Bundesamt für
Verfassungsschutz

ASW
Bundesverband

Neue Gefahren für Informationssicherheit und Informationshoheit

10. Sicherheitstagung BfV und ASW Bundesverband am 9. Juni 2016

Deloitte. nedap POWER PERSONEN-OBJEKT-WERKSCHUTZ GMBH

Neue Gefahren für Informationssicherheit und Informationshoheit

10. Sicherheitstagung BfV und
ASW Bundesverband am 9. Juni 2016

Tagungsband

Inhaltsverzeichnis

Seite

Einleitung **1**

Begrüßung und Eröffnung **2**
Volker Wagner, Vorsitzender, ASW Bundesverband

Begrüßung und Keynote **7**
Thomas Haldenwang, Vizepräsident, Bundesamt für Verfassungsschutz

„Zum Schutz von Informationen müssen Staat und Wirtschaft eng und arbeitsteilig zusammenarbeiten“ **14**
Dr. Emily Haber, Staatssekretärin, Bundesministerium des Innern

Propaganda und politische Einflussnahme als strategische Handlungsoption ausländischer Nachrichtendienste **24**
Dr. Burkhard Even, Abteilungsleiter Spionageabwehr und Geheimschutz, Bundesamt für Verfassungsschutz

Von Sockenpuppen und Trollen – Desinformation im Netz und wie man sich schützt **33**
Prof. Dr. Martin Grothe, complexium

Das Zusammenspiel von Unternehmenssicherheit und Unternehmenskommunikation **70**
Ronald Pofalla, Deutsche Bahn AG

Identitätsdiebstahl/-missbrauch in Europa **74**
Jürgen Kempf, Result Group, Vertreter des EU-Projektes V.I.S.I.T.

Wie Drohnen die „Lufthoheit“ über Unternehmensinformationen bedrohen **95**
Christian Janke, European Aviation Security Center

Der deutsche Journalismus: Auf der Suche nach der Wahrheit oder einer möglichst großen Quote **119**
Paul Elmar Jöris, WDR

Pressemitteilung und Bildmaterial **125**

10. Sicherheitstagung BfV und ASW Bundesverband am 9. Juni 2016

BfV-Vizepräsident Thomas Haldenwang und der ASW-Vorsitzende Volker Wagner

Am 9. Juni fand in Berlin die 10. Gemeinsame Sicherheitstagung des BfV und des ASW Bundesverbandes statt. Sie stand unter dem Motto "Neue Gefahren für Informationssicherheit und Informationshoheit". Rund 160 Teilnehmer aus Unternehmen, aus Wirtschafts- und Sicherheitsverbänden, aus Wissenschaft und Forschung sowie aus Sicherheitsbehörden und Ministerien erörterten auf der Jubiläumstagung unter anderem die Themen Desinformation, Identitätsdiebstahl, neue Risiken für den Know-how-Schutz durch Drohnen sowie Fragen zur Kommunikation und Sicherheit.

Begrüßung und Eröffnung

Volker Wagner, Vorsitzender, ASW Bundesverband

Sehr geehrte Staatssekretärin Dr. Haber, sehr geehrter Herr Vizepräsident, lieber Herr Haldenwang, liebe ASW Mitglieder, Vertreter der Wirtschaft und der Sicherheitsbehörden, sehr geehrte Medien- und Pressevertreter, verehrte Gäste!

Wir freuen uns, Sie heute hier auf unserem 10. Sicherheitstag des Bundesamtes für Verfassungsschutz und des ASW Bundesverbandes begrüßen zu dürfen.

Die erste gute Nachricht vorab!

Ja, wir feiern heute unser zehnjähriges Jubiläum! Darauf sind wir sehr stolz, und wir freuen uns auch sehr, dass Sie alle heute mit uns bei diesem Jubiläum dabei sind.

Die schlechte Nachricht:

Präsident Maaßen kann heute nicht bei uns sein, da zeitgleich der NSA-Untersuchungsausschuss angesetzt wurde.

Die zweite gute Nachricht:

Viezpräsident Haldenwang übernimmt die Keynote von Herrn Dr. Maaßen, so dass Sie inhaltlich nichts verpassen werden.

Wenn wir auf die gemeinsamen Veranstaltungen der letzten Jahre zurückblicken, dann finden wir viele Themen wieder, die auch heute noch von hoher Relevanz sind, wie beispielsweise:

- Proaktiver Wirtschaftsschutz: Prävention durch Information
- Braucht Ihr Sicherheitsbewusstsein ein Update?
- Zuletzt im Jahr 2015: Innentäter - eine unterschätzte Gefahr

Aber eines steht fest. Auch wenn viele Themen Dauerbrenner sind, hat doch die Geschwindigkeit, Intelligenz und Komplexität der Angriffe durch die Digitalisierung und Vernetzung weiter zugenommen. Und aus genau diesem Grund haben wir auch für heute unseren Schwerpunkt gewählt.

Neue Gefahren für Informationssicherheit und Informationshoheit. Dabei geht es unter anderem um Desinformation im Netz, das Zusammenspiel von Unternehmenssicherheit und Unternehmenskommunikation und Identitätsdiebstahl.

Wer sich mit dem Thema befasst, wird schnell erkennen, welche Brisanz und Relevanz in diesem Thema steckt.

Anfang des Jahres haben wir ein Whitepaper veröffentlicht – es ist übrigens nach wie vor auf unserer Homepage als Download verfügbar. In diesem Whitepaper haben wir ausgeführt, dass aus unserer Sicht eine Reihe globaler Trends die Sicherheit Deutschlands im Ganzen und die Sicherheit der deutschen Wirtschaft im Speziellen bedrohen.

Wir haben diese zu vier globalen Megatrends zusammengefasst:

1. Megatrend Staatszerfall
2. Megatrend klimatische und ökologische Verwerfungen
3. Megatrend asymmetrische Bedrohung und hybride Kriegsführung
4. Megatrend Digitalisierung und Vernetzung

Diesen 4. Megatrend „Digitalisierung und Vernetzung" möchte ich im Folgenden kurz skizieren, da er von besonderer Relevanz für unsere heutige Veranstaltung ist.

Vieles wird für uns dank Technik komfortabler, günstiger, sicherer, schneller erreichbar oder überhaupt erst erreichbar – einschließlich eines längeren Lebens. Wer mit seinem Auto von A nach B möchte, gibt das Ziel in sein Navigationssystem ein und wird geführt – Nachschlagen in Karten ist nicht mehr notwendig. Auf der Fahrt warnen Abstandssensoren bei Gefahr, Bremsassistenzsysteme helfen in kritischen Momenten und im Falle des Falls schützen einen Airbags.

Aber die Technik bietet auch zahllose neue Angriffsflächen. Sie macht uns verwundbarer. Wo sich Gasventile aus der Ferne regeln lassen, können diese auch bewusst fehlgesteuert werden. Wenn Stromzähler an das Internet angeschlossen sind, lassen sich diese von überall auf der Welt manipulieren und das Netz kann überlastet werden. Ein System, dass immer online ist, ist auch immer angreifbar. Wenn Computer miteinander vernetzt sind, kann ich über jeden dieser Computer das gesamte System angreifen.

Die breite Vernetzung und das ständige Onlinesein erlauben es Angreifern, jederzeit von jedem Fleck der Erde jedes System anzugreifen – ohne dabei entdeckt zu werden. Die erforderlichen Fähigkeiten sind vergleichsweise einfach zu erwerben.

Große internationale Unternehmen sind genau wie mittelständische und kleinere Unternehmen von den Megatrends betroffen und stehen im Fokus von Angreifern. Hier lässt sich als Einzelkämpfer nicht genug ausrichten. Fehlende Informationen, Erfahrungswerte und Ressourcen, um mit Sicherheitsvorfällen in diesem Spektrum umzugehen, sind ein Grund dafür. Für einen nachhaltigen und umfassenden Wirtschaftsschutz muss al-

lerdings mehr getan werden. Der Austausch von Best-Practice-Erfahrungen mit anderen Unternehmen und eine aktive wie innovative Zusammenarbeit mit Instituten und Behörden sind ein unerlässlicher Zusatzschutz. Erst durch die enge Kooperation mit anderen nationalen und internationalen Sicherheitsentscheidern wird ein umfassendes Sicherheitslagebild erkennbar, mit dem weitere Schwachstellen identifiziert und beseitigt werden können. Daher ist die Vernetzung in sämtliche Richtungen ein ausschlaggebendes Mittel, um einen Wirtschaftsschutz auf hohem Niveau zu generieren. Für die Zukunft und mit Blick auf die absehbaren neuen Herausforderungen für die Unternehmenssicherheit durch Industrie 4.0 und das Internet der Dinge wird das noch entscheidender sein, als es heute schon ist.

Der ASW Bundesverband fördert die Entwicklung eines gemeinsamen Sicherheitsverständnisses durch enge Zusammenarbeit zwischen Unternehmen, staatlichen Stellen und Verbänden auch über Landesgrenzen hinaus. So unterstützen wir die Institutionalisierung der Zusammenarbeit für einen nachhaltigen Wirtschaftsschutz, damit alle Beteiligten Zugang zu den entscheidenden Sicherheitsakteuren haben, sei es in der Politik, in den Behörden, der Wirtschaft oder der Wissenschaft.

Gerade deshalb ist es so wichtig, dass wir unter Federführung des BMI die Initiative Wirtschaftsschutz ins Leben gerufen haben – sozusagen als Public Private Partnership zwischen Regierungsstellen, Sicherheitsbehörden und Wirtschaftsverbänden. Die gelungene Vorstellung der ersten Ergebnisse erfolgte am 26. April diesen Jahres durch den Bundesinnenminister und die Projektpartner hier in Berlin. Wir werden Sie auch heute im weiteren Verlauf des Tages über den aktuellen Status informieren. Dazu haben wir Informationsmaterial für Sie vorbereitet, und Frau Dr. Haber wird in Ihrem Vortrag auf die Highlights eingehen.

Nun aber zum heutigen Tag! Dass Sie so zahlreich erschienen sind, zeigt mir, dass wir hier das richtige Thema ansprechen und es freut mich, Ihnen auch dieses Jahr eine abwechslungsreiche Agenda mit hervorragenden Referenten präsentieren zu können. Das Leitthema unserer heutigen Veranstaltung ist: Neue Gefahren für Informationssicherheit und Informationshoheit. Und damit starten wir gleich mit einer sicherlich bereichernden Keynote unseres BfV Vizepräsidenten zur aktuellen Situation. Im Anschluss hören wir Staatssekretärin Dr. Emily Haber mit ihrer Sicht auf die strategischen und geopolitischen Entwicklungen sowie deren Implikationen für die deutsche und europäische Wirtschaft. Zudem wird Frau Dr. Haber über den erfolgreichen Start unseres gemeinsamen Projektes Initiative Wirtschaftsschutz berichten.

Am Nachmittag warten dann auf uns noch weitere praxisorientierte Themen. Es geht um:

- Die Aktivitäten ausländischer Nachrichtendienste
- Desinformation im Netz
- Die Managementperspektive zum Thema Sicherheit bei der Deutschen Bahn
- Identitätsdiebstahl und -missbrauch

Wir freuen uns dafür hochkarätige Referenten gewonnen zu haben:

Dr. Burkhard Even, Prof. Dr. Martin Grothe, Ronald Pofalla und Jürgen Kempf

Wir sind gespannt auf Ihre Ausführungen!

Zum Abschluss werfen wir noch einen Blick auf die Herausforderungen durch Drohnen und auf die Rolle der Medien.

Schon jetzt vorab vielen Dank an unsere beiden Referenten Christian Janke und Paul Elmar Jöris.

- Ich bin sicher, auch in diesem Jahr wird unsere „traditionelle“ und bereits 10te BfV/ASW Kooperationsveranstaltung erfolgreich sein. Die langjährige, gute und vertrauensvolle Zusammenarbeit ist die beste Basis für ein gutes Gelingen.
- Erlauben Sie mir noch kurz zu erwähnen, eine solche Veranstaltung ist nur mit Unterstützung möglich. Neben dem BfV, mit dem wir als ASW Bundesverband die Organisation und Inhalte des heutigen Tages gemeinsam gestaltet haben, möchte ich mich auch bei unseren Sponsoren Deloitte und der Power Unternehmensgruppe bedanken, die mit dazu beigetragen haben, das heutige Setting in diesem Umfang möglich zu machen.
- Zudem haben wir eine kleine Ausstellung von Produkten und Lösungen für Sie organisiert. Hier können Sie Fachgespräche mit Experten zu folgenden Themen führen.

  Wie Sie alle wissen werden immer mehr Schließsysteme und Videokameras über das Internet verbunden gesteuert. Dies erleichtert das Incident Management deutlich, birgt aber auch das Risiko, dass die Sicherheitssysteme gehackt werden können. Die Fa. nedap stellt hier aus meiner Sicht eine besonders innovative integrierte Zutrittstechnologie vor, die besonders auf den Schutz vor Cyberattacken ausgerichtet ist.

Zudem haben wir das Team Lauschabwehr der Deutschen Telekom vor Ort. Hier können Sie mehr über die neuesten Spionagetechniken erfahren – und vor allem was man dagegen tun kann.

Darüber hinaus sollten Sie es nicht versäumen, sich mit einem unserer Referenten, Professor Grothe, näher auszutauschen. Der Begriff „Social Media Monitoring" beschreibt nur im Ansatz, was sein Unternehmen leistet und ich bin froh, dass er uns heute nicht nur als Referent zur Verfügung steht, sondern dass wir als ASW Bundesverband auch das eine oder andere Projekt zusammen durchführen.

Vielen Dank auch an die Vertreter der Presse und Medien, dass Sie unserer Einladung zum ersten Teil der Veranstaltung nachgekommen sind! Die Pressekonferenz findet in der Kaffeepause statt.

Lassen Sie uns nun mit der ersten Keynote den Tag beginnen: Herr Haldenwang, wir sind sehr gespannt auf Ihre Gedanken zur Verbesserung der Informationssicherheit und garantieren Ihnen durch unsere uneingeschränkte Aufmerksamkeit die absolute Informationshoheit, zumindest in den nächsten 30 Minuten. In diesem Sinne, lieber Herr Haldenwang, die Bühne gehört Ihnen!

Begrüßung und Keynote

Thomas Haldenwang, Vizepräsident des Bundesamtes für Verfassungsschutz

1. Begrüßung

(Anrede),

ein herzliches Willkommen auch von mir. Ein besonderer Willkommensgruß gilt „unserer" Staatssekretärin Frau Dr. Emily Haber aus dem Bundesministerium des Innern. Dass sie heute nicht nur hier ist, sondern auch eine Keynote sprechen wird, freut uns. Dies dokumentiert den hohen Stellenwert, den das Thema für die Bundesregierung genießt.

Kommunikation bleibt die Basis für Vertrauen. Deshalb sind solche Tagungen, wie die heutige, über die jeweiligen Themenfelder hinaus von unschätzbarem Wert. Dass wir heute bereits die zehnte gemeinsame Sicherheitstagung von BfV und ASW durchführen, ist ein Beleg für Kontinuität und Wertschätzung. Die Teilnehmerzahlen haben sich gegenüber den Anfängen Mitte der 2000er Jahre – damals fand die Sicherheitstagung in kleinerem Rahmen in Köln statt – mehr als verdoppelt.

Das halte ich für sehr erfreulich. Das zeigt mir aber auch, wie bedeutsam das Thema Wirtschaftsschutz ist. Und es unterstreicht den großen Bedarf an Information und Austausch zu allen Aspekten des Wirtschaftsschutzes.

Gerade vor dem Hintergrund der neuen Informationstechnologien gilt: Sicherheit muss national beginnen. Aber: Ohne internationale Verflechtung bleibt sie Stückwerk. Gestatten Sie mir deshalb an dieser Stelle, die Vertreter unserer Partnerdienste aus Italien, Österreich, Schweiz und Ungarn hier besonders zu grüßen. Mein Dank gilt Ihnen für die enge Kooperation unserer Dienste – nicht nur im Bereich des Wirtschaftsschutzes!

Basis für Vertrauen in Fragen von Sicherheit und Unsicherheit ist auch die öffentliche Kommunikation. Darum begrüße ich auch die Vertreter der Medien, die bis zur Pressekonferenz mit der Unterzeichnung des Perspektivpapiers von BfV und ASW am ersten Teil der Tagung teilnehmen werden.

2. Thematische Hinführung Tagungsmotto

„Neue Gefahren für Informationssicherheit und Informationshoheit" lautet das Thema der 10. BfV/ASW-Sicherheitstagung. Wir – BfV und ASW – haben das Thema bewusst breit gewählt: denn es geht uns um mehr als IT-Sicherheit. Ja, es geht auch um mehr als ein kluges ganzheitliches Informationsschutz-Managementsystem im Sinne eines Grundschutzes Wirtschaftsschutz. Heute geht es um die übergeordnete Frage, ob und wie wir noch die Herrschaft über Informationen und Nachrichten behalten können in Zeiten von Digitalisierung und Globalisierung.

Wir verzeichnen seit einigen Jahren einen rapiden Anstieg internetbasierter Kommunikationskanäle, insbesondere im Social Media-Bereich. Zugleich zersplittert und beschleunigt sich die klassische Medienlandschaft immer stärker. Ein „roter Faden" ist für einen normalen Nutzer der Medienlandschaft immer schwerer zu erkennen.

Heute stellt sich die Frage: „Wer hat Agenda Setting Power im öffentlichen Diskurs?" Wer tritt offen auf – und wer verfolgt eine „Hidden Agenda"? Wie bewegen wir uns in dem digitalen Raum, der uns alle verbindet und der zu einem Raum der Unsicherheit geworden ist – dem Internet?

Eine gängige Redewendung lautet: „Nicht ist so alt wie die Zeitung von gestern." Im Zeitalter von „Social Media" und „Internet of Things" erfreut sich digitale Echtzeit-Kommunikation großer Beliebtheit. Deshalb gilt heute auch: „Nichts ist so überholt wie mein Tweet von vor 2 Stunden." Und andererseits: das Web vergisst nicht. Der Shitstorm kann jederzeit ausbrechen. Oder auch: Meine Information kann jederzeit von Anderen im Netz in ihrem Sinne „gedreht" werden. Denn mit Hilfe des Internets sind heute einzelne Informationen dauerhaft verfügbar. Diese können, losgelöst von der Herkunftsquelle, verändert, verkürzt, manipuliert oder in einem anderen Kontext zitiert oder genutzt werden, sodass der Rechteinhaber die Hoheit und Steuerbarkeit über seine eignen digitalen Inhalte und Informationen einbüßt.

Die Fotos und Berichte über den Absturz der Linienmaschine MH 17 der Malaysian Airlines am 17. Juli 2014 in der umkämpften Ost-Ukraine mit rund 300 Toten sind ein Beispiel für diese „Wandlung" digitaler Inhalte und den bis heute anhaltenden Kampf um die Deutungshoheit dazu im Netz. Unmittelbar nach dem Abschuss entbrannte ein politischer wie medialer Streit. War ein ukrainisches Flugzeug oder ein bodengestütztes Geschütz der Rebellen ursächlich? Konnten die Rebellen überhaupt das russische Luftabwehrsystem BUK bedienen? Oder war das die russische Armee selber? Später wurde deutlich, dass die Fotos des Abschusssystems dieses einer russischen Luftabwehrbrigade zuordnen lassen. Doch auch der Untersuchungsbericht der niederländischen Behörden aus dem Oktober 2015 enthält sich einer Aussage zu der möglichen Schuldfrage. Allerdings hat die niederländische Staatsanwaltschaft an diesem Montag ein BUK-Raketenstück von der Absturzstelle der Boeing MH17 präsentiert. Ein Bericht des Vereinten Internationalen Ermittlerteams soll zum Herbst 2016 vorgelegt werden, so die niederländische Justiz.

Anrede,
nicht nur der Luftraum, auch der Cyber-Raum steht jedermann offen. Allen Akteuren, die die Sicherheitsbehörden aus der Realwelt kennen, eröffnet er neue, mitunter bessere Handlungsräume: Agenten, Kriminellen, Ex-

tremisten und Terroristen sowie Hackern mit unterschiedlichen Motiven. Sie alle bereiten uns Probleme in der Cyberwelt wie der Realwelt.

Denken Sie an die Welt der Spionage. Hier beobachten wir breit angelegte Angriffskampagnen mit Herkunft auch Russland und China wie auch gezielte Angriffe auf einzelne Rechner.

Die Einzelangriffe werden in der Regel gezielt vorbereitet und sind passgenau auf das Opfer zugeschnitten. Was bedeutet das? Damit ist vor allem gemeint, dass der Angreifer im Vorfeld versucht, so viel wie möglich über sein Opfer zu lernen. Eine Methode dafür ist das sogenannte „social engineering". Viele von Ihnen werden es kennen: Für Führungskräfte in Wirtschaftsunternehmen ist es heutzutage beinahe obligatorisch, sich in sozialen Medien darzustellen - Stichwort XING oder LinkedIn. Dort sind möglicherweise auch Einsatzbereiche oder Perspektiven der Zielperson im jeweiligen Unternehmen zu erkennen. In weiteren Netzwerken, sagen wir zum Beispiel Facebook, können Informationen wie der Musikgeschmack, das letzte Reiseziel oder die bevorzugte Automarke abgeschöpft werden.

Somit können mit wenigen Mausklicks erste Schritte für eine erfolgreiche Ansprache unternommen werden. In vordigitaler Zeit war hierfür noch ein immenser Ermittlungsaufwand erforderlich! Erst im vergangenen August warnte der britische Inlandsnachrichtendienst, dass russische und chinesische Nachrichtendienste die Angaben von Beschäftigten der britischen Regierung für nachrichtendienstliche Anbahnungen missbrauchen.

Neben den Einzelangriffen stellen wir aber auch sogenannte Angriffskampagnen fest. Diese erstrecken sich meist über einen längeren Zeitraum und betreffen verschiedene Opfer(-typen).

Eine der derzeit wohl aktivsten und aggressivsten Kampagnen stellt die Kampagne „Sofacy" dar. Vielleicht ist sie Ihnen auch unter dem Namen „APT 28" ein Begriff. Es handelt sich um eine langjährige, international angelegte Angriffsoperation mit Opfern weltweit, deren Anfänge mindestens bis ins Jahr 2007 zurückreichen. Der Bundesverfassungsschutz sieht in der Kampagne Anhaltspunkte für eine russische staatliche Steuerung beobachtet sie bereits seit mehreren Jahren. So war es uns auch möglich, den Deutschen Bundestag auf eine Kompromittierung seines Datennetzes durch „Sofacy" hinzuweisen. Die Angreifer konnten sich damals partiell Administratorenrechte verschaffen und Daten in großem Umfang abschöpfen. In Konsequenz musste das Datennetz in Teilen neu aufgesetzt werden.

