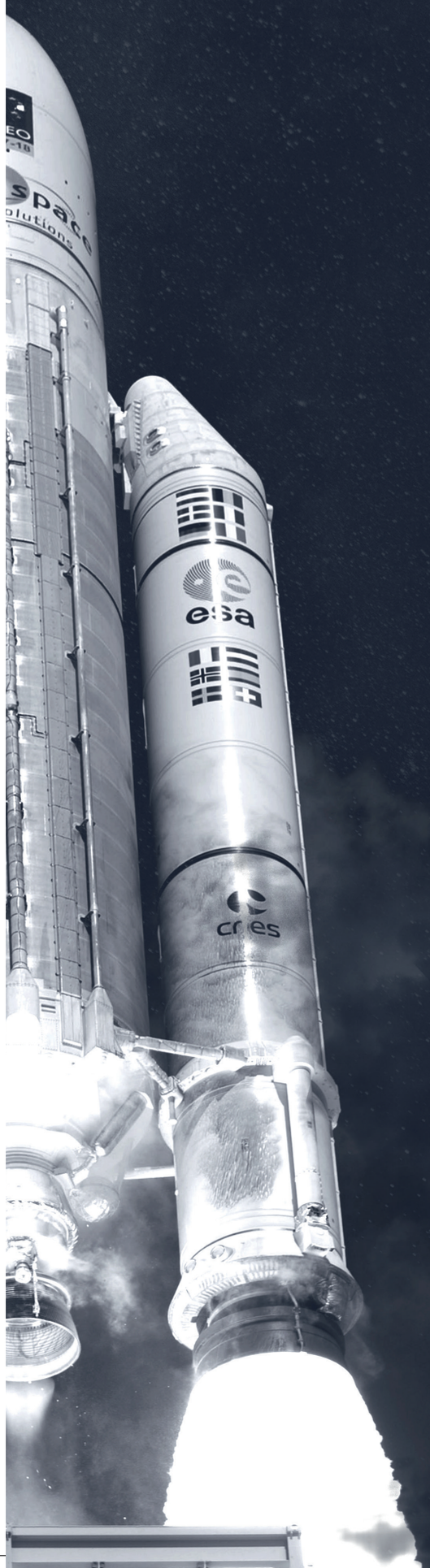
Ich möchte zunächst eines vorausschicken: Wir liefern unseren Kunden mit der A400M das beste und modernste Transportflugzeug der Welt. Und was die Auslieferungen anbelangt, so haben wir das Programm stabilisiert. Die A400M-Flotten der einzelnen Länder wachsen also kontinuierlich auf. Unser grundsätzliches Problem ist, dass wir bei A400M unter einem Vertrag leiden, der auf unrealistischen Annahmen sowohl auf Seiten der Käufernationen als auch der Industrie basierte. Die grössten Schwierigkeiten bei solchen grossen multinationalen Projekten entstehen dann, wenn aufgrund politischer Einflussnahme wirtschaftliche Gesetzmässigkeiten ignoriert werden. Das trifft für die Lieferplanung genauso zu wie für die Ausrüstung des Flugzeugs. Hier wurden bei der Vertragsunterzeichnung 2003 Fehler auf Seiten der Industrie und Politik gemacht, die wir in Zukunft vermeiden müssen. Was heisst das konkret für uns? Nur ein Beispiel dazu: Die Industrie muss bei Hochtechnologieprogrammen, die mitunter an die Grenze der Physik gehen, Partner gemäss ihrer Expertise aussuchen dürfen - und nicht nach Nationalproporz.

Nachdem lange Zeit der Markt für Grossraumflugzeuge von Airbus und Boeing dominiert wurde, hat besonders in China die Konkurrenz stark aufgeholt. Nachdem vor kurzem der chinesische Hersteller COMAC ein direktes Konkurrenzmodell zur A320-Familie präsentiert hat, stellt sich die Frage, wie Airbus seine Marktposition halten kann und welche Ziele im stark wachsenden chinesischen Markt verfolgt werden? Welchen Herausforderungen muss sich auch Airbus Defence and Space stellen, nachdem China mit der Entwicklung eigener Kampfjets begonnen hat?

China ist für unser ziviles Geschäft ein wichtiger Markt. Vierundzwanzig Prozent der Flugzeugauslieferung gehen derzeit in das Land. Unsere Experten bei Commercial Aircraft gehen davon aus, dass die Anzahl der Airbus-Flugzeuge bis 2020 auf über 2.000 Maschinen steigen wird. Ich glaube, dass wir auch in Zukunft in China sehr erfolgreich sein können. Zum einen haben wir über die letzten Jahre unsere eigene Fertigungslinie im Land aufgebaut. Zum anderen sind wir ein äusserst innovativer Hersteller. Wir waren die ersten, die «fly-by-wire» eingeführt und Komposit-Materialien im Flugzeugbau verwendet haben. Man muss immer einen Schritt voraus sein, dann bleibt man auch erfolgreich. Was den Kampfflugzeugbau angeht, sind wir am grössten europäischen Verteidigungsprojekt, dem Eurofighter, massgeblich beteiligt und haben aus vielen anderen Projekten jahrzehntelange Erfahrung. Ausserdem arbeiten wir derzeit an Studien für eine Tornado-Nachfolge – ein Projekt, das auch nur in einem europäischen Verbund gelingen wird. Wenn es uns gelingt, diese politische und industrielle Allianz in Europa in den kommenden Jahren zu schmieden, muss uns um die Zukunft im Kampfflugzeugmarkt nicht bang sein.



Defense_v6.indd 8 28.11.17 01:57



Die Wahlen in Frankreich und Deutschland 2017 sind geprägt von einem Einflussgewinn populistischer Parteien und der Kritik an Freihandel, sowie der Europäischen Union. Wie stark würde Airbus als Gemeinschaftsprojekt europäischer Staaten mit Standorten in Deutschland, Frankreich, Spanien, Grossbritannien und Polen von einem Austritt des Vereinigten Königreichs infolge des Brexit geschwächt werden?

Der Airbus-Konzern ist das beste Beispiel dafür, dass Europa funktionieren kann. Aus Sicht der Wirtschaft gibt es keinen Rückzug mehr hinter nationale Grenzen. Inwieweit uns der Brexit beeinflussen wird, hängt massgeblich von den Verhandlungen der EU mit der britischen Regierung ab. Ich könnte mir allerdings vorstellen, dass eher der Wirtschaftsstandort Grossbritannien geschwächt wird, als dass Airbus hier längerfristige Turbulenzen zu befürchten hätte.

Wie kann Airbus Defence and Space auf angedrohte Strafzölle der Regierung der Vereinigten Staaten von Amerika reagieren?

Ich glaube nicht, dass es dazu kommen wird. Airbus hat zahlreiche Standorte in den USA. In Alabama bauen wir Passagierflugzeuge, in Columbus fertigen wir die Lakota-Helikopter, die wir höchst erfolgreich an die US-Armee und die Nationalgarde ausliefern. Auch die NASA zählt zu unseren Kunden und in Kürze werden wir in Florida ein Werk zur Serienfertigung von Satelliten eröffnen. Und zu guter Letzt: Mit einem jährlichen Einkaufsvolumen von rund 15 Milliarden Dollar ist Airbus der grösste ausländische Kunde für Luft- und Raumfahrtgüter in den USA. Sprich: Airbus und die USA – das ist ein gewachsenes Verhältnis. Beide Seiten dürften kaum Interesse haben, es zu schwächen.

Im Silicon Valley wird neben der Entwicklung neuer Antriebskonzepte für das Automobil auch in der Luft- und Raumfahrt nach neuen Antriebs- und Steuerungskonzepten gesucht. Welchen Einfluss sehen sie in der Digitalisierung auf die Luftfahrt und wie kann sich Airbus gegen Konkurrenten wie SpaceX behaupten?

Digitalisierung und Industrie 4.0 sind wichtig für die Innovationsfähigkeit unserer Branche. Kein anderes Thema beschäftigt uns derzeit intensiver. Wie können wir unsere Produkte smarter machen, welche Möglichkeiten gibt es durch die Digitalisierung neue Produkte und Dienstleistungen auf den Markt zu bekommen? Die Antworten auf solche Fragen sind Teil unserer neuen strategischen Ausrichtung. Space X ist sicher ein Vordenker in diesem Bereich. Der dadurch entstandene Druck hat uns bei der Diskussion um die Entwicklung der neuen europäischen Trägerrakete Ariane 6 in den Verhandlungen mit den europäischen Raumfahrtbehörden sehr geholfen, wirtschaftlichere Strukturen einzuführen. Space X ist ein neuer Spieler auf dem Markt mit stimulierenden Ideen in Bezug auf die wirtschaftlichen Herangehensweise. Was Umsatz, Mitarbeiter und Produktvielfalt in der Raumfahrt anbelangt, sind wir immer noch um das Vierfache grösser. Innovation findet eben auch bei uns statt. In diesem Jahr starten wir – wie erwähnt – die weltweit erste Serienfertigung für Satelliten. Für das OneWeb Projekt werden wir damit innerhalb von drei Jahren 900 Satelliten bauen.

Defense_v6.indd 9 28.11.17 01:57

In mehreren Staaten werden heutzutage unbemannte Fluggeräte zur Aufklärung oder bei direkten Kampfhandlungen eingesetzt. Mit welchen technologischen Entwicklungen und ist in den kommenden 5-10 Jahren zu rechnen und wie wird sich die Zahl der Nutzer verändern?

Jede Nation wird in Zukunft Drohnen als Teil ihrer Streitkräfte haben. Die militärischen Einsatzmöglichkeiten ergeben sich immer dann, wenn Missionen für den Menschen zu langweilig, ermüdend oder zu gefährlich sind. Ein Beispiel: Wenn Sie ein Krisengebiet über längere Zeit beobachten wollen, können Sie das mit einem bemannten Flugzeug machen oder mit einer Drohne. Der Unterschied liegt darin, dass Sie mit dem bemannten Flugzeug nach spätestens 18 Stunden wieder landen müssen, weil die Crew ausgetauscht und der Flieger aufgetankt werden muss. Eine Drohne fliegt dieselbe Mission bis zu 36 Stunden am Stück. Die Technik für unbemannte Systeme ist in vielen Fällen bereits ausgereift. Woran wir aber jetzt arbeiten, ist das Thema Vernetzung und Auswertung der gesammelten Daten. Wie können Informationen von Flugzeugen, Satelliten und Drohnen in Echtzeit gesammelt und verarbeitet werden, um ein möglichst exaktes und aktuelles Lagebild zu haben und Entscheidungen zügig umzusetzen. Die Digitalisierung spielt auch hier eine führende Rolle.

Ein weiterer Schritt ist die Entwicklung des autonomen Fliegens, welches auch mit dem Ziel einer weiteren Senkung von Unfällen im Luftverkehr verbunden ist. Was sind die grössten technischen Hindernisse und wie können Kunden von diesem Konzept überzeugt werden?

Fakt ist, dass Fliegen statistisch bereits die sicherste Art der Fortbewegung ist und die wenigen Unfälle, die es gibt, meist auf menschliches Versagen zurückzuführen sind. Rein technisch ist autonomes Fliegen schon heute möglich. Im militärischen Bereich ist der Grad an Autonomie weit höher als in der zivilen Luftfahrt. Aber auch der Autopilot ist nichts anderes als eine abgemilderte Stufe autonomen Fliegens. Kritischer als die technische Komponente ist die Frage nach der luftfahrtrechtlichen Zulassung und der Akzeptanz bei den Nutzern und Passagieren. Wir fahren zwar schon ohne Lokführer in der U-Bahn, aber es wird noch eine Weile dauern, bis sich die Passagiere im Flugzeug an eine solche Situation gewöhnen werden. Was wir aber bald sehen werden sind unbemannte Frachtflugzeuge – den Trend zu mehr Autonomie in der Mobilität wird keiner aufhalten.

Dirk Hoke

CEO Airbus Defence and Space

Dirk Hoke ist seit dem 1. April 2016 Chief Executive Officer (CEO) von Airbus Defence and Space und Mitglied des Airbus Group Executive Committee.

Davor war Dirk Hoke bei Siemens, wo er seit 2014 CEO der Large Drives Business Unit war. Seit der Ernennung zum CEO des Siemens Cluster Western & Central Africa im Jahre 2008 bekleidete er bei Siemens verschiedene Führungspositionen. Seine Karriere umfasst 21 Jahre und 5 Kontinente.

Dirk Hoke besitzt einen Abschluss als Maschinenbauingenieur von der Technischen Universität Braunschweig. Im Jahre 2010 wurde er Mitglied der Young Global Leader Class des World Economic Forum.

Defense_v6.indd 10 28.11.17 01:57

KOK Kratzer
Kriminalpolizeidirektion Freiburg im Breisgau

Enkeltrick am Telefon

Der Betrug am Telefon nimmt seit Jahren weiter zu und besonders ältere Menschen werden Opfer von Tathandlungen wie Enkeltrick oder falschen Gewinnversprechen. KOK Kratzer von der Kriminalpolizeidirektion Freiburg im Breisgau erklärt im Interview das neue Vorgehen der Täter, Tipps gegen Betrugsversuche und warum man misstrauisch sein sollte, wenn man von der Nummer 110 angerufen wird.

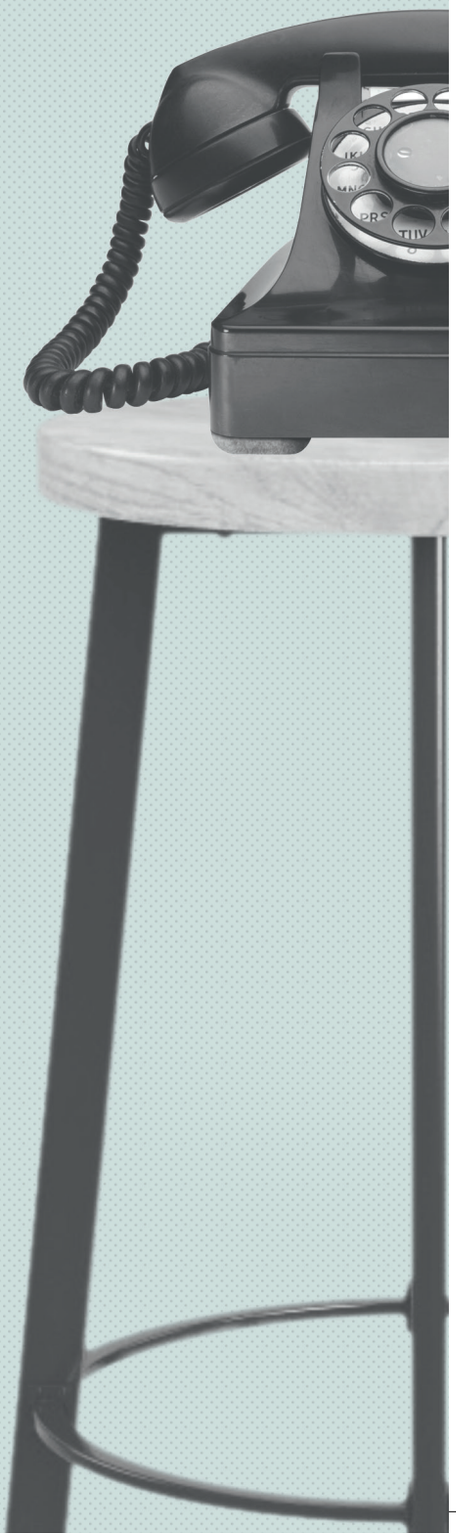
In den letzten Jahren ist in den Nachrichten vermehrt von Betrugsfällen am Telefon berichtet worden, bei welchen Täter grosse Mengen Bargeld erbeuten konnten. Besonders der Enkeltrick wird hierbei genutzt, um als vermeintlicher Verwandter eine Notlage vorzutäuschen. Welches Vorgehen ist bei den Tätern zu beobachten?

KOK Kratzer: Die Zahl der Betrugsdelikte ist in den vergangenen Jahren massiv gestiegen. Insbesondere beim Betrug werden zuletzt verschiedenste Tathandlungen angewandt. So kann man oft gar nicht mehr vom klassischen Enkeltrick, Gewinnversprechen oder falschen Polizeibeamten sprechen. Bei sehr vielen Tathandlungen wird das Vertrauen in die Polizei missbraucht und angebliche Polizeibeamte agieren als Täter, um die Geschädigten von der Richtigkeit der Geschichte zu überzeugen oder um Informationen zu erhalten.

Defense_v6.indd 11 28.11.17 01:57

Der Enkeltrick hat immer wieder Erfolg, obwohl davon seit längerem gewarnt wird. Was sind die Gründe dafür? Hat sich das Vorgehen der Täter in den letzten Jahren verändert?

Der Durchschnitt der Bevölkerung wird immer älter. Und gerade ältere Menschen haben häufig ihre Ersparnisse zu Hause oder auf der Bank - auch wenn sie nur klein sind. Die häufig bei dieser Altersgruppe vorhandene Hilfsbereitschaft wird durch die aus dem Ausland agierenden Täter ausgenutzt. In den vergangenen Jahren waren der Enkeltrick und das Gewinnversprechen das meist verübte Betrugsdelikt unter den Anrufstraftaten. Um davor zu warnen und für die Thematik insgesamt zur sensibilisieren, betreiben wir seit mehreren Jahren hierzu offensive Öffentlichkeitsarbeit. In den vergangenen Jahren kam eine weitere Abwandlung der Anrufstraftaten hinzu: Der falsche Polizeibeamte. Bei dieser Betrugsmasche geben sich die Täter am Telefon als Polizeibeamte aus. Mit dem sogenannten Call-ID-Spoofing wird vorgetäuscht, sie würden von der Notrufnummer «110» aus anrufen, häufig auch mit der örtlichen Vorwahl. So erschleichen sie sich das Vertrauen der Angerufenen. Mit geschickter Gesprächsführung erwecken die vermeintlichen Polizisten den Eindruck, die Angerufenen seien im Visier von Einbrechern, die es auf ihr Geld und ihre Wertgegenstände abgesehen haben. Die falschen Amtsträger gaukeln den Leuten ausserdem vor, dass deren Wertsachen weder zu Hause noch auf der Bank sicher seien. Deshalb sollten die Opfer auch ihre Konten und Bankdepots leeren. Es wird ein Bote vorbeigeschickt, der das Geld und sämtliche Wertsachen abholt, um sie vermeintlich «in Sicherheit» zu bringen.



Manchmal fordern die Betrüger ihre Opfer auch auf, ihr Geld mit einem Finanzdienstleister bar ins Ausland zu transferieren. Daneben existieren vielfältige Variationen und von den Tätern erfundene Nebenszenarien wie z.B. abgehörte Telefonate zwischen den Tätern, von der Bank durch korrupte Bankmitarbeiter untergeschobenes Falschgeld, dass überprüft werden müsse, usw. Insbesondere dieser Phänomenbereich bereitet der Polizei bei ihrer Arbeit gegenwärtig Schwierigkeiten. Ein Geschädigter, welcher durch einen falschen Polizeibeamten kontaktiert und instruiert wurde ist manchmal im Rahmen der Ermittlungen schwer von der Wahrheit zu überzeugen. Das Schlimmste für uns ist allerdings, dass das Vertrauen in die richtige Polizei durch diese Taten nachhaltig geschädigt wird.

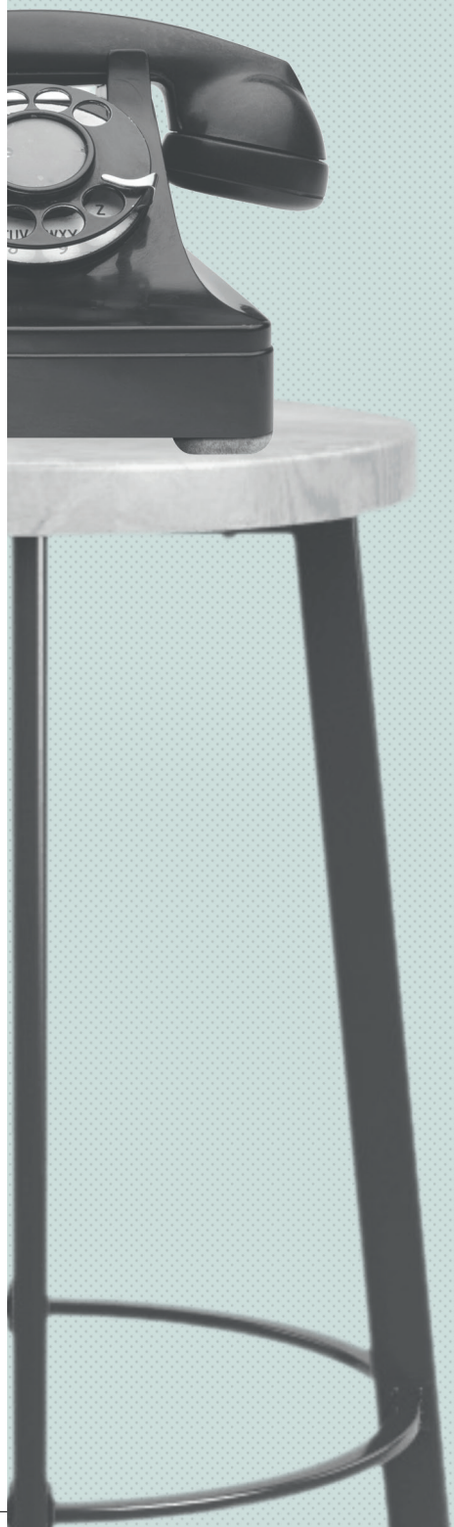
Wie sollten Betroffene solcher Anrufe reagieren und welche Tipps gibt die Polizei? Welche Beratungsangebote bietet die Polizei für Senioren an, um auf die Gefahren aufmerksam zu machen?