Die Frage nach dem Motiv lässt mehrere Antworten zu:

- bloße Spionage, also reine Informationsabschöpfung, ggf. in Richtung Adressbücher/Terminkalender oder gar Kompromate

- Beeinträchtigung der Funktionsfähigkeit des Parlamentes, also Sabotage, oder aber
- ein politisches Signal - Bloßstellung der deutschen Behörden; ein Indiz dafür ist die Tatsache, dass der Angriff kaum verschleiert war.

Mindestens genauso gefährlich wie die Cyber-Spionage ist die Cyber-Sabotage: Der Angriff auf den französischen Sender TV 5 Monde im April letzten Jahres steht dafür beispielhaft. Das Verändern oder Blockieren von Webseiten mag dabei noch als lediglich lästig erscheinen. Anders sieht es aus, wenn das Ziel nicht Internetauftritte sind, sondern lebensnotwendige Einrichtungen: Mithin Kritische Infrastrukturen.

Eine Kampagne, die solche Art von Cyber-Sabotage zum Ziel hat, ist die Kampagne „Sandworm". Die Ziele der Kampagne sind besorgniserregend: Es sind die NATO, Telekommunikationsfirmen und Energieversorger, aber auch Regierungsstellen und Bildungseinrichtungen. Immer wieder spielen dabei SCADA-Systeme – also Industriesteuerungsanlagen –eine besondere Rolle. Sandworm führte im Winter 2015/2016 offensichtlich zu einem Stromausfall bei 700.000 Haushalten in der Westukraine. Die Infektion des Systems des Energiebetreibers erfolgte dabei über Phishing-Mails, denen teilweise ein social engineering vorausging. Auch Computer am Flughafen Kiew waren mit der Schadsoftware infiziert.

Informationshoheit kann es in einer demokratischen Gesellschaft nicht geben, erst recht nicht im Zeitalter von social media. So wie jede Form von Information verbreitet sich auch Desinformation im Netz rasend schnell; eine Gegenaufklärung, die erst zeitverzögert anlaufen kann, ist fast immer chancenlos.

Hier öffnet sich ein weites Handlungsfeld – für Extremisten und Terroristen, aber eben auch für fremde Staaten und ihre Nachrichtendienste: Ich spreche von digital basierten Manipulationsversuchen, von systematischen Desinformationskampagnen, um die Bevölkerung zu manipulieren und in eine bestimmte politische Richtung zu drängen.

Der „Infokrieg im Internet" ist nicht nur eine Ergänzung konventioneller Kriege, sondern wird zu einem eigenständigen Kampfplatz: ein Element hybrider bzw. asymmetrischer Kriegführung.

Doch eine offene und hochkomplexe Gesellschaft ist existenziell auf Informationsaustausch angewiesen. Die Integrität informationstechnischer Systeme und die Vertraulichkeit der dort vorhandenen Daten sind entscheidenden Zukunftsfragen. Die Herrschaft über die Daten ist damit eine Frage der Macht geworden. Sie ist heute eine Frage individueller Integrität, beispielsweise auch von Unternehmen, sie ist auch ein Frage staatlicher Souveränität.

Der Schutz geheimhaltungsbedürftiger Informationen aus Politik, Militär und Wirtschaft, insbesondere auch der Kritischen Infrastrukturen sind von herausragender Bedeutung. Neben der Manipulation der Technik verdient deshalb zukünftig auch die neue Qualität der Manipulationsmöglichkeiten der Öffentlichkeit ein hohes Maß an Aufmerksamkeit.

Dabei beobachtet das BfV seit geraumer Zeit auch „aktive Maßnahmen" im Netz, die von Russland ausgehen, um so die öffentliche Wahrnehmung und Meinung in unserem Land gezielt – und zu Lasten der Bundesregierung – zu beeinflussen.

3. Wirtschaftsschutz 4.0 – neue Risikoeinschätzung erforderlich

Der Bundesverband der Digitalwirtschaft BITKOM dokumentiert in seiner aktuellen Sicherheitsstudie vom April, dass bei rund 75% der Unternehmen Angriffe auf die Firmen-IT fester Bestandteil des Unternehmensalltags sind. Zugleich sind 65 % der vermuteten Täter Mitarbeiter oder ehemalige Mitarbeiter. Damit wird deutlich, dass und wie sich die Risiken der Informationssicherheit und Informationshoheit in der Realwelt wie der Cyberwelt verschränken.

Die zunehmende elektronische Vernetzung der Wirtschaft – Stichwort „Industrie 4.0" und „Internet der Dinge" – eröffnet der deutschen Wirtschaft neue Chancen und Perspektiven. Aber eben auch konkurrierenden Unternehmen und fremden Nachrichtendiensten. Die neuartigen komplexen Vernetzungen in der gesamten Wertschöpfungskette erhöhen sogar noch die Risiken. Das Internet ist nicht nur ein Wachstumsmotor. Es ermöglicht auch: Identitätsdiebstahl, CEO-Fraud, Web-Defacement, Elektronische Angriffe.

Deshalb brauchen Staat und Wirtschaft eine neue Risk Map für die Gefahren des Cyberraums, gleichsam einen „Wirtschaftsschutz 4.0". Es gilt nicht nur, was der Bundestag im November letzten Jahres beschloss, dass nämlich „eine vernetzte Industrie … ein hohes Maß an IT-Sicherheit voraussetzt."

Wie wir freiheitlich und sicher in Zeiten der Digitalisierung wirtschaften, muss sorgfältig erwogen werden. Damit eben nicht gilt, was der Direktor des Digital Society Institute Berlin, Dr. Sandro Gaycken, am 4. März 2016 fragte „Waren wir alle viel zu naiv bei der Digitalisierung?"

Anrede,
es geht um einen umfassenden Wirtschaftsschutz. Dazu gehören personelle, prozessuale, organisatorische, technische wie IT-technische Aspekte.

Sicherheit ist eine Voraussetzung für Industrie 4.0. Es geht bei der Debatte um Industrie 4.0 also nicht um „digitale Maschinenstürmerei", wenn auf die Sicherheitsrisiken hingewiesen wird sondern um eine realistische

ganzheitliche Herangehensweise an Chancen und Risiken für unsere Volkswirtschaft wie jedes einzelne Unternehmen.

4. Ausblick – Gemeinsames Handeln von Bundesverfassungsschutz und ASW Bundesverband

Das BfV versteht sich als Dienstleister für Wirtschaftsschutz und als Partner der Wirtschaft. Seit vielen Jahren ist pro-aktiver Wirtschaftsschutz einer der Schwerpunkte des BfV. Er umfasst insbesondere die präventive Spionageabwehr. In den letzten Jahren sind zunehmend auch Gefährdungen durch Sabotage, Terrorismus und gewaltorientierte extremistische Kampagnen hinzugetreten. Das BfV sieht sich einem ganzheitlichen Wirtschaftsschutz verpflichtet, der alle Gefährdungsfelder der deutschen Wirtschaft, die wir als Inlandsnachrichtendienst abdecken, im Blick behält.

Bei der Information und Prävention benötigt das BfV Partner. Zusammenarbeit und Dialog mit unseren Partnern sind wichtige Voraussetzungen für einen zielgerichteten und nachhaltigen Wirtschaftsschutz.

Gerade deshalb halte ich die Ende April vom Bundesinnenminister Dr. Thomas de Maizière gestartete „Initiative Wirtschaftsschutz“ für so wertvoll: Erstmals haben sich Staat und Wirtschaft verabredet, gemeinsam das Schutzniveau der deutschen Wirtschaft mit konkreten gemeinsamen Informations-, Schulungs- und Unterstützungs-angeboten zu verbessern. Auf der webbasierten Wissens- und Dialogplattform der „Initiative Wirtschaftsschutz“ bündeln die Sicherheitsbehörden BfV, BND, BKA und BSI ihre Angebote zum Thema Wirtschaftsschutz für Wirtschaft und Wissenschaft. Unter dem Motto „Gemeinsam. Werte. Schützen.“ arbeiten in der „Initiative Wirtschaftsschutz“ auch BfV und ASW mit.

Mit dem ASW Bundesverband teilt der Bundesverfassungsschutz ein gemeinsames Interesse: Sicherheit. Die bisher 10 gemeinsamen Fachtagungen sind dafür ausdrucksstarker Beleg. Sie haben sich in den letzten Jahren positiv entwickelt. Für das gemeinsame Eintreten für die Sicherheit der deutschen Wirtschaft steht auch die rund 20 Jahre währende und sich intensivierende vertrauensvolle Zusammenarbeit von BfV und ASW.

Dafür bedanke ich mich bei Ihnen, lieber Herr Wagner sowie bei allen Mitarbeiterinnen und Mitarbeitern der ASW-Geschäftsstelle und auch bei allen Verbänden für Sicherheit in der Wirtschaft in den Ländern. In diesen Dank schließe ich auch die im Wirtschaftsschutz mitarbeitenden Kolleginnen und Kollegen des Verfassungsschutzverbundes ein, die diese Zusammenarbeit mit ASW und VSW mit Leben erfüllen.

Damit verdeutlichen wir: Wirtschaftsschutz ist ein Thema für jetzt und die Zukunft. „Prävention durch Dialog und Information“ ist das Leitbild des Zukunftskonzepts Wirtschaftsschutz des BfV. Prävention, Dialog und In-

formation verbinden auch BfV und ASW bei ihrem Einsatz für Security-Awareness.

Anrede,
wir haben heute ein hochaktuelles, ein wichtiges Thema. Und wir haben kompetente Referenten. Referenten, die das Thema Informationssicherheit und Informationshoheit in seiner Breite beleuchten werden: von den Implikationen aus unternehmerischer und wissenschaftlicher Sicht über den journalistischen Zugang bis hin zu den strategischen Handlungsoptionen, die sich fremden Nachrichtendiensten eröffnen.

Austausch, Dialog und das gegenseitige Kennenlernen sind wichtige Faktoren für wachsendes Vertrauen. Dazu will auch die 10. Sicherheitstagung von BfV und ASW beitragen. Nutzen Sie den heutigen Tag! Es liegen alle Voraussetzungen für eine spannende, informationsreiche Veranstaltung vor – einschließlich der Kommunikationspausen! Ich meine: Sie werden als Gäste dieser 10. Sicherheitstagung nicht enttäuscht sein!

Ich freue mich, das Wort nun an die Staatssekretärin im Bundesinnenministerium, Frau Dr. Emily Haber übergeben zu können und wünsche uns allen einen guten Austausch!

„Zum Schutz von Informationen müssen Staat und Wirtschaft eng und arbeitsteilig zusammenarbeiten“

Dr. Emily Haber, Staatssekretärin im Bundesministerium des Innern

Es gilt das gesprochene Wort. [Rede auf der 10. Sicherheitstagung des BfV und der ASW]

[Anrede]

Die Frankfurter Buchmesse, das Handelsblatt und die Investmentbank Goldman Sachs vergeben jedes Jahr den Preis für das Wirtschaftsbuch des Jahres.

Im letzten Jahr 2015 erhielt ein Buch diese Auszeichnung, über das die Jury in seiner Begründung unter anderem folgenden Satz schrieb.

Ich zitiere: „Dieses Buch ist der aktuell wichtigste Debatten-Beitrag zum digitalen Wandel.“ Komischerweise schaffte es dieses Buch nicht dauerhaft auf die Bestellerlisten.

Der breiten Öffentlichkeit ist es eher weniger bekannt. Sein Name lautet „The Second Machine Age“ - vielleicht kennen es ja einige von Ihnen. Das Buch bietet mehrere interessante Gedanken, aber ich will mich auf einen Gedanken beschränken, weil er für unser Thema eine besondere Bedeutung hat.

Dieser Gedanke betrifft das sogenannte „Alles-oder-nichts“ Prinzip in der digitalen Welt. Die Autoren sagen, dass sich die verschiedenen digitalen Märkte immer mehr zu „Alles-oder-nichts“ Märkten entwickeln - nur ein Anbieter könne und werde bei digitalen Dienstleistungen erfolgreich sein.

In Zukunft werde es „vieles“ geben, aber davon oft nur „eines“: Ein soziales Netzwerk, einen Kurznachrichtendienst oder eine Seite, die die Nachrichten des Tages zusammenfasst. Der Grund dafür liege in der oft unbegrenzten Skalierbarkeit des Angebotes.

Das beste Angebot setze sich gegen die Konkurrenz durch, weil es attraktiv ist und sehr schnell und unbegrenzt verbreitet werden kann - das seien die zwei entscheidenden Parameter für den Erfolg in der digitalen Welt.

[Anrede]

Was hat das für Folgen für die Politik und den Staat, wenn wir über Informationen sprechen?

Gibt es „attraktive“ und „unattraktive“ politische Informationen? Gibt es Informationen, die sich schneller und besser verbreiten als andere?

Was bedeutet das in einer Welt, in der man sich „theoretisch“ Informationen von vielen Stellen holen kann? Macht man das aber auch praktisch - oder bleibt man auf den eigenen und bekannten Plattformen?

Wie wertvoll werden besondere Informationen, wenn man damit auf einmal zum Gewinner am Markt wird oder einen Staat in Ungleichgewicht bringen kann?

Ich will Ihnen heute vier Gedanken vortragen. Und mich jedem dieser Gedanken jeweils mit einem Beispiel nähern.

Mein erstes Beispiel betrifft den sogenannten „Fall Lisa“, der Fall der 13-jährigen russisch-deutschen Schülerin, der Anfang des Jahres durch die Medien ging.

Es wurde kolportiert, dass Lisa von zwei Männern - Asylbewerber, so klang es an - missbraucht worden sei. Dieser Vorwurf konnte relativ rasch widerlegt werden.

Die losgelöste Empörungswelle war aber nicht mehr zu stoppen.

Bei Russlanddeutschen stieß die Nachricht auf fruchtbaren Boden. Sie wurde dann vom rechtsextremen Spektrum in Deutschland aufgegriffen.

Der Fall wurde mit den Vorfällen in der Silvesternacht in Köln verknüpft. Eine eigene Facebook-Gruppe gründete sich. Bundesweit kam es zu zahlreichen Demonstrationen in mehreren Dutzend Städten mit insgesamt über 20.000 Teilnehmern.

Der Sachverhalt über das Mädchen war frei erfunden.

Dennoch: Berichterstattung zur besten russischen Sendezeit im „Pjervij Kanal“ und die Äußerungen des russischen Außenministers während einer Pressekonferenz gaben ihm einen zusätzlichen Anstrich besorgniserregender Echtheit - obwohl der Sachverhalt zum Zeitpunkt der Pressekonferenz längst aufgeklärt war.

Aber was wir dann sahen, war die Instrumentalisierung des Falles im Netz, die Ressentiments in der die Republik tief bewegenden Flüchtlingsfrage bespielte und mit atemberaubender Choreographie Demonstrationen und Bürgerproteste produzierte.

Die blitzschnelle, lawinenartige Verbreitung im Netz, die Serie von Demonstrationen gegen eine früh widerlegte Phantommeldung verweisen auf ein Phänomen unserer Zeit.

Meine These ist:

Die hohe Skalierbarkeit von Falschinformationen in der digitalen Welt hat erhebliche und noch nicht absehbare Folgen für Politik und Staat.

Informationen im Netz können ihre eigene Wirklichkeit entfalten: Im „Fall Lisa“ hatte die Ursprungsmeldung für viele offenbar eine größere und glaubwürdigere Legitimität als die Widerlegung - auch die von staatlichen Stellen.

Man wird mir entgegenhalten, dass in einer breiten Öffentlichkeit längst die Richtigstellung und die Verantwortlichkeiten registriert worden waren.

Wohl wahr. Aber die Informationsmanipulation hatte nichts von ihrer politischen Wirksamkeit bei denen eingebüßt, die ihr Adressat gewesen waren - die auf die Straße gingen, sich in Ängsten und Abwehrgefühlen bestätigt und in richtigstellender Berichterstattung eine staatliche gewollte Vertuschung sahen.

Der polarisierende Effekt blieb.

Der Fall „Lisa“ zeigt Grenzen staatlichen Handelns gegen Desinformationskampagnen. Ein Rechtsstaat kann nicht mit gleicher Münze reagieren. Die Urheber zurück zu verfolgen und zu stellen, ist oft illusorisch.

Wir können nur offenlegen, dass es sich beim Fall „Lisa“ um gezielte Desinformation handelt und wie der dahinter stehende Prozess abgelaufen ist.

Aufklärung reicht aber nicht. Aufklärung kann nur reaktiv erfolgen, die Desinformation bleibt immer einen Schritt voraus - das ist sozusagen ein struktureller Nachteil des Rechtsstaates.

Es gibt Angst vor Veränderungen, die wir wahrscheinlich nicht erfolgreich mit Sachargumenten bekämpfen können. Wir werden mit ihnen durch Handeln in der physischen Welt umgehen müssen.

In der Flüchtlingsfrage, aus der im Fall Lisa der Resonanzboden kam, heißt das:

- Funktionierende Flüchtlingsaufnahme, die die Steuerungsfähigkeit des Staates belegt.
- Persönliche Kontakte und die selbst erlebte Erfahrung, dass sich Vorurteile nicht bestätigen.
- Funktionierende Integration, die so rasch und so breit wie möglich ansetzt. Mit dem Integrationsgesetz haben wir Bedingungen formuliert, die Leistungen und Angebote des Staates mit Erwartungen und Forderungen an die zu Integrierenden verbindet.

Staat und Politik können diesen Kampagnen nur mit dem Handwerkszeug des Rechtsstaats begegnen.

Das ist nicht spektakulär - aber ich denke, es ist auch das, was der Publizist

Joachim Fest als „offene Flanke der offenen Gesellschaft“ bezeichnete. Und um es klar zu sagen: Lieber so als anders! Freiheit und eine liberale Ordnung haben ihren Preis.

Mein zweites Beispiel betrifft das Phänomen des IS. Der IS ist die brutalste terroristische Kraft mit globalem Anspruch.

In der physischen Welt hat er staatsähnliche Strukturen geschaffen - er treibt Steuern ein, unterhält Verwaltungsapparate, Armeen.

In der virtuellen Welt hat seine Propaganda eine parallele Scheinexistenz geschaffen, die das Leben im Kalifat verherrlicht, exklusive Gemeinschaft verspricht und den Schrecken zum Abenteuer macht.

Die Propaganda hat zweifellos Wirkung gezeigt: Menschen aus aller Welt sind dem Vexierbild nach Syrien und in den Irak gefolgt, um dort an den Kämpfen teilzuhaben.

Darunter 4.500 aus Europa, junge Männer, aber auch viele Frauen und Jugendliche. Es sind nicht immer die vermeintlich benachteiligten Gruppen darunter - was vermutet werden könnte - wie Arbeitslose, Schulabbrecher oder Menschen mit kleinkrimineller Vergangenheit.

Auch gute Schüler, erfolgreiche Sportler, Akademiker und junge Familien aus der Mitte unserer Gesellschaft fühlen sich angesprochen.

Als erste Terrororganisation nutzte der IS dabei die sozialen Medien in höchst professioneller Weise. In einer Untersuchung hat das Simon-Wiesenthal-Center kürzlich über 200.000 tägliche Tweets des Islamischen Staates und seiner Unterstützer festgestellt.

Über Whatsapp vermitteln Syrien-Kämpfer in ihrem Freundeskreis ein plastisches Bild von Syrien als Abenteuerland, unterlegt mit der Authentizität des persönlichen Austauschs.

Gezielt sprechen Agiteure des IS über Facebook und Twitter zum Beispiel religiös Suchende an und versuchen, sie für ihre Ideologie zu gewinnen. Auch hier spielt der - wenngleich virtuelle - persönliche Kontakt eine große Rolle.

Die Flexibilität der vielfältigen Kommunikationsmöglichkeiten über das Internet ermöglicht dem IS auch, in großer Geschwindigkeit auf Veränderungen in der physischen Welt zu reagieren und das Personalreservoir seiner Anhängerschaft weltweit umzusteuern.

So sehen wir gegenwärtig, dass der IS nach seinem anfänglich unaufhaltsam scheinenden Vormarsch in den letzten Monaten deutliche Rückschläge hinnehmen musste und Terrain in Syrien und im Irak verlor.

Die Attraktivität des IS in den Augen der angehenden Jihadisten scheint abzunehmen - jedenfalls sehen wir einen Rückgang derjenigen Personen, die aus Deutschland nach Syrien oder in den Irak reisen.

Die Folge: Er hat begonnen, Teile seiner Operationsbasis nach Libyen zu verlegen. Wahrscheinlich wird ihn dies zu einer stärker abgeschichteten Adressatenorientierung seiner Propaganda im Netz zwingen müssen.

In Nahost wird nämlich eine Verlagerung des IS aus dem historischen Herkunftsraum des abbasidischen Kalifats an die libyschen Außengebiete der arabischen Welt durchaus als Abstieg wahrgenommen werden; mag sein, dass die IS-Propaganda dort künftig stärker „Überlebensstereotype“ als antiwestlichen Kampf bedienen wird.

In Europa wird dies kaum Mobilisierungswirkung entfalten - hier wird er Erfolge vorweisen müssen. Es ist nur folgerichtig, dass der IS massiv dazu übergegangen ist, Ziele in Europa ins Visier zu nehmen und hier zu Anschlägen, auch zu Kleinstanschlägen, aufzurufen.

Seine Strategie ist diverser geworden: Er setzt auf spontane Individualtaten - wie die der 15 jährigen Hannoveranerin, auf Kleinstgruppen, die im Verbund agieren und auf komplexe Tatplanungen, die eingeschleuste Kämpfer des IS, Rückkehrer aus den Kampfgebieten sowie lokale radikale Islamisten einbeziehen.

Er braucht Erfolge jenseits der Region, und seine Propaganda hier läuft auf ein „anything goes“ hinaus.

In den jüngsten IS-Verlautbarungen wird daher die Bedeutung auch bereits kleinster Anschläge im Westen herausgehoben. Er braucht sie, als Gegengeschichte zum Abstiegsnarrativ.

Dies führt mich zu meiner zweiten These:

Politik und Staat müssen sich darauf einstellen, dass Informationen, die aus der digitalen Welt kommen, stärker von Polaritäten und Extremen geprägt sein werden, als in der Zeit, in der wir Informationen aus der Zeitungen erhielten.

Und das hat Auswirkungen auf unsere Gesellschaft und die Politik in unserem Land - manche kennen wir schon, viele haben wir sicher noch nicht erkannt.

Wenn wir dem begegnen wollen, müssen wir die Gründe und Mechanismen verstehen, die extreme Meinungen und Radikalisierungen auslösen oder bestärken können und die fast immer aus der physischen Welt kommen.

Wir müssen es schaffen, radikalisierungsgefährdete Jugendliche zu motivieren und zu befähigen, mündig, kritisch und aktiv am politischen Leben teilzunehmen.

Dass in dieser Gegengemeinschaft das Internet auch der Motor für die selbstreferentielle Bestätigung und den Ausschluss anderer Wahrnehmungen ist - seine Algorithmen sind ja darauf angelegt, Gleichdenkende zu verbinden -, ist mit Blick auf das Transparenz- und Informationsfreiheitsversprechen des Internets auch ein Paradox.

Wir haben spezielle Deradikalisierungsprogramme entwickelt, die vor allem in der realen Welt ansetzen - in Schulen, beim Sport, der Angehörigenberatung.

Der Staat macht auch im Internet viel: Informationen zur politischen Bildung und vieles andere mehr.

Trotzdem: Wir werden in Zukunft darauf natürlich einen stärkeren Fokus legen.

[Anrede]

Mein drittes Beispiel betrifft die kriminellen Geschäftsfelder gezielter Falschinformation, nämlich die - vor allem im letzten Herbst - migrationsverstärkend wirkenden Gerüchte, die über das Internet im Umlauf waren.

Damals hatte sich beispielsweise in Afghanistan das hartnäckige Gerücht festgesetzt, dass die Bundesregierung händeringend nach bis zu 1,8 Millionen Arbeitskräften suche und deshalb 5.000 Migranten täglich aufnähme.

Siemens, Mercedes-Benz und BMW wurden explizit als interessierte Arbeitsgeber genannt. Als Anreiz für ihr Kommen erwarte die Migranten ein Einkommen von 1.000 € monatlich und ein eigenes Haus.

Das klingt in Ihren Ohren absurd. Bei den Menschen in Afghanistan war dies anders. Sie konnten die Plausiblität der Information nicht einschätzen und glichen lediglich ihre Perspektiven und die ihres Landes mit den hochgeschraubten Erwartungen an ein Leben in Deutschland ab.

Das sich rasant verbreitende Gerücht gehörte mit zu der Initialzündung für zigtausende, die sich aus Afghanistan auf den Weg machten. Die angeblichen Aussichten zogen auch bis dahin nicht Ausreisewillige, gutsituierte Bürger und Akademiker, ganze Familienverbände an, die Hausstand und Besitz verkauften.

Die Gerüchte wurden bestärkt und scheinverifiziert durch Handy-Photos von applaudierenden Bürgern an deutschen Bahnhöfen und anderen Begrüßungsszenen.

Die Zahl der Ausreisewilligen aus Afghanistan und die Asylanträge zeigen

die Wirkung drastisch: Im September 2015 kamen ca.18.000 Flüchtlinge aus Afghanistan, im Oktober 31.000, im November 44.000. Im gesamten Vorjahr 2014 waren es knapp 10.000 Asylantragsteller aus Afghanistan.

Die Verbreitung des Gerüchts war Teil eines gigantischen business - Migration ist ein business. Die sich modernster Kommunikationstechnologien bedienende Schleusungskriminalität ist der am schnellsten wachsende Zweig der organisierten Kriminalität, schneller wachsend als der Handel mit Waffen oder Drogen.

Migranten sind auf der Flucht häufig allein auf die Informationen angewiesen, die sie über ihr Smartphone beziehen können. Dies machen sich Schleuser zu Nutze. Sie bieten ihre Dienste in sozialen Netzwerken wie Facebook an. Die Aufmachung ihrer Seiten ist hochprofessionell - und irreführend.

Da kann die Überfahrt über das Mittelmeer auf den ersten Blick an eine Kreuzfahrt erinnern. Es ist eine Tatsache, Schleuser beeinflussen durch gezielte Informationen Migrationsbewegungen. Ohne Smartphones wäre die Schleuserkriminalität nicht so schnell gewachsen.

Das führt mich zu meiner Dritten These:

Wenn Falschinformation zu einem kriminellen Geschäftsmodell wird, darf und muss Staat und Politik auch selbst in die Informationsauseinandersetzung eintreten.

Und das haben wir auch getan.

Die afghanische Regierung und Medien zeigten in Aufklärungskampagnen die brutale Realität: überfüllte Boote, leblose Körper und Kinder in Flüchtlingslagern.

Auch das Auswärtige Amt führte in Informationsfilmen vor, was sie wirklich in Deutschland erwarte: eine unsichere Zukunft.

Mindestens so glaubwürdig und daher enorm wichtig sind aber auch die Nachrichten der Asylbewerber, die sie über ihre Erfahrungen - wiederum oft genug per Smartphone - nach Hause berichten. Und es spielt eine Rolle, ob sie schreiben: Dass die Erwartung trügt, auf alle warteten Jobs bei Mercedes und BMW; oder aber: dass man, selbst bei einem negativen Bescheid, in Deutschland bleiben könne, weil Abschiebung nicht drohe.

Die Verkürzung der Asylverfahren, die Anpassung des Leistungssystems, die konsequente Rückführung abgelehnter Asylbewerber, die strikte Trennung zwischen Schutzbedürftigen und Nicht-Schutzbedürftigen, die unser Land wieder verlassen müssen - das sind aber alles zwingende Gegenbotschaften aus der physischen Welt, die sich als Summe von Einzelerfahrungen verbreiten wird.

Dies benötigt Zeit. Deswegen ist es so wichtig, dass wir gleichzeitig konsequent gegen irreguläre Migration und gegen Schleusungen vorgehen; dass wir Schritte zur Sicherung eines funktionierenden Außengrenzschutzes unternehmen und das europäische Asylsystem so verändern, dass sekundäre Migration eingedämmt und eine freie Wahl des Ziellandes nicht mehr möglich wird.

Wenn das Schleusernarrativ große Versprechungen enthielt mitsamt der Sicherheit, dass das Erreichen europäischer Grenzen leicht möglich und die Wahl des Ziellandes frei sei, so wird Gegenaufklärung nicht reichen, um die Werbungsmaschinerie des Wirtschaftszweiges zu entkräften.

Fakten, die wir schaffen, werden dazu beitragen müssen.

[Anrede]

Mein letztes Beispiel ist ein Beispiel aus einer möglichen Zukunft. Es stammt aus dem Buch „Germany 2064“ des schottischen Schriftstellers Martin Walker.

In diesem Deutschland der Zukunft bestimmt High-Tech mit selbstlenkenden Fahrzeugen und Robotern das Stadtbild - beinahe alles läuft automatisch.

Was für ein Stadtbild entstünde wohl, wenn es einen Cyberangriff geben sollte? Diese Frage beantwortet Martin Walker leider nicht.

Der Staat muss sich über diese Schattenseiten der digitalen Kommunikationsrevolution aber Gedanken machen: Die neuen Kommunikationsformen bieten Einfallstore für Angriffe.

Die IT-Systeme in Unternehmen und in der Verwaltung sind geschützt. Die Sicherheitsverantwortlichen sind sich der Risiken bewusst und treffen Vorkehrungen: Firewalls, Virenscanner etc.

Dennoch sind sie gegen hochprofessionell arbeitende Täter kaum gefeit, die schon neue Schadprogramme entwickeln, noch bevor das eigentliche Schutzprogramm zum Einsatz kommt.

Oder bildlich gesprochen: Noch bevor Sie Ihre Eingangstür einbauen, hat der Dieb schon den Schlüssel gefertigt.

Das Bundesamt für Sicherheit in der Informationstechnik stellt in seinem jüngsten Bericht zur IT-Sicherheitslage fest, dass nach wie vor viele IT-Systeme viele Schwachstellen und Verwundbarkeiten aufweisen.

Einige dieser Schwachstellen offenbaren schwerwiegende Sicherheitslücken. Als Beispiel nennen möchte ich nur den Angriff auf ein Krankenhaus in Neuss, das wegen eines Cyberangriffs kurzzeitig geschlossen werden musste.

Vor allem Phishing-Mails, also E-Mails mit schadhaften Anhängen, sind derzeit sehr verbreitet.

Die Risiken für IT-Systeme steigen exponentiell, wenn Mitarbeiter und Mitarbeiterinnen mobile Endgeräte wie Smartphones, Tablet-PCs oder auch USB-Sticks nutzen und Sicherheitsvorkehrungen dadurch umgangen werden.

Letzte Woche ging der Angriff auf das AKW im bayerischen Gundremmingen durch die Presse, wo die Verwendung eines schadhaften USB-Sticks der Auslöser gewesen sein soll.

Für die Gefahren für die IT-Sicherheit gilt wiederum: Der Staat kann nur bedingt davor schützen. Gefragt sind die Eigenverantwortung der Bürger und der Unternehmen, der Staat unterstützt sie dabei.

Mit dem Beschluss der Cyber-Sicherheitsstrategie für Deutschland im Jahr 2011 hat die Bundesregierung wesentliche Weichen für eine zukunftsgerichtete Cyber-Sicherheitspolitik gestellt.

Herausheben möchte ich die Gründung des Nationalen Cyber-Sicherheitsrates und die Einrichtung des Nationalen Cyber-Abwehrzentrums. Die wesentlichen Aussagen der Cyber-Sicherheitsstrategie 2011 haben zwar auch heute noch Bestand.

Trotzdem müssen wir sie fortschreiben.

Dafür hat das Bundesinnenministerium die Länder und die Wirtschaft bereits in einem frühen Stadium umfassend einbezogen.

In der neuen Strategie werden die Möglichkeit zu sicherem und selbstbestimmtem Handeln im Netz auf Basis sicherer Systeme und die Bedeutung von Bildung und Forschung eine ebenso wichtige Rolle spielen wie die mit dem IT-Sicherheitsgesetz etablierte Kooperation mit der Wirtschaft.

Wir wollen uns zudem der Cyber-Sicherheitsarchitektur in Deutschland widmen. Die Zuordnung von Aufgaben und Befugnissen sowie die technischen Fähigkeiten der Behörden und die Möglichkeiten ressortgemeinsamer Zusammenarbeit werden hierbei näher zu betrachten sein.

Die Arbeiten sind in vollem Gange. Die neue Cyber-Sicherheitsstrategie wird nach derzeitiger Planung im Herbst dem Bundeskabinett zur Beschlussfassung vorgelegt.

Neben der Sicherung der IT-Systeme spielt der Faktor Mensch als Sicherheitsrisiko eine bedeutende Rolle. Die Vorbeugung und Bekämpfung der Wirtschaftsspionage, Konkurrenzausspähung und Sabotage – also ein Bereich, mit dem Sie sich vermutlich täglich befassen - sind auf eine stärkere Vernetzung der Maßnahmen gegen digitale und klassische Wirtschaftsspionage angewiesen.

In der Initiative Wirtschaftsschutz arbeiten die vier Sicherheitsbehörden des Bundes BfV, BKA, BSI und BND mit den Spitzen- und Sicherheitsverbänden der deutschen Wirtschaft BDI, DIHK, ASW und BDSW zur Verbesserung des Schutzes für deutsche Unternehmen zusammen.

Auf einer gemeinsamen Internetplattform (www.wirtschaftsschutz.info) erhalten nunmehr alle interessierten Unternehmen exklusive Informationen zu allen relevanten Themen, Hinweise für betroffene Unternehmen im Sinne einer Hilfe zur Selbsthilfe sowie Ansprechpartner auf Bundes- und Landesebene.

[Anrede]

Zum Schutz von Informationen müssen Staat und Wirtschaft eng und arbeitsteilig zusammenarbeiten. Das tun wir schon. Und wir wollen es in Zukunft ausbauen.

An dieser Stelle möchte ich ganz ausdrücklich das Engagement aller beteiligten Verbands- und Unternehmensvertreter, allen voran des heutigen Gastgebers, des ASW Bundesverbandes als einem aktiven Mitglied der Initiative Wirtschaftsschutz, hervorheben.

Dieses arbeitsteilige Zusammenwirken ist beispiellos in Deutschland und Europa und ich hoffe, es macht Schule.

In der Mittagspause wird ein kurzer Informationsfilm über die Arbeit und Angebote der Initiative Wirtschaftsschutz gezeigt, den ich Ihnen ans Herz legen möchte.

In Deutschland brauchen wir mündige, aufgeklärte und starke Bürger. Die Aufgabe des Staates ist und bleibt es, dafür die Bedingungen zu schaffen, über Gefahren aufzuklären und Selbstschutz zu unterstützen.

Der Staat kann dabei nicht alles tun. Gerade beim Thema „Informationen“ und „Informationssicherheit“.

Wer für Sicherheit eintritt, muss mit Unsicherheit rechnen und mit ihr umgehen. Das heißt auch, er muss mit Angriffen rechnen und umgehen können.

Das gilt für Sie und Ihre Unternehmen und das gilt in gleicher Weise für mich und den Staat - sozusagen für uns alle.

Es ist gut, dass wir einiges davon gemeinsam angehen.

Ihnen und uns allen einen wunderbare Jubiläumstagung.

Vielen Dank.

Propaganda und politische Einflussnahme als strategische Handlungsoption ausländischer Nachrichtendienste

Dr. Burkhard Even, Leiter der Abteilung Spionageabwehr im BfV

Anrede,

nicht wenige Anwesende sind regelmäßige Besucher unserer Sicherheitstagung, manche können wir heute erstmals begrüßen.

Der ungebrochene Zuspruch ist ein gutes Zeichen und steht dafür, dass unser gemeinsames Thema – Wirtschaftsschutz – nach wie vor und sicher auch künftig eine hohe Priorität genießt.

Der pro-aktive Wirtschaftsschutz des BfV im Sinne einer präventiven Spionageabwehr ist eine auf Partnerschaft angelegte Dienstleistung des Staates. Hierüber haben wir in den vergangenen Sicherheitstagungen mehrfach gesprochen und unser Angebot in Kooperation mit den Verbänden der Wirtschaft entwickelt.

Wiederholt wurde auf den bisherigen neun Sicherheitstagungen von BfV und ASW Wirtschaftsspionage und Konkurrenzausspähung als Teil eines zunehmend intensiveren globalisierten Wettbewerbs diskutiert.

Zuletzt wurde im vergangenen Jahr schwerpunktmäßig das vielfach unterschätzte Risiko von Innentätern erörtert.

Die Facetten der Spionage sind nach wie vor zahlreich.

Auch vergleichsweise neue Methoden wie die Nutzung Elektronischer Angriffe für Spionage- und auch Sabotagezwecke sind seit ein paar Jahren fest im Werkzeugkasten der Angreifer verankert und waren und sind deshalb selbstverständlicher Gegenstand unserer Arbeit.

Allerdings beschränken sich Handlungsauftrag und Handlungsmöglichkeiten zahlreicher Nachrichtendienste nicht nur darauf. Eine selten beachtete Tätigkeitsform ist Titel meines heutigen Vortrags, nämlich die Propaganda und politische Einflussnahme als eine strategische Handlungsoption von Nachrichtendiensten.

Klassische und neuartige Methoden ergänzen sich zu einem umfassenden Risikopotenzial und das werde ich versuchen, an ein paar Beispielen zu verdeutlichen.

Anrede,

morgen beginnt die Fußball-Europameisterschaft mit dem Eröffnungsspiel Frankreich gegen Rumänien.

Am Sonntag greift die deutsche Mannschaft – hoffentlich erfolgreich – gegen die Ukraine in das Turniergeschehen ein.

Einen Monat lang wird die EM im Fokus der Medien stehen und uns einmal mehr zeigen, dass die Medien für die öffentliche Wahrnehmung eine herausragende Bedeutung genießen.

Für den Sport, die damit verbundene Begeisterung und die völkerverbindende Idee ein gute Sache.

Aber bekanntlich hat eine Medaille zwei Seiten.

Lassen Sie uns daher heute über ein vermeintlich neues Phänomen – die andere Seite der Medaille – sprechen.

Die herausragende Funktion der Medien und die öffentliche Wahrnehmung der Berichterstattung haben im Zeitalter neuer elektronischer Medienformate und Medienanbieter weiter zugenommen.

In der Medientheorie trägt dies zu einem ausgeprägten demokratischen und pluralistischen Diskurs bei. Das ist sicher richtig.

Doch gleichzeitig bieten sich denjenigen, die nicht der unabhängigen Meinungsbildung verpflichtet sind, sondern manipulative Zwecke verfolgen, zusätzliche Möglichkeiten in der digitalen Medienwelt, die öffentliche Meinung in ihrem Sinne zu beeinflussen.

Die Geschichte der Nachrichtendienste bietet eine Vielzahl an Beispielen. Sogenannte „aktive Maßnahmen" – also gezielte Manipulationen von Medienvertretern und Politikern durch Angehörige eines gegnerischen Nachrichtendienstes – waren schon immer ein probates Mittel zur Beeinflussung der öffentlichen Meinung und letztendlich von politischen Entscheidungen.

Fast schon in Vergessenheit geraten sind beispielsweise die Aktivitäten der Abteilung X der Hauptverwaltung Aufklärung (HVA) des Ministeriums für Staatssicherheit (MfS) der DDR. Ihre Aufgabe war die bewusste und legendierte Verbreitung von Falschinformationen zur Beeinflussung der Öffentlichkeit und der Regierungsverantwortlichen. Die „Antisemitismus-Affäre" zu Beginn der 60er Jahre in Westdeutschland steht dafür beispielhaft.

Hierzu diente letztendlich auch die Unterstützung von Einflussorganisationen und Parteien in der Bundesrepublik Deutschland.

Faktenreich belegt ist dies in den Aktenbeständen der Stasi-Unterlagenbehörde.

Gefälschte Dokumente, lancierte Falschinformationen und z.B. auch die finanzielle Unterstützung von bestimmten Organisationen fanden noch

bis in die achtziger Jahre, so z. B. im Zusammenhang mit der Nachrüstungsdebatte, statt.

Entsprechende Maßnahmen gehörten auch zum Standardrepertoire des früheren sowjetischen Geheimdienstes KGB. Auch hier gibt es viele Beispiele.

Propaganda und Desinformation waren und sind selbstverständliche Handlungsoption zahlreicher Staaten und damit sehr häufig auch der jeweiligen Nachrichtendienste.

Betrachten wir die Gegenwart:

Globalisierung heißt nicht nur zunehmender globalisierter Wettbewerb um Produkte, Strategien und Märkte.

Das damit verbundene Know-how, auch aus Forschung und Entwicklung, sind die besonders schützenswerten Kerninformationen, die sogenannten „Kronjuwelen".

Der globale Wettbewerb findet auch auf diversen anderen Feldern statt.

Hier geht es letztlich um Einfluss und den eigenen z. B. politischen Vorteil. Letztlich besteht dabei meist auch eine Wechselwirkung zwischen Politik und wirtschaftlichen Einfluss, mit Folgen auch ganz konkret für Unternehmen.

Ein Beispiel hierfür ist der Ukraine-Konflikt mit den daraufhin eingeführten Wirtschaftssanktionen gegen die Russische Föderation, was wiederum sehr konkrete Auswirkungen für diverse Branchen und natürlich auch für die einzelnen Unternehmen hat.

Manche aktuelle Entwicklung und Konfrontation erinnert uns wieder an die eigentlich schon vergessene Zeit des Kalten Krieges.

Gleichzeitig haben Macht und Möglichkeiten bei der Nutzung von Medien deutlich zugenommen – eine qualitativ neue Situation im Vergleich mit der Vergangenheit.

Medien dienen zwar dem Austausch von Informationen und Meinungen, und damit der freien Meinungsbildung in der Gesellschaft. Sie können aber eben auch als Werkzeug zur Desinformation und Beeinflussung genutzt bzw. missbraucht werden.

„Die Bundesregierung beobachtet seit geraumer Zeit verstärkte russische Versuche, auf die öffentliche Meinung auch außerhalb Russlands Einfluss zu nehmen. Das gilt auch für Deutschland", so lautete die Antwort auf eine entsprechende parlamentarische Anfrage Anfang des Jahres 2016.

Schon seit Jahren, die Initialzündung waren Osterweiterung der Europäischen Union und der NATO, berichten uns Partner vor allem aus verschie-

denen osteuropäischen Ländern, dass Russland in vielfacher Weise Propagandaaktivitäten anwendet, um insbesondere die Haltung bestimmter Bevölkerungsteile massiv zu beeinflussen. Und dabei wurde auch nicht vor bewussten Falschdarstellungen zurückgeschreckt. In Deutschland konnten wir im gleichen Zeitraum zwar durchaus auch russische Versuche feststellen, einzelne Wissenschaftler und Journalisten zu beeinflussen. Dies erfolgte jedoch insgesamt nur in geringem Umfang und entfaltete bei uns praktisch keine relevante Außenwirkung.

Das hat sich seit dem Ukraine-Konflikt geändert.

Die Ukraine-Krise war von Anfang an begleitet von intensiven Aktivitäten russischer Medien im Hinblick auf eine Beeinflussung bzw. Desinformation der Öffentlichkeit und verschiedener Adressatengruppen, und das auch sehr bald in Deutschland.

Wichtige Plattformen für pro-russische Medienaktivitäten sind:

- Der regierungsnahe russische Auslandssender „RT“ (Russia Today), der seit September 2014 auch in deutscher Sprache sendet. „RT“ wird von der russischen Regierung finanziert und hat nach eigenen Angaben eine Reichweite von weltweit mehr als 700 Millionen Empfängern.
- Die digitale Medienplattform „Sputnik News“ verbreitet ebenfalls seit November 2014 in deutscher Sprache russlandfreundliche Propaganda. Sie sieht sich nach eigener Darstellung auch selbst als Propagandainstrument der russischen Regierung.
- „Russia Beyond the Headlines“ ist ein von der russischen Regierung finanziertes und seit Januar 2015 auch in Deutsch erscheinendes Online-Portal. Es wird zudem als Beilage europäischer und deutscher Tageszeitungen verbreitet.

Diese Medien sollen in zeitgemäßer und sachlich wirkender Präsentation dazu beitragen, einen Gegenpol in der Öffentlichkeit herzustellen und verbinden dabei geschickt propagandistische Meinungsmache und boulevardorientierte Beiträge. Manche Angebote, so z.B. die Internet-Serie „Der ultimative Mainstreammedien-Guide“ von „RT-Deutschland“, sehen sich als Gegenpol zu den bundesdeutschen Medien und grenzen sich von einer angeblichen „Lügenpresse“ ab.

Ein Vorwurf, der aus der „rechts-populistischen“ Ecke hinlänglich bekannt ist.