Bitte beachten Sie: Die Polizei ruft Sie niemals unter der Notrufnummer 110 an. Seien Sie misstrauisch, wenn Sie diese Nummer auf Ihrem Telefon sehen. Jeder, der durch einen Betrüger kontaktiert wurde sollte unverzüglich den Notruf 110 wählen und den Sachverhalt zur Anzeige bringen. Hier können auch kleinste Informationen zum Erfolg der Festnahme führen.

— Sollten Sie von einem Betrüger angerufen werden, lassen Sie sich nicht unter Druck setzen. Legen Sie den Hörer auf, wenn Ihnen etwas merkwürdig erscheint.

— Sprechen Sie am Telefon niemals über Ihre persönlichen und finanziellen Verhältnisse.

Defense_v6.indd 12 28.11.17 01:57



— Übergeben Sie niemals Geld oder Wertgegenstände an unbekannte Personen.

— Sprechen Sie mit Ihren Familien oder anderen Vertrauten über den Anruf.

Durch unseren Fachbereich Prävention werden regelmässig Veranstaltungen in Einrichtungen durchgeführt, in denen lebensältere Menschen wohnen oder sich aufhalten. Dort informieren wir regelmässig durch geschulte Polizeibeamte zu neuesten Betrugsvarianten.

Gibt es für nahe Angehörige von Betrugsopfern Anzeichen, um solche Taten frühzeitig zu erkennen?

Die Dunkelziffer in diesem Deliktsbereich ist leider immens hoch. Geschädigte, die zum Teil ihre gesamten Ersparnisse den Tätern übergeben haben schämen sich für ihr Handeln. Oft erkennen sie zu spät, dass sie einem Betrüger zum Opfer gefallen sind. Aber nicht nur Geschädigte, die Geld oder Wertsachen übergeben haben, leiden unter den Anrufen. Auch bei Versuchstaten leiden die Geschädigten zum Teil noch Wochen nach der Tat. Haben Sie als Angehörige lebensältere Menschen in Ihrem Bekanntenkreis sprechen Sie diese gegebenenfalls sensibel auf die Möglichkeit solcher Betrugsvarianten an.

Handelt es sich bei den Betrügern eher um Einzeltäter, oder organisierte Banden?

Anrufstraftaten wie der Enkeltrick und der Betrug durch falsche Polizeibeamte funktionieren in der Regel nur durch banden- und gewerbsmässiges Handeln. Die Tätergruppierungen sind straff organisiert, wobei mehrere Täter arbeitsteilig agieren. Diese Betrugshandlungen stellen strafrechtlich eine schwere Straftat dar, die den Rechtsfrieden empfindlich stört, indem sie bedeutsame Rechtsgüter wie Eigentum von bedeutendem Wert verletzt. Für diese Straftaten liegt die Mindeststrafandrohung nicht unter einem Jahr, womit sie einen Verbrechenstatbestand darstellen.

Wie können Bankangestellte verdächtige Abhebungen erkennen und entsprechend geschult werden? Wie kooperiert die Polizei mit Banken?

Gerade ältere Menschen sind häufig über viele Jahre hinweg Kunde/Kundin derselben Bank. Deshalb kennen die Bankmitarbeiter oft die persönlichen Verhältnisse und Lebensumstände dieser Senioren und diese sollten aufmerksam werden:

— wenn lebensältere Menschen, die sich sonst begleiten lassen, alleine zur Bank kommen,

— oder zu einer völlig atypischen Zeit (Tageszeit, Wochentag) kommen,

— und ohne vorherige Anfrage oder Ankündigung hohe Geldbeträge sofort bar auszahlen lassen wollen.

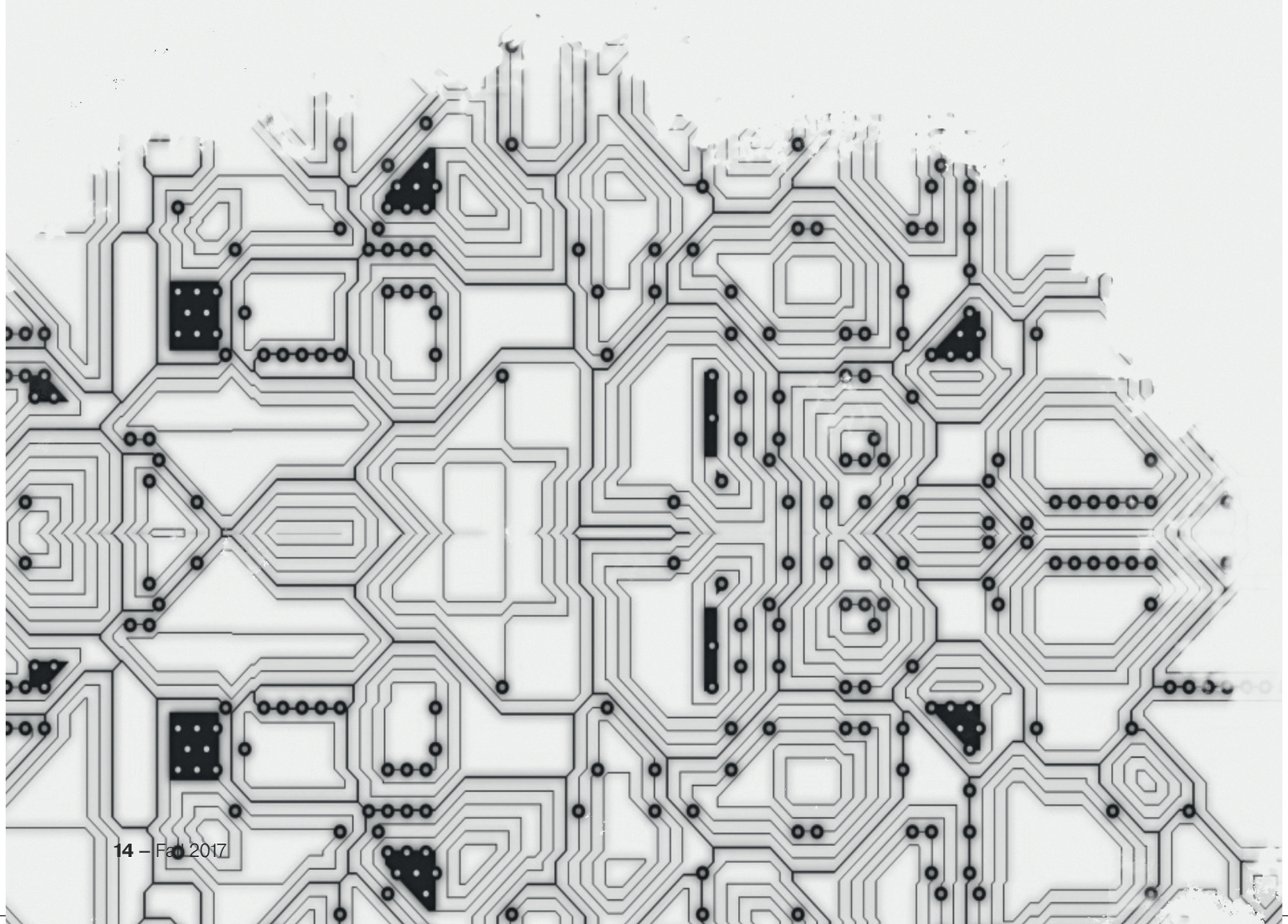
Bei Verdachtsfällen auf einen Betrug sollte unverzüglich die Polizei informiert werden.

Defense_v6.indd 13 28.11.17 01:57

Wolfgang Ischinger
Chairman of the Munich Security Conference

Security Policy

Rules for Cyberspace



Defense_v6.indd 14 28.11.17 01:57

A computer worm infests Iranian nuclear power plant systems, a cyberattack cripples sections of the Ukrainian electrical grid, intruders penetrate the German Parliament's IT system and steal sensitive data. No longer merely the stuff of science fiction novels cyberspace as a setting for security policy disputes and even a stage for conflicts, has long since become part of our reality.

«I have given Cyber Command . . . really its first wartime assignment,» declared United States Secretary of Defense Ashton Carter in Washington in early April 2016 (Financial Times 2016) in a statement directed against ISIS and interpreted by many as the first governmental cyberwar declaration. It is no longer possible to address security policy challenges or to lay out strategies today without factoring in the digital realm.

In fact, our current situation is similar to that some 70 years ago, when the invention of the nuclear bomb fundamentally changed the strategic landscape. The technical possibilities offered by the information revolution are less tangible, and their effects are considerably more complex and multi-faceted, but as in the nuclear revolution, they are fundamentally changing the playing field for international security policy. We are already facing massive challenges along with complex ethical, legal and political questions as the result of attacks by hackers on critical infrastructure, the online recruiting of jihadi fighters and the development of autonomous weapons systems. And technological change will march on, bringing new possibilities that open up any number of opportunities, while at the same time further magnifying the potential dangers associated with cyberspace. We must continually assess the opportunities – as well as the risks – of digital progress in terms of security policy and consider the necessary steps for dealing with them appropriately.

Taking Stock: Digital Warfare in the 21st Century

The possibilities of cyberwarfare have radically changed the character of modern conflict. In particular, one trend that we have observed increasingly in recent decades continues unabated: Conflicts are often asymmetrical, i.e., they no longer take place between state actors. Compared with the building of nuclear weapons, the barriers to entry for a «cyberwarrior» are, of course, far lower. It is true that major cyberwarfare operations, such as the one that damaged Iranian centrifuges by introducing the Stuxnet virus, are only possible when backed by substantial resources at a level generally only available to state actors. However, a far smaller amount of money combined with the necessary skills is enough to cause significant damage.

Terrorist groups have also discovered the digital world for themselves. ISIS makes use of the opportunities offered by cyberspace extensively and effectively: A significant factor in the organization's expansion is its digital strategy (see Munich Security Report 2016). Whether it is recruiting new members, spreading its propaganda messages, or communicating internally, the group known as the «Islamic State» is constantly expanding – not just physically, but digitally as well. As early as 2014, Robert Hannigan, head of the UK's GCHQ intelligence service, warned that social networks had already become the «command-and-control networks of choice» (Financial Times 2014) for groups such as ISIS. At this year's Munich Security Conference, he underscored this observation and called for more active and more effective measures to be taken in the online fight against jihadi terror (see Munich Security Conference 2016).

This battle is also being fought by private hacker groups like Anonymous, which provides a fitting illustration of today's digital battlefield: «Make no mistake: #Anonymous is at war with #Daesh. We won't stop opposing #IslamicState. We're also better hackers.» This tweet was sent out by Anonymous after the Paris attacks in November 2015. In other words, a private hacker group operating in a space that was barely there 25 years ago, has declared digital war on the world's most powerful and dangerous terrorist group, which was non-existent just a few years ago. What would have sounded like an absurd description of a conflict not too long ago, is reality today. And this type of asymmetrical, multi-layered conflict will only become more prevalent in the future.

State actors are becoming increasingly active as well – partly in order to develop offensive capabilities and partly to ready themselves for the countless threats they face in cyberspace – and these activities extend far beyond online jihadism. The dissemination of falsified information for the purpose of intentionally manipulating certain segments of the population has become commonplace and is being given a huge boost by the opportunities offered by the online world. This was demonstrated quite recently in the calculated dissemination of false information in the «Lisa Case» in early 2016 (see Federal Academy for Security Policy 2016). Some states maintain entire «troll armies» that comment on news articles or distribute news and opinions favorable to those governments in social media. The ability of the public in our democracies to form opinions suffers as a result, particularly when this creates alternative public spheres that exist in their own reality, almost entirely walled off from political discourse and the facts.

Defense_v6.indd 15 28.11.17 01:57

Another danger stems from attacks on and damage to the institutions of democracy themselves. The large-scale assault on the German Parliament in summer 2015 made this very clear to us here in Germany (see FAZ 2016b). Attacks on critical infrastructure also have the potential to cause untold loss and damage. For instance, more than 700,000 households were temporarily left without electricity as a result of the strike against the Ukrainian power grid in December 2015 (see FAZ 2016a). It is hard to imagine what would happen if such attacks were even more widespread, and mobile communications, transportation and the water supply in densely populated regions were to be crippled in a matter of hours. Speaking on the sidelines of the 2016 Munich Security Conference, the Netherlands' foreign minister Bert Koenders called cyber arms «weapons of mass disruption,» in contrast with nuclear, chemical or biological weapons of mass destruction (see Rijksoverheid 2016). Add to that billions in losses for companies as a result of corporate espionage, sabotage and data theft, the cost of which amounts to 51 billion euros each year in Germany alone (see Bitkom 2015), along with other financial losses occurring as «side effects» of digital progress.

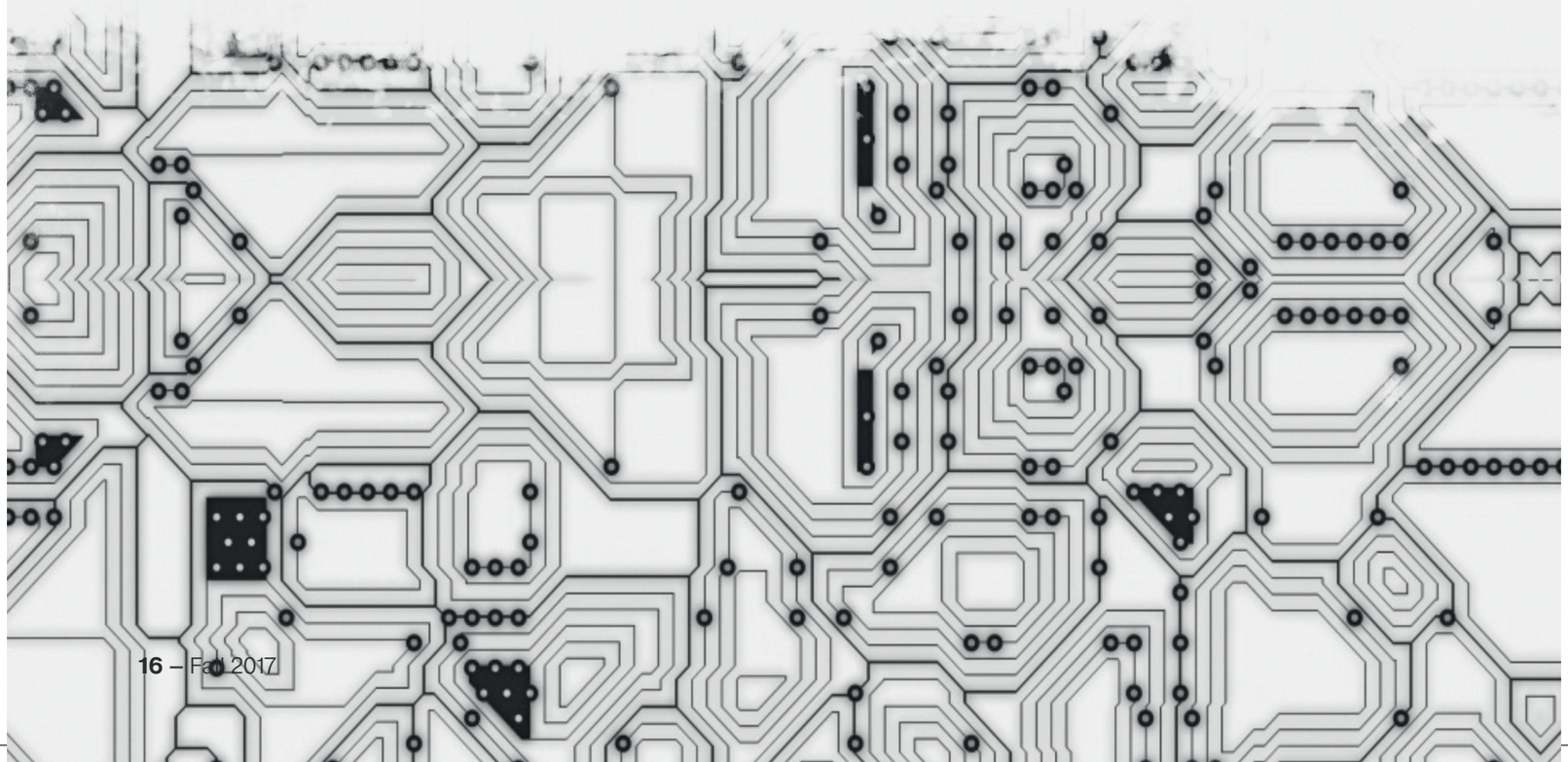
Incidentally, such threats are anything but a purely Western problem. The expanding economies of the Global South are particularly vulnerable to the dangers of cyberspace. Often, the digitalization processes in these countries are especially rapid, sometimes occurring without any sort of safeguards whatsoever. A recently published report put economic losses in Kenya due to cybercrime at 146 million US dollars (see Serianu 2015). And South Africa saw approximately 6,000 attacks on its infrastructure, Internet providers and companies in October 2015 alone (see Times Live 2015).

Challenges for the Political Sphere: Rules, Resources and Expertise

Thus, politicians have to take faster and more effective action against cyberspace threats. One of the most basic problems in this regard is that, in many cases, politicians do not have the necessary expertise in this area. But they must make critical decisions nonetheless. The general public also frequently lacks sufficient understanding and basic knowledge of the topic in view of its complexity and the continual change in cyberspace. This is why we need digital «interpreters» to explain complex processes in simple terms everyone can understand. In the vast majority of cases, today's decision-makers have no affinity for digital issues, let alone professional expertise. And often, there is no common language for dialog between experts and politicians, although this is a basic prerequisite for the implementation of the necessary decisions.

In Germany these days, there is at least awareness of the immense challenges posed by cybersecurity, and initial key steps have been taken. A welcome announcement was made in spring 2016 by the German Federal Ministry of Defense when it said that the German armed forces (Bundeswehr) would be restructured and a cyberforce added, and that the number of cyberexperts in the Ministry would be massively increased (see Wiegold 2016).

But we still have to ask ourselves whether our efforts are enough. Has society understood how greatly our future security and prosperity will depend on how wellprepared we are digi-



Defense_v6.indd 16 28.11.17 01:57

tally? Former US President Barack Obama wanted to earmark line items totaling 19 billion US dollars for cybersecurity in the country's 2017 budget (see Reuters 2016). The British government has announced that it will nearly double its expenditure on cybersecurity over the next five years (see Gov. uk 2015). These are the orders of magnitude in which we must think.

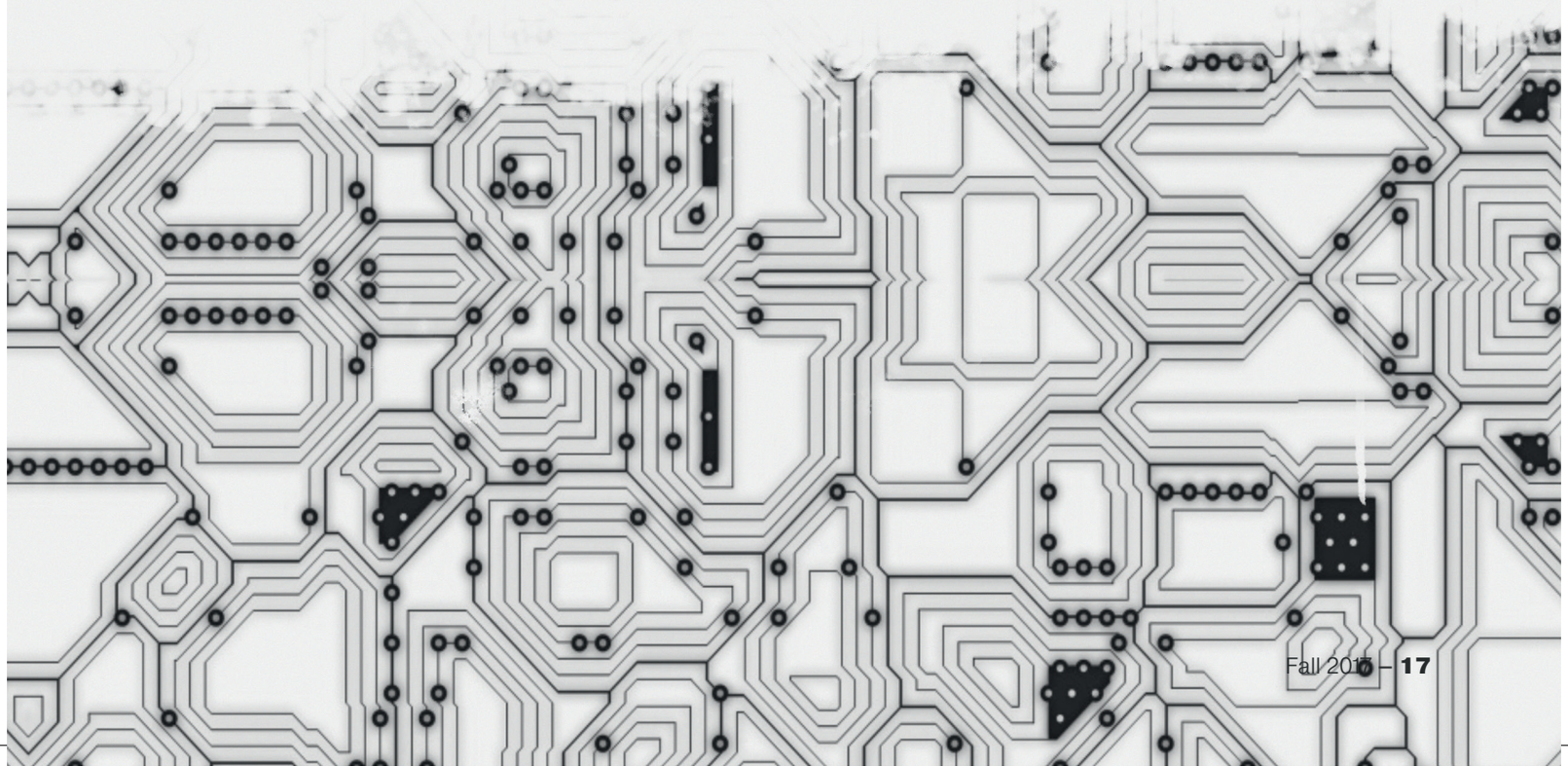
We thus need more expertise, but also more capabilities in terms of resources and structures – well beyond what is called for in the German Ministry of Defense's reform. Universities and other institutions of higher education must be integrated into this effort so that professionals receive training and continuing education at an early stage. Implementation of even the best plans for new cybersecurity structures will fail if we do not succeed in recruiting computer and software specialists, developers and programmers. Thus, one of the key questions will therefore be how to inspire an interest in German military service among younger people who are not necessarily passionately interested in security and defense policy – and how these experts entering the defense ministry can work under Germany's complex public service legislation.

Many significant issues can no longer be resolved by politicians alone: Which technical resources do we have at our disposal for gaining the upper hand over terrorist organizations on the digital battlefield? How can we protect ourselves from attacks by foreign intelligence services that attempt to steal state secrets or sabotage our elected representatives and their independent decision-making process? In order to address these questions together and jointly create the conditions for a free, secure and open Internet, politicians require the support and trust of the private sector and other non-state experts in the field. Last summer, a reporting requirement was introduced in Germany as part of the IT Security Act, which will also be implemented across the EU as part of the Network and Information Security (NIS) Directive. This constitutes another important step toward closer cooperation.

Other questions also remain largely unanswered: What line has to be crossed for cyberattacks to be considered an act of war? How can we respond appropriately to such attacks, and what rules should be followed in carrying out such a response? What happens if there are strong indications as to who is responsible for a massive cyberattack, but no conclusive evidence is available? What implications do these considerations have on Article 5 of the NATO Treaty? NATO has declared that cyberspace will be acknowledged as an independent operational area in the future (see NATO 2016). This could also mean that cyberattacks could trigger the mutual defense clause (see NATO 2015).

Due to the fact that national borders are very fuzzy in cyberspace, transnational forms of cooperation such as NATO play a particularly important role here. Although it is primarily the job of each nation state to guarantee its own security, some responsibilities could be in much better hands at European or NATO level.

In recent years, the practices of some intelligence services have led many Germans to view cooperation with international partners with some skepticism. Particularly their attitude towards

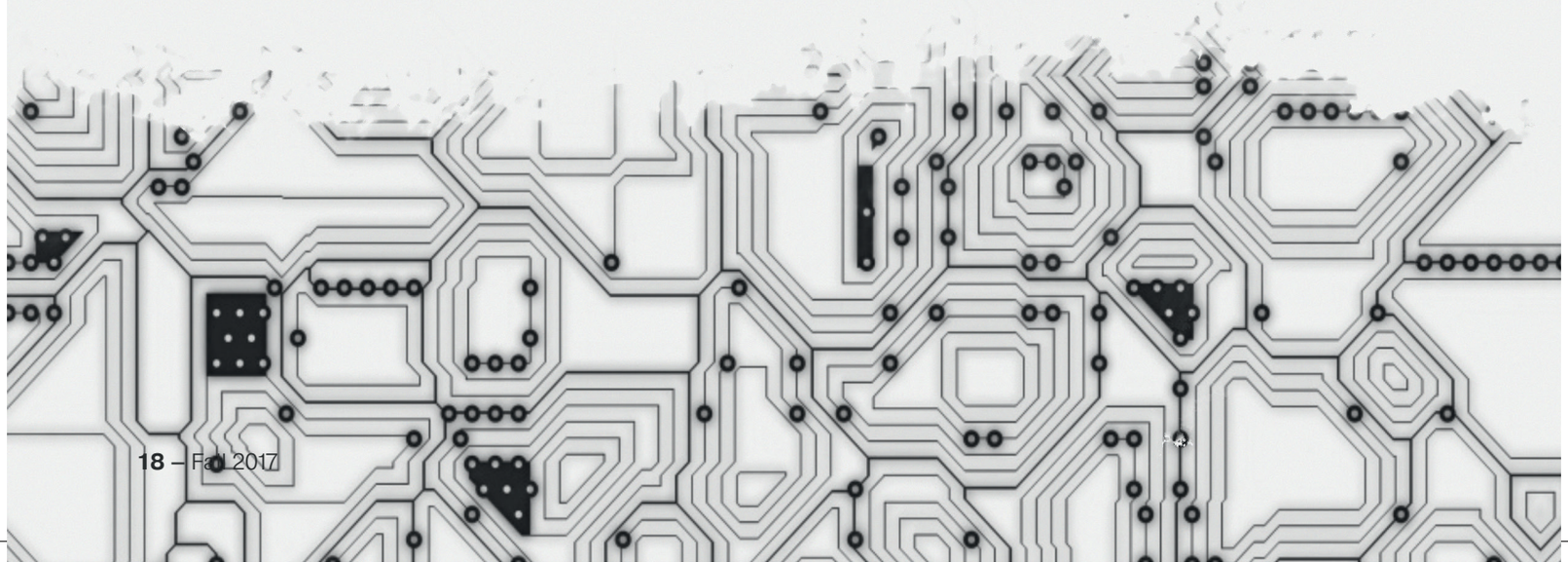


Defense_v6.indd 17 28.11.17 01:57

the American partner has deteriorated substantially as a result of the NSA affair. According to a survey by the German Marshall Fund, the number of all individuals surveyed in Germany who view the United States positively dropped a full 14 percent points from 2011 to 2014, from 72 to 58 percent (see The German Marshall Fund of the United States 2015). Fortunately, both sides have slowly inched back together in the meanwhile. In May 2015, German confidence in the bilateral alliance had again risen to 62 percent (see Pew Research Center 2015). Some skepticism remains, however, along with fundamental differences in the cyberpolicy of the two countries. This is also reminiscent of the early days of the nuclear age when US allies had to come together before their concerns would be heard by Washington (see Ischinger et al. 2014). For this reason, one of the key objectives must be for Germany and the United States, along with other countries, to build a consensus on the basic pillars of international cyberpolicy. Only based on a clear EU position can we succeed in gradually reaching transcontinental agreement on «reliable rules of the game» (see FAZ 2014) for cyberspace – as called for by Telekom CEO Timotheus H€ottges as early as 2014 at the Cyber Security Summit in Bonn, organized by the company and the Munich Security Conference. For several years now, the Munich Security Conference along with Deutsche Telekom has been organizing roundtables and summits on cybersecurity issues, bringing together decision-makers and experts from across the globe, for instance in Silicon Valley in the fall of 2016.

The more sophisticated the possibilities provided by cyberspace become, the more important it is to underpin them with a set of norms and rules. Key here is fundamentally updating international law, which does not yet address or govern cyberwarfare as such. In contrast to nuclear security, for instance, the cyberarena to date has no internationally recognized, multilateral body of regulations that specifically governs the conduct of cyberwar. Nonetheless, some countries, including the two cybergiants – China and the United States – were able to reach initial agreement on the subject of industrial espionage in the fall of 2015. Attempts to arrive at more far-reaching standards for cyberspace have also been underway for some time now. These include the (further) development of the Tallinn Manual, which was initiated in 2009 and elaborated by legal experts from various NATO member states. An initial draft was presented in 2013 (see CCDCOE 2013). However, this standard is not legally binding, and thus international implementation and enforcement of the recommendations have been lacking to date.

Democracies in particular, such as the member states of the European Union, should strive for a free, open and secure Internet as a global public asset. The European Union can still be much more active in this regard and drive the development of international standards. During this process, it will repeatedly run into obstacles. While there already are fundamental differences in cyberpolicy even in transatlantic relations, authoritarian states weigh up security and freedom on the Internet very differently. For this reason, German mistrust of the United States on the issue of data security is largely misguided: We face much greater danger from other directions. According to information by the German Federal Intelligence Service, the attack on the German Bundestag was steered by Russia (see Zeit 2016). And recently, CIA Director James R. Clapper, speaking before the US Senate, emphasized that, «Russia and China continue to have the most sophisticated cyberprograms» (The Diplomat 2016). Many other countries are also working on offensive cybercapabilities. We are, there is no other way to put it, in the middle of a digital arms race. Precisely for this reason, it is all the more important to work out common minimum standards and fundamental rules as quickly as possible.



Defense_v6.indd 18 28.11.17 01:57

Outlook: A Strategy for the Digital Age

As I wrote at the beginning, in some ways we find ourselves in a situation similar to around 70 years ago, when the invention of the nuclear bomb fundamentally changed the strategic landscape. Although the parallels should not be overemphasized in view of the obvious differences between a nuclear warhead and code, we stand at the beginning of an era of uncertain developments, and that is similar to the post-1945 period. The full effects of new cyber instruments on international security policy and on how wars and conflicts are fought cannot really be foreseen yet. Cyberregulations do not (yet) exist.

But we are experiencing the risks of cyberspace every day. We must seize the opportunity arising from this: the potential for better preparing against these hazards and for developing means of addressing them effectively. For this reason, new approaches are needed. This applies to the national level first of all. The recent restructuring of the German armed forces and the Ministry of Defense is an important step in this regard that must be followed by others. Additional momentum is expected from the new German federal cybersecurity strategy, which will replace the predecessor document written in 2011 (see German Federal Government 2016). At the regional level, what is necessary first and foremost is better coordination within the EU and a drive toward joint initiatives to set comprehensive standards for cyberspace. Ultimately, the greatest challenge appears to be developing and implementing authoritative standards worldwide and agreeing on the basic tenets of international cybersecurity policy.

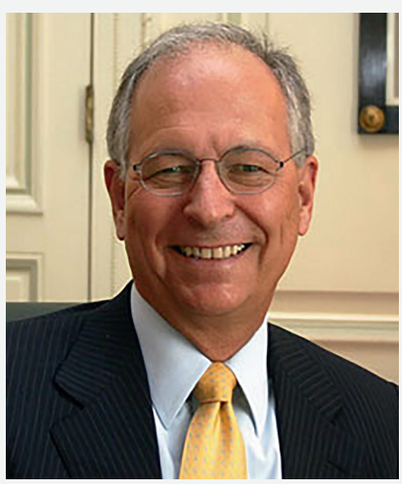
The process will be long, but it has prospects for success. The attempt in the 1960s to develop rules for the nuclear age was equally complex, but ultimately successful: Steps were taken toward arms control and disarmament, even though the danger was only contained, not eliminated. In this day and age, we must succeed in carrying out a similar international process to develop a common strategy for the significantly more complex digital age. Only then can we ensure together that the potential risks of cyberspace are minimized as much as possible and the numerous opportunities offered by a free, open and secure Internet are realized. It is not yet too late.

Springer Nature Book/Cyber Security. Simply. Make it Happen. 2017 Leveraging Digitization Through IT Security, chapter: «Security Policy: Rules for Cyberspace», 2017, p. 13-20, Wolfgang Ischinger, Herausgeber: Ferri Abolhassan, With permission of Springer Nature

Defense_v6.indd 19 28.11.17 01:57

Wolfgang Ischinger

Ambassador Ischinger is Chairman of the Munich Security Conference and Senior Professor for Security Policy and Diplomatic Practice at the Hertie School of Governance in Berlin. A graduate in law and international relationships, Ischinger first worked in the cabinet of the UN Secretary-General before moving to the German Federal Foreign Office in 1975. This included postings to the embassies in Washington, D.C. and Paris, and a period from 1982 to 1990 as a senior assistant to Hans-Dietrich Genscher, the German Minister for Foreign Affairs at the time. From 1993 to 1998, he was Director of the Policy Planning Staff and later Political Director, before serving as State Secretary from 1998 to 2001. He was Ambassador to the USA from 2001 to 2006, and Ambassador to the United Kingdom from 2006 to 2008. He was appointed Chairman of the Munich Security Conference in 2008. He also held the position of Global Head of Governmental Relations at Allianz SE (Munich) from 2008 to 2015. Ambassador Ischinger represented the EU in the Troika Kosovo negotiations in 2007 and the OSCE in efforts to establish a national dialog in Ukraine in 2014. In 2015, he was appointed Chairperson of an OSCE-mandated Panel of Eminent Persons to strengthen the European security architecture. He currently advises companies, governments and international organizations. He is a member of the Supervisory Board of Allianz Deutschland AG and Allianz Private Krankenversicherung (APKV), and a member of the European Advisory Council of Investcorp (London/New York). He also serves on the Steering Committee of the German Council on Foreign Relations (DGAP), the Board of Atlantik-Br€ucke, the Board of Trustees for SWP (Berlin), SIPRI (Stockholm), AICGS (Washington, DC) and The American Academy in Berlin, the Advisory Board of the Federal Academy for Security Policy (BAKS) and the Center for European Reform (London), and the Board of Directors of the Atlantic Council. He received the Leo Baeck Medal in 2008 and was decorated with the Federal Cross of Merit in 2009.



Defense_v6.indd 20 28.11.17 01:57

References

Bitkom (2015). Studie zu Wirtschaftsschutz und Cybercrime. Accessed June 16, 2016, from https://www.bitkom.org/Presse/Presseinformation/Studie-zu-Wirtschaftsschutz-und-Cybercrime.html

CCDCOE (2013). Tallinn manual process. Accessed June 16, 2016, from https://ccdcoe.org/ tallinn-manual.html

Die Bundesregierung (2016). Kabinettsklausur in Meseberg – Digitalisierung gemeinsam vorantreiben. Accessed June 16, 2016, from https://www.bundesregierung.de/Content/DE/Artikel/2016/05/2016-05-24-digitalisierung-meseberg.html

FAZ (2014). Cyber security summit – Jeder ist bedroht. Accessed June 16, 2016, from http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/telekom-chef-thimotheus-hoettges-jeder-istbedroht- jeder-staat-jedes-unternehmen-jeder-buerger-13243841.html

FAZ (2016a). Cyber-Sicherheit: Die Hackerdämmerung. Accessed June 16, 2016, from http://www.faz.net/aktuell/wissen/physik-mehr/ukrainischer-stromausfall-war-ein-hacker-angriff- 14005472-p2.html?printPagedArticle=true#pageIndex_2

FAZ (2016b). Netzangriff auf Bundestag – Es begann mit einer E-Mail. Accessed June 16, 2016, from http://www.faz.net/aktuell/feuilleton/medien/neue-details-zum-cyberangriff-auf-denbundestag- 14114851.html

Federal Academy for Security Policy (2016). The Lisa Case – STRATCOM lessons for European States (Security Policy Working Paper, No. 11/2016). Accessed June 16, 2016, from https://www.baks.bund.de/sites/baks010/files/working_paper_2016_11.pdf

Financial Times (2014). The web is a terrorist's command-and-control network of choice. Accessed June 16, 2016, from http://www.ft.com/intl/cms/s/2/c89b6c58-6342-11e4-8a63- 00144feabdc0.html#axzz3rjx7E4aL

Financial Times (2016). US launches online assault against Isis. Accessed June 16, 2016, from http://www.ft.com/cms/s/0/4d98edd0-fba5-11e5-b3f6-11d5706b613b.html#axzz4BkAXAl00

Gov.uk (2015). Chancellor's speech to GCHQ on cyber security. Accessed June 16, 2016, from https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

Ischinger, W., & Bunde, T. (2014). Die Zukunft des Westens im digitalen Zeitalter. FAZ of January 30, 2014.

Munich Security Conference (2016). Panel discussion "'Daeshing' terror and safeguarding liberties". Accessed June 16, 2016, from https://www.securityconference.de/mediathek/video/panel-discussion-daeshing-terror-and-safeguarding-liberties/filter/video/?tx_dreipctv mediacenter_mediacenter[venue]=36&cHash=3c81bfeba609faf81063d1ece9232f09

Munich Security Report (2016). Munich security report 2016. Accessed June 16, 2016, from https://www.securityconference.de/aktivitaeten/munich-security-report/

NATO (2015). Keynote speech by NATO Secretary General Jens Stoltenberg at the Opening of the NATO transformation seminar. Accessed June 16, 2016, from http://www.nato.int/cps/fr/natohq/opinions_118435.htm?selectedLocale=fr

NATO (2016). NATO Defence Ministers agree to enhance collective defence and deterrence. Accessed June 17, 2016, from http://www.nato.int/cps/en/natohq/news_132356.htm?