Ein weiteres Beispiel für russische Propagandaaktivitäten ist die kremelnahe Biker-Vereinigung „Night-Wolves“. Diese führt eine jährliche sogenannte Siegesfahrt zum Jahrestag des Endes des Zweiten Weltkriegs durch

mehrere europäische Länder nach Berlin durch und dies mit entsprechender pro-russischer medialer Begleitung.

Auch das Tolstoi-Institut kann hier erwähnt werden, ein Verein zur Förderung der deutsch-russischen Freundschaft, der dabei allerdings mit einseitig wie eindeutig pro-russischen Positionen auftritt.

Auch die Nationale Befreiungsbewegung Russlands (NOD) wendet sich als Verein mit Spendenaufrufen zu „humanitärer Hilfe“ für Donbass insbesondere an Russlanddeutsche. Darüber hinaus vertritt er quasi „groß-russische“ Positionen, mit denen er die geschwundene Machtposition nach dem Ende der Sowjetunion revidieren möchte. Mit seinen eurasischen Politikkonzeptionen knüpfen Vertreter dieser russischen Imperialtheorien an Vorstellungen deutscher Rechtsextremisten an, die ebenfalls ein Europa ohne die als „raumfremd“ titulierte USA mit eine Achse Berlin-Moskau anstreben.

Eine andere Form und Möglichkeit der bewussten Manipulation sind teilweise aggressive pro-russische und antiwestliche Positionen in Internetblogs und –foren durch sogenannte “Internet-Trolle“.

Diese Internet-Söldner verfolgen das Ziel, Meinungen im Internet mit Hilfe von bezahlten Kommentaren zu beeinflussen und zu manipulieren. Wir werden in dem anschließenden Vortrag von Herrn Prof. Dr. Grothe mehr dazu hören.

Der „Fall Lisa“ vor einigen Monaten zeigte, dass Maßnahmen zur gezielten Beeinflussung der öffentlichen Wahrnehmung in Deutschland nicht nur auf den Ukraine-Konflikt beschränkt sind.

Russische Medien griffen die angebliche Entführung und Vergewaltigung des russlanddeutschen Mädchens („Lisa“) auf und verwendeten hierbei eine tendenziöse und falsche Berichterstattung.

Eine außenpolitische Dimension erhielt der Vorfall durch wiederholte Äußerungen des russischen Außenministers Lawrov, der deutschen Behörden Vertuschung und Benachteiligung von Russlanddeutschen vorwarf.

Der Eindruck, der damit vermittelt werden soll, ist deutlich: das Leben in Deutschland ist gefährlich geworden, die innere Sicherheit bedroht.

Staatliche Stellen sind nicht mehr in der Lage, die Sicherheit ihrer Bürger zu gewährleisten.

Das Ziel dieser Desinformationen war ebenso offenkundig: die Flüchtlingsdebatte zu Lasten der Flüchtlinge in Deutschland anzuheizen und die deutsche Innenpolitik zu diskreditieren.

Hierzu diente auch die Mobilisierung von in Deutschland lebenden Russlanddeutschen. An mehreren Demonstrationen im Zusammenhang mit

dem „Fall Lisa“ nahmen in Deutschland insgesamt etwa 12.000 Russlanddeutsche an nur einem Wochenende teil. Bei der Mobilisierung spielten soziale Netzwerke (u. a. Whatsapp-Gruppen) ein zentrale Rolle.

Russische staatliche Stellen präsentieren sich auf diese Weise auch als deren Interessenswahrer. Immerhin leben mehr als drei Millionen Russlanddeutsche im Bundesgebiet. Ein Teil dieser Gruppe bezieht seine Nachrichten unter anderem durch in Deutschland empfangbare einseitige und propagandistisch ausgerichtete russische Medien (TV-Sendungen).

Als weiteres Bespiel sei die Berichterstattung über die Ereignisse in der Silvesternacht in Köln genannt, die in den russischen Medien vergleichbar instrumentalisiert wurden. Deutschen Behörden wurde Versagen beim Schutz der eigenen Bevölkerung und deutschen Medien eine manipulative Berichterstattung vorgeworfen.

Wir sehen bei übereinstimmenden Positionen auch ein zumindest punktuelles Zusammenwirken von Rechtsextremisten und Russlanddeutschen. So beteiligten sich wiederholt Russlanddeutsche an Demonstrationen von Rechtsextremisten gegen die weitere Aufnahme von Flüchtlingen. Rechtsextremistische Organisationen, so z. B. die NPD, haben zunehmend prorussische und Pro-Putin Einstellungen übernommen.

Rechtsextremisten aus mehreren europäischen Ländern nahmen im März 2015 in St. Petersburg an der Tagung des russischen „Konservativen Forums Europa“ teil. Als Referent sprach u. a. der NPD-Europaabgeordnete und ehemalige NPD-Vorsitzende Udo Voigt.

Neben einer Vielzahl einzelner Kontakte zeigen solche strategisch ausgerichteten Treffen auch die europäische Dimension russischer Bündnisbestrebungen. Europaweit werden extremistische Gruppierungen gezielt unterstützt.

Aus Sicht Russlands ist Deutschland der wichtigste wirtschaftliche und politische Akteur in Europa und genießt daher hohe Aufmerksamkeit und Interesse. Die erkannten und beschriebenen Aktivitäten zur Desinformation und Beeinflussung stehen eindeutig und im nachhaltigen staatlichen Interesse Russlands. Sie sollen langfristig zu einer unkritischen pro-russischen Öffentlichkeit in Deutschland führen und mittelbar die deutsche Politik im Sinne Russlands beeinflussen.

Im Rahmen der versuchten Einflussnahme auf die deutsche Innenpolitik besteht zumindest abstrakt die Gefahr auch einer innenpolitischen Destabilisierung. Deutlich erkennbar ist in diesem Zusammenhang eine Diskreditierung des pluralistischen demokratischen Systems in Deutschland, das angeblich gescheitert und nicht zukunftsfähig sei.

Gleichzeitig beinhaltet es auch den Versuch, außenpolitische Entscheidungen zu beeinflussen, so beispielsweise die Position Deutschlands zu den Sanktionen der EU gegen die Russische Föderation im Zusammenhang mit dem Ukraine-Konflikt.

Die skizzierten Umstände haben eine eindeutig internationale Dimension. Daher beschlossen die Staats- und Regierungschefs der EU schon im März 2015 einen Aktionsplan gegen antieuropäische Propaganda. Seit September 2015 arbeitet in Brüssel ein Expertenteam – die East StratCom Task Force – daran, russische Propaganda zu erfassen, zu analysieren und mit diesen Ergebnissen zu informieren und aufzuklären.

Die Bundesregierung beteiligt sich selbstverständlich an solchen internationalen Handlungsinitiativen und begegnet auch in Deutschland den beschriebenen Bedrohungen mit verschiedenen Maßnahmen.

Für den Bereich der Nachrichtendienste kann ich aus der Perspektive der Spionageabwehr folgendes sagen:

Auch wenn eine Steuerung der aktuellen Propaganda und Desinformationskampagnen durch russische Nachrichtendienst-Strukturen in Deutschland bislang nicht konkret feststellbar ist, handelt es sich jedoch eindeutig um staatlich aus Moskau gesteuerte Aktivitäten, bei denen die Nachrichtendienste eine nicht unwesentliche Rolle einnehmen. Deshalb ist für uns klar, dass wir uns – gemeinsam mit anderen staatlichen Stellen – um dieses Thema kümmern.

Die vorgenannten Entwicklungstendenzen dürfen allerdings nicht isoliert betrachtet werden. Sie sind aus Sicht des BfV eingebunden in eine Entwicklung, in der die zunehmende Digitalisierung gleichzeitig Angriffswaffe und Angriffsziel darstellt.

Beispielhaft dafür steht der Hackerangriff auf die Internetseiten der Bundeskanzlerin Anfang 2015. Eine pro-russische Hackergruppe „CyberBerkut“ erklärte in einer Selbstbezichtigung, dass man den zeitgleich stattfindenden Besuch des ukrainischen Ministerpräsidenten zu diesem Cyberangriff genutzt habe. Deutschland dürfe dem „kriminellen Regime in Kiew, das einen blutigen Bürgerkrieg entfesselt habe“, keine politische und finanzielle Unterstützung leisten. „CyberBerkut“ war bereits vorher mit verschiedenen politisch motivierten Cyber-Angriffen – u.a. 2014 gegen die NATO – bekannt geworden.

Neben der Webseite der Bundeskanzlerin wurde auch die Homepage des deutschen Bundestags mit einer sog. „DDoS–Attacke“ angegriffen.

Dabei wurden die jeweiligen Server mit einer Vielzahl an Datenanfragen lahmgelegt, so dass deren Angebote vorübergehend nicht genutzt werden konnten.

Bereits kurze Zeit später war der Deutsche Bundestag erneut - und diesmal gravierender - Ziel eines Elektronischen Angriffs. Im Mai 2015 wurde uns bekannt, dass das IT-Netzwerk des Bundestages ausgespäht wurde. Diesmal führte eine „Trojaner"-Schadsoftware zur Infiltrierung von Servern des Bundestages. Über eine stufenweise Aktivierung und Ausbreitung der Schadsoftware wurde ein umfassender Schaden ausgelöst. Ausgangspunkt war offenbar eine zielgerichtete E-Mail, die als Mitteilung der UNO getarnt war.

Dies war kein Angriff von Computerfreaks oder Nerds. Ein Angriff dieser Dimension und Zielrichtung weist auf einen Täter mit erheblichem Know-how und damit verbundenen Ressourcen hin. Die daraufhin geführten Ermittlungen haben daher auch rasch zu der Erkenntnis geführt, dass diese Elektronische Attacke russischen Ursprungs war; es handelt sich um einen Teil der dem BfV seit Jahren bekannten Sofacy-Kampagne. Ziel war zum einen ein nicht unerheblicher Abfluss von Informationen aus den Büros verschiedener Abgeordneter. Zum anderen war es aber auch eine Demonstration der Stärke, verbunden mit dem deutlichen Hinweis auf die Angreifbarkeit unseres Parlaments.

Ein weiterer Cyber-Angriff kurz zuvor im Mai 2015 ging offenkundig ebenfalls von Russland aus: Der französische Fernsehsender „TV5-Monde" wurde elektronisch angegriffen und u.a. über Stunden die Ausstrahlung des TV-Programms unterbrochen. Gleichzeitig wurde die Homepage des Senders mit Propaganda für den sog. „Islamischen Staat/IS" manipuliert. Dies war nach Einschätzung der zuständigen Sicherheitsstellen jedoch offensichtlich Tarnung mit dem Ziel, Angst vor einem in dieser Form nicht existierenden Cyber-Dschihad zu schüren.

Wir werden damit leben müssen, dass Konflikte in der Realwelt auch im Cyberraum stattfinden und die damit verbundenen Möglichkeiten umfassend genutzt werden. Und wir müssen uns verstärkt darauf einstellen, dass ausländische Staaten und deren Nachrichtendienste nicht nur isolierte Angriffe mit nur einer Methodik durchführen. Vielmehr nutzen sie oft im Rahmen einer zentral gesteuerten Gesamtstrategie die Kombination verschiedener Handlungsziele und verschiedener Handlungsoptionen. Dabei geht es längst nicht nur um „schlichte Spionage" mit verschiedenen Mitteln, was für sich allein schon bedrohlich genug wäre. Hinzu kommt zunehmend auch der Aspekt der „Politikgestaltung" mit unredlichen Mitteln und zwar mit dem Ziel der Verunsicherung und Schwächung von Bevölkerung und Staat.

Eine besondere Bedrohung besteht in diesem Zusammenhang für Kritische Infrastrukturen – wesentliche Einrichtungen der Energie- und Wasserversorgung, der Informations- und Telekommunikationstechnik, der

Lebensmittelversorgung und weiterer wichtiger Bereiche, die eine grundlegende Bedeutung für das Funktionieren unseres Gemeinwesens darstellen. Beispiele für die Gefährlichkeit solcher Angriffe gibt es außerhalb Deutschlands genügend. Und ihre Einbeziehung in die Gesamtstrategie verschiedener Angreifer ist ein nicht nur theoretisches Risiko.

Hier sind wir im Rahmen der Cybersicherheitsstrategie der Bundesregierung und des im vergangenen Jahr verabschiedeten IT-Sicherheitsgesetzes auf einem guten Weg, den es gilt weiter voranzuschreiten.

Wir alle – wir als Gesellschaft – müssen uns darauf einstellen, unser Sicherheitsbewusstsein weiter zu stärken und präventive Schutzmöglichkeiten zu ergreifen, um im Schadensfall schnell und angemessen reagieren zu können. Hier besser zu werden, ist wichtige Aufgabe und zugleich ein mühsamer und dauernder Prozess für alle Beteiligten.

Das Bundesamt für Verfassungsschutz wird sich hier maßgeblich beteiligen. Seit Jahren sind wir ein aktiver Dienstleister im Wirtschaftsschutz und Partner von Unternehmen, Verbänden und Institutionen der Wissenschaft. Unser Leitmotiv „Prävention durch Dialog und Information“ steht für ein umfangreiches Angebot zur Sensibilisierung vor den Risiken von Spionage und anderen Gefahren. Die Stärkung der Präventionstätigkeit ist unser erklärtes Ziel.

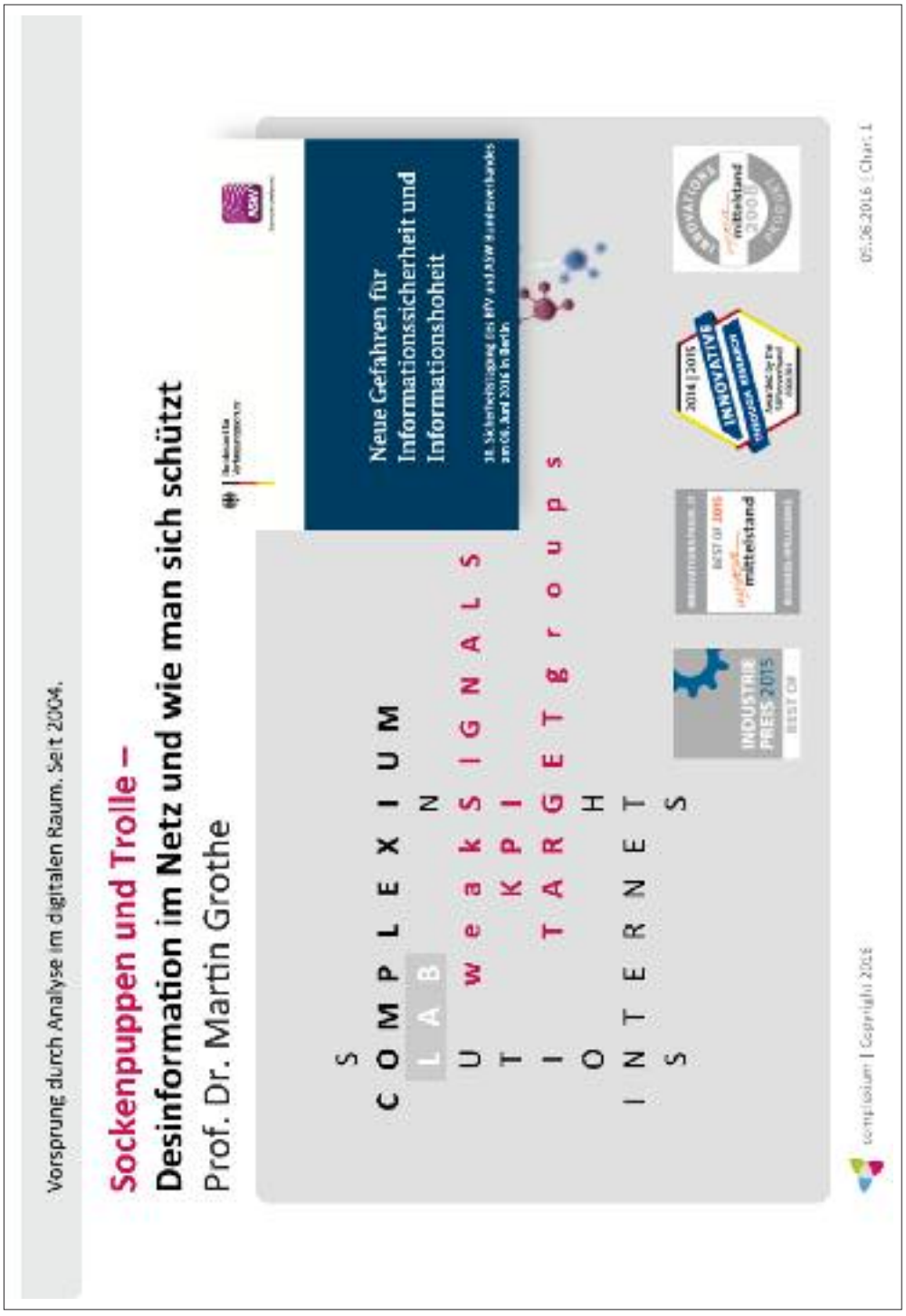
In diesem Kontext möchte ich auf unser Engagement im Rahmen der gemeinsamen „Initiative Wirtschaftsschutz“ hinweisen. Das im April gestartete Informationsportal Wirtschaftsschutz ist zentrale Wissensbasis zum Wirtschaftsschutz und zugleich eine gute Möglichkeit, uns zu testen, aber auch um selbst mitzuwirken. Sie erreichen es im Internet unter www.wirtschaftsschutz.info. Für registrierte Teilnehmer gibt es einen Mehrwert an Informationen und Angeboten u. a. in Form spezialisierter Informationsangebote sowie verschiedene Dialog- und Veranstaltungsformate. Die Plattform von BfV, BND, BKA und BSI ist auf Kooperation angelegt.

Auch hier wird deutlich, dass es Sicherheit nicht als umfassendes Gratisangebot der Sicherheitsbehörden gibt. Sicherheit gibt es nur, wenn alle mitmachen, wenn alle ihr Verantwortung annehmen und handeln: der Staat, die Wirtschaft und jeder einzelne. Auch in Zeiten von Globalisierung und Digitalisierung gilt:

Wirtschaftsschutz ist Teamwork!

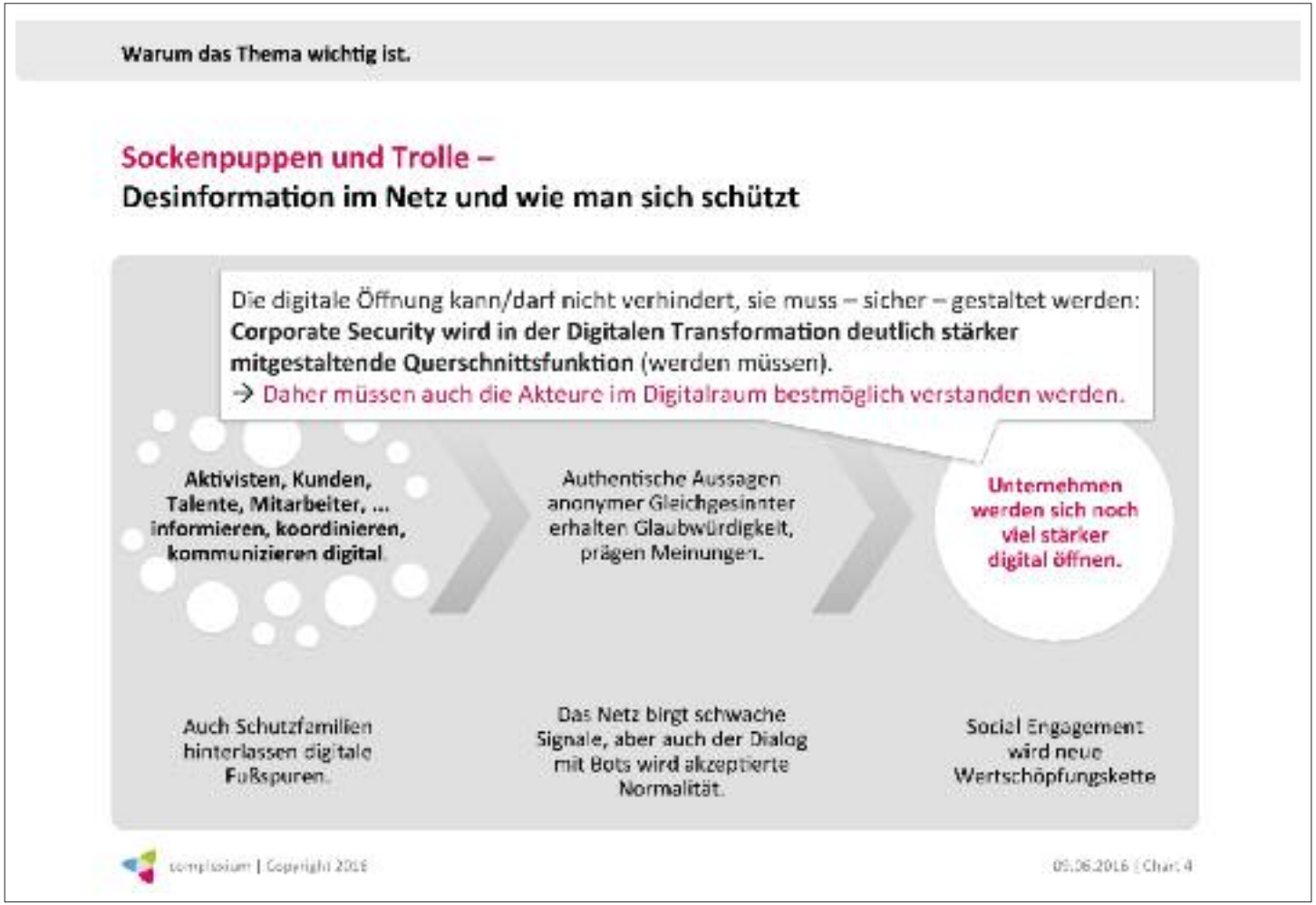
Von Sockenpuppen und Trollen – Desinformation im Netz und wie man sich schützt