Pew Research Center (2015). Germany and the United States: Reliable allies. Accessed June 16, 2016, from http://www.pewglobal.org/2015/05/07/germany-and-the-united-states-reliableallies/

Reuters (2016). Concerned by Cyber Threat, Obama seeks big increase in funding. Accessed June 16, 2016, from http://www.reuters.com/article/us-obama-budget-cyber-idUSKCN0VI0R1

Rjiksoverheid (2016). Toespraak van minister Koenders bij de M€unchner Sicherheitskonferenz. Accessed June 16, 2016, from https://www.rijksoverheid.nl/regering/inhoud/bewindspersonen/bert-koenders/documenten/toespraken/2016/02/12/toespraak-van-minister-koenders-munchnersicherheitskonferenz

Serianu (2015). Kenya cyber security report 2015. Accessed June 16, 2016, from http://serianu.com/downloads/KenyaCyberSecurityReport2015.pdf

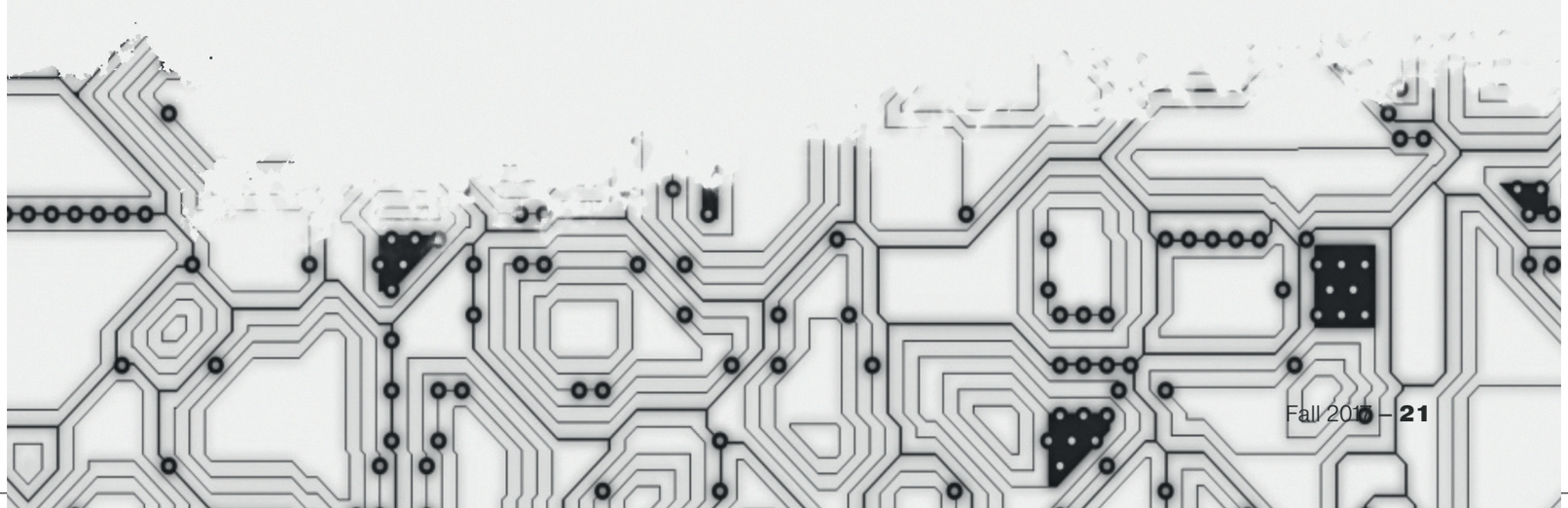
The Diplomat (2016). Top US spy chief: China still successful in cyber espionage against US. Accessed June 16, 2016, from http://thediplomat.com/2016/02/top-us-spy-chief-china-still-successful- in-cyber-espionage-against-us/

The German Marshall Fund of the United States (2015). Report of the task force on the future of German-American relations. Accessed June 16, 2016, from http://www.gmfus.org/publications/longstanding-partners-changing-times

Times Live (2015). It's one hack of a problem. Accessed June 16, 2016, from http://m.timeslive.co.za/thetimes/?articleId=15801457

Wiegold, T. (2016). Cyberkrieger, Computernerds und IT-Eink€aufer: Bundeswehr stellt sich neu auf. Accessed June 16, 2016, from http://augengeradeaus.net/2016/04/cyberkriegercomputernerds-und-it-einkaeufer-bundeswehr-stellt-sich-neu-auf/

Zeit online (2016). Deutscher Bundestag – Hackerangriff wurde aus Russland gesteuert. Accessed June 16, 2016, from http://www.zeit.de/digital/2016-01/hackerangriff-bundestag-russlandnachrichtendienst-bundesanwaltschaft

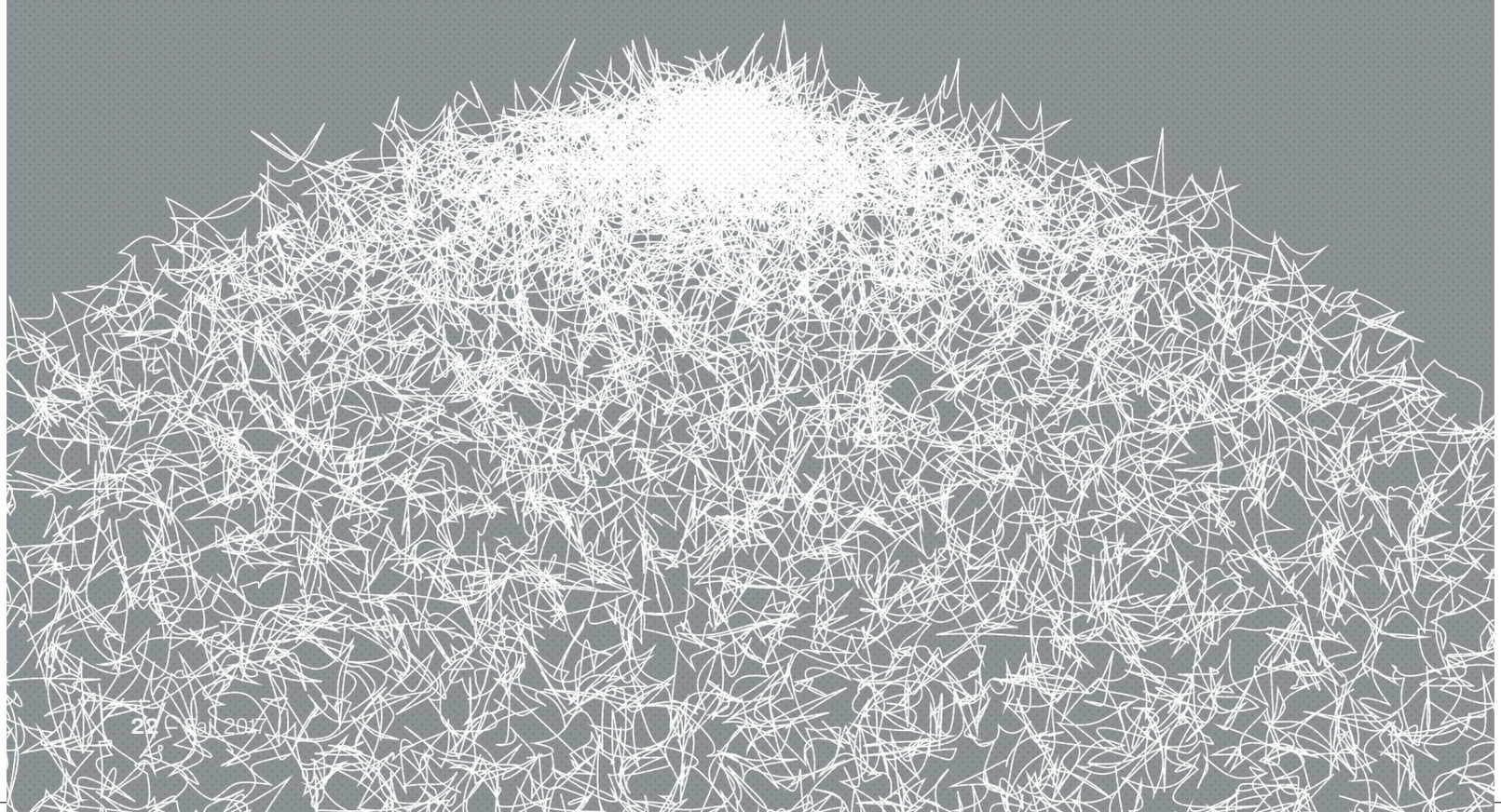


Defense_v6.indd 21 28.11.17 01:58

Kai Grunwitz
Senior Vice President EMEA bei NTT Security

Die Digitale Transformation

Wie Unternehmen die Herausforderungen der Digitalisierung bewältigen können ohne Sicherheitslücken entstehen zu lassen.



Defense_v6.indd 22 28.11.17 01:58

Heutzutage ist in Unternehmen die «Digitale Transformation» ein wichtiges Thema, welches ganze Geschäftsbereiche betrifft und die Möglichkeit zur Erschliessung neuer Geschäftsmodelle bieten kann. Auch aufgrund der immer schneller voranschreitenden Entwicklung wird in vielen Branchen die passgenaue Ausgestaltung im Kontext der eigenen Wertschöpfung als grosse Herausforderung betrachtet. Es stellt sich deshalb die Frage, wie Unternehmen von der Transformation profitieren und sich gleichzeitig vor Cyber-Angriffen schützen können?

Kai Grunwitz: Eine Digitale Transformation ohne eine ganzheitliche Sicherheitsstrategie ist schlichtweg unmöglich. Im Rahmen der IDG IT-Strategietage in Hamburg sahen 78% der Teilnehmer IT-Security als Hauptherausforderung für eine erfolgreiche Transformation.* Dies impliziert auch die Kernaufgabe für das Überleben eines Unternehmens in der agilen digitalen Wirtschaft.

Leider sehen wir heute immer noch viele Projekte, bei denen die Sicherheit erst kurz vor dem Start mit einbezogen wird. Unserer Penetration-Tester finden hier in der Regel eine Vielzahl von Schwachstellen, die dann mit grossem Aufwand und unter Zeitdruck geschlossen werden sollen. Aus diesem Grund sehen wir die frühzeitige Einbindung von Sicherheitsthemen in die Entwicklung neuer Lösungen als kritischen Erfolgsfaktor für die «Digitale Transformation». «Security by Design» in diesem Kontext heisst, sich bereits während der Planung Gedanken über mögliche Risiken zu machen, diese zu bewerten und durch geeignete Gegenmassnahmen abzustellen. Mittelfristig wird kein Unternehmen innovative Lösungen ohne integrierte Sicherheit am Markt etablieren können. Kunden erwarten sichere Lösungen – es geht ihnen nicht nur um die Funktionalität, auch wenn diese noch immer das Hauptkriterium ist. Die Sicherheit von Produkten bezieht sich heutzutage nicht mehr nur auf den Schutz vor unmittelbaren physischen Gefahrenquellen, sondern gerade auch auf den Schutz vor Hackern, Manipulationen und den Zugriff auf persönliche Daten. Sicherheit ist somit auch aus wirtschaftlichen Aspekten alternativlos!

Dies erfordert auch ein Umdenken vieler Sicherheitsverantwortlicher. In vielen Unternehmen werden diese als «Projektverhinderer» wahrgenommen, die überall nur Risiken sehen und jegliche Innovationen verlangsamen oder in der Tat unterbinden. Tatsächlich sind jedoch viele heutige Services erst durch IT-Sicherheit möglich. Ohne Transport- und Datenverschlüsselung wären moderne und agile Cloud-Projekte undenkbar. Eine sichere Authentisierung wird heute durch SaaS-Angebote ermöglicht.

Um bei dem Beispiel Cloud zu bleiben: In den Anfangstagen haben viele Unternehmen aus vorgeschobenen Sicherheitsgründen auf die Nutzung von Cloud-Diensten verzichtet. Bei der «Digitalen Transformation» müssen die Sicherheitsverantwortlichen mit in Projekte einbezogen werden und diese aktiv unterstützen, um so Wettbewerbsnachteile zu verhindern.

Dass Sicherheit künftig ein ausschlaggebendes Differenzierungsmerkmal sein wird, verdeutlicht ein weiteres Beispiel: das Auto der Zukunft! Schon heute verbauen die Hersteller im Auto eine Vielzahl von Schnittstellen zur Aussenwelt, die

*IDG, Studien zu den Hamburger Strategietagen 2017, «4Digital – Die vier Disziplinen der Digitalisierung»

Defense_v6.indd 23 28.11.17 01:58

unterschiedliche Informationen austauschen und die über das Netz kommunizieren. Das «Connected Eco System» mit dem Austausch von Fahrer-, Fahrzeug- und Umgebungsdaten, das Versenden und der Empfang grosser Informationspakete, Autonomes Fahren, Remote Software Updates sind nur einige Teilaspekte unseres zukünftigen mobilen Fahrerlebnisses.

Wie kann eine Sicherheitsstrategie erfolgreich in die «Digitale Transformation» eingebaut werden und auch mögliche zukünftige Risiken abdecken?

Der wichtigste Punkt innerhalb der Sicherheitsstrategie im Rahmen der «Digitalen Transformation» ist, dass man seine spezifischen Risiken kennt und diese entsprechend des eigenen Risikoprofils bewertet. Hierfür bietet NTT Security Methoden zur Risikoanalyse für seine Kunden an. Nur wer seine Risiken kennt, kann gezielt Massnahmen zur Prävention in Sicherheitsarchitekturen einbauen. Für das IT-Management bietet dies den Vorteil, dass jegliche Sicherheitsmassnahmen nicht willkürlich, sondern strukturiert und bewertet umgesetzt werden. Durch strukturierte Analysen müssen auch Aspekte und Szenarien betrachtet werden, die im Rahmen der Standard-IT bisher nur wenig Relevanz hatten. Im Rahmen der «Digitalen Transformation» hat z.B. die starke Vernetzung von Produktionssystemen extrem an Wichtigkeit gewonnen, da hier ganz neue Angriffsvektoren für Cyber-Angriffe entstanden sind.

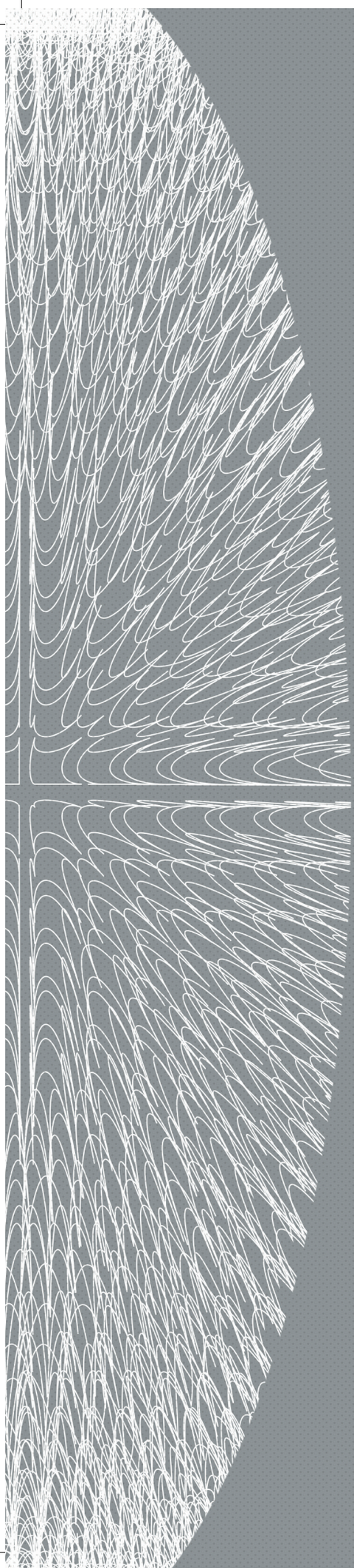
Allgemein ist festzustellen, dass die Menge der von Unternehmen gespeicherten Daten und deren Wert immer weiter zunimmt. Sie müssen zum einen immer verfügbar sein, zum anderen vor Missbrauch geschützt werden. In welchem Masse ist dieses Bewusstsein in den Vorstandsetagen vorhanden und welche konkreten Handlungen leiten die Verantwortlichen daraus ab?

Grundsätzlich ist ein gestiegenes Bewusstsein zu beobachten, welches jedoch von Branche zu Branche etwas differenziert. In Branchen, die seit Jahren mit hohen regulatorischen Anforderungen umgehen müssen, besteht auch bei Vorständen eine signifikant höhere Awareness für Security-Anforderungen und ein Verständnis für deren Relevanz für das eigene Geschäftsmodell. Überraschenderweise finden sich auch immer noch Unternehmen, die gemäss dem Motto «Uns wird es schon bei einem Cyber-Angriff nicht treffen» handeln.

Oftmals klaffen auch noch immer Anspruch und tatsächliche Umsetzung von Sicherheitsmassnahmen auseinander: IT-Sicherheit ist solange wichtig, bis entsprechende Budgets beantragt werden. Je nach Branche sollten mindestens zwischen 5% und 8% des IT-Budgets für IT-Sicherheit vorgesehen werden.

Mit dem richtigen Budget ist aber nur die Anfangshürde genommen. Wie setze ich dieses sinnvoll ein? Wie finde ich den richtigen Mix zwischen Prävention und Detektion? Sind meine Sicherheitsmassnahmen noch angemessen? Make-or-Buy-Entscheidung in Bezug auf den Aufbau eigener Kapazitäten oder die Nutzung von Managed-Security-Providern?

Defense_v6.indd 24 28.11.17 01:58



Mit der «Digitalen Transformation» ändern sich viele Parameter. Ladenöffnungszeiten verschwinden – Onlineshops sind rund um die Uhr geöffnet, entsprechend muss die Cyber-Abwehr auch rund um die Uhr einsatzbereit sein. Klassische Perimeter sind nicht mehr vorhanden. Aufzüge, Produktionsmaschinen und IT-Geräte kommunizieren in der ganzen Welt mit den internen Systemen – traditionelle Firewalls sind hier machtlos.

Dieses Bewusstsein für neue Chancen, aber auch damit verbundene Risiken wächst und ist dringend notwendig, um das Überleben und die Wettbewerbsfähigkeit eines Unternehmens in der digitalen Neuzeit zu gewährleisten. Das Zusammenwachsen von Digitalisierung und IT-Sicherheit – auch organisatorisch oder zumindest in Projekten – ist daher unabdingbar.

Neben der freiwilligen Implementierung von Massnahmen zur Erhöhung der Cybersicherheit für Unternehmen tritt im Mai 2018 die Datenschutz-Grundverordnung in Kraft, welche den Schutz personenbezogener Daten der Bürger im Europäischen Wirtschaftsraum vereinheitlichen soll. Welche Konsequenzen hat dies für Unternehmen bzw. mit welchen Chancen und Risiken müssen sie sich auseinandersetzen?

Die DSGVO hat die Sicherheit und Bedeutung von IT Security nochmals erhöht. Umso überraschender war für mich das Ergebnis der von NTT Security in Auftrag gegeben Risk-Value-Studie, nach der gerade mal die Hälfte der Unternehmen die Relevanz der DSGVO für ihr Geschäft sehen.

Durch die Vorgaben der DSGVO werden die personenbezogenen Daten von EU-Bürgern weltweit geschützt. Die Datenhoheit liegt dann nicht mehr bei dem Unternehmen, welches die Daten erfasst hat, sondern bei dem EU-Bürger selbst. Meiner Meinung nach bietet die DSGVO für EU-Unternehmen viele Wettbewerbsvorteile auf dem globalen Markt. Nicht nur, dass die DSGVO als Vorlage für viele andere Länder genutzt werden soll, sie zeigt den Kunden auch, dass innerhalb der EU sehr sorgsam mit personenbezogenen Daten umgegangen wird. Besonders im Wettbewerb mit amerikanischen Unternehmen, können EU-Firmen im Umgang mit personenbezogenen Daten auf grösseres Vertrauen der Kunden bauen. Nichtdestotrotz ist für die Unternehmen viel zu tun, um alle Vorgaben der DSGVO zeitgerecht umzusetzen.

Welche Folgen kann der Nachweis einer Nichteinhaltung der Vorschriften haben und wie können Sie Unternehmen unterstützen, um den Grad der Betroffenheit von der neuen Verordnung zu analysieren?

Im Falle einer vorsätzlichen Nichteinhaltung der DSGVO-Vorgaben besteht für alle Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten, die Strafandrohung von 20 Mio. Euro bzw. 4 % des Konzernjahresumsatzes. Die NTT Gruppe unterstützt Kunden – angefangen von der strukturierten Analyse der Vorgaben und dem Mapping auf das jeweilige Unternehmen bei der Etablierung von Prozes-

Defense_v6.indd 25 28.11.17 01:58

sen bis hin zur technischen Umsetzung geeigneter Maßnahmen. Die größte Herausforderung für viele Kunden ist die strukturierte Analyse, an der Stelle, an der personenbezogene Daten im Unternehmen verarbeitet werden.

Hierbei sind die Standard IT-Systeme relativ schnell analysiert. Oft liegen aber auch personenbezogene Daten in lokalen Access Datenbanken, auf externen Servern für z. B. Marketingaktionen oder Cloud-Anwendungen, die ausserhalb der Corporate IT betrieben werden. Diese Systeme können nur durch eine Kombination von strukturierten Analysen mit Assessments und technischen Lösungen identifiziert werden.

Mit welchen Schritten kann ein Unternehmen fit für die neuen EU-Vorgaben gemacht werden?

Ganz am Anfang steht die Schaffung einer Awareness für die DSGVO. Bei der Analyse vorhandener Datenschutzdokumentationen und Prozesse und der Erkennung der Gaps zur DSGVO kann strukturiert vorgegangen werden. In der Identifikation der Systeme mit personenbezogenen Daten liegt die grösste Herausforderung vieler Unternehmen. Danach können Prozesse für Auskunft, Löschen und Übertragung personenbezogener Daten aufgestellt werden. Die Umsetzung in allen IT-Systemen insbesondere für das Löschen von Daten wird oft unterschätzt, da viele Systeme für diese Anforderung nur bedingt ausgelegt sind bzw. die Auswirkung des Löschens von Daten auf Folgesysteme nur mit hohem Aufwand abgeschätzt und implementiert werden kann. Auch die Einbindung der Rechtsabteilung zur Beurteilung von Vorgaben der DSGVO auf Verträge mit Kunden und Zulieferern muss parallel erfolgen. Nicht zu vergessen ist natürlich die Vorgabe «Datenschutz by Design» für alle neuen Anwendungen und Systeme. Viele unserer Kunden denken bei der DSGVO oft nur an ihre Kundendaten. Wichtig ist, dass die Vorgaben für alle personenbezogenen Daten von EU-Bürgern gelten, also z.B. auch für Mitarbeiterdaten.

Ein nicht zu unterschätzender Aspekt für die DSGVO ist zudem die Meldepflicht innerhalb von 72 Stunden, die neben einem durchgängigen Incident-Response-Prozess auch die entsprechenden technischen Lösungen für die Früherkennung erfordert, so dass ein Unternehmen einen potenziellen Datenverlust nicht erst aus der Presse erfährt. Hier sind Unternehmen im Vorteil, die schon durchgängige Information-Security-Management-Systeme (ISMS) implementiert haben, jedoch gilt es diese zu validieren und entsprechend zu erweitern.

Defense_v6.indd 26 28.11.17 01:58

Kai Grunwitz

Kai Grunwitz ist seit Juli 2017 Senior Vice President EMEA bei NTT Security und für das Business und die Entwicklung der Go-To-Market-Strategien der Consulting- und Managed-Security-Bereiche verantwortlich. Der Diplomkaufmann verfügt über mehr als 20 Jahre Erfahrung in Top-Management-Positionen in der IT-Branche. Vor seiner Tätigkeit bei NTT Security war er Vice President Consulting Northern Europe bei der Oracle Corporation sowie Mitglied des Country-Leadership-Teams in Deutschland. Zuvor zeichnete er als Head of Professional Services Central Europe bei Sun Microsystems verantwortlich.