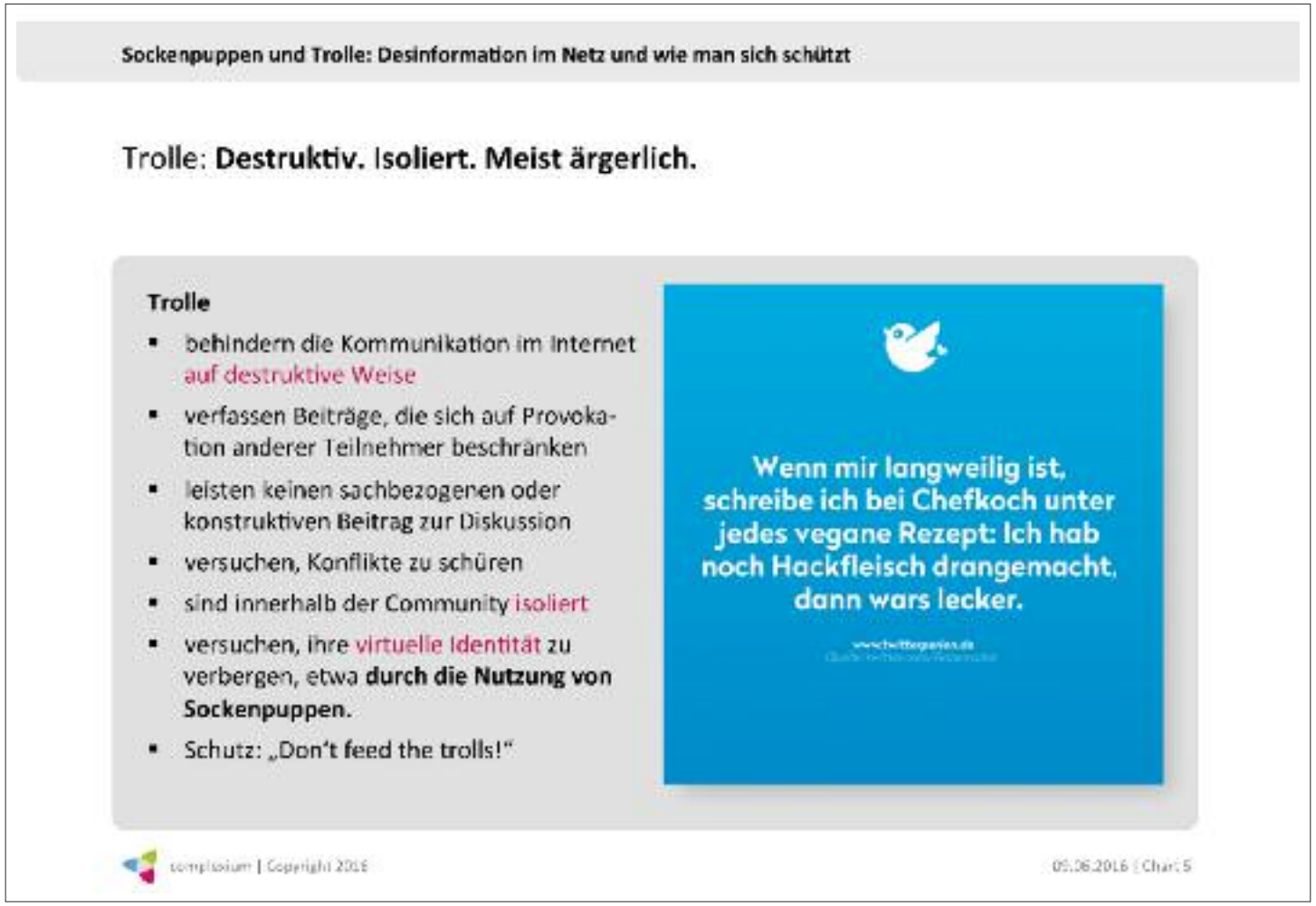
Prof. Dr. Martin Grothe, complexium




Prof. Dr. Martin Grothe. complexium: Vorsprung durch Analyse im digitalen Raum. Seit 2004.
"Discovery consists in seeing what everyone else has seen and thinking what no one else has thought."
Albert Szent-Gyorgyi (ungarischer Biochemiker, 1937 Nobelpreis Medizin, 1893-1986)
complexium
UNTERNEHMENSBERATUNG
Arbeitsfelder
Corporate Security
• Partner des ASW Bundesverbandes Allianz für Sicherheit in der Wirtschaft e.V.
• Klientenbranchen: Bank, Energie, FMCG, Pharma, Versicherung
Employer Intelligence, z.B.
• E.ON: Zielgruppen Hotspots und Themen
• BIG4: Reports/Alerts → Talente erreichen
• UniCredit: Mitarbeiter für Call Center finden
Market Intelligence, z.B.
• Greenpeace: GALAXY nach Sinus-Milieus
• Lufthansa/Eurowings: Reporting, Krise
• Oracle: Lead Generation
• vfa, Pharma-Konzerne: Indikationen, Transparenz, Kovigilanz
complexium GmbH, Berlin, gegründet 2004
Gründer & CEO: Prof. Dr. Martin Grothe
Ein Entwicklerteam (Computerlinguisten), ein Analyseteam.
Zahlreiche Publikationen und Vorträge:
Digitalisierung, Digitale Transformation, Disruption, Controlling, Business Intelligence, Social Media Analyse, Früherkennung von Risiken/Bedrohungen ...
Lehr- und Verbandsfunktionen
• Vorstandsvorsitz @ Bundesverband Wettbewerbs- & Marktanalyse dcif e.V.
• Faculty @ Institute for Competitive Intelligence ICI
• Beirat @ Bundesverband Employer Branding, Personalmarketing & Recruitng QUEB e.V.
• Jury @ trendence Awards und Personalmarketing Innovator PMI
• Honorarprofessor @ Universität der Künste Berlin: Leadership in digitaler Kommunikation
Universität der Künste Berlin
Leadership in Digitaler Kommunikation
complexium | Copyright 2016
05.06.2016 | Chart 2


complexium: Analyseprozess: Algorithmen (Scope, Speed) und Analysten (Qualität)
complexium nimmt öffentliche digitale Beiträge zeitnah auf.
Algorithmen entdecken Auffälligkeiten und definierte Begriffe. Auch rückwärts.
Analysten fügen Ergebnisse zusammen, bewerten Issues und stellen Ableitungen dar.
Wir unterstützen unsere Klienten mit Früherkennung und Inhaltserschließung.
Analyseprozess:
Klienten-Branchen:
• Bank
• Energie
• FMCG
• Pharma
• Versicherung
MATRIX
Identification & Extraction:
Hot topics & issues
GALAXY
Realtime-Listening & Exploration:
Weak Signals
Lagebild
Reports, System, Dialog!
Sie kennen die Lage früher besser einschätzen und reduzieren Überraschungen.
Iteratives Finden
1 Data Collection:
2 Processing:
3 Analysis:
4 Presentation & Results:
Reports, alerts
complexium | Copyright 2016
05.06.2016 | Chart 3


Warum das Thema wichtig ist.
Sockenpuppen und Trolle –
Desinformation im Netz und wie man sich schützt
Die digitale Öffnung kann/darf nicht verhindert, sie muss – sicher – gestaltet werden:
Corporate Security wird in der Digitalen Transformation deutlich stärker mitgestaltende Querschnittsfunktion (werden müssen).
→ Daher müssen auch die Akteure im Digitalraum bestmöglich verstanden werden.
Aktivisten, Kunden, Talente, Mitarbeiter, ... informieren, koordinieren, kommunizieren digital.
Authentische Aussagen anonymer Gleichgesinnter erhalten Glaubwürdigkeit, prägen Meinungen.
Unternehmen werden sich noch viel stärker digital öffnen.
Auch Schutzfamilien hinterlassen digitale Fußspuren.
Das Netz birgt schwache Signale, aber auch der Dialog mit Bots wird akzeptierte Normalität.
Social Engagement wird neue Wertschöpfungskette
complexium | Copyright 2016
05.06.2016 | Chart 4


Sockenpuppen und Trolle: Desinformation im Netz und wie man sich schützt
Trolle: Destruktiv. Isoliert. Meist ärgerlich.
Trolle
behindern die Kommunikation im Internet auf destruktive Weise
verfassen Beiträge, die sich auf Provokation anderer Teilnehmer beschränken
leisten keinen sachbezogenen oder konstruktiven Beitrag zur Diskussion
versuchen, Konflikte zu schüren
sind innerhalb der Community isoliert
versuchen, ihre virtuelle Identität zu verbergen, etwa durch die Nutzung von Sockenpuppen.
Schutz: „Don't feed the trolls!"
Wenn mir langweilig ist, schreibe ich bei Chefkoch unter jedes vegane Rezept: Ich hab noch Hackfleisch drangemacht, dann wars lecker.
complexium | Copyright 2016
05.06.2016 | Chart 5

Sockenpuppen: **Vielschichtig. Mitunter unauffällig und gefährlich.**

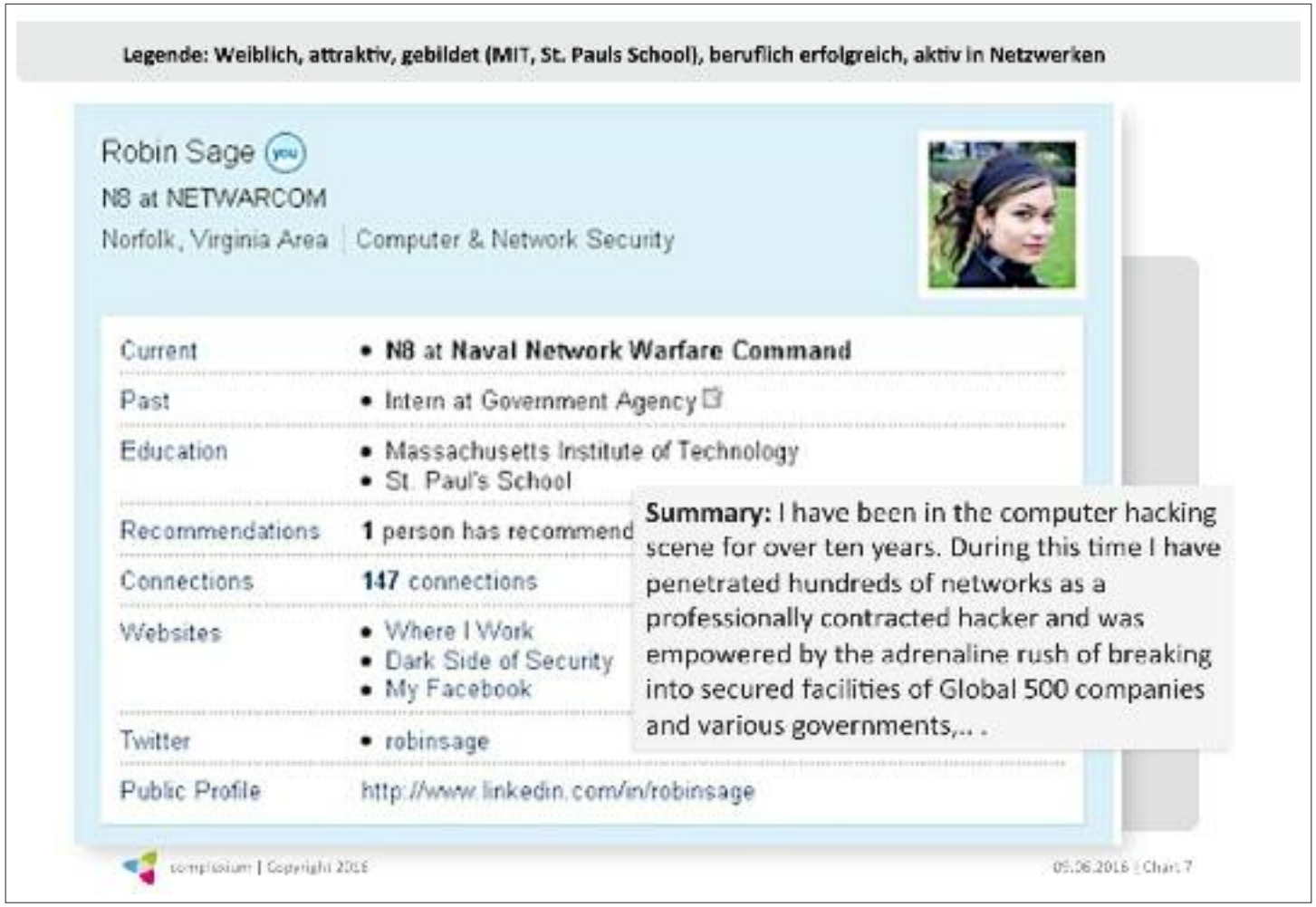
Sockenpuppen

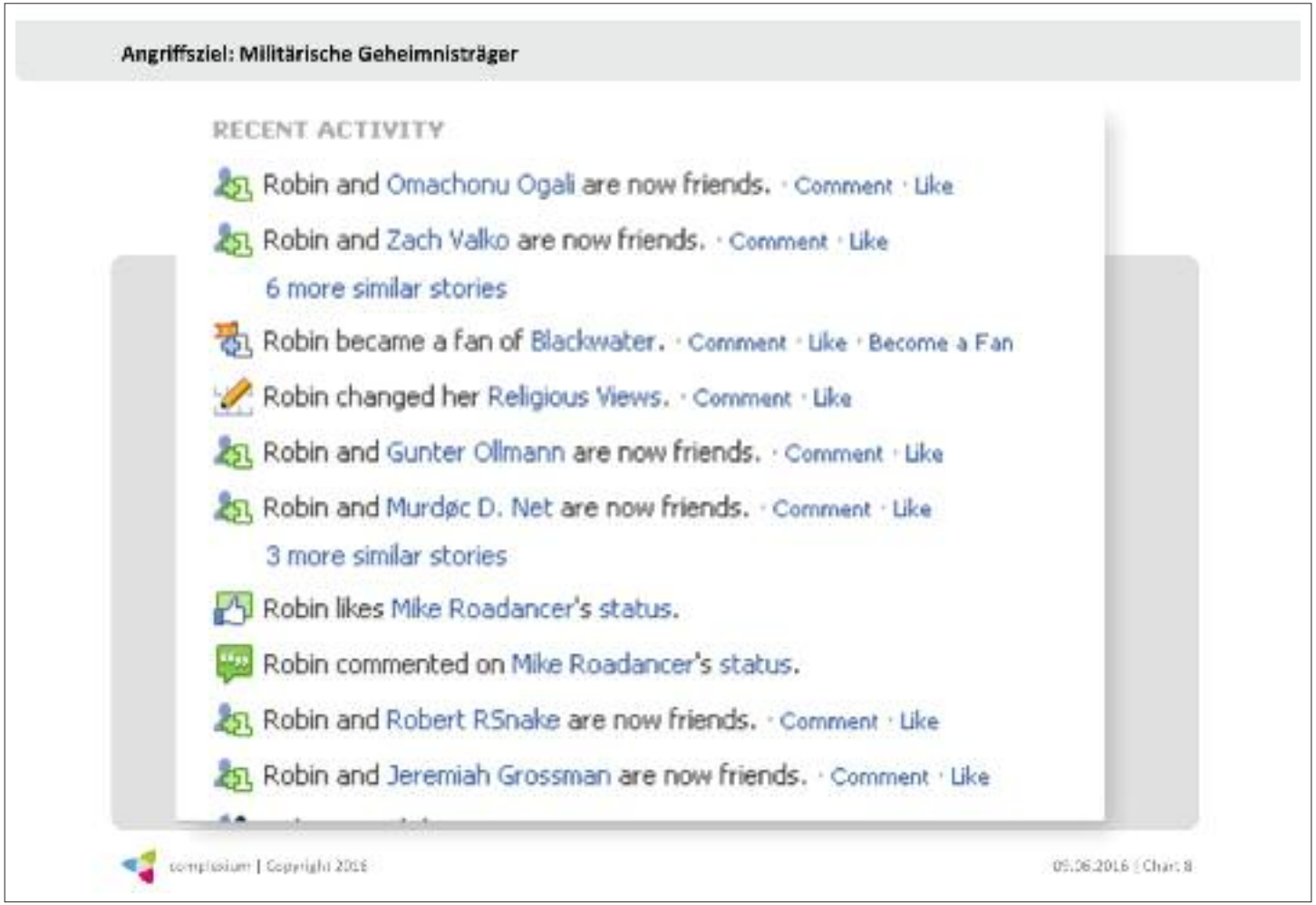
Ein zusätzliches Benutzerkonto, ...

- um etwa die eigene Privatsphäre zu schützen,
- um die Regeln einer Community zu unterlaufen,
- um andere Benutzer oder deren Argumente zu diskreditieren,
- um Meinungen oder Vorschläge mit mehreren „Stimmen" zu verstärken,
- um ganz allgemein illegitime Zwecke zu verfolgen.

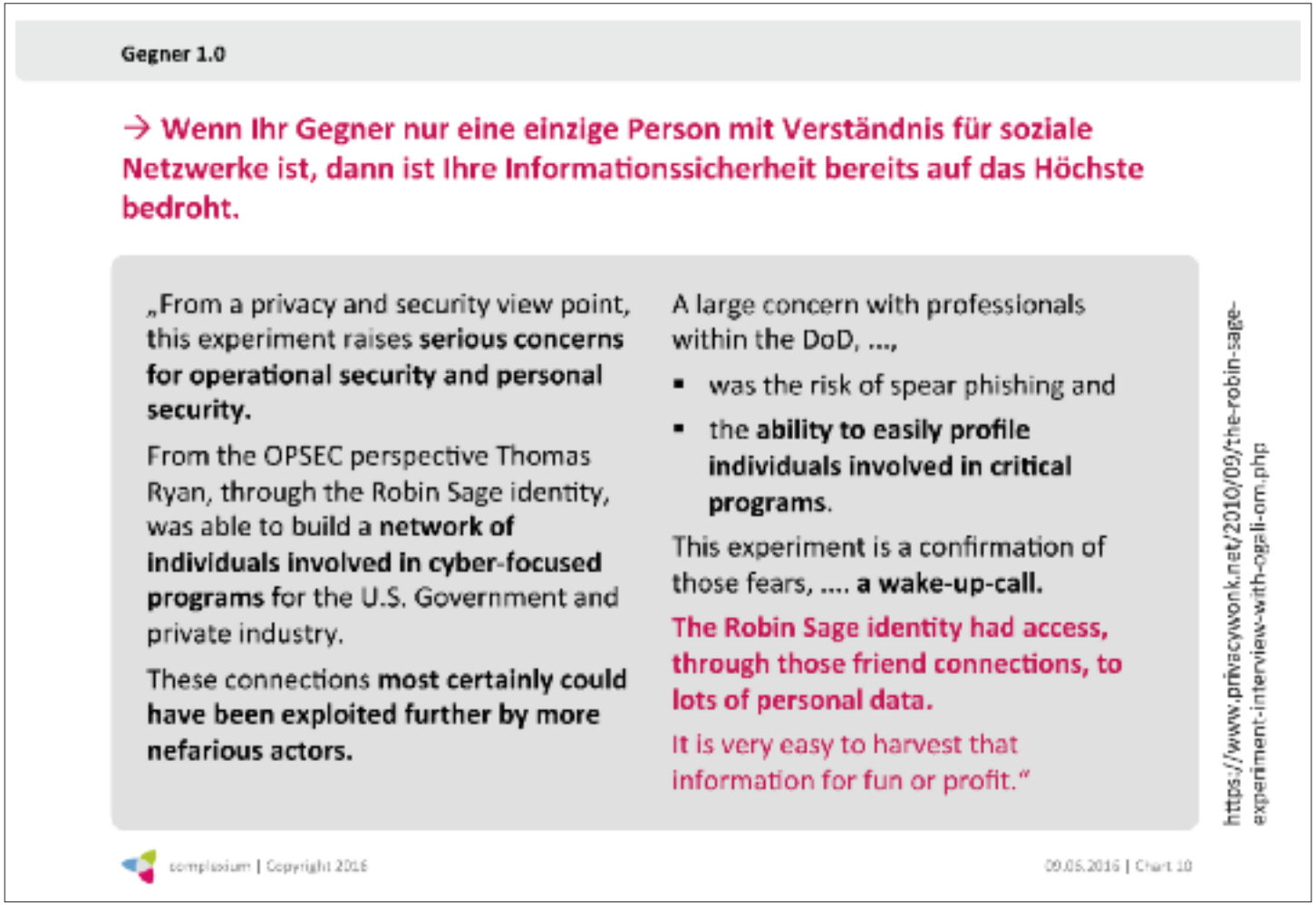
z.B. **Robin Sage**

Legende: Weiblich, attraktiv, gebildet (MIT, St. Pauls School), beruflich erfolgreich, aktiv in Netzwerken




Angriffsziel: Militärische Geheimnisträger
RECENT ACTIVITY
Robin and Omachonu Ogali are now friends. · Comment · Like
Robin and Zach Valko are now friends. · Comment · Like
6 more similar stories
Robin became a fan of Blackwater. · Comment · Like · Become a Fan
Robin changed her Religious Views. · Comment · Like
Robin and Gunter Ollmann are now friends. · Comment · Like
Robin and Murdøc D. Net are now friends. · Comment · Like
3 more similar stories
Robin likes Mike Roadancer's status.
Robin commented on Mike Roadancer's status.
Robin and Robert RSnake are now friends. · Comment · Like
Robin and Jeremiah Grossman are now friends. · Comment · Like
complosium | Copyright 2016
05.06.2016 | Chart 8


Erfolgreich trotz Widersprüche.
Eine Kunstfigur wird zur Falle für Geheimnisträger.
Ergebnis des Experiments:
✓ Angebote von Headhuntern
✓ Freundschaftsanfragen von MIT- und St. Pauls-Absolventen
✓ Über 300 Kontakte zu hochrangigen Mitarbeitern in Militär, Rüstung, Diensten
✓ Erhielt militärische Geheim-dokumente zu Einsätzen in Afghanistan
✓ ... sowie zahlreiche Einladungen zum Essen.
robinsage
@johntiessen I'm not a reporter, it was an experiment! Didn't matter if I was busted....still got your info :)
@boerror funny they detained you about #wikileaks http://tinyurl.com/ajOntp I saw a photo of you with a FED and a signed CI doc at #DEFCON
complexium | Copyright 2016
05.06.2016 | Chart 9



Gegner 1.0

→ Wenn Ihr Gegner nur eine einzige Person mit Verständnis für soziale Netzwerke ist, dann ist Ihre Informationssicherheit bereits auf das Höchste bedroht.

„From a privacy and security view point, this experiment raises **serious concerns for operational security and personal security.**

From the OPSEC perspective Thomas Ryan, through the Robin Sage identity, was able to build a **network of individuals involved in cyber-focused programs** for the U.S. Government and private industry.

These connections **most certainly could have been exploited further by more nefarious actors.**

A large concern with professionals within the DoD, ...,

- was the risk of spear phishing and
- the **ability to easily profile individuals involved in critical programs**.

This experiment is a confirmation of those fears, ... **a wake-up-call.**

The Robin Sage identity had access, through those friend connections, to lots of personal data.

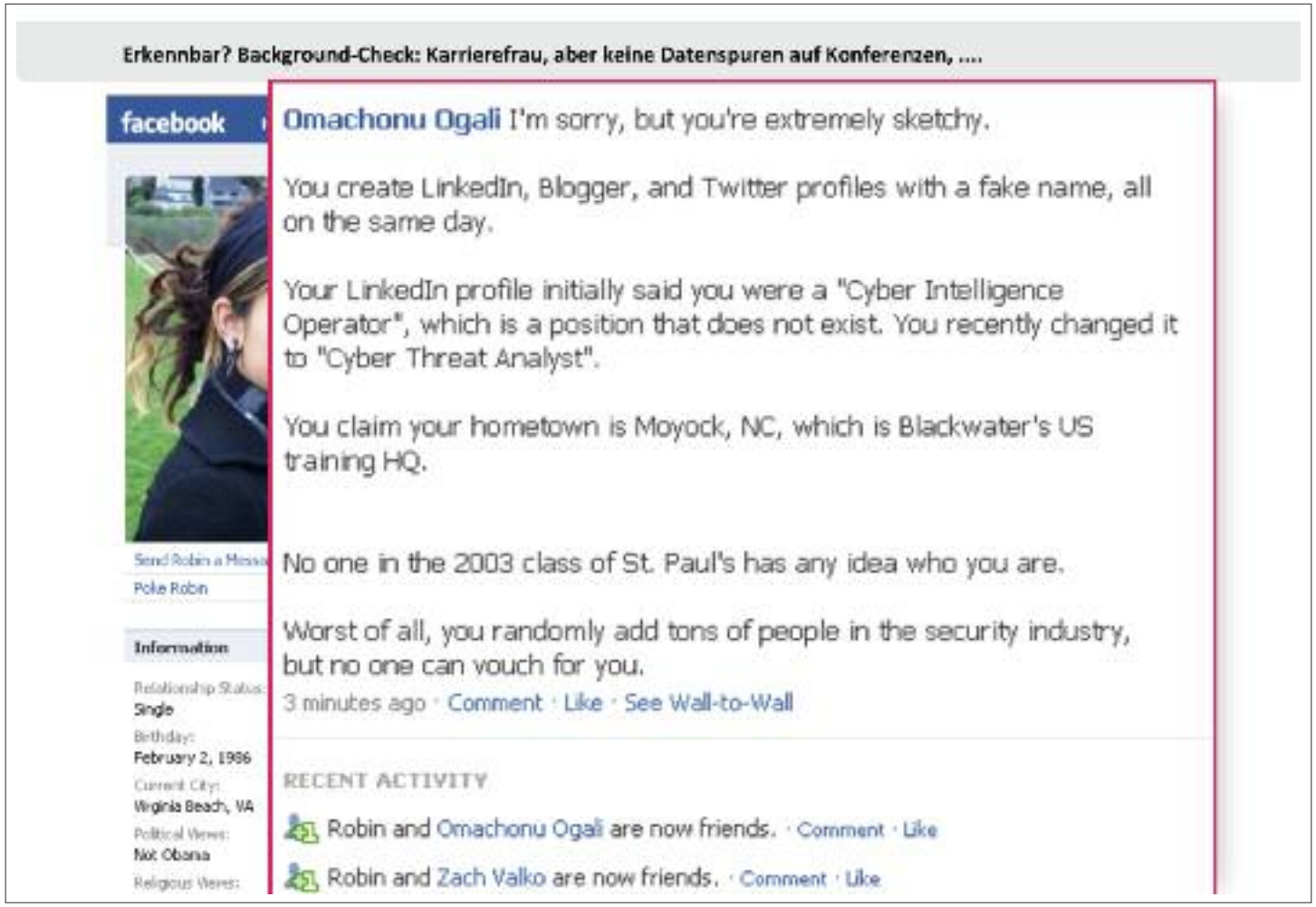
It is very easy to harvest that information for fun or profit."

https://www.privacyworknet/2010/09/the-robin-sage-experiment-interview-with-ogali-orn.php

complexium | Copyright 2016

09.05.2016 | Chart 10

Erkennbar? Background-Check: Karrierefrau, aber keine Datenspuren auf Konferenzen, ...



Sockenpuppen: Gefährlich.

Jeder vorschnelle Connect stärkt die Legende, verschafft der Sockenpuppe positive Netzeffekte.
Schon einfache Checks reduzieren das Risiko.

„Examine profiles prior to accepting connection requests:

- Careful reviews of small details such as pictures, work experience, and credentials may provide just enough insight to refrain from linking to harmful individuals.
- Take the extra time to consult mutual friends or quickly perform your own research (...).
- More often than not, false identities, just like Robin Sage, intentionally and unintentionally, leave simple clues for you along the way."

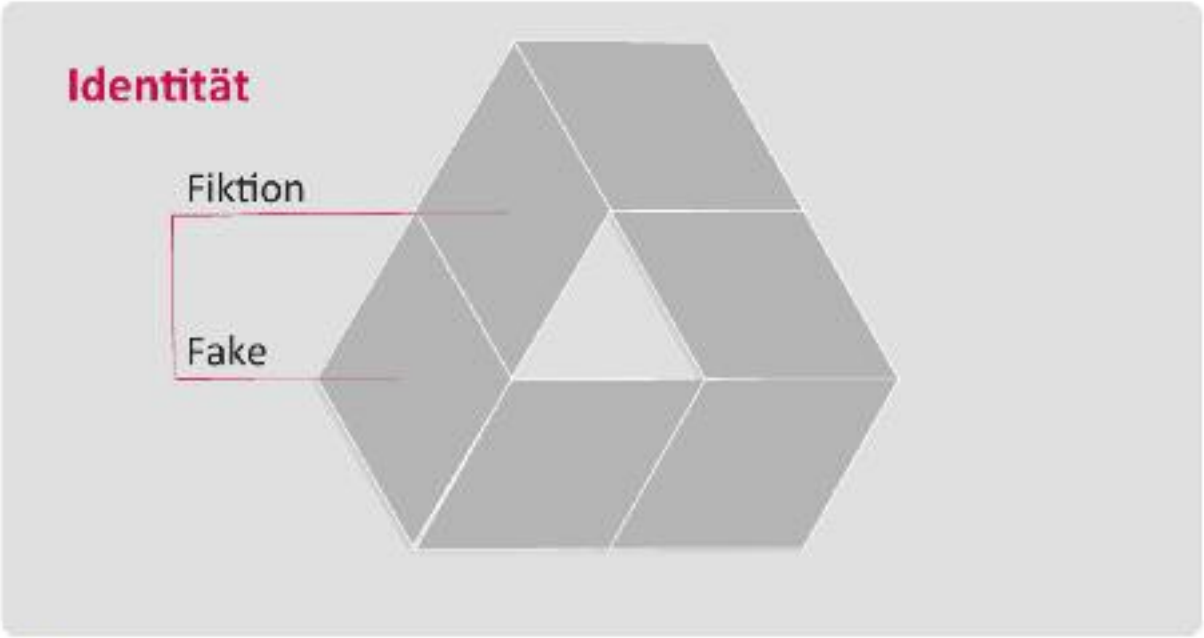
Getting-In-Bed-With-Robin-Sage
Ein Experiment von Thomas Ryan

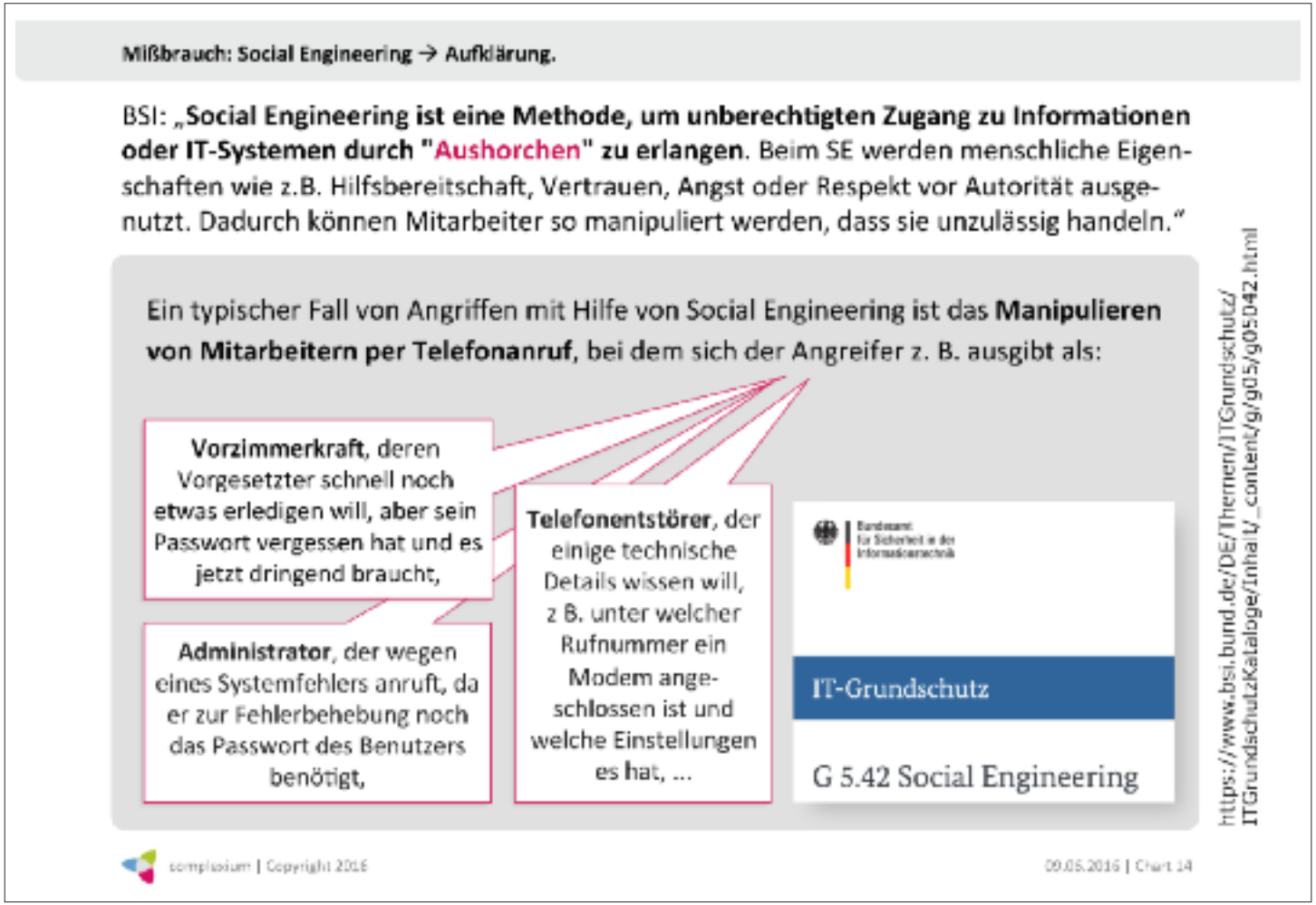
https://www.privacywonk.net/download/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf

Desinformation im Netz

Digitale Akteure können sich fiktiver oder falscher Identitäten bedienen.

- **Identitätsdesign** (z.B. Robin Sage) oder
- **Identitätsdiebstahl** (temporäre Übernahme von digitalen Profilen).




Mißbrauch: Social Engineering → Aufklärung.
BSI: „Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch "Aushorchen" zu erlangen. Beim SE werden menschliche Eigenschaften wie z.B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln."
Ein typischer Fall von Angriffen mit Hilfe von Social Engineering ist das Manipulieren von Mitarbeitern per Telefonanruf, bei dem sich der Angreifer z. B. ausgibt als:
Vorzimmerkraft, deren Vorgesetzter schnell noch etwas erledigen will, aber sein Passwort vergessen hat und es jetzt dringend braucht,
Administrator, der wegen eines Systemfehlers anruft, da er zur Fehlerbehebung noch das Passwort des Benutzers benötigt,
Telefonentstörer, der einige technische Details wissen will, z B. unter welcher Rufnummer ein Modem angeschlossen ist und welche Einstellungen es hat, ...
IT-Grundschutz
G 5.42 Social Engineering
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05042.html
complexium | Copyright 2016
09.05.2016 | Chart 14

Social Engineering → Aufklärung 2.

Zur Sensibilisierung von Mitarbeitern ...

Who am I - Kein System ist sicher

Elyas M'Barek (Darsteller), Tom Schilling (Darsteller), Baran Odar (Regisseur)

Altersseinstufung: Freigegeben ab 12 Jahren

4.5 von 5 Sternen

5 Sterne	258
4 Sterne	50
3 Sterne	15
2 Sterne	11
1 Stern	15

Alle 349 Rezensionen anzeigen ›

Social Engineering, Personenschutz → Aufklärung 3. Sichtbarkeitsanalyse/VIP-Security Profile

Sensibilisierung von Führungskräften.
Was finden Dritte zu Schutzpersonen/-familien im Netz?

Sichtbarkeitsanalyse/VIP Security-Profile
mit Rekonstruktion von

WER: Familie

WAS: Aktivitäten, Routinen, Vermögen, Vorwürfe

WO: Arbeits-/Schulwege, Lokationen, Wohnen/Aufenthaltsorte

WANN: Termine

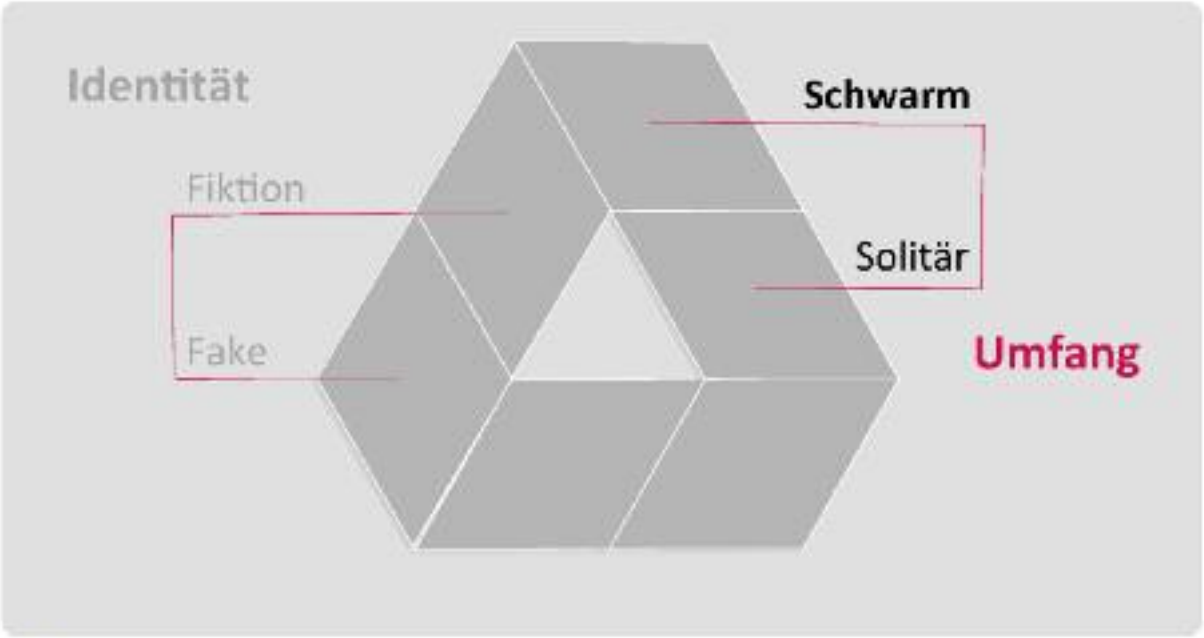
Jeweils Einschätzung der Kritikalität.

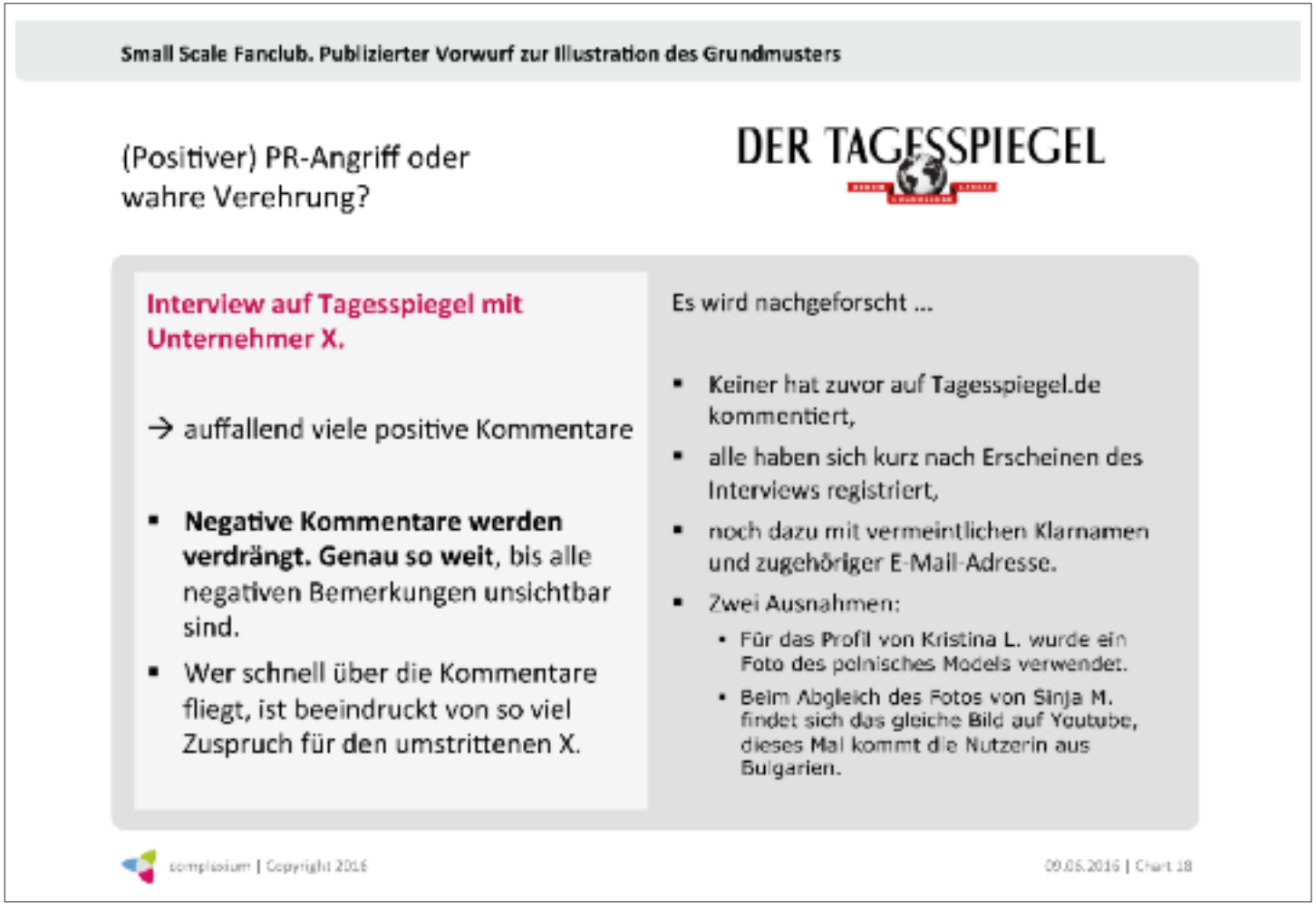
Strukturierter Sicherheitsbericht:
üblicherweise 30-40 Seiten

Beispiel complexium

Desinformation im Netz

Solitäre zielen auf – ggf. mehrere – einzelne Zielpersonen.
Schwärme zielen über Meinungs(trug)bilder auf die jeweilige Öffentlichkeit.
Ausprägungen: Smale Scale Fanclubs → … → Large Scale Troll-Army




Small Scale Fanclub. Publizierter Vorwurf zur Illustration des Grundmusters
(Positiver) PR-Angriff oder wahre Verehrung?
DER TAGESSPIEGEL
Interview auf Tagesspiegel mit Unternehmer X.
→ auffallend viele positive Kommentare
Negative Kommentare werden verdrängt. Genau so weit, bis alle negativen Bemerkungen unsichtbar sind.
Wer schnell über die Kommentare fliegt, ist beeindruckt von so viel Zuspruch für den umstrittenen X.
Es wird nachgeforscht …
Keiner hat zuvor auf Tagesspiegel.de kommentiert,
alle haben sich kurz nach Erscheinen des Interviews registriert,
noch dazu mit vermeintlichen Klarnamen und zugehöriger E-Mail-Adresse.
Zwei Ausnahmen:
Für das Profil von Kristina L. wurde ein Foto des polnisches Models verwendet.
Beim Abgleich des Fotos von Sinja M. findet sich das gleiche Bild auf Youtube, dieses Mal kommt die Nutzerin aus Bulgarien.
complexium | Copyright 2016
09.05.2016 | Chart 18

Small Scale Fanclub.

Unternehmer X: Verdächtige Claqueure im Kommentarbereich

NETZPOLITIK.ORG

Über 30 Mitglieder zählt der Fanclub, der neben dem **Unternehmer** auch seine prominente **Ehefrau** und einen befreundeten **Sportler** begleitet.

Nachzulesen sind ihre Beiträge in den Kommentarspalten zahlreicher Medien wie *Bild.de, Welt.de, Focus.de, Sport1.de, Blick.ch, Gründerszene.de, Finanzen.net, DasInvestment.com und MyHelmat.de.*

Nach Veröffentlichung des kritischen Tagesspiegel-Artikels sind fast alle Facebook-Profile nicht mehr erreichbar.

Sockenpuppen aus dem Fanclub

- Facebook-Profile inaktiv
- Profilbilder von bulgarischen Models
- Namenssuche Google: keine passenden Treffer

- Nützliches Tool : z.B. Namecheckr.com

Large Scale Troll-Army: Info Warfare. Publizierter Vorwurf zur Illustration des Grundmusters

In vielen Quellen wird eine staatlich geführte „**digitale Infanterie**" beschrieben.
In den Vorwürfen werden Meinungsziele wie Finnland und die Ukraine genannt.

„How Putin Secretly Conquered Russia's Social Media Over the Past 3 Years"
Posted 30 January 2015

„It seems like a joke, but **thousands of hired bloggers** "go to work" every day, writing online about Vladimir Putin's greatness and the decay of the West.
They're on Facebook, Twitter, news sites, and anywhere else the Kremlin feels threatened and outnumbered."

Vladimir Putin at a press conference on December 18, 2014. Kremlin press service, public domain.

„ ... Combined, these efforts field **a troll army of thousands**. In some areas, like on the outskirts of St. Petersburg, the enterprise is so big that there are whole office buildings for these people."

https://globalvoices.org/2015/01/30/how-putin-secretly-conquered-russias-social-media-over-the-past-3-years/

Gegner 2.0

Wenn Ihr Gegner eine Gruppe von Akteuren (Sockenpuppen) steuert, dann kann ein Meinungsbild/-umfeld wirksam beeinflusst werden.