We hope that you enjoyed our event.

Are you ready to join the TEDxHSG community?

www.tedxhsg.org

Dr. Ursula von der Leyen
German Minister of Defence

The Digital Transformation of the Bundeswehr

The German Minister of Defence describes in what way the most recent technological innovations influence the Federal Defence. However, the Bundeswehr faces challenges with digitalisation, too, whether they emerged internally or they revealed themselves as a serious external threat.

Defense_v6.indd 28 28.11.17 01:58

Digitalisation will without a doubt be one of the major topics of the coming decade. There is not a single area that will not be hugely impacted by it – administration, economy, and ultimately our entire society. The change has already begun – and it is gaining momentum. Here are some figures and keywords to illustrate this: This year, 8.4 billion devices are said to be connected to the Internet of Things – more than people living on this planet. 3-D printing, 3-D scanning and reverse engineering are turning entire industries upside down. Education and science are being revolutionised by cloud computing and streaming technologies.

Of course, all this has had an impact on the internal and external security of nations and their armed forces. They, too, must face the facts of digitalisation and go along with the changes, which hold tremendous opportunities for the operational readiness and combat efficiency of the military. However, there are also challenges, both technical and cultural in nature. Let me illustrate this by taking a look at the Bundeswehr.

The Bundeswehr is a major organisation. It employs about 260,000 men and women, roughly 180,000 of which are soldiers. Approximately 1.1 million e-mails are sent from Bundeswehr offices every day. Digitalisation thus offers the opportunity to make the administration of the Bundeswehr more efficient and effective. In 2017 alone, we have spent about 1.6 billion euros just on digitalisation and IT. Add to that another 1 billion euros in personnel expenditure. The range of investments is wide, from new radio equipment to computer hardware and contracts with service providers.

But digitalisation is not only important in administration. It is also the key to modern management and crucial in military operations. Because everything that moves, whether on land, at sea or in the air, is increasingly supported by digital systems: The Eurofighter, for instance, contains 80 computers and 100 km of wires – which is, of course, a dream come true for any hacker. It therefore comes as no surprise that an average of 4,500 attacks are carried out on Bundeswehr systems every day.

This is not only a matter of equipment, however, but also of data and communication. Because every «battle», whether it is fought on land, at sea or in the air, is at the same time always a battle for «informational power». This is why armed forces such as the Bundeswehr need their own networks and software to be both functional and resilient.

New Structures

Therefore, we have created completely new structures in the Bundeswehr for the past three years: In a first important step, we pooled all cyber and IT responsibilities within the Ministry of Defence in a new Directorate-General in October 2016. It is headed by a Chief Information Officer, a newly established post, who has architecture and budget authority.

In a next step, the German Cyber and Information Domain Service Headquarters began operation in April 2017. In addition to the «traditional» services – the Army, Air

Defense_v6.indd 29 28.11.17 01:58

Force and Navy – the Bundeswehr now disposes of cyber forces amounting to approximately 13,500 troops. This way, we are responding to the demands of the cyber and information domain as a military dimension, thus increasing visibility, efficiency and the flow of knowledge in this strategically crucial area. Because by now, cyber/IT forces are no longer secondary service providers nor «mere» facilitators, they have become essential.

Expanding our digital capabilities

These organisational decisions and the subsequent restructuring have made us something of a trailblazer in Europe, as not many nations have dared to take this step yet. We intend to maintain this leadership role and expand it, particularly in terms of technology. First of all, we will earmark funds explicitly for disruptive and exponentially developing technologies. And secondly, we will enhance our own digital capabilities. To this end, we opened a ministerial research facility entitled Cyber Defence and Smart Data at the Bundeswehr University in Munich in June 2017. We are investing heavily in this project, including more than 70 million euros for new infrastructure and over 12 million euros of permanent investments. Hereby we will create 13 new professorships and 65 permanent positions for research and technical associates. In the long run, we want Munich Bundeswehr University to become one of the key research and development facilities in governmental IT security research.

Along with the research activities, we are also massively expanding academic training. In January 2018, a new international and interdepartmental master's programme for cybersecurity will begin at the Munich Bundeswehr University. Moreover, Pöcking on Lake Starnberg is home to the Bundeswehr Communication and Information Systems School. It hosts around 500 training courses annually with 5,000 participants.

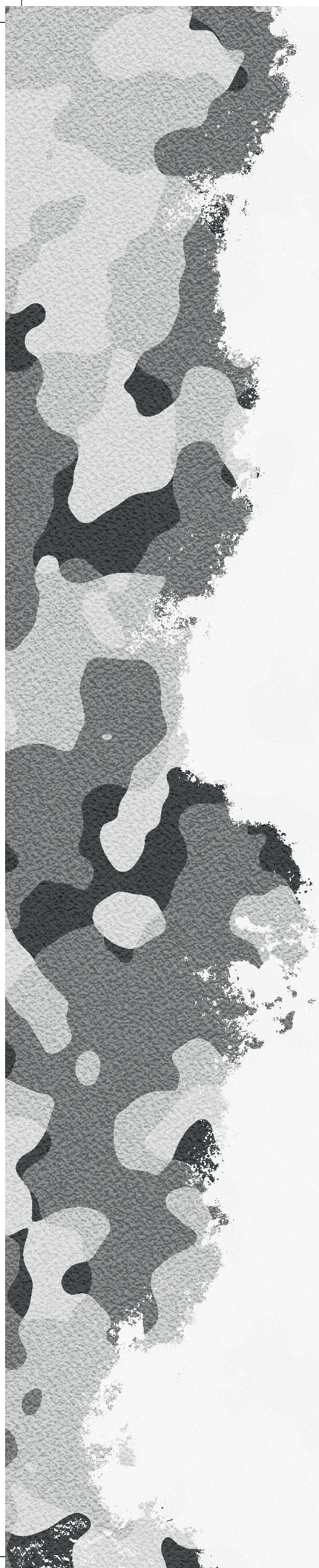
In order to expand our digital capabilities, we must also take account of key drivers and sources of innovation such as start-up and digital companies in a more systematic fashion. This is why we have been testing what we refer to as the Cyber Innovation Hub since September 2016. Its task is to identify and promote disruptive technologies. In this context, we are actively approaching drivers of innovation and start-up companies.

With the Cyber Innovation Hub we have established a platform that is urgently needed to deal with rapidly changing technological innovation. The US Army used to make essential contributions to new technological developments in accordance with this principle. Just think about ARPANET in the 1960s and 70s, which played a huge part in the development of the internet. Today, however, the military is often left behind by technological innovation in the IT sector. We must change that.

Incorporating digitalisation in leadership training

Digitalisation is of course more than just a technological challenge, it has also a massive impact on the conditions of underlying leadership and leadership culture.

Defense_v6.indd 30 28.11.17 01:58



Thanks to digitalisation, all hierarchical levels have unlimited access to very diverse information today. Communication between superiors and subordinates can be transmitted virtually in real-time across these levels. All of a sudden, the highest-ranking leaders at home are able to «look over the shoulder» of common soldiers in their country of deployment. While there are benefits to this scenario, it also entails the temptation of giving orders over a distance of thousands of kilometres – and going over the head of the superior in theatre. Whenever someone uses technological innovation and a computer screen to interfere with somebody else's work, this is more than just distrustful and patronising – it fails to recognise the simple fact that the soldier in theatre usually has the best qualification for the specific situation and also has a lot more information at their disposal.

And then there is still the matter of responsibility: Permanent «remote micromanagement» will ultimately eradicate independent thinking and acting among our military personnel. This would spell the end of mission-type command and control, which is one of the successful leadership principles practiced in the Bundeswehr. What we want to achieve is quite the opposite. For this reason, we must incorporate digitalisation, particularly into leadership training.

Another task is to develop processes in order to securely and profitably use the exponentially growing amount of information and data we can collect today thanks to modern technology. Our problem nowadays is no longer a lack of data, as it used to be for military leaders in past centuries. Our challenge lies in rapidly and effectively filtering and interpreting this gigantic amount of information.

Generally speaking, digital transformation requires organisational culture to be transparent and open. We must transform the well-known «need-to-know" principle into a «need to share». But at the same time, we must see to it that information and data reach their destination accurately – in terms of both time and level of detail.

Handling Big Data

Finally, training and leadership must deal with some key questions created by big data and advanced analytics: How do we train users in handling data, but also in handling algorithms? Big data analysis is always based on assumptions which lead to statistical probabilities. This ranges from tools rating the creditworthiness of individuals to programs forecasting the progression of crises and conflicts. The models underlying these tools may be based on wrong assumptions or assumptions that can change over time. This is why it is so important to know and to discuss them. Moreover, predictions – even if they are based on Big Data – are never more than probabilities. They are not predetermined, they are not «facts». For instance, while the highest probability level in a scenario may be only 30 percent, a program would rate such a scenario as dominant. But 70 percent would contradict this scenario! This is why algorithms, their functions, the opportunities and risks they entail are a top priority at the command level. That is the ambition of the Bundeswehr.

Defense_v6.indd 31 28.11.17 01:58

Digitalisation as an opportunity for armed forces

As we see it, digitalisation is more than a leap in technology. We want to use digitalisation as an impetus for re-evaluating our structures, our work processes and our «corporate culture». We want to modernise, learn and innovate – without abandoning what is tried and trusted. For armed forces such as the Bundeswehr, digitalisation is a great opportunity to increase effectiveness and efficiency, which in turn increases operational readiness and combat efficiency. This will enable us to better fulfill our mission: to continue to protect the security of our people despite the crises and new dangers of the 21st century.

Dr. Ursula von der Leyen

Ursula von der Leyen studied economics at the University of Göttingen, the University of Münster and the London School of Economics and Political Science. From 1980 to 1987 she attended Hanover Medical School (MHH). She obtained her Dissertation in Medicine in 1991 and was awarded the degree of Dr. med. Ursula von der Leyen started her political activities in 1990 when she became a member of the Christian Democratic Union (CDU). In 2003 she became a member of the Lower Saxony state parliament and was appointed State Minister of Social Affairs, Women, Family Affairs and Health. In 2005 Ursula von der Leyen started her career in federal politics as Federal Minister of Family Affairs, Senior Citizens, Women and Youth. In 2009 she became a Member of Parliament (Deutscher Bundestag) and was appointed as Federal Minister of Labour and Social Affairs. In 2013 she was appointed as Minister of Defence.

Ursula von der Leyen was born in Brussels in 1958. She lives near Hanover. She is married with Professor Heiko von der Leyen. The couple has seven children.

Defense_v6.indd 32 28.11.17 01:58

Max Hofmann

Generalsekretär für den Verband der Schweizerische Polizei-Beamter VSPB

Herausforderungen des polizeilichen Alltages

Die zunehmende Gewaltbereitschaft gegenüber Polizisten bereitet Max Hofmann Sorgen. Im Interview mit dem St. Gallen Business Review geht er zudem unter anderem auf die Veränderung im polizeilichen Alltag, die Anforderungen an private Sicherheitsfirmen und die sich stellenden Herausforderungen in der Zukunft ein.

Herr Hofmann, können Sie uns Ihren Werdegang beschreiben?

Max Hofmann: Ich bin 53 Jahre alt und habe 1982 die Matura erlangt. 1988 habe ich die Polizeischule im Kanton Tessin absolviert. Zwischen 1989 und 1998 war ich in verschiedenen Bereichen der Sicherheitspolizei tätig. 1998 wechselte ich in die Kriminalpolizei, wo ich verschiedene Spezialisierungen– vom Dezernat Leib und Leben bis hin zur BetMG Bekämpfung ausgeübt habe. Seit dem 1. Juli 2005 arbeite ich vollamtlich als Generalsekretär für den Verband der Schweizerische Polizei-Beamter VSPB in Luzern.

In vielen Städten hat die Gewalt gegenüber der Polizei in den letzten 10 Jahren zugenommen. Kann man dieses Phänomen erklären?

Der VSPB verfolgt seit Jahren mit grossem Interesse und Besorgnis die Problematik der Gewalt gegen Behörden und Beamte, die in Artikel 285 des Strafgesetzbuches Geahndet wird. Wenn wir im Jahr 2000 noch 774 Anzeigen gegen diesen Artikel zu verzeichnen hatten, waren es im Jahr 2015 über 2800. Dieses Phänomen zu erklären ist gar nicht einfach und bräuchte sehr wahrscheinlich einen grösseren Beitrag für sich selbst. Was aber festgestellt werden kann, ist ganz klar ein genereller

Defense_v6.indd 33 28.11.17 01:58

Verlust des Respektes gegenüber alles was Autorität ist oder Autorität darstellt. Somit sind offensichtlich Polizistinnen und Polizisten generell ein Feindbild in bestimmten Situationen. Alkohol, die 24-Stunden-Gesellschaft oder die Angst vor einer unsicheren Zukunft können dann rasch Auslöser einer Auseinandersetzung sein.

Die Petition «Stopp der Gewalt gegen die Polizei» ist beim ersten Anlauf gescheitert. Was erhoffen Sie sich von der neuen Arbeitsgruppe «Gewalt gegen die Polizei»?

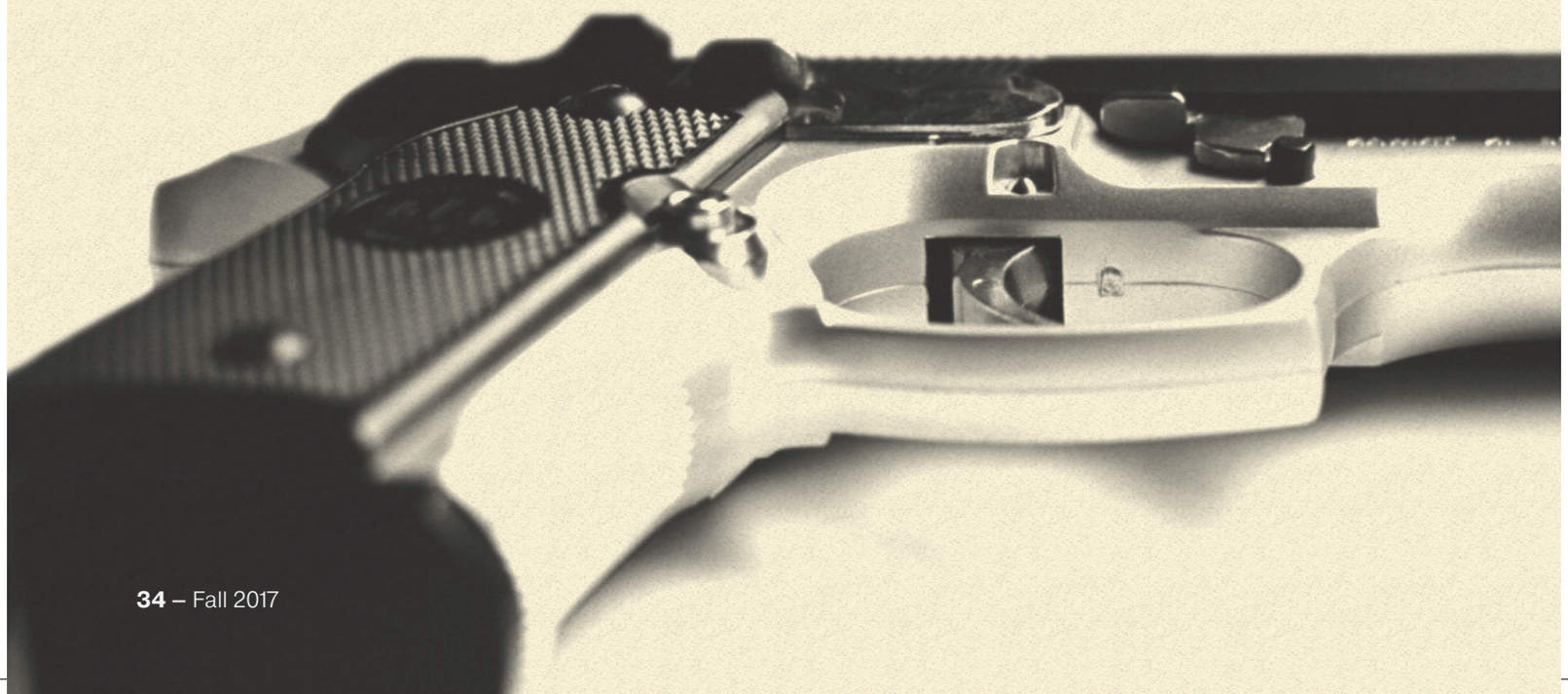
Leider konnten wir mit unserer Petition vom 2009 nicht das erreichen was wir uns als Schlussresultat vorgestellt hatten. Auch wenn es eventuell als eher unwichtig angeschaut werden könnte, haben wir aber erreicht, dass Politik, Medien und auch die Bevölkerung sich mit diesem sehr schlimmen Phänomen auseinandersetzen mussten und weiterhin müssen. So konnten wir auch dieses Anliegen in der parlamentarischen Gruppe für Polizei und Sicherheitsfragen einfliessen lassen. Durch die Arbeit der Arbeitsgruppe des VSPB-Zentralvorstands wurden dann die nötigen Argumente, Fakten und Ideen zusammengestellt und vorbereitet. Diese Vorarbeit hat mitgeholfen, dass die zwei parlamentarischen Initiativen letztlich im Parlament eingereicht wurden. Hier sehen wir im Moment die besten Chancen für unser Anliegen und erhoffen uns viel durch die beiden politischen Vorstösse.

Höhere Strafen können abschrecken, scheinen alleine aber nicht genug zu erreichen, werden weitere Massnahmen eingesetzt um Polizisten zu beschützen?

Es ist offensichtlich, dass nur höhere Strafen das Problem der Gewalt nicht lösen kann und auch, dass andere Massnahmen im Einklang zusammen eingesetzt werden müssen. Das Problem ist sehr gross und muss als soziales Phänomen betrachtet werden. Darum müssen unbedingt die nötigen Mittel und Instrumente eingesetzt werden, damit nicht nur der Respekt zurückgewonnen werden kann, sondern auch der Staat wieder Herr der Lage wird. Hierfür hat das EJPD eine durch fedpol dirigierte Arbeitsgruppe ins Leben gerufen, die mögliche Strategien, Ansatzpunkte und Lösungen vorschlagen sollte. Wir warten gespannt auf die ersten Informationen.

Welche Auswirkungen hat die steigende Präsenz von Internet und Sozialen Medien auf Ihre Arbeit?

Die neuen Medien sind ein Hilfsmittel und ein Kommunikationsinstrument, welche heutzutage als selbstverständlich gebraucht werden. Auch die Polizei kann und muss diese Instrumente nutzen und somit die ab und zu negativen Aspekte derselben akzeptieren. Wenn heute diese Medien genutzt werden so müssen wir uns auch damit befassen und



Defense_v6.indd 34 28.11.17 01:58

auch über diese Medien kommunizieren. Somit bleiben wir in Kontakt mit den Benutzern und auch der 2.0 Bevölkerung. Es ist somit unabdingbar die nötigen Mittel einzusetzen (finanzieller Art) damit wir diese Medien haben und nutzen können.

Private Sicherheitsdienste wachsen rasant und oft gibt es kein «Gütesiegel« für diese Unternehmen. Nach welchen Kriterien sollte man diese Firmen beurteilen?

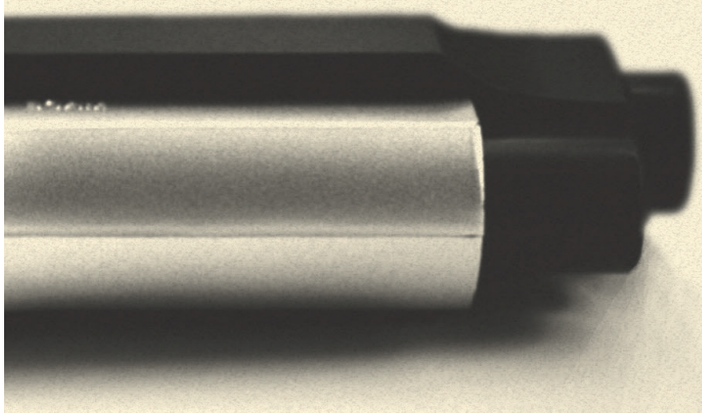
Private Sicherheitsunternehmungen machen generell einen guten Job und können – wenn sie in einem eingerahmten, klaren und geregeltem Aufgabenbereich tätig bleiben – als wahre Unterstützung für die innere Sicherheit des Landes sein. Es ist aber wichtig, dass hier für alle die gleichen Spielregeln und Vorschriften gelten. Ein Gütesiegel wäre allerdings ein wichtiger Schritt in dieser Richtung. Dazu braucht es aber zuerst eine schweizweite Regelung dieser Firmen. Ausbildung, Weiterbildung, Kompetenzen und Haftung sind nur einige der Punkte, die in so einer Regelung Platz finden müssen. Leider hat sich herausgestellt, dass ein schweizweites Konkordat nicht zustande kommen wird. Das ist schade, denn man arbeitete schon seit Jahren daran. Unserer Meinung nach kann nur eine Bundeslösung diese fehlende Regelung sein. Interessant ist auch zu wissen, dass hier der Verband Schweizerischer Sicherheitsdienstleistungs-Unternehmen VSSU auf unsere Linie ist und dieselbe Idee verfolgt.