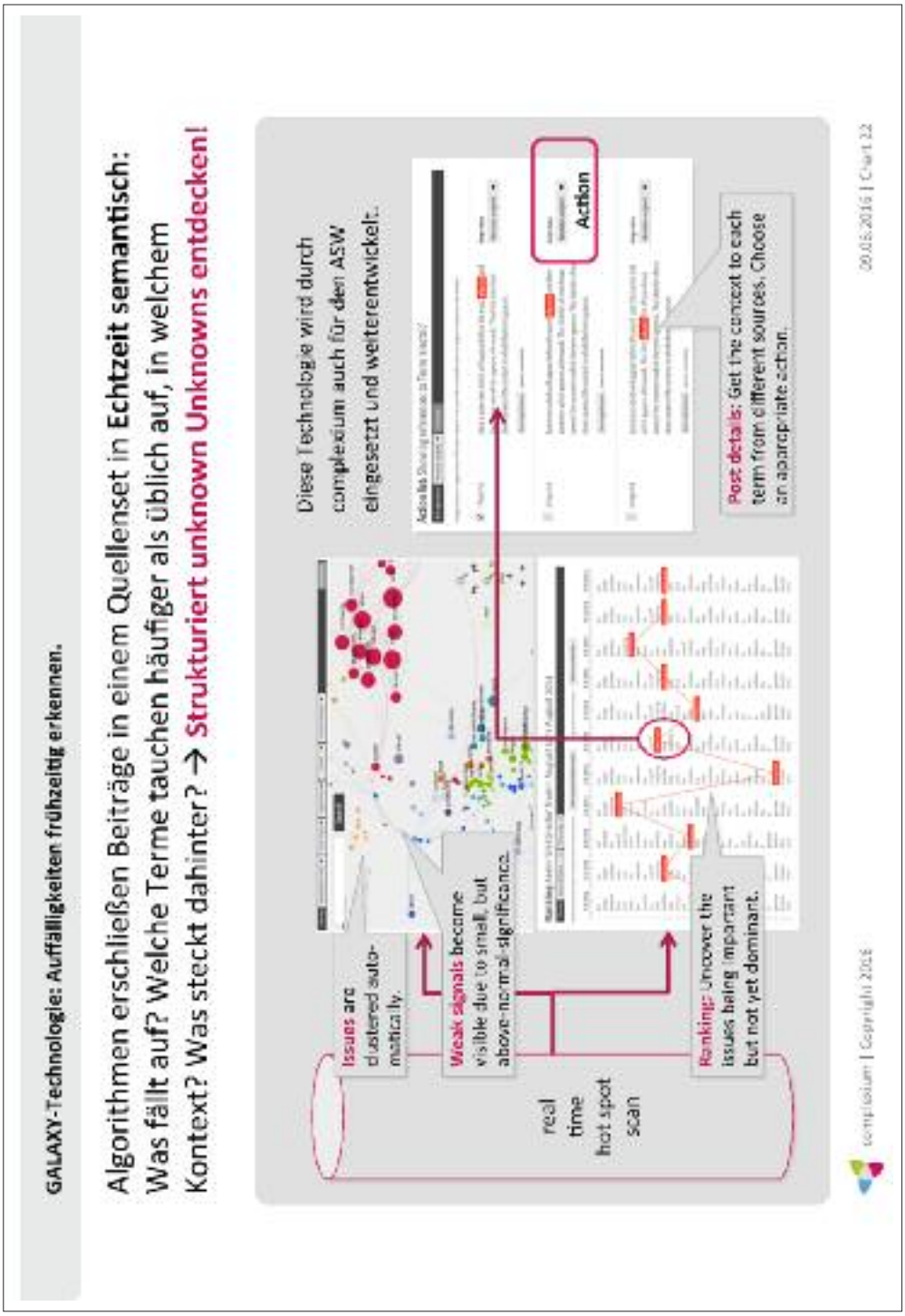
Dies kann

- die **Reputation** des Unternehmens und seiner Vertreter belasten,
- **Geschäftspartner** irritieren,
- potenzielle **Kunden** abschrecken,
- geeignete **Talente** ablenken,
- **Wettbewerbern** einen Vorteil verschaffen,
- persönlichen **Stress** aufbauen.

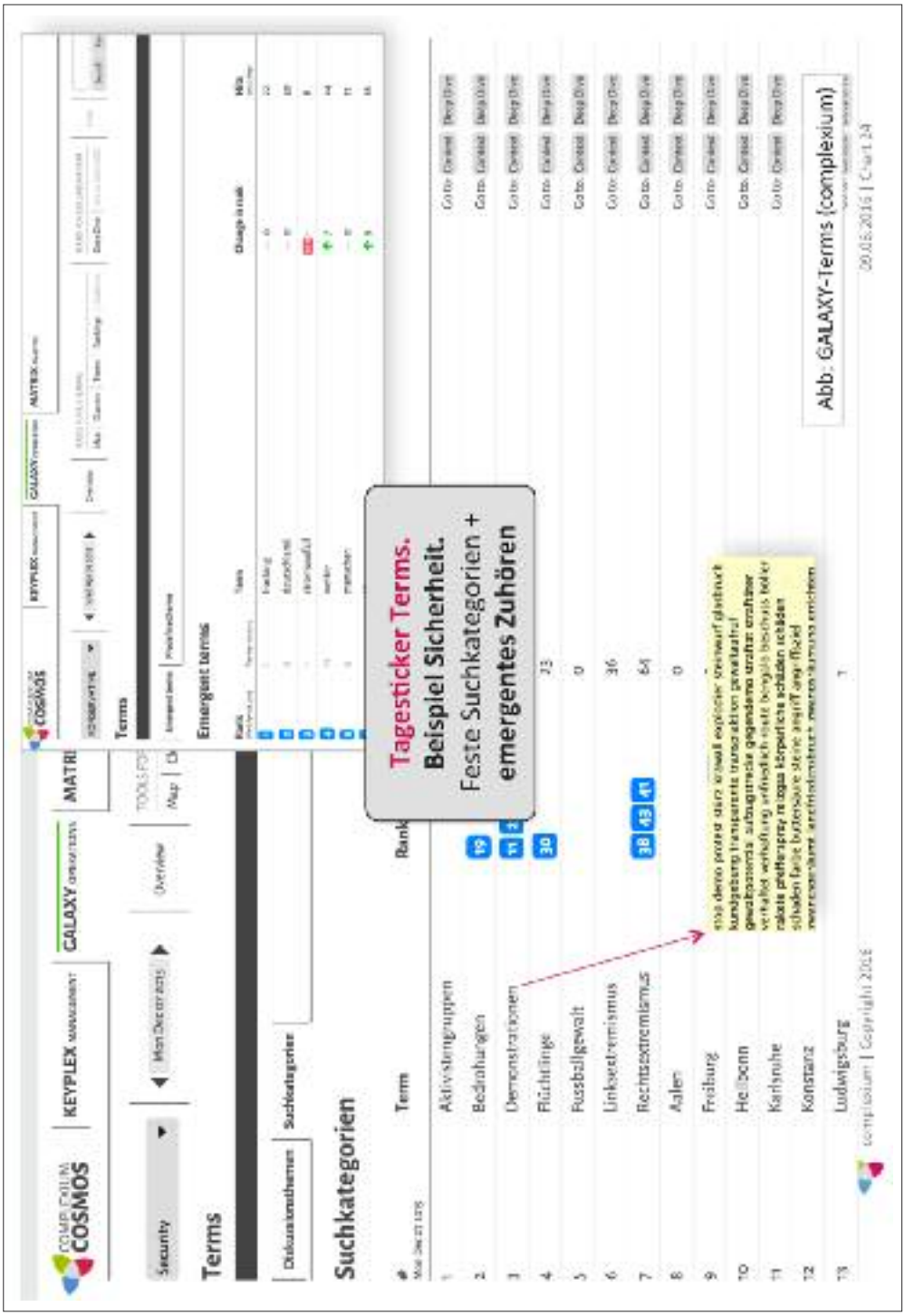
Es können damit alle vier **Strategie-Perspektiven** der Corporate Balanced Scorecrd (zugleich) angegriffen werden.

Empfehlung: Früherkennung durch Social Listening

Abb: GALAXY-Ranking (complexium)


GALAXY-Technologie: Auffälligkeiten frühzeitig erkennen.
Algorithmen erschließen Beiträge in einem Quellenset in Echtzeit semantisch:
Was fällt auf? Welche Terme tauchen häufiger als üblich auf, in welchem Kontext? Was steckt dahinter? → Strukturiert unknown Unknowns entdecken!
Diese Technologie wird durch complexium auch für den ASW eingesetzt und weiterentwickelt.
Issues are clustered automatically.
Weak signals become visible due to small, but above-normal significance.
Ranking: Uncover the issues being important but not yet dominant.
real time hot spot scan
Action
Post details: Get the context to each term from different sources. Choose an appropriate action.
complexium | Copyright 2016
20.06.2016 | Chart 22


Rankings
Emergente Themen – ohne Vorgabe
Auf-/Absteiger.
Beispiel Sicherheit.
Erkannte Diskussions-
themen im Ranking.
Abb: GALAXY-Ranking (complexium)
complexium | Copyright 2016
20.02.2016 | Chart 13


COSMOS
KEYPLEX
GALAXY
Terms
Suchkategorien
Tagesticker Terms.
Beispiel Sicherheit.
Feste Suchkategorien +
emergentes Zuhören
Abb. GALAXY-Terms (complexium)

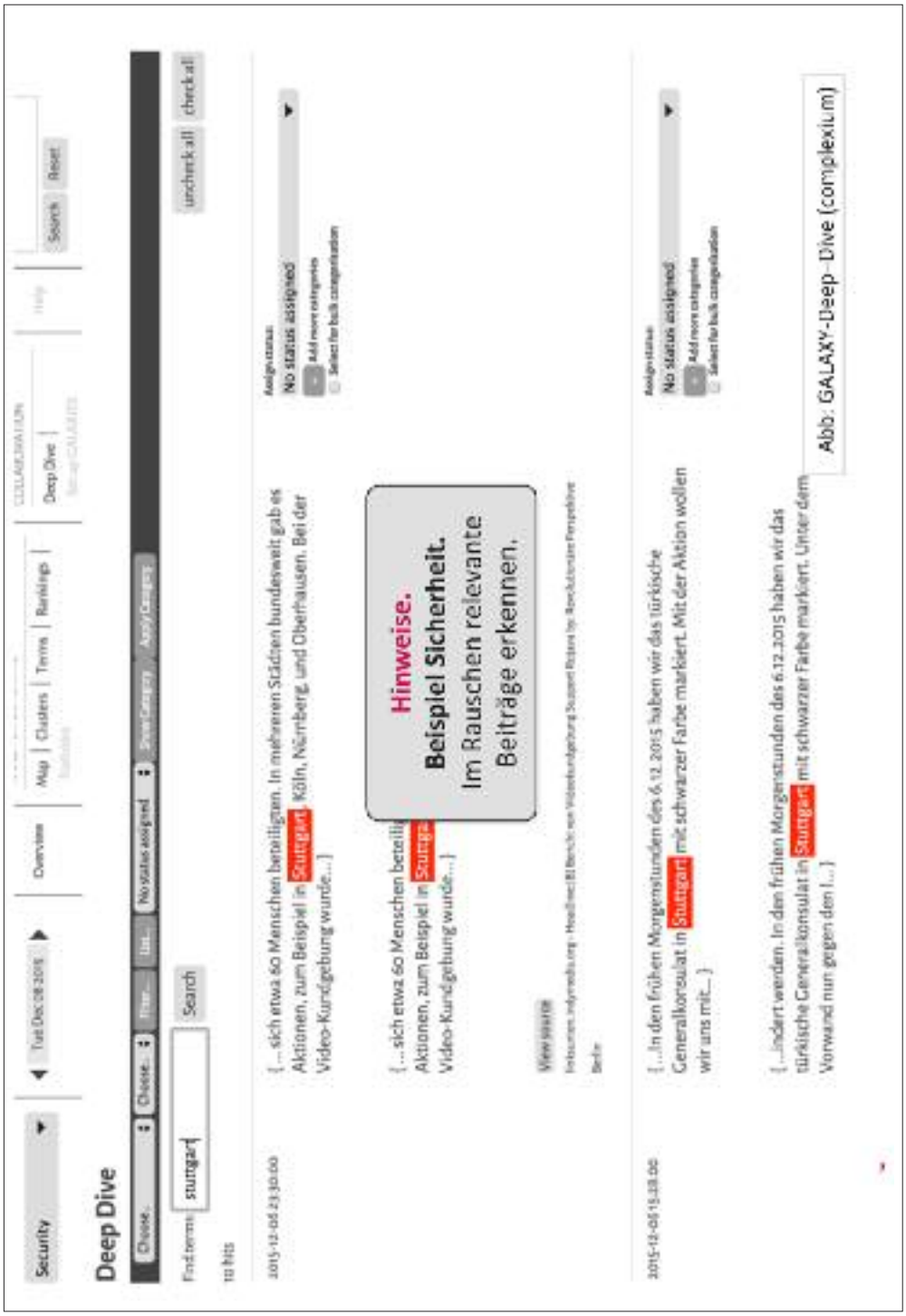
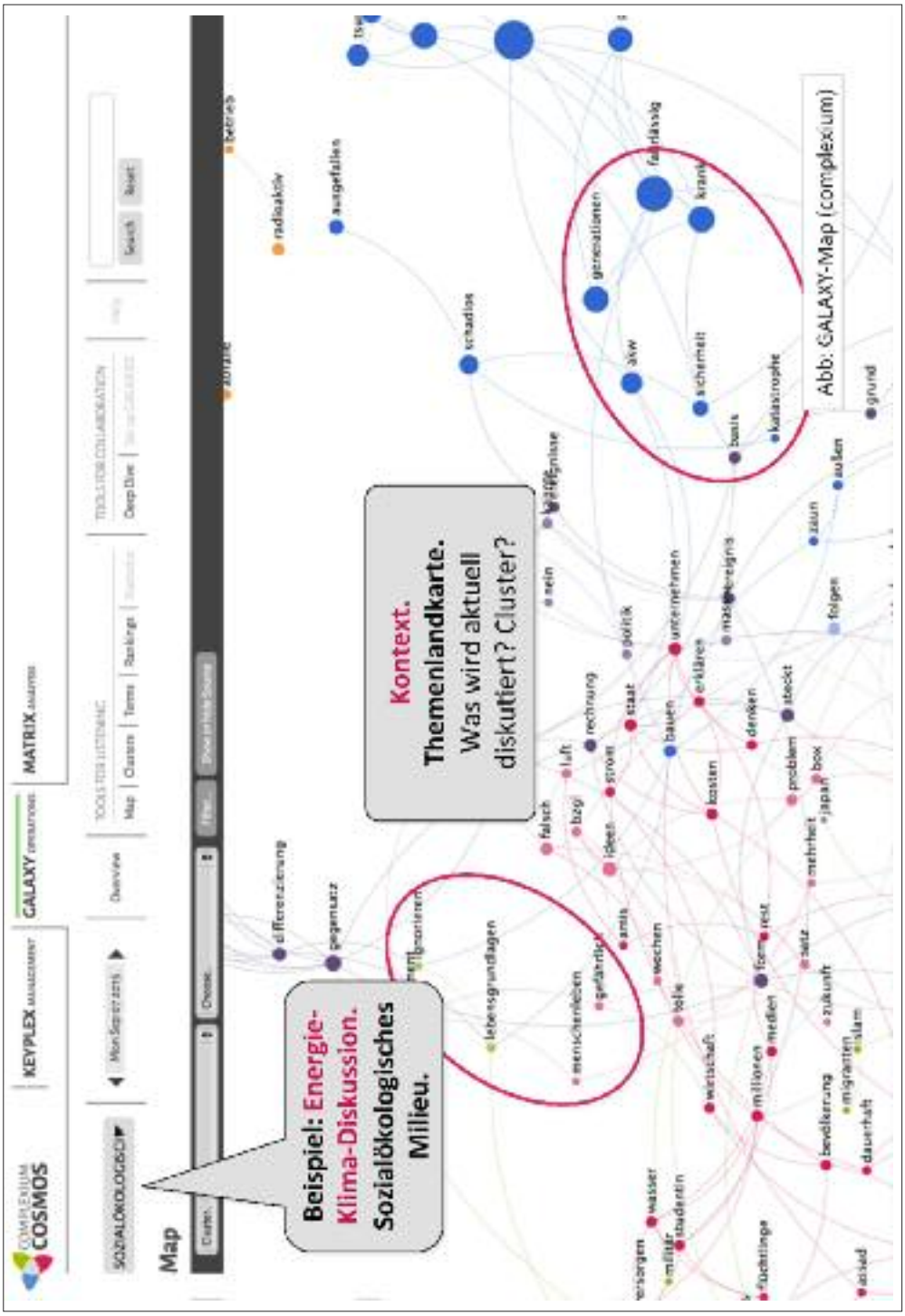
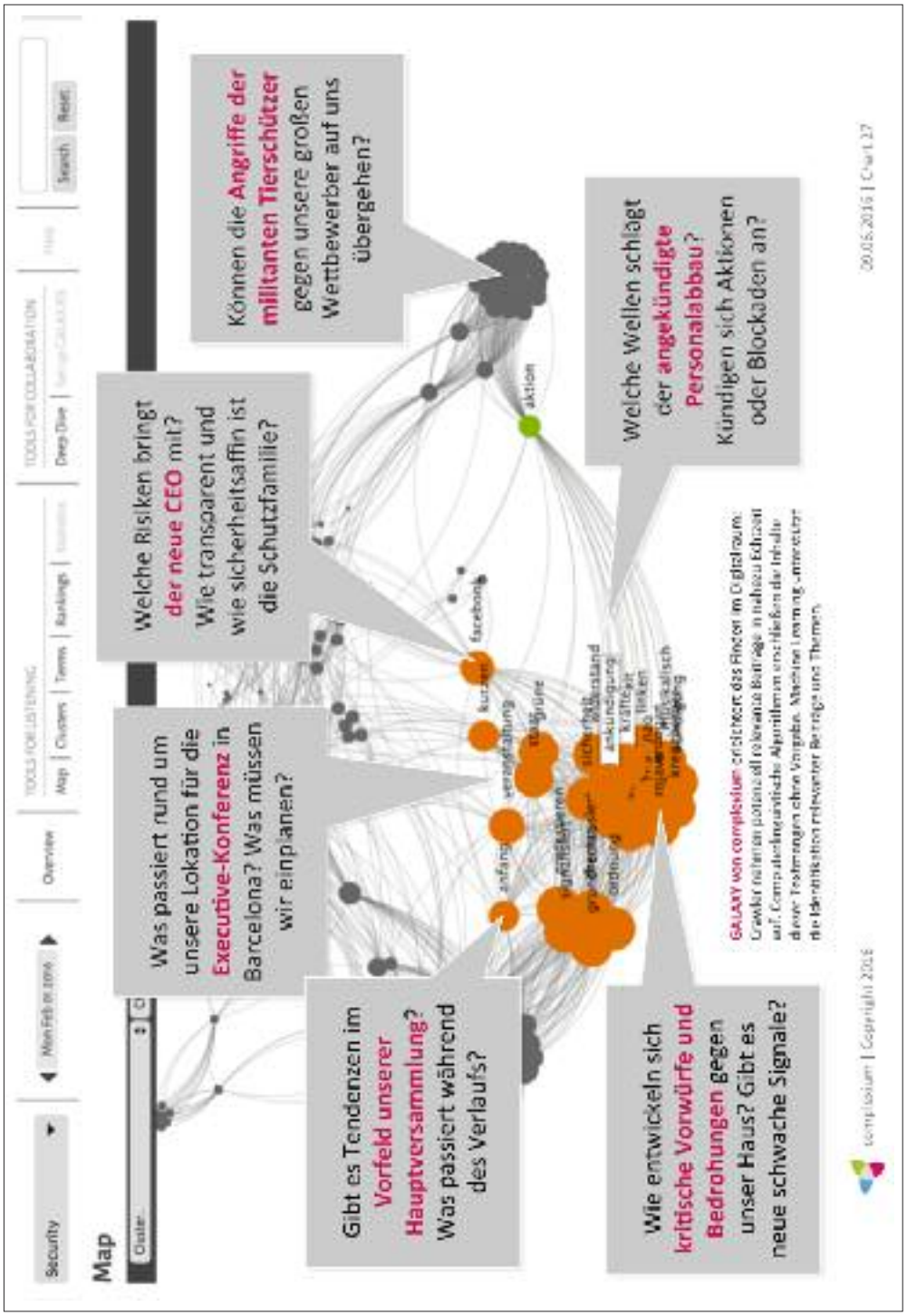


Abb: GALAXY-Deep-Dive (complexium)


COMPLEXIUM
COSMOS
KEYPLEX
GALAXY
MATRIX
Map
Beispiel: Energie-Klima-Diskussion.
Sozialökologisches Milieu.
Kontext.
Themenlandkarte.
Was wird aktuell diskutiert? Cluster?
Abb: GALAXY-Map (complexium)


Security
Map
Cluster
Was passiert rund um unsere Lokation für die Executive-Konferenz in Barcelona? Was müssen wir einplanen?
Welche Risiken bringt der neue CEO mit? Wie transparent und wie sicherheitsaffin ist die Schutzfamilie?
Können die Angriffe der militanten Tierschützer gegen unsere großen Wettbewerber auf uns übergehen?
Welche Wellen schlägt der angekündigte Personalabbau? Kündigen sich Aktionen oder Blockaden an?
Gibt es Tendenzen im Vorfeld unserer Hauptversammlung? Was passiert während des Verlaufs?
Wie entwickeln sich kritische Vorwürfe und Bedrohungen gegen unser Haus? Gibt es neue schwache Signale?
facebook
aktion

PREMONITOR: Nutzen und Aufbau der innovativen GALAXY-Technologie.

Was ist Thema auf digitalen Hotspots? Was ist neu? Was wird wichtig?

GALAXY-Technologie filtert relevante Inhalte aus dem digitalen Rauschen.
Algorithmen blicken unter das Bekannte: Sie zeigen entstehende Auffälligkeiten.