Wie ist es zu diesem «Security Branchen Boom» gekommen?

Die Frage nach Sicherheit ist in den letzten Jahren gestiegen und das subjektive Sicherheitsgefühl spielt natürlich eine ganz grosse Rolle. Prävention und Präsenz sind eines der wichtigsten Aspekte um das Sicherheitsgefühl zu stärken und auch als abschreckende Massnahme gegenüber der Kriminalität zu wirken. Somit ist das Aufbieten von Sicherheitsfirmen eine Antwort auf das Bedürfnis der Präsenz und Sichtbarkeit von Sicherheitsstrukturen. Dies muss auch der Staat als Hilferuf wahrnehmen und im Sinne von Aufstockungen des Personal und mit dem Einsatz der nötigen finanziellen Mitteln konsequent handeln, damit die innere Sicherheit weiterhin gewährleistet werden kann.

Die polizeiliche Zusammenarbeit soll im europäischen Raum verbessert werden. Wie wichtig ist diese Zusammenarbeit für den VSPB?

Zusammenarbeit und Informationsaustausch sind in dieser grenzenlosen und globalisierten Welt eines der Mittel die absolut ausgenutzt werden müssen. Ohne hier in eine politische Debatte einzutreten ob Schengen ja oder nein oder ob EU ja oder nein (was grundsätzlich die Zusammenarbeit oder den Datenaustausch nicht in Frage stellen sollte) ist es allen klar geworden, dass ohne Informationen die Arbeit



Defense_v6.indd 35 28.11.17 01:58

stark erschwert wird. Somit steht auch fest, dass alles daran gesetzt werden muss damit Informationen und Zusammenarbeit eines der Prioritäten im Rahmen der inneren Sicherheit bleibt.

Jeder Polizist, der im Aussendienst arbeitet sollte sehr stress beständig und versiert im Umgang mit Menschen sein. Welche speziellen Trainings folgen Ihre Polizisten?

Mit der beruflichen Anerkennung auf Bundesebene im Jahr 2003 hat die Ausbildung der Polizistinnen und Polizisten einen wichtigen Schritt vorwärts gemacht. In den regionalen Ausbildungszentren werden die nötigen Instrumente und Fähigkeiten erlernt, damit in den verschiedensten Situationen korrekt und richtig gehandelt werden kann. So sind z.B. Ethik und Psychologie wichtige Schulungs- und Prüfungsfächer. Ausbildung und Weiterbildung sind und bleiben eines der wichtigsten Instrumente für die Polizistinnen und Polizisten. Demzufolge sind die Diskussionen und Vorbereitungen zur Modernisierung und Anpassung des Bildungspolitischen Gesamtkonzeptes BGK 2020 für die Strafverfolgungsbehörden sehr wichtig und werden durch den VSPB auch unterstützt.

Wie hat sich die Arbeit der Polizei in den letzten Jahren verändert?

Die Aufgaben der Polizei sind in den Jahren stetig gestiegen und auch die Anforderungen an die Polizistinnen und Polizisten haben diese Entwicklung mitgemacht. Die rasante Kommunikation, die Grenzenlose Kriminalität, die Globalisierung der Polizeiarbeit, die 24-Stunden-Gesellschaft und die sinkende Hemmschwelle gegenüber jeglicher Autorität haben natürlich unsere Arbeit nicht erleichtert. Aber die Professionalität aller Polizistinnen und Polizisten hat und wird es auch in Zukunft schaffen, dem alles Stand zu halten und weiterhin die innere Sicherheit des Landes zu garantieren.

Welche Entwicklungen sehen Sie voraus?

Die Technologie wir uns weiterhin in unserer Arbeit prägen – sowohl im positiven wie aber auch im negativen Sinne. Das heisst, dass wir immer auf dem höchsten Niveau in Sachen Material und Ausbildung stehen müssen, um die Kriminalität mit den richtigen Instrumenten bekämpfen zu können. Schön wäre es all die nötigen Mittel zu haben damit wir diese Phänomene voraussehen und verhindern könnten.

Einige Berufsverbände klagen über mangelndes Interesse für ihren Berufsstand und können nicht ausreichend Nachwuchskräfte rekrutieren. Hat die Polizei das gleiche Problem?

In den letzten Jahren haben sich laut Aussage einiger Kantone vereinzelt Engpässe ergeben. Nach unseren Informationen hat es aber immer noch genügend junge Frauen und Männer, die sich für den schönen und abwechslungsreichen Polizeiberuf interessieren. Ganz klar ist es sehr wichtig, dass die Rahmenbedingungen stimmen, damit der Beruf auch weiterhin attraktiv bleibt. Es geht natürlich nicht nur um den Lohn - der sicher ein wichtiger Bestandteil ist – sondern auch um Pensionierungsalter, Rechtschutz, Ausrüstung usw.

Max Hofmann

Generalsekretär für den Verband Schweizerischer Polizei-Beamter VSPB

Defense_v6.indd 36 28.11.17 01:58

Jean-Michel Rousseau

Programme Manager at the Geneva Centre for the Democratic Control of Armed Forces (DCAF)

A good governance

Why regarding human rights is essential for growing a sustainable business.

Security functions traditionally provided by the state are increasingly undertaken by a range of private actors, such as private military and security companies. Moreover, extractives and other 'large footprint' industries (such as agribusiness, infrastructure, and telecoms) that operate in complex environments not only contract private security services, but also cooperate directly with the police, the armed forces, and ministries of interior and of defence. To give just two examples, 2.5 million private security guards are legally registered in Latin America and the Caribbean, meaning they outnumber police forces in nearly every state in the region; and oil, gas and mining companies frequently sign agreements with the police (and sometimes the armed forces) to protect their sites, upon remuneration. Due to the challenging environments in which they operate, certain companies favour a hard security stance over a softer approach that would focus on prevention and active engagement with the citizens and communities around them.

Thinking of security in terms of governance is useful because it emphasizes how a variety of public and private actors exercise power and authority over security, both formally and informally. Democratic oversight and accountability – pillars of good governance – have not kept up with the growing role of private actors in the security domain. Private security legislation does not include human rights obligations for companies and their staff; public entities staffed by a few civil servants are

Defense_v6.indd 37 28.11.17 01:58

supposed to certify and monitor tens of thousands of private security guards and security arrangements between companies and police are not effectively controlled by governments. Under-capacitated national authorities and underrepresented communities and citizens cannot adequately oversee the activities of private actors and hold them accountable in case of human right violations. This is a lose-lose situation. The absence of effective regulation contributes to an uneven economic playing field that discourages companies from carrying out the investments necessary to ensure stronger human rights compliance and provides a permissive environment for corruption and human rights abuses. This undermines any sustainable approach to preventing conflicts, further fuelling fragility while undermining social and economic development.

The human rights impacts of companies operating in fragile environments are prominent on the international policy agenda. Indeed, the protection of human rights is a crucial aspect of companies being responsible corporate citizens. This is also in their own corporate interest: respect for human rights and the promotion of good governance reduces risks for companies and their staff; lowers transaction costs; results in cost savings and limits legal liabilities. The United Nations Guiding Principles on Business and Human Rights (UNGPs), as well as sector-specific initiatives such as the Voluntary Principles on Security and Human Rights (VPs), have made security issues an established part of the business and human rights discourse. Numerous companies have publicly stated their compliance with human rights norms and allocated financial resources to support the implementation of the UN's Sustainable Development Goals, which include a goal on peaceful and inclusive societies. However, there is increasing concern that these initiatives, while being of great relevance in terms of reflection and discourse, have not yet led to a broad, sustainable strengthening of capacities on the ground, close to the lives and concerns of people. This is the key element required to protect and strengthen human rights over the middle and long run.

The UN's Sustainable Development Goals underline that good governance is key to sustainable development, peace, and security. Given its economic weight and political cloud, the private sector has the potential to act as a positive force multiplier in support of good governance in complex environments. This begins with leading by example on its own security set-up, notably prioritizing in-depth prior risk analysis and soft security measures. It means actively engaging public institutions and communities and strengthening them in their roles and mandates, for example by supporting human rights trainings for police forces assigned to production sites and the monitoring of the human rights impact of private security companies by national human rights institutions and by civil society. It is about making the case to other companies, decision-makers and the wider public that efficient regulation in the field of business and security actually strengthens (and not weakens) professional businesses, by reducing corruption possibilities and leveling the playing field with irresponsible competitors. A company's «social license to operate» can crumble quickly in the face of security incidents and human rights violations; only companies that can demonstrate through concrete deeds that their security approach is human rights compliant will be able to maintain this «social license» and thus be able to sustainably grow.

Defense_v6.indd 38 28.11.17 01:58

DCAF is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law and respect for human rights. It notably supports multi-stakeholder approaches that foster and strengthen innovative partnerships between states, parliaments, international organizations, civil society and the private sector. Concretely, this includes sensitisation and awareness-raising of these stakeholders on key private security governance concepts, and the support for the development of effective legal and policy frameworks at the national and regional level, via guiding tools, capacity-building, and training. For more information, please visit www.ppps.dcaf.ch and www.securityhumanrightshub.org.

Jean-Michel Rousseau

Jean-Michel Rousseau is a Programme Manager within the Public-Private Partnerships Division at the Geneva Centre for the Democratic Control of Armed Forces (DCAF). Jointly with the Head of Division, he is responsible for general management processes as well as a variety of programme management processes. He also leads the divisional engagement to strengthen private security regulation in Latin America and the Caribbean.

Prior to joining the Public-Private Partnerships Division, Jean-Michel Rousseau was Head of the North Africa desk at DCAF's Middle East and North Africa Division, a position in which he coordinated DCAF's operations in Egypt, Libya, Morocco, and Tunisia. He previously worked as a global strategy, governance, and organisational development consultant, and for German development agency GIZ in Colombia.

Jean-Michel Rousseau studied at Sciences Po Paris, Georgetown University, and the University of Oxford's Saïd Business School. He has taught at the Geneva Centre for Security Policy (GCSP) and at the Universidad Externado de Colombia.

Defense_v6.indd 39 28.11.17 01:58

Hans Lüber

Botschaftsrat und Militärberater bei der ständigen Vertretung der Schweiz bei der OSZE

Die OSZE

Ein Champion der «Soft Security»

Mit ihren 57 Teilnehmerstaaten in Nordamerika, Europa und Asien ist die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) die weltweit grösste regionale Sicherheitsorganisation. Hans Lüber, Militärberater bei der Ständigen Vertretung der Schweiz bei OSZE, schreibt in diesem Artikel über die Entwicklung der Organisation OSZE und erklärt, warum sie eine der wichtigsten friedensfördernden Organisationen der Welt ist.

Defense_v6.indd 40 28.11.17 01:58

Mit ihren 57 Teilnehmerstaaten in Nordamerika, Europa und Asien ist die Organisation für Si-cherheit und Zusammenarbeit in Europa (OSZE) die weltweit grösste regionale Sicherheitsorga-nisation. Sie setzt sich durch politischen Dialog über gemeinsame Werte und durch praktische Arbeit im Feld, die nachhaltige Veränderungen bewirkt, für Stabilität, Frieden und Demokratie für mehr als eine Milliarde Menschen ein.

Die OSZE bietet in erster Linie ein Forum für politischen Dialog zu einem breiten Spektrum von Sicherheitsfragen und eine Plattform für gemeinsames Handeln, welches letztlich auf die Ver-besserung der Lebensbedingungen der Menschen und Gemeinschaften abzielt. Mit ihrem um-fassenden Sicherheitsbegriff, abgebildet durch die politisch-militärische, die ökonomisch-ökologische und die menschliche Dimension, hilft die OSZE durch Zusammenarbeit bei Kon-fliktverhütung, Krisenmanagement und Konfliktnachbearbeitung Differenzen zu überwinden und Vertrauen zu schaffen. Vertrauens- und sicherheitsbildende Massnahmen (VSBM) bilden die wichtigsten traditionellen Mittel der OSZE, um mit Konfliktsituationen umzugehen.

Über ihre Institutionen, ihre Fachstellen, ihr Netz von Feldoperationen und eine grosse Anzahl von Feldprojekten befasst sich die OSZE heute mit Themen, die unsere gemeinsame Sicherheit betreffen: u.a. demokratische Kontrolle von Streit- und Sicherheitskräften, konventionelle Rüs-tungskontrolle und Abrüstung, Cybersicherheit, Terrorismus, Migration, Good Governance, Energiesicherheit, Menschenhandel, Demokratisierung, Medienfreiheit, Genderfragen und nati-onale Minderheiten.

Fakten und Zahlen:

Die OSZE umfasst 57 Teilnehmerstaaten und 11 Kooperationspartnerschaften mit Nachbarstaa-ten. Das OSZE-Gebiet wird deshalb illustrativ «from Vancouver to Wladiwostok» bezeichnet.

Der jährliche ordentliche Haushalt der OSZE beträgt für 2017 138.9 Millionen Euro, wobei die OSZE-Sonderbeobachtermission in der Ukraine (SMM), die Beobachtermission an der rus-sisch-ukrainischen Grenze und weitere, sog. extra-budgetäre Projekte aus ausserordentlichen Haushalten, gesponsert von Teilnehmerstaaten, finanziert werden. Die OSZE beschäftigt ge-genwärtig 3461 Mitarbeiter. Die Mehrheit davon (2868) arbeitet in den insgesamt 16 Feldopera-tionen. Der Rest ist im Sekretariat und den Institutionen tätig.

Ein Blick in die Geschichte: Die OSZE geht auf die frühen 70-er Jahre des letzten Jahrhunderts zurück, die Zeit des Kalten Krieges. Die Gründung der Konferenz über Sicherheit und Zusam-menarbeit in Europa (KSZE) schuf ein sehr wichtiges multilaterales Dialog- und Verhandlungs-forum zwischen Ost und West und die Schlussakte von Helsinki (1975) bildete einen politi-schen Meilenstein auf dem Weg zur Überwindung von Spannungen und des Wettrüstens. Eine Reihe von ausschlaggebenden Verpflichtungen und die zehn Grundprinzipien, der «Helsinki-Dekalog», regelten den Umgang der Staaten miteinander (inter-state) und mit ihren Bürgern (intra-state). Der Helsinki-Dekalog hat bis heute nichts von seiner Relevanz eingebüsst und wird in aktuellen Debatten, z.B. jener zum Konflikt in und um die Ukraine, oft zitiert. Von 1975 bis in die 1980er Jahre baute die KSZE im Zuge einer ganzen Reihe von Konferenzen die Ver-pflichtungen der Teilnehmerstaaten aus und verifizierte regelmässig deren Umsetzung. Nach dem Ende des Kalten Krieges leiteten die Teilnehmer-

Defense_v6.indd 41 28.11.17 01:58

staaten anlässlich des Gipfeltreffens von Paris eine Kursänderung der KSZE ein. In der Charta von Paris für ein neues Europa erhielt die KSZE den Auftrag, die sich durch erfolgreiche Entspannungspolitik ergebenden Chancen zu nutzen und aktiv zur Gestaltung des in Europa vor sich gehenden Wandels beizutragen und sich den neuen Herausforderungen der Zeit zu stellen. Die KSZE schuf ständige Strukturen, ein-schliesslich eines ständigen Sekretariats und einigen Institutionen und Feldoperationen. Nach dem Zerfall von Ex-Jugoslawien und den dadurch entstandenen Konflikten bemühte sich die KSZE an vorderster Front um Bewältigung der Krise und die Wiedererlangung des Friedens. 1994 wurde aus der KSZE, die inzwischen weit über ihre ursprüngliche Rolle hinausgewachsen war, die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE). Dank ihrer um-fassenden Mitgliedschaft und der Entwicklung von Partnerschaften mit angrenzenden Ländern, ihres ganzheitlichen Sicherheitsbegriffs und ihrer Flexibilität gibt die OSZE ihren Teilnehmer-staaten effektive und effiziente Instrumente und Hilfsmittel für die Auseinandersetzung mit ak-tuellen Sicherheitsfragen in die Hand.

Die Arbeitsweise der OSZE kann als inklusiv bezeichnet werden. Alle Teilnehmerstaaten der OSZE sind gleichberechtigt. Beschlüsse werden immer im Konsens gefasst, d.h. niemals wird eine Massnahme gegen den geäusserten Willen auch nur eines einzigen Teilnehmerstaates ge-troffen. Der Entscheidungsfindungsprozess ist deshalb oft herausfordernd, aber einmal gefasste Beschlüsse sind stark und von allen Teilnehmerstaaten mitgetragen. Organe der Beschlussfas-sung gibt es zwei: Die Botschafter kommen allwöchentlich im Ständigen Rat, dem regulären Beschlussfassungsorgan, und im Forum für Sicherheitskooperation, welches Beschlüsse zu militärischen Aspekten der Sicherheit fasst, zusammen. Einmal im Jahr treffen sich die Aus-senminister der Teilnehmerstaaten am Ministerrat und in unregelmässigen Abständen treffen sich die Staats- und Regierungschefs zu einem Gipfeltreffen, um auf höchster politischer Ebene Prioritäten zu setzen.

Der Generalsekretär, gegenwärtig der Schweizer Thomas Greminger, steht an der Spitze des ständigen Sekretariats in Wien. Dieses umfasst ein Konfliktverhütungszentrum und weitere Abteilungen und Dienststellen. Das Sekretariat unterstütz den amtierenden Vorsitz, welcher jeweils für ein Kalenderjahr von einem Teilnehmerstaat gestellt wird. Weiter befassen sich die nach Schwerpunkten gegliederten Abteilungen mit Themen wie Wirtschaft und Umwelt, Zu-sammenarbeit mit Partnerstaaten und anderen Internationalen und Regionalen Organisationen, Geschlechtergleichstellung, Bekämpfung des Menschenhandles sowie grenzüberschreitende Bedrohungen einschliesslich Terrorismus und Cybergefahren, Grenzmanagement und Reform der Polizeiarbeit. Sie verfolgen Trends, formulieren Expertengutachten und führen Feldprojekte (z.B. zur Munitionsvernichtung) vor Ort durch. Weitere Institutionen der OSZE sind der Beauf-tragte für Medienfreiheit (Instrument zur Frühwarnung im Falle von Verletzungen der Mei-nungs- und Medienfreiheit) der Hohe Kommissar für nationale Minderheiten (Instrument zur Verhütung von Konflikten, hervorgerufen durch ethnische Spannungen) und die Parlamen-tarische Versammlung (vereint mehr als 300 Parlamentarier und Parlamentarierinnen aus den OSZE Teilnehmerstaaten, um den Dialog und die Zusammenarbeit zu begünstigen und demo-kratische Compliance zu fördern).

Was tut die OSZE auf dem Feld? Die meisten Mitarbeiter und Ressourcen der OSZE kommen in den Feldoperationen in Südosteuropa, Osteuropa, im Kaukasus und in Zentralasien zum Ein-satz. Feldoperationen werden auf Einladung des jeweiligen Gastlan-

Defense_v6.indd 42 28.11.17 01:58

des eingerichtet und ihre Mandate werden von den Teilnehmerstatten vereinbart. Sie unterstützen die Gastländer bei der Entwicklung ihrer Kapazitäten durch Projekte, die auf deren Bedürfnisse abgestimmt sind.

Die OSZE befasst sich auch mit Langzeitkonflikten in ihrer Region im Rahmen vereinbarter Formate. Dazu zählen die Verhandlungen zur Herbeiführung einer umfassenden politischen Lösung im Transnistrien-Konflikt, die Mink-Gruppe der OSZE, die sich um eine friedliche Lö-sung für den Bergkarabach-Konflikt bemüht, und die internationalen Genfer Gespräche, die nach dem Georgien-Konflikt vom August 2008 aufgenommen wurden. Gemeinsam unterstüt-zen die einzelnen Bestandteile der OSZE die Teilnehmerstaaten beim Aufbau von Vertrauen und ihren Bemühungen um eine freie, demokratische, gemeinsame und unteilbare euroatlantische und eurasische Sicherheitsgemeinschaft.

Das Aufflammen des Konfliktes in und um die Ukraine könnte eine neue Phase der OSZE ein-geleitet haben. Da der inklusive Charakter der Strukturen und Prozesse der OSZE, so schwer-fällig diese auch erscheinen mögen, einvernehmliche Beschlüsse auch in Zeiten erhöhter politi-scher Spannungen besser ermöglicht als beispielsweise die UNO, sind die Dienste der OSZE zum Management von Konflikten aktuell sehr gefragt. Die OSZE arbeitet als ein Champion der «Soft Security» aber lediglich mit ihren noch im Kalten Krieg konzipierten Werkzeugen der Vertrauens- und Sicherheitsbildung, um aktuell schwelende, heisse Konflikte anzugehen. Ver-trauensbildung ist ein Unterfangen das langfristig wirkt. Aktuell sind jedoch kurzfristigere Er-folge bei der Befriedung einer Region gefragt. Es muss der OSZE deshalb gelingen, ihre Tool-box zu aktualisieren und zu modernisieren, um weiterhin als effektiver Akteur, in Zusammenar-beit und komplementär zu anderen internationalen und regionalen Organisationen und NGOs nachhaltig erfolgreich zu sein.

Hans Lüber

Hans Lüber ist seit April 2012 als Botschaftsrat und Militärberater bei der Ständigen Vertretung der Schweiz bei der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), den Vereinten Nationen und bei den Internationalen Organisationen in Wien tätig. In dieser Funktion war er Teil des Schweizer OSZE-Vorsitzes 2014. Zusätzlich hat Hans Lüber gegenwärtig ein Mandat des FSK-Vorsitzes als Koordinator für das Wiener Dokument. Vor seinem Transfer nach Wien war er im Führungsstab der Armee als Chef Trainer auf operativer Stufe und als Verantwortlicher des Lessons Learned Prozesses der Armee tätig. Bis 2008 arbeitete Hans Lüber in diversen leitenden Funktionen im Bank- und Finanzsektor in Zürich und Genf. Er studierte in Bern Jurisprudenz, besitzt ein Anwaltspatent sowie und ein MBA des IMD. Parallel zu seiner beruflichen Tätigkeit machte Hans Lüber eine Karriere als Milizoffizier. Er kommandierte Verbände der Gebirgsinfanterie vom Kompanie bis zum Regimentsniveau, bestand die Generalstabsausbildung und wird aktuell als Generalstabsoberst noch immer für die operative Schulung eingesetzt.

Defense_v6.indd 43 28.11.17 01:58

Ueli Zoelly
Chef der Flughafenpolizei Zürich

Zukunftsmusik am Zürcher Flughafen

Ueli Zoelly, der amtierende Chef der Zürcher Flughafenpolizei, erklärt in diesem Interview das vielseitige Gefährdungspotenzial am Zürcher Flughafen und nimmt unter anderem Stellung zu neuen Technologien wie biometrischen Gesichtsvergleichen und der Drohnentechnologie.

Defense_v6.indd 44 28.11.17 01:58

Wie unterscheidet sich die polizeiliche Aufgabe an einem Flughafen von der in einer Stadt? Gibt es Unterschiede bezüglich der Sicherheitsbedürfnisse von Passagieren am Flughafen und Passanten in der Stadt?

Ueli Zoelly: Die Aufgaben der Polizei an einem Flughafen konzentrieren sich - namentlich an einem internationalen Landesflughafen - auf ein Objekt mit einem speziellen Bestimmungszweck. Das dürfte den wesentlichen Unterschied ausmachen.

Sind die relativ klaren geografischen Grenzen eines Flughafens ein Vor- oder Nachteil für die Gewährleistung der Sicherheit?

Sowohl als auch: Einerseits kann der Auftrag dadurch effizient erfüllt werden; anderseits schränkt das auf einem Flughafen geltende Regulativ die Bewegungsfreiheit ein.

Stellen Sie in den letzten Jahren eine Änderung der elektronischen Bedrohungslage am Flughafen fest? Sind Risiken im Zuge der Digitalisierung überhaupt noch greifbar?

Die sogenannten «Cyber Threats» sind in den letzten Jahren nicht nur für die Flughafenpolizei, sondern überhaupt für die Kantonspolizei Zürich zur immer grösseren Herausforderung geworden. Dem längst unbestrittenen Nutzen digitaler Technik steht ihre ebenso unbestreitbare hohe Verletzlichkeit gegenüber. Dies gilt gerade auch für einen modernen Flughafen.

Wie hat sich die Bedrohungslage aufgrund jüngster Ereignisse am Flughafen Zürich verändert? Wie reagiert man darauf?

Die potenzielle Gefährdung ist auch für den Flughafen Zürich grösser geworden, daran besteht kein Zweifel. Aber die Kantonspolizei (und mit ihr auch die Flughafenpolizei) hat reagiert: Das Dispositiv wurde angepasst, Ausbildung und Ausrüstung unserer Mitarbeitenden wurden auf die neue Bedrohung ausgerichtet, und die Kantonspolizei Zürich war das erste Korps, das eine breit abgestützte Sonderkommission zur Prävention und Bekämpfung terroristischer Gewalttaten auf die Beine stellte. Sodann finden - auch am Flughafen - regelmässig gemeinsame Übungen statt, in denen es darum geht, die ständige Einsatzbereitschaft zur Bewältigung komplexer Ereignisse zu trainieren.

Wie hat sich aufgrund der Drohnentechnologie das Gefährdungspotenzial aus der Luft verändert? Fällt das auch in den Zuständigkeitsbereich der Flughafenpolizei?

Zivile Drohnen werden derzeit in grosser Zahl verkauft und zunehmend von professionellen und privaten Nutzern hauptsächlich zum Fotografieren und Filmen eingesetzt. Dadurch steigt zumindest das hypothetische Unfallrisiko. Im Vordergrund stehen Zwischenfälle, die auf Fahrlässigkeit, Fehlbedienung oder ganz einfach Unvermögen zurückzuführen sind. So kann es - trotz an sich klarer Vorschrif-

Defense_v6.indd 45 28.11.17 01:58

ten (das Fliegen von Drohnen mit über 500 g Startgewicht in einem Radius von 5km um die Pisten ist verboten) - im Umfeld des Flughafens zu Annäherungen an startende, landende oder stehende Flugzeuge sowie an die Infrastruktur kommen. Denkbar sind ebenso deliktische Tätigkeiten mit Drohnen, wie das absichtliche Eindringen in gesperrte Zonen, das absichtliche Stören des öffentlichen Verkehrs oder Sabotageversuche. Mit all diesen Risiken befasst sich - zusammen mit der FZAG und dem Bundesamt für Zivilluftfahrt (BAZL) - selbstverständlich auch die Kantons- bzw. die Flughafenpolizei.

Wäre eine Nutzung von polizeilichen Drohnen am Flughafen Zürich eine Option bzw. gibt es bereits Projekte in diese Richtung? Wie beurteilt man diesbezüglich den Datenschutz?

Die Nutzung von Drohnen für polizeiliche Tätigkeiten wird zurzeit durch die Kantonspolizei Zürich praktisch geprüft. Es geht dabei vor allem um Einsätze zur Gefahrenabwehr. Erhebung, Aufbewahrung und Löschung von Daten richten sich nach den bestehenden Rechtsgrundlagen.

Am Flughafen Zürich gibt es ein Pilotprojekt zur Gesichtserkennung von Passagieren. Gibt es dazu bereits eine Zwischenbilanz bzw. Wie sehen Sie zukünftige Anwendungsmöglichkeiten solcher Projekte in Bezug auf den Datenschutz?

Das Pilotprojekt betrifft die geplante Einführung automatisierter Passkontrollschleusen für die Ein- und Ausreise am Flughafen Zürich. Mit «Gesichtserkennung» hat dieses Projekt allerdings nichts zu tun - es geht lediglich um eine biometriegestützte Vergleichsprüfung zwischen dem live aufgenommenen Gesichtsbild und dem im biometrischen Pass gespeicherten elektronischen Gesichtsbild, wobei parallel zur biometriegestützten Gesichtsprüfung die Passdaten im Fahndungsregister überprüft.

Wie stellt die Flughafenpolizei sicher, mit den Screening Methoden immer auf neustem Stand zu sein? Gibt es Kooperationen mit Sicherheitsbeauftragten anderer internationaler Flughäfen?

Die Hauptverantwortung für technologische und methodische Fragen, welche die Sicherheitskontrolle betreffen, liegt bei der Flughafen Zürich AG (FZAG) als verantwortliche Flughafenbetreiberin. Sie arbeitet aber eng mit der Flughafenpolizei zusammen, speziell bei der Grundlagenforschung - beispielsweise zu Fragen der Ausbildung - oder bei der Evaluation neuer Geräte. Und selbstverständlich werden immer wieder auch die Erfahrungen ausländischer Flughäfen berücksichtigt.

Defense_v6.indd 46 28.11.17 01:58

Wie relevant ist der finanzielle Aspekt bei den Sicherheitsbeauftragten/Flughafenpolizei? Gibt es gewisse Technologien, die zwar verfügbar wären, jedoch ausserhalb des Budgets liegen?

Der Entscheid darüber, in welche Technologie im Rahmen des Luftfahrtregulativs investiert werden soll, liegt letztlich bei der Flughafenbetreiberin.

Woher kommen die Informationen zur Bedrohungslage am Flughafen? Arbeiten Sie mit dem schweizerischen Nachrichtendienst zusammen? Gibt es womöglich sogar internationale Kooperationen?

Die Flughafenpolizei ist eng vernetzt sowohl mit korpsinternen Stellen als auch mit dem Bundesamt für Polizei und dem Nachrichtendienst des Bundes. Je nach konkretem Fall finden zudem auch Kontakte mit Sicherheitsbehörden im Ausland statt.

Ueli Zoelly, lic. iur.

Chef der Flughafenpolizei Zürich

Der gebürtige Zürcher kam 1960 zur Welt. Nach einem Juristischen Studium an der Universität Zürich machte er 1994 sein Rechtanwaltspatent. Bis 1997 arbeitete er als Rechtsanwalt mit den Schwerpunkten Straf-, Versicherungs- und Raumplanungsrecht. 1997 wechselte Ueli Zoelly als Offizier zur Stadtpolizei Zürich. Von 2003 bis 2006 arbeitete er als Chef der Kriminalabteilung bei der Schaffhauser Polizei. Im Jahre 2006 zog es ihn als Polizeioffizier und Geschäftsleitungsmitglied zurück nach Zürich zur Kantonspolizei. Seit dem 1. Mai 2013 ist Ueli Zoelly Chef der Flughafenpolizei Zürich.

Defense_v6.indd 47 28.11.17 01:58

Rolf Thomas Jufer

Partner und Mitglied der Geschäftsleitung
der Funk Insurance Brokers AG

Cyberrisiken ganzheitlich angehen

Immer mehr Unternehmen nehmen Cyberrisiken ernst und wappnen sich gegen Hackerangriffe. Verwaltungsrat und Geschäftsleitung sind besonders gefordert. Wollen sie doch einerseits die Chancen der Digitalisierung optimal nutzen und andererseits Angriffe wirksam abwehren.

Defense_v6.indd 48 28.11.17 01:58

Digitalisierung, Industrie 4.0, IoT - Begriffe, die eine neue Epoche für die Gesellschaft und Wirtschaft eingeläutet haben und so auch den Unternehmensalltag massgeblich prägen. Es geht für Unternehmen einerseits darum, die Chancen dieser Entwicklung optimal zu nutzen und sich andererseits auch den Risiken der dynamisch voranschreitenden Vernetzung von Menschen, Maschinen und Prozessen zu stellen.

Eine komplexe Aufgabenstellung, die zwar einen Projektanfang aber kein Projektende kennt. Die kontinuierliche Auseinandersetzung mit den neusten technischen Mitteln der Cyber-Abwehr/Cyber-Security als auch das Antizipieren von künftigen Angriffsformen (Threat Intelligence) gehören im Rahmen des IT-Risikomanagements ebenso dazu, wie das konsequente Umsetzen von operativen Massnahmen und das Durchführen von Kontrollen.

Kontinuierlicher Prozess mit spezialisierten Partnern

Etwas konkreter heisst das, regelmässig die Robustheit der eigenen Unternehmung zu prüfen, Mitarbeitende kontinuierlich zu sensibilisieren, die IT-Sicherheit permanent zu optimieren sowie sich im Rahmen und Zyklus des Cyber-Risikomanagements kontinuierlich ein Bild über das finanzielle Cyber-Restrisiko zu machen. Dieses Cyber-Restrisiko ist dann zu bewerten und gegebenenfalls in den Versicherungsmarkt zu transferieren.

Die Funk Gruppe beschäftigt sich seit Jahren mit Cyberrisiken. Via ihr internationales Netzwerk «The Funk Alliance» war sie am Puls der ersten grossen Fälle von Cyber-Kriminalität in den USA. «In unserer Branche herrschte damals grosse Unsicherheit», erinnert sich Rolf Th. Jufer, Geschäftsleitungsmitglied von Funk Insurance Brokers in der Schweiz. «Weder wir noch die Versicherer hatten Erfahrungen, wie mit diesem Thema umzugehen ist. Aber uns war sofort klar, da kommt ein neues und sehr komplexes Risiko auf unsere Kunden zu». Erst seit kurzer Zeit sind nun umfassende und kundenfreundliche Versicherungslösungen im europäischen Raum erhältlich, mit der die Kunden heute unterschiedliche Bedürfnisse abdecken können. Doch Versicherung ist nur ein kleiner aber wichtiger Teil der Lösung. Weil Cyberrisiken Unternehmen in ihrer Gesamtheit durchdringen, braucht es zusätzliche Spezialisten aus den Bereichen Informatik und Recht.

Nur so lässt sich beurteilen, ob das IT-System sowie die Aufbau- und Ablauforganisation gängigen Sicherheitsanforderungen genügen und ob der Umgang mit dem Datenschutz im Einklang mit der Rechtsordnung steht. Aus diesem Grund arbeitet Funk in der Schweiz im Cyber-Risikomanagement mit **InfoGuard** und **MME** zusammen. InfoGuard ist ein Spezialist für Cyber-Security. Die Anwaltskanzlei MME ist u.a. auf Datenschutz und IT-Recht spezialisiert und vergibt das Zertifikat **«ePrivacy»** in der Schweiz. Gemeinsam stehen die drei Partner für einen umfassenden und stringenten Beratungsansatz im Umgang mit Cyberrisiken. Ebenso wichtig wie erfahrene Partner ist, was sich allgemein im Risikomanagement bewährt. Der Erfolg hängt davon ab, dass sich die Unternehmensleitung der Problematik bewusst ist und sich dafür zuständig fühlt.

Defense_v6.indd 49 28.11.17 01:58

Mehrheit der Unternehmen mit Handlungsbedarf

Gemäss einer Unternehmensumfrage im deutschsprachigen Raum vom Frühjahr 2017 sind grosse börsenkotierte Unternehmen durchaus Cyberfit. Kleine und mittlere Unternehmen hinken jedoch hinterher. Bemerkenswert ist, dass nur ein Drittel der Entscheider von mittleren Unternehmen der Meinung ist, im Fokus von gezielten Hackerangriffen zu sein. Die meisten finden ihr Unternehmen entweder zu klein oder zu uninteressant für Kriminelle. Diese Haltung kommt Rolf Th. Jufer bekannt vor. Bereits im Jahr 2013 organisierte Funk Kundenevents mit Live-Hacking. «Diese Demonstrationen kamen zwar gut an», erinnert sich Jufer. Am Ende bezweifelten viele Unternehmer jedoch, dass Hacker sich ihr Unternehmen aussuchen würden. «Wären wir ein lohnenswertes Ziel, hätte man uns doch schon längst angegriffen», so der Tenor.

Auch die IT-Spezialisten der InfoGuard haben diese Aussagen früher oft gehört. In den letzten zwei Jahren hat aber ein Umdenken stattgefunden. Dazu hat die Publizität rund um Hackerangriffe sicher das ihre dazu beigetragen. Das Outing von Edward Snowden wirkte nachhaltig. Mit den Enthüllungen zu den Cyberaktivitäten der amerikanischen Geheimdienste war das Thema definitiv in den Chef-Etagen angekommen. Interessierten sich früher fast nur IT-Leute für das Thema und liefen damit intern oft ins Leere, wird InfoGuard heute aktiv von Verwaltungsräten oder Unternehmensinhabern angefragt, um die Cybersicherheit im Unternehmen zu beurteilen.

Verschärfung der Datenschutzgesetze

Die Erfahrung von MME zeigt, dass der Datenschutz heute ganz klar ein Verwaltungsratsthema ist. Dabei geht es nicht nur um die Reputation des Unternehmens - verstärkt steht auch die Reputation der einzelnen Verwaltungsräte respektive der Geschäftsleitungsmitglieder selbst im Fokus.

Die aktuellen Verschärfungen der Datenschutzgesetzgebung auf europäischer Ebene und der Vorentwurf zum Datenschutzgesetz in der Schweiz haben selbstverständlich auch zur Sensibilisierung auf höchster Stufe beigetragen. Die vorgesehenen Strafen bei fahrlässigem oder gar vorsätzlich destruktivem Umgang mit Daten, können für Unternehmen schmerzhafte finanzielle Folgen haben.

Cyber-Krisenmanagement

Unternehmen müssen sich bewusst sein, dass es trotz allen präventiven Massnahmen und hohen Investitionen keine 100%-ige IT-Sicherheit gibt. Zu dynamisch organisieren sich die Angreifer und zu kreativ agieren sie. So hat der globale Umsatz der Cyberkriminellen bereits den Umsatz des globalen Drogenhandels übertroffen.

Defense_v6.indd 50 28.11.17 01:58

Trotz aller Sensibilisierungen und Warnungen wird es immer Mitarbeitende geben, die verdächtige Mails samt Anhängen öffnen («einer klickt immer»). Ferner ist insbesondere bei gezielten Cyberangriffen (z.B. Social Engineering) eine Abwehr sehr anspruchsvoll. Deshalb sollte auch der Notfall im Rahmen des Business Continuity Managements (z.B. IT-Systemausfall verursacht durch eine Ransomware) und des Krisenmanagements (z.B. Diebstahl von sensiblen Kundendaten) vorbereitet und geübt werden.

Cybersicherheit – die letzte Meile konsequent gehen

Im letzten Schritt der ganzheitlichen Behandlung von Cyberrisiken im Rahmen des Risikomanagements sollten Unternehmen sich den Cyber-Restrisiken bewusst werden. In der Praxis hat sich gezeigt, dass der im Funk RiskLab entwickelte Cyber Risk Calculator (Funk CRC) die Unternehmensleitung wirksam in diesem Prozess unterstützt. Auf Basis konkreter unternehmensspezifischer Informationen werden Schadenswerte ermittelt (Betriebsunterbruch, Kosten für Wiederherstellung, Rechtsberatung und Forensik sowie realistische Diebstahl- und Erpressungssummen). In einem Cyber-Risikodialog wird das Resultat zusammen mit der Unternehmensleitung detailliert überprüft und gegebenenfalls noch angepasst.

Die Unternehmensleitung erhält so eine Entscheidungsgrundlage ob - und wenn ja - zu welchen Konditionen die Cyber-Restrisiken in den Versicherungsmarkt transferiert werden sollen. Diese letzte Meile ist für die Verantwortlichen elementar. Nur so kann im Schadenfall dargelegt werden, ob die Unternehmensleitung die Prozesse im Rahmen des Risikomanagements vollständig abgearbeitet hat und der Entscheid «Versicherung - ja oder nein» gut dokumentiert wurde.

Defense_v6.indd 51 28.11.17 01:58

Rolf Thomas Jufer

Rolf Thomas Jufer ist Partner und Mitglied der Geschäftsleitung der Funk Insurance Brokers AG in der Schweiz. Er ist seit 2013 für Marketing, Vertrieb und das Funk RiskLab verantwortlich. Zuvor leitete Rolf Jufer die Tochtergesellschaften von zwei US-Beratungs- und Brokergesellschaften in der Schweiz nachdem er für einen Schweizer Lebensversicherungskonzern die Märkte Nordamerika, UK und Irland verantwortete.

Funk in der Schweiz rät nicht nur seinen Kunden, sich gegen Cyberrisiken zu wappnen, sondern handelt auch selber danach. Der Risikomanagement-Berater und Versicherungsbroker hat sein Kundenportal nach «ePrivacy» zertifizieren lassen. Das Assessment erfolgte durch InfoGuard und MME. Das Label hat seinen Ursprung in Deutschland und orientiert sich an den EU-Richtlinien. Auch in der Wirtschaft wächst das Bedürfnis nach Klarheit darüber, welche Anbieter im Umgang mit Cyberrisiken und dem Thema Datenschutz zeitgemässen Anforderungen genügen. Während InfoGuard das technische Gutachten macht, fokussiert MME auf rechtliche Faktoren (Datenschutz). Weil die EU-Richtlinien und auch die Datenschutzgesetzgebung in der Schweiz verschärft werden, ist zu erwarten, dass auch die Bedeutung von «ePrivacy» zunimmt.

Der inhabergeführte und unabhängige Versicherungsbroker Funk ist in der Schweiz seit 30 Jahren aktiv. Funk Insurance Brokers AG ist die Schweizer Organisation der 1879 gegründeten Funk Gruppe, Hamburg. Das in der 5. Generation geführte Familienunternehmen ist der grösste eigenständige Risikoberater und Versicherungsbroker im deutschsprachigen Raum. In den Niederlassungen Basel, Bern, Luzern, St. Gallen sowie Zürich beschäftigt Funk über 80 Spezialisten verschiedenster Fachrichtungen. Funk in der Schweiz zeichnet sich durch Nähe zum Kunden, Kompetenz und Begeisterung bei Bewertung und Management von Risiken für Unternehmen aus. Über ihr Brokernetzwerk Funk Alliance stellt Funk die weltweite Betreuung ihrer Kunden im gesamten betrieblichen Risiko-, Vorsorge- und Versicherungsmanagement sicher und bietet nationalen und internationalen Unternehmen einen individuellen Service aus einer Hand. Funk ist zertifiziert nach ISO 9001 und betreibt das erste Kundenportal der Schweiz mit dem ePrivacyseal (IT-Security und Datenschutz nach EU DSGVO).

Defense_v6.indd 52 28.11.17 01:58

Funk CyberSecure
Modulare Versicherungs-lösung für Cyber Risiken

Mit Funk CyberSecure bietet Funk als erster Broker in der Schweiz den umfassendsten Versicherungsschutz gegen digitale Bedrohungen.

Ihr Mehrwert:

- Unternehmensspezifische Bewertung des Cyber-Restrisikos
- Umfassende Versicherungsdeckung weit über den marktüblichen Standards
- Ideale Abstimmung auf das aktuelle Versicherungsportfolio
- Zugriff auf Fachspezialisten in den Bereichen IT-Sicherheit und Datenschutz
- Sicherstellung der Notfallorganisation im Cyberzwischenfall

Versicherungsmanagement, Vorsorge, Risikomanagement
www.funk-gruppe.ch

Defense_v6.indd 53 28.11.17 01:58

Mark Carter
Managing Partner Risk Advisory, Deloitte Switzerland

Klaus Julisch
Partner, Cyber Risk Services, Deloitte Switzerland

Cyber security

Cyber risk is the «new normal»

Today, the image of the computer geek breaking into protected systems for fun and bragging rights seems almost old-fashioned. Cybercrime has gone professional, with hackers targeting large organisations and organised crime and government-sponsored cyberattacks making headline news, such as the cyber war against the military programmes of other nations, cyber extortion against Swiss hospitals, and the Carbanak heist that stole over one billion francs from an estimated 100 financial services organisations around the world.

Defense_v6.indd 54 28.11.17 01:58

There is no reward without risk—and this, in a world where digital technology is vital to all aspects of business, is especially true of cyber risk. Much has been written about the dangers of cyber risk, with reports of breaches and attacks surfacing in high frequency. These writings tend to focus on the negative impacts of cyber risk: the data stolen, the value lost, the damage done. And this is understandable. It's a lot easier to build a story around nefarious state actors and criminals out to steal someone's secrets than it is to present solutions.

It is clear that no organisation is immune to cyberattacks in today's world – it's the 'new normal'. But despite the fact that cybercrime is growing in number and strength and the future of cybersecurity is looking ever more complex and challenging, companies are not defenceless. Specifically, a crucial key to the puzzle is how an organisation responds to incidents as well as how it acts upon lessons learned.

Deloitte advises its clients to design their cyber defences according to the paradigm: Secure – Vigilant – Resilient.

1

Being secure means implementing and maintaining foundational security capabilities to protect against threats and to comply with industry standards and regulations. These capabilities are preventive and include, for example, firewalls, data loss prevention and enterprise digital rights management, which is discussed further below.

2

Being vigilant is the ability to detect cyberattacks and incidents, as well as vulnerabilities and emerging threats. Vigilance is the cyber equivalent of surveillance cameras. It allows organisations to detect problems so that they can respond to them.

3

Being resilient means being able to respond effectively to cyber incidents, threats and attacks. At its core are the ability to contain attacks, repair any damage to the business and return to normal operations as quickly as possible.

Finally, as a fourth foundational discipline, organisations need to maintain a sound cyber strategy, which gives them effective risk management and cultural awareness so that they can properly prioritise and focus their other efforts.

Case in point: Enterprise Digital Rights Management

Enterprise Digital Rights Management (EDRM) is an innovative technology that has gained popularity over the past couple of years. It was born out of the realisation that traditional perimeter-based security is not sufficient to protect data when there is an increasingly mobile and collaborative workforce operating on a multitude of platforms such as their employer's IT systems, private laptops and third-party cloud systems. The solution proposed by EDRM is to protect the data itself,

Defense_v6.indd 55 28.11.17 01:58

along its entire lifecycle, starting from when it is created, throughout its usage, storage and replication, until it is finally archived or deleted. In this way, no matter where a piece of data is sent, stored or processed, it is intrinsically protected, and does not depend for its security on controls in its environment, such as Anti-Virus Scanners and firewalls.

Here is how it works. In a first step, content owners define the protection policies that apply to their content. A typical protection policy will define who can use a particular piece of data, what they can do with it (for example, read, edit, print, save, forward), and when they can use it. Content is frequently stored in content repositories, from where potential users request it; other distribution mechanisms such as email are also possible. On request, the content is returned from the repository and throughout its entire lifecycle, content is encrypted to protect its security. Potential users further have to authenticate to a licence server in order to obtain a licence for using the content. The licence grants certain rights to the user – as defined in the protection policy – and these rights are enforced by the rendering application, through which the user interacts with the content. As such, EDRM is a clever combination of encryption with identity and access management, which makes protection inseparable from the data that is being protected.

EDRM is a good example of an innovative security technology that has gained popularity as organisations respond to ever-increasing cyber threats. It is used typically to protect emails and sensitive documents that are exchanged among multiple parties, such as board memos, product designs, M&A (merger and acquisition) plans and financial reports. It is also a useful countermeasure against threats from insiders — malicious employees who abuse their rights and privileges for their own personal benefit.

Outlook

Unfortunately, the battle against cyber adversaries is inherently unbalanced. Organisations must protect complex operations that include a multitude of technologies and human users, as well as buildings and sites. Attackers, by contrast, only need to find a single weakness to succeed. Phishing – the use of deceptive emails in an attempt to trick users into subverting their security – provides a good illustration. Research has found that there is a 90 percent chance that at least one person will fall victim to a phishing campaign with just ten emails . Using widely-available information on the Internet, it is not difficult to design a phishing campaign that targets hundreds of users within an organisation, which for all intents and purposes raises the likelihood of success to 100 percent.

Mark Carter

Mark Carter leads Deloitte's Risk Advisory practice in Switzerland. He has over eighteen years of IT consultancy experience helping organisations to transform their information and cyber security capabilities. Mark Carter has worked across various risk management functions including IT security, information risk management, operational risk, and data privacy. He holds a Master's degree in Law (MA Cantab) from Cambridge University.

Defense_v6.indd 56 28.11.17 01:58

The ingenuity and commitment of cyber adversaries is another challenge for defenders. The Stuxnet virus that was discovered in a uranium enrichment plant in Iran demonstrates this point. The computers that Stuxnet infected were 'air-gapped' and could not be reached from the Internet. The attackers therefore designed malware to infect systems via USB flash drives. To get Stuxnet to the targeted machines, they first infected computers of external third-party providers, and from these the malware spread to the target system via flash drives and other means such as four different 'zero-day exploits' (attacks that exploit previously unknown vulnerabilities). Stuxnet also went through multiple releases with increasing sophistication, and used advanced techniques to remain stealthy and undetected. One such technique was the use of stolen digital certificates to sign and legitimise malicious files.

These challenges are driving organisations and the security industry to innovate and evolve their defences constantly. Fusion centres are an example of an organisational rather that technological innovation, showing how companies adapt in order to become more 'vigilant', in the sense of Deloitte's 'Secure – Vigilant – Resilient' framework. Fusion centres assemble multi-disciplinary teams from different parts of the organisation, combining diverse skills from intelligence, forensics, operations, physical security, fraud prevention and data science. The purpose of the team is to create around-the-clock situational awareness, rapidly share intelligence across the organisation, and break down organisational barriers to taking action, as well as act as a 'hub' when dealing with crises. Fusion centre teams can also work across the ecosystem (with partners, vendors, customers and others) to extend situational awareness. Organisational innovations such as these are important because technologies and tools alone cannot provide adequate cyber security.

It is this continuous innovation that makes cyber security one of the most rewarding career fields in today's job market. As former buzzwords such as 'cloud', 'BYOD', and 'digital' turn into billion-franc businesses, cyber threats evolve and the security industry adapts. For cyber professionals, this creates a challenging and rewarding opportunity to grow professionally and add value to enterprises and society.

Dr. Klaus Julisch

Dr. Klaus Julisch is a Partner in Deloitte's Cyber Risk Services practice in Switzerland. He leads the cyber security and data protection teams and specialises on helping financial services clients resolve their most challenging security issues. Klaus' work has been published internationally and resulted in 15 patents in the areas of security and privacy. He holds a Ph.D. in Computer Science from the University of Dortmund, Germany, and an MBA from Warwick Business School, UK.

Defense_v6.indd 57 28.11.17 01:58

Raphael Blatter

Information Security Officer bei
Glencore International

Mitarbeiter als Risikofaktor

Wie der weltweit größte Rohstoffhändler mit Gefahren in der Cyber-Security umgeht und warum ein besonderer Fokus auf die Mitarbeitenden gelegt werden muss.

Defense_v6.indd 58 28.11.17 01:58

Viele Unternehmen lagern ihre IT-Abteilung mittlerweile aus. Glencore hingegen betreibt seine gesamte IT Abteilung am Hauptsitz in Baar, in der Schweiz. Warum ist das so?

Raphael Blatter: Ich muss da etwas präzisieren. Glencore hat nicht die gesamte IT-Abteilung in der Schweiz, wir sind aber gewissermassen der Hauptsitz der firmenweiten IT. Dadurch, dass mit Ausnahme vom Ölgeschäft, alle Geschäftseinheiten in Baar am Hauptsitz untergebracht sind, sind wir sehr nah am Geschehen dran. Das heisst, wir können direkt mit den verschiedenen Abteilungen IT-Architekturen, Programme und Serviceleistungen entwickeln, die genau deren Bedürfnissen entsprechen. Externen Firmen fehlt oftmals das spezifische Branchenwissen und die persönliche Beziehung zu den Mitarbeitenden, um deren Anforderungen zu verstehen und passgenau umsetzen zu können. Deshalb produzieren wir auch die Programme, die für uns zentral sind, selbst. Da können wir nicht auf Standardprodukte zurückgreifen.

Ein weiterer Grund, warum die IT-Zentrale in Baar ist, hat auch mit der Qualität der Arbeitskräfte in der Schweiz zu tun. Es gibt hier sehr gute IT-Fachkräfte. Das ist nicht zuletzt dem guten Ausbildungsangebot zu verdanken. Wir beobachten aber, dass der Bedarf an IT-Spezialisten wächst. Deshalb sind wir letztes Jahr eine Partnerschaft mit dem Lehrstuhl für Informationstechnologie an der Hochschule Luzern eingegangen, um die Ausbildung von IT-Fachkräften zu fördern.

Aktuell sind wiederholt Cyber-Attacken publik geworden, welche Mitarbeitende als Schwachstelle nutzen. Hacker verschaffen sich durch Phishing oder Ransomware Zugang zu sensiblen Daten. Wie machen Sie Mitarbeitende auf diese Risiken aufmerksam?

Auch wir haben festgestellt, dass Angreifer vermehrt über unsere Mitarbeitenden versuchen, unsere IT-Infrastruktur anzugreifen und an Daten zu gelangen. Wir führen schon länger Mitarbeiter-Trainings durch, um sie auf mögliche Angriffe zu sensibilisieren. Jeder, der an unserem Hauptsitz neu anfängt, erhält gleich zu Beginn ein Face-to-Face Training in Sachen IT-Sicherheit. Es gibt auch regelmässig Refresher-Trainings. Dieser persönliche Ansatz unterscheidet uns wahrscheinlich von den meisten anderen Firmen. Auf globaler Ebene müssen alle Mitarbeitenden, die bei der Arbeit Zugang zu einem Computer haben, E-Learning Module absolvieren. Diese sind in neun Sprachen verfügbar. Es ist wichtig, dass alle Mitarbeitenden die Risiken kennen. Wir führen auch regelmässig Stichproben-Tests durch. Das heisst, wir schicken unseren Mitarbeitenden E-Mails, die auch von einem potenziellen Angreifer hätten verschickt werden können. Werden die Anhänge geöffnet oder die Links angeklickt, kontaktieren wir diese Person und erklären ihr in einem zusätzlichen Training, wie sie zukünftig potenzielle Hacker-Mails entlarven kann. Un-

Defense_v6.indd 59 28.11.17 01:59

ser Ziel ist es, dass die Mitarbeitenden einen Radar für verdächtige E-Mails entwickeln und dass sie sich bei uns melden, wenn sie nicht sicher sind, ob sie einen Anhang öffnen dürfen oder nicht. Im Intranet informieren wir zudem über publik gewordene Cyberangriffe, die auf grosse Firmen verübt worden sind.

IT-Security lässt sich nicht allein durch technische Lösungen sicherstellen. Dieses Bewusstsein scheint sich in der Firma mittlerweile etabliert zu haben. Unsere Mitarbeitenden haben verstanden, dass sie uns dabei helfen können und müssen, die Firma vor Angreifern zu schützen.

Eine bekannte Unternehmensberatung hat in einem Bericht zu Cyber-Security festgehalten, dass Rohstoffhändler einem besonderen Risiko von Cyberangriffen ausgesetzt sind. Stellen Sie in den letzten Jahren Veränderungen in der Anzahl und Art der Attacken fest?

Ja, wir stellen durchaus fest, dass sich die Attacken häufen. Das ist bei uns aber nicht anders als bei anderen Firmen. Es ist aber auch so, dass wir mit dem Aufrüsten unserer IT-Security, auch mehr Angriffe identifizieren können als früher. Hier arbeiten wir mit diversen Warnsystemen – so genannten Intrusion Detection Systemen.

Was die Art der Attacken angeht, so hat sich sicherlich der Umfang an Geräten, mit denen Cyberangriffe verübt werden, erhöht. Früher hat ein Hacker beispielsweise den Angriff mit dutzenden von Computern ausgeführt. Heute macht er das mit hunderttausenden von Geräten und nutzt darüber hinaus das Internet of Things, also beispielsweise Netzwerkkameras, Drucker oder Mobiltelefone.

Wie lassen sich Risiken frühzeitig identifizieren? Antworten Sie reaktiv auf Bedrohungen, oder wird eine proaktive Cyberabwehr verfolgt?

Wir arbeiten mit diversen Organisationen zusammen, darunter auch mit den Schweizer Behörden, die uns über Trends und potenzielle Angriffe informieren. Wir sind auch in diverse Arbeitsgruppen involviert. Da tauschen wir mit anderen Unternehmen unsere Erfahrungen aus und erarbeiten Lösungen, um uns gegen zukünftige Cyberangriffe zu schützen. Letztendlich ist es aber so, dass Cyber-Security immer eine Kombination aus proaktiver und reaktiver Cyberabwehr sein wird. Ohne reaktive Cyberabwehr geht es nicht. Man kann nicht alles vorhersehen. Die kontinuierliche Weiterentwicklung beider Instrumente ist deshalb unerlässlich.

Auf der technischen Seite sind unsere Firewall und andere Security Systeme auf dem neusten Stand. Sie haben uns bisher gut gegen potenzielle Cyber-Angriffe geschützt. Mails beispielsweise durchlaufen mehrere Stufen an Sicherheitssystemen und bösartige Mails werden von unserem

Defense_v6.indd 60 28.11.17 01:59

System meistens direkt gelöscht. Sollte es doch einmal zu einem Vorfall kommen, können wir schnell reagieren und den Schaden eingrenzen.

Wir sehen innerhalb der Firma ein wachsendes Bewusstsein dafür, dass IT-Security immer wichtiger wird. Entsprechend investieren wir heute mehr in die Sicherheit unserer IT-Systeme als früher. Mit Threat Intelligence versuchen wir zudem, allgemeine Trends in Sachen Hackerangriffen zu identifizieren. Threat Intelligence hilft uns auch herauszufinden, ob Daten über Glencore im Netz kursieren, die dafür missbraucht werden könnten, in unser System einzudringen.

Wie kann eine Cyber-Security Infrastruktur gestaltet werden, die trotz nötiger Komplexität für die Mitarbeitenden verständlich bleibt?

Für normale Mitarbeitende ist Security ein wenig wie ein Eisberg. Ein Grossteil von dem, was im Bereich Security läuft und getan wird, ist für die Mitarbeitenden nicht sichtbar. Die Mitarbeitenden sehen nur das, was an der Oberfläche und für sie relevant ist. Unser Job ist es, unseren Mitarbeitenden ein System zur Verfügung zu stellen, mit dem sie ihre Arbeit so gut und effizient wie möglich, aber trotzdem sicher erledigen können. Die IT-Security darf sie nur wo nötig einschränken. Die wahre Komplexität ist für die Mitarbeitenden also gar nicht sichtbar. Die Trainings sind entsprechend auch so gestaltet, dass die normalen Mitarbeitenden nur zu den relevanten Regeln und Vorgehensweisen geschult werden. Wie eingangs erläutert, geht es darum, ihr Bewusstsein für Cyber-Angriffe zu stärken. Spezifisch für IT-Mitarbeitende werden erweiterte Security Trainings durchgeführt. In diesen wird dann auch die zusätzliche Komplexität mitberücksichtigt.

Wie kann Glencore eine Harmonisierung der Cyber-Security Massstäbe an Standorten in verschiedenen Ländern gewährleisten und adäquat auf die sich ständig verändernde Gesetzeslage zu Cyber-Security weltweit reagieren?

Wir publizieren global gültige Standards und Richtlinien. Um Zugriff auf globale IT-Systeme zu erhalten, müssen die lokalen Standorte diese erfüllen. Überprüft wird das mittels Security Audits. Zudem werden gewisse Schlüsselsysteme im Bereich Security zentral aus der Schweiz verwaltet.

Trotzdem ist die Harmonisierung absichtlich nicht komplett. Zugriff auf globale IT-Systeme und Daten wird auch bei bestandenem Security Audit nur gewährt, wenn dies für das Geschäft vor Ort erforderlich ist. Der Vorteil einer solchen «De-Harmonisierung» ist, dass im Falle eines Cyberangriffs, die Hacker nicht gleich auf alle Daten zugreifen können.

Defense_v6.indd 61 28.11.17 01:59

Was die Gesetzeslage angeht, halten wir uns jeweils an die im Land geltenden Gesetze. Eventuelle Veränderungen werden durch unsere Spezialisten vor Ort umgesetzt. Grundsätzlich orientieren wir uns aber an der Schweizer Rechtslage und an globalen Standards. Da die Gesetzeslage im Bereich Datenschutz in der Schweiz aber ohnehin streng ist und demnächst noch strenger wird, tangieren uns allfällige Gesetzesanpassungen auf lokaler Ebene normalerweise kaum.

Raphael Blatter

Information Security Officer

Raphael Blatter arbeitet seit rund drei Jahren bei Glencore in Baar im Bereich Information Security. Schon im jugendlichen Alter interessierte er sich fürs Codieren und entschied sich deshalb für ein Informatikstudium an der Universität Zürich. Kurz nach seinem Masterabschluss stieg Raphael bei Pricewaterhouse-Coopers ein. Dort beriet er Firmen in Sachen Cyber-Security. Gleichzeitig absolvierte er ein Nachdiplomstudium an der Hochschule Luzern und spezialisierte sich so im Bereich «Information Security». Nach seinem zweiten Masterabschluss wechselte Raphael zu Glencore.

Defense_v6.indd 62 28.11.17 01:59

Besonderen Dank an unseren Verein ESPRIT St.Gallen – Consulting by Students

Ausserdem möchten wir uns für die Unterstützung folgender studentischen Unternehmensberatungen bedanken

Imprint

Contact	St. Gallen Business Review Guisanstrasse 19 CH-9010 St. Gallen Telefon: +41 (0) 71 220 14 01 Fax: +41 (0) 71 220 14 04 Email: sgbr@espritsg.ch
Publisher	ESPRIT Consulting
Main Editorial	Isabel Hoffet & Niklas Zeller
Editorial Office	Lars Decker Milan Schéda Philipp Kreiner
Layout and Illustration	Patrick Buess, buesspatrick@gmail.com
Publication Frequency	Semestral
Copyright	No part of this publication and/or website may be reproduced, stored in a retrieval system or transmitted in any form without prior written permission of the Publisher.
Subscribe	www.stgallenbusinessreview.com
Disclaimer	The author's views and opinions do not necessarily match the opinion of the St. Gallen Business Review. The St. Gallen Business Review does not assume liability for the content of the submitted articles.

Defense_v6.indd 63 28.11.17 01:59

Deloitte.

Break the status quo

Nextland is not a place, it's a way of thinking.
We challenge conventions. We always look at things
from every angle. We allow ourselves to think big.
Welcome to Nextland.

What impact will you make?
deloitte.com/ch/careers/nextland

© 2017 Deloitte AG. All rights reserved.