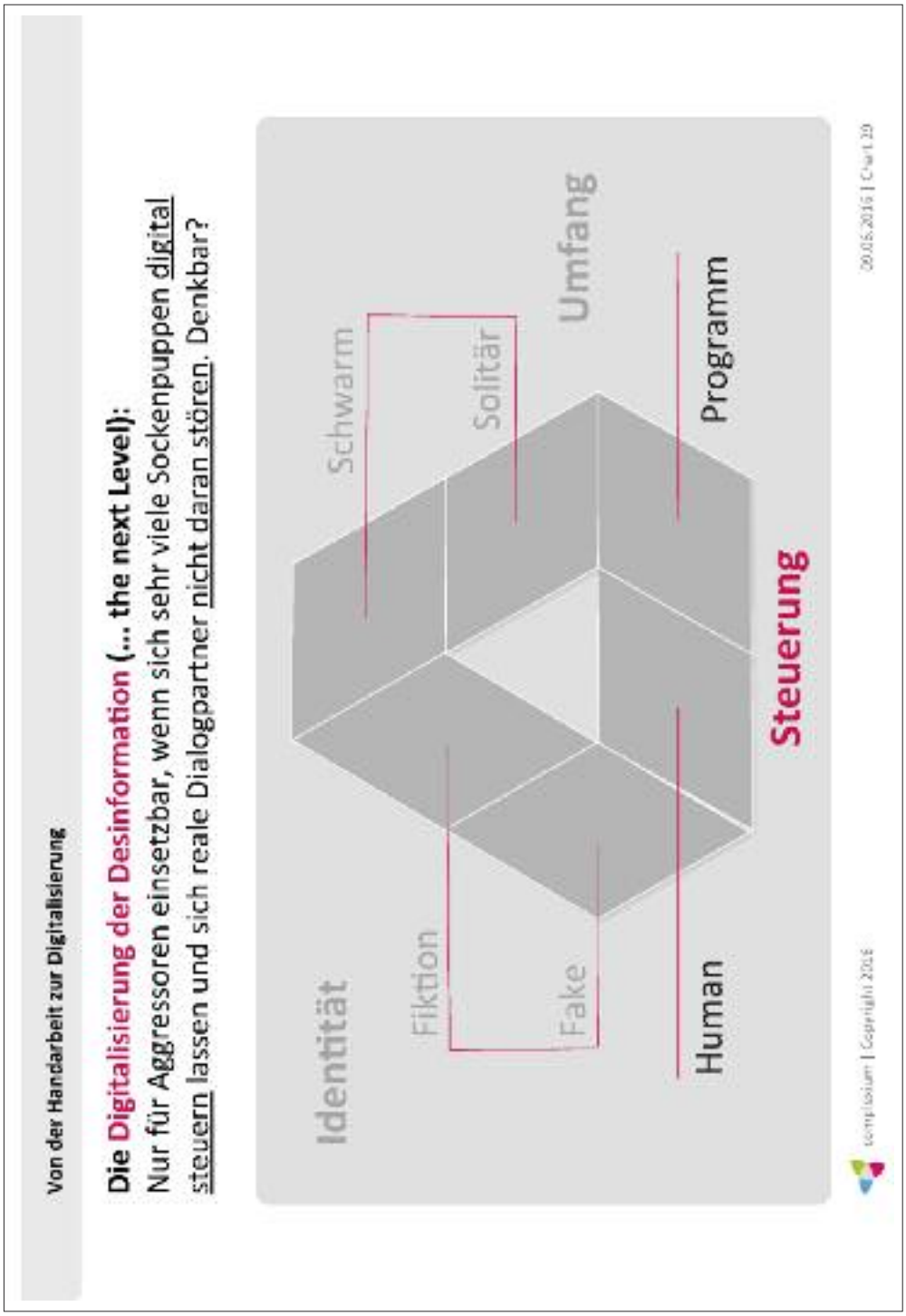
GALAXY-Technologie:
ENTDECKEN!

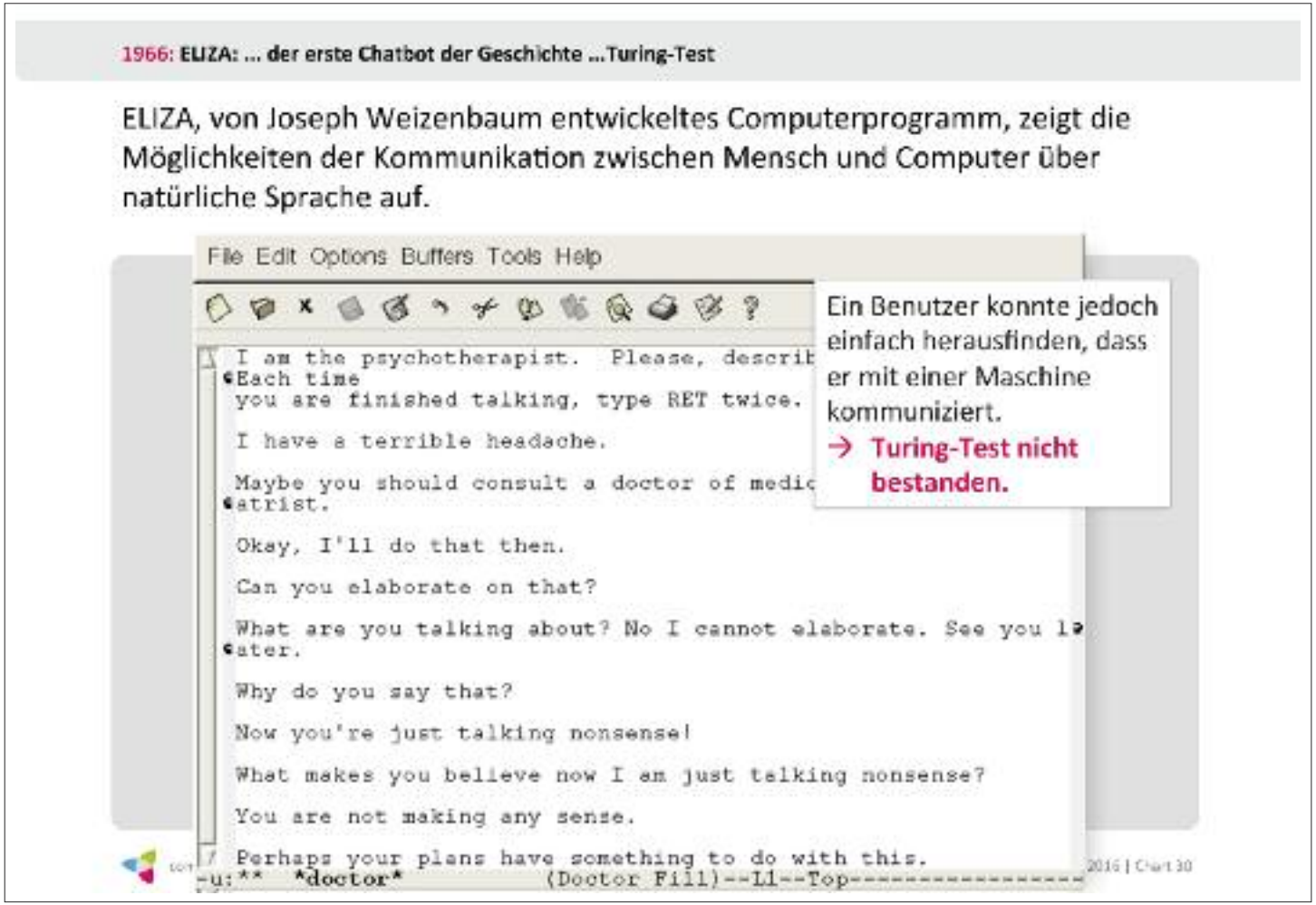
- Quellen werden breit eingelesen, Eingangsfilter schließen Irrelevantes aus.
- Über definierte Suchbegriffe hinaus hört das System frei zu: Systematisch werden auch unerwartete Themen erkannt, sobald die linguistische Signifikanz steigt.

→ **Known und unknown Unknowns!**

Herkömmlicher Monitoring-Ansatz:
SUCHSTRINGS.

- Festlegung aller Suchbegriffe im Voraus.
- Unerwartetes und Überraschungen werden per Definition ausgeblendet.


Von der Handarbeit zur Digitalisierung
Die Digitalisierung der Desinformation (... the next Level):
Nur für Aggressoren einsetzbar, wenn sich sehr viele Sockenpuppen digital steuern lassen und sich reale Dialogpartner nicht daran stören. Denkbar?
Identität
Fiktion
Fake
Schwarm
Solitär
Umfang
Human
Programm
Steuerung


1966: ELIZA: ... der erste Chatbot der Geschichte ...Turing-Test
ELIZA, von Joseph Weizenbaum entwickeltes Computerprogramm, zeigt die Möglichkeiten der Kommunikation zwischen Mensch und Computer über natürliche Sprache auf.
File Edit Options Buffers Tools Help
I am the psychotherapist. Please, describ
Each time
you are finished talking, type RET twice.
I have a terrible headache.
Maybe you should consult a doctor of medic
atrist.
Okay, I'll do that then.
Can you elaborate on that?
What are you talking about? No I cannot elaborate. See you l
ater.
Why do you say that?
Now you're just talking nonsense!
What makes you believe now I am just talking nonsense?
You are not making any sense.
Perhaps your plans have something to do with this.
-u:** *doctor* (Doctor Fill)--L1--Top--
Ein Benutzer konnte jedoch einfach herausfinden, dass er mit einer Maschine kommuniziert.
→ Turing-Test nicht bestanden.


2016
JOBmehappy
Benutzer haben bisher kein Problem damit, auch persönliche Themen mit Bots zu „besprechen".
→ Turing-Test? Egal!
Erster Job Bot über den Facebook Messenger entwickelt
Nachdem Facebook am 12.4.2016 auf der F8 Konferenz in San Francisco die neuen Chat Bots für den Messenger vorgestellt hat, haben wir von Jobmehappy.de die neue Funktion getestet und unseren eigenen Job Bot entwickelt. Das Ergebnis ist überraschend gut. Wie genau unser Job Bot aber funktioniert, könnt ihr in diesem Screencast sehen.
+++ Update: 3.5.2016 Der Job Bot wurde heute Nacht aus der Facebook Review Phase entlassen und ist damit ohne Beschränkung zu erreichen +++
https://www.facebook.com/jobmehappy/
complexium | Copyright 2016
20.05.2016 | Chart 31

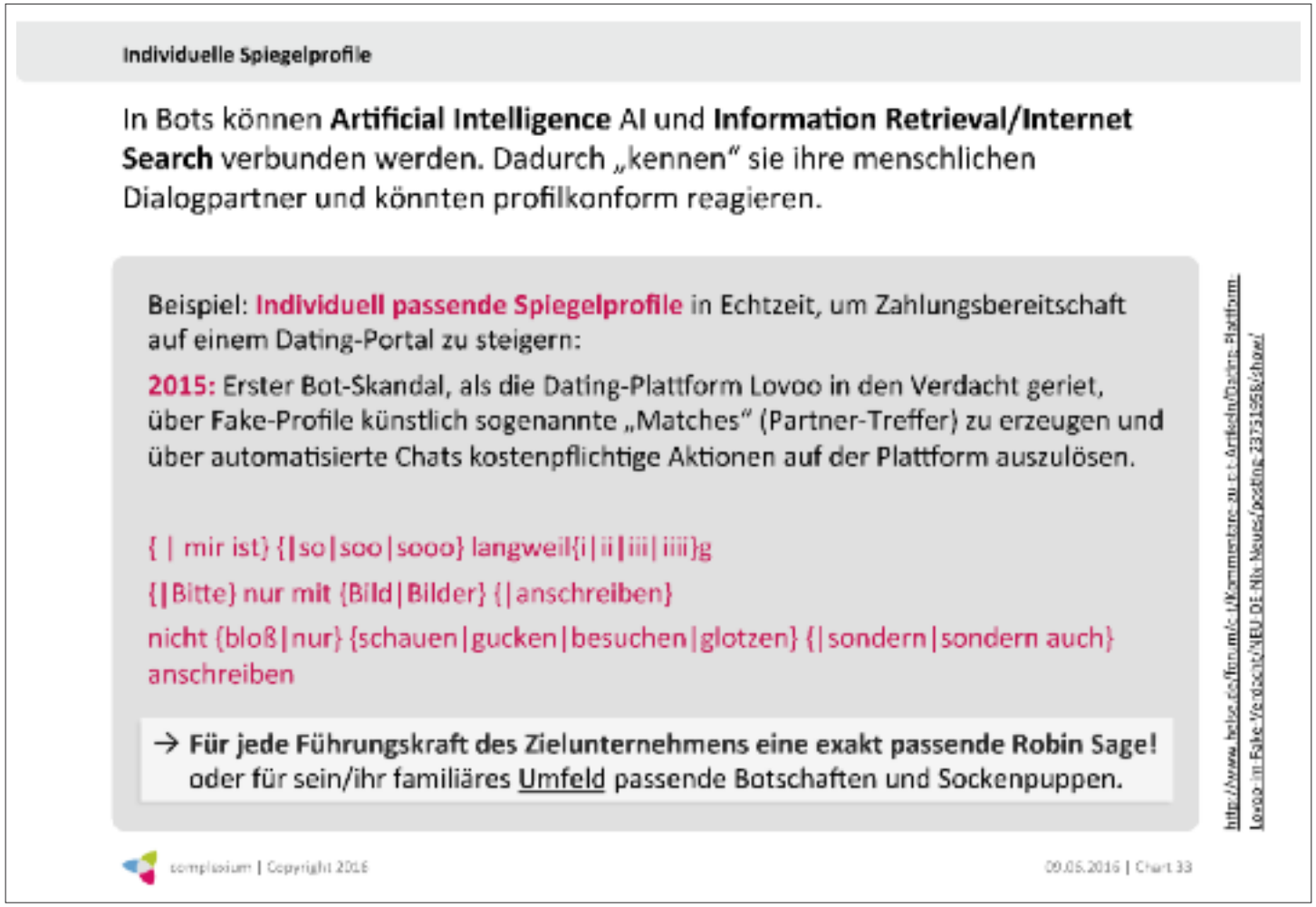
Chatbots via Facebook Messenger

„Nachdem Facebook letzte Woche auf der F8 conference Einblicke in die zukünftige Entwicklung von Chatbots auf Basis des Facebook Messengers gewährt hat, werden **diese schon bald massiven Einfluss auf die Art und Weise haben, wie Menschen nach Informationen suchen und wie sie zum Beispiel mit Unternehmen kommunizieren.**"

Persoblogger
Stefan Scheller
06/05/2016

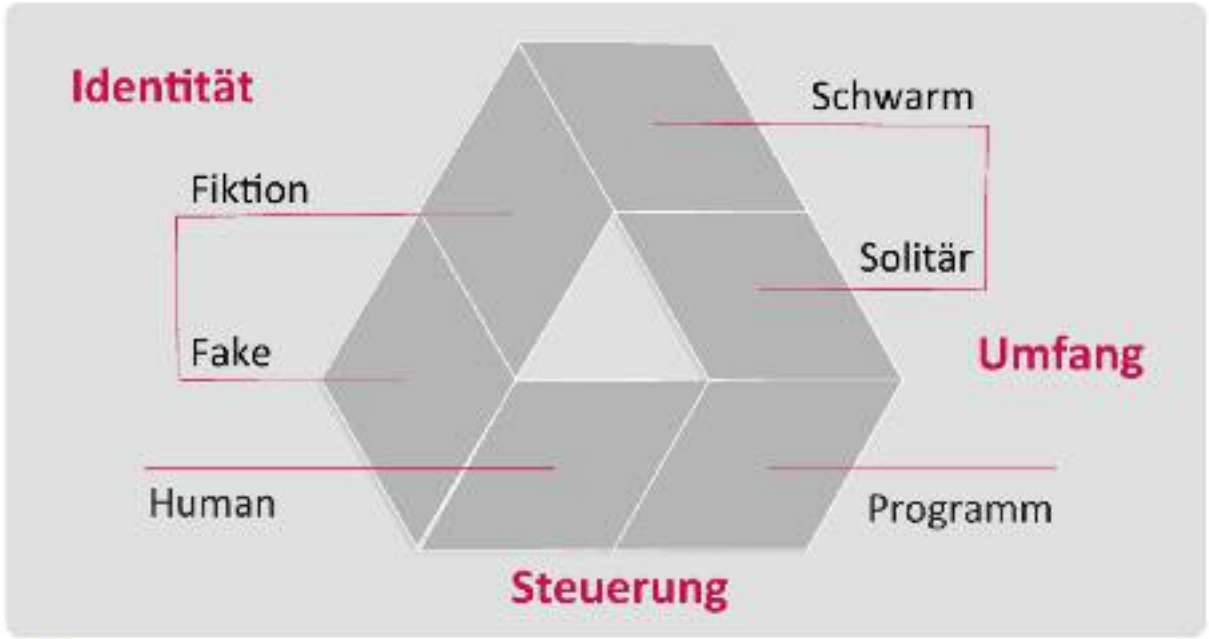
Chatbots im Recruiting – einen ersten HR Jobbot via Facebook Messenger testen

complexium | Copyright 2016 06.05.2016 | Chart 32


Individuelle Spiegelprofile
In Bots können **Artificial Intelligence** AI und **Information Retrieval/Internet Search** verbunden werden. Dadurch „kennen" sie ihre menschlichen Dialogpartner und könnten profilkonform reagieren.
Beispiel: **Individuell passende Spiegelprofile** in Echtzeit, um Zahlungsbereitschaft auf einem Dating-Portal zu steigern:
2015: Erster Bot-Skandal, als die Dating-Plattform Lovoo in den Verdacht geriet, über Fake-Profile künstlich sogenannte „Matches" (Partner-Treffer) zu erzeugen und über automatisierte Chats kostenpflichtige Aktionen auf der Plattform auszulösen.
{ | mir ist} {|so|soo|sooo} langweil{i|ii|iii|iiii}g
{|Bitte} nur mit {Bild|Bilder} {|anschreiben}
nicht {bloß|nur} {schauen|gucken|besuchen|glotzen} {|sondern|sondern auch} anschreiben
→ **Für jede Führungskraft des Zielunternehmens eine exakt passende Robin Sage!** oder für sein/ihr familiäres Umfeld passende Botschaften und Sockenpuppen.
http://www.heise.de/ffm.mdr.t/Kommentare-zu-rbb-Artikeln/Dating-Plattform-Lovoo-im-Fake-Verdacht;NEU,DE,Nix-Neues/posting-23731958/show/
complexium | Copyright 2016
09.05.2016 | Chart 33

Von der Handarbeit zur Digitalisierung: Trolle, Sockenpuppen ... Propaganda via Social Bots

Social Bots werden ein Problem. Via Fake-Accounts werden nicht-menschliche Profile angelegt, die programmiert sind, sich **selbstständig an Diskussionen zu beteiligen oder eigenständig Informationen zu versenden** (z.B. via Twitter), um einen bestimmten Zweck zu erfüllen: z.B. Meinungsbeeinflussung, Diskredition. **Aber: Detektierbar.**



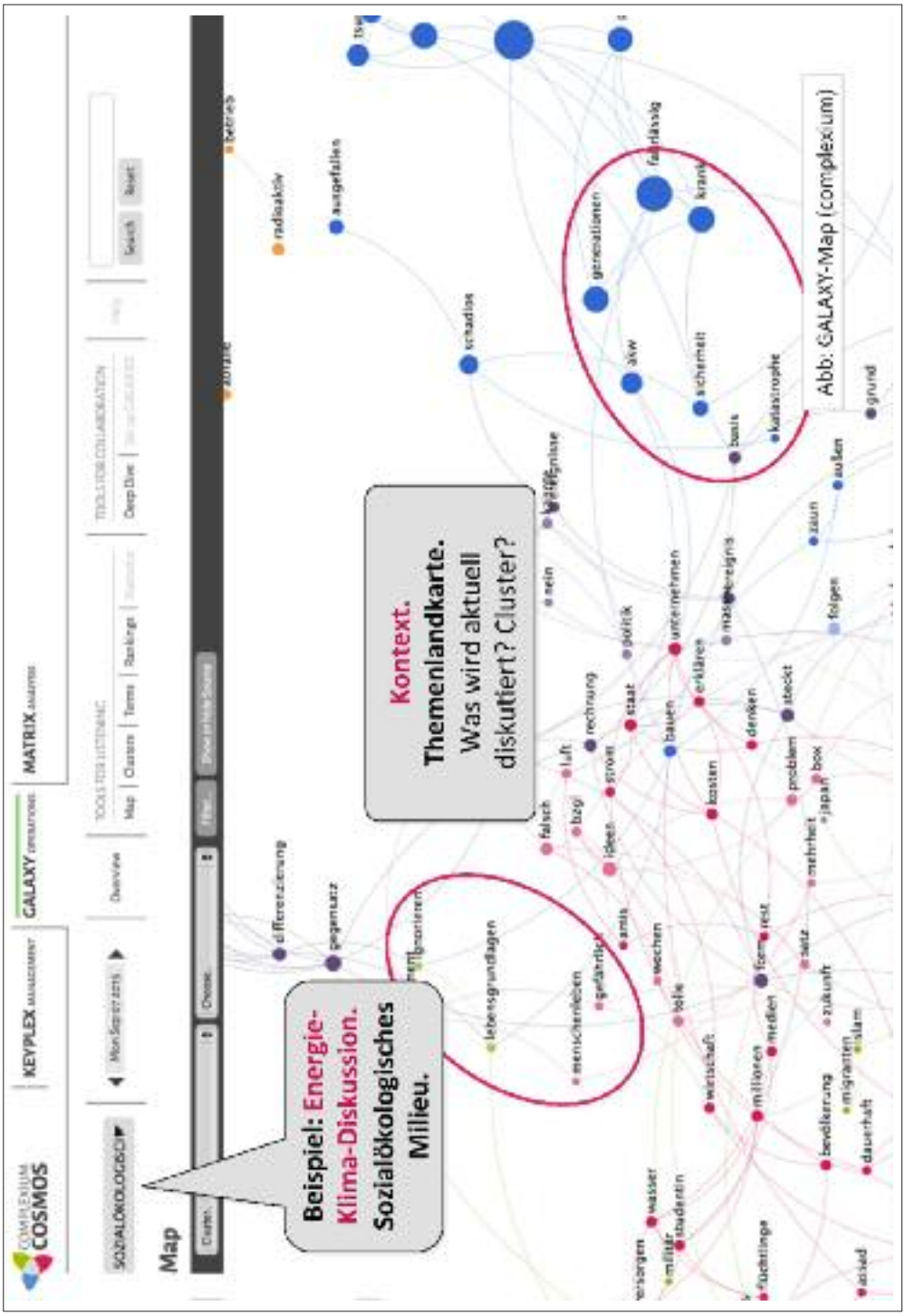
http://www.mobilegeeks.de/artikel/manipulation-social-bots/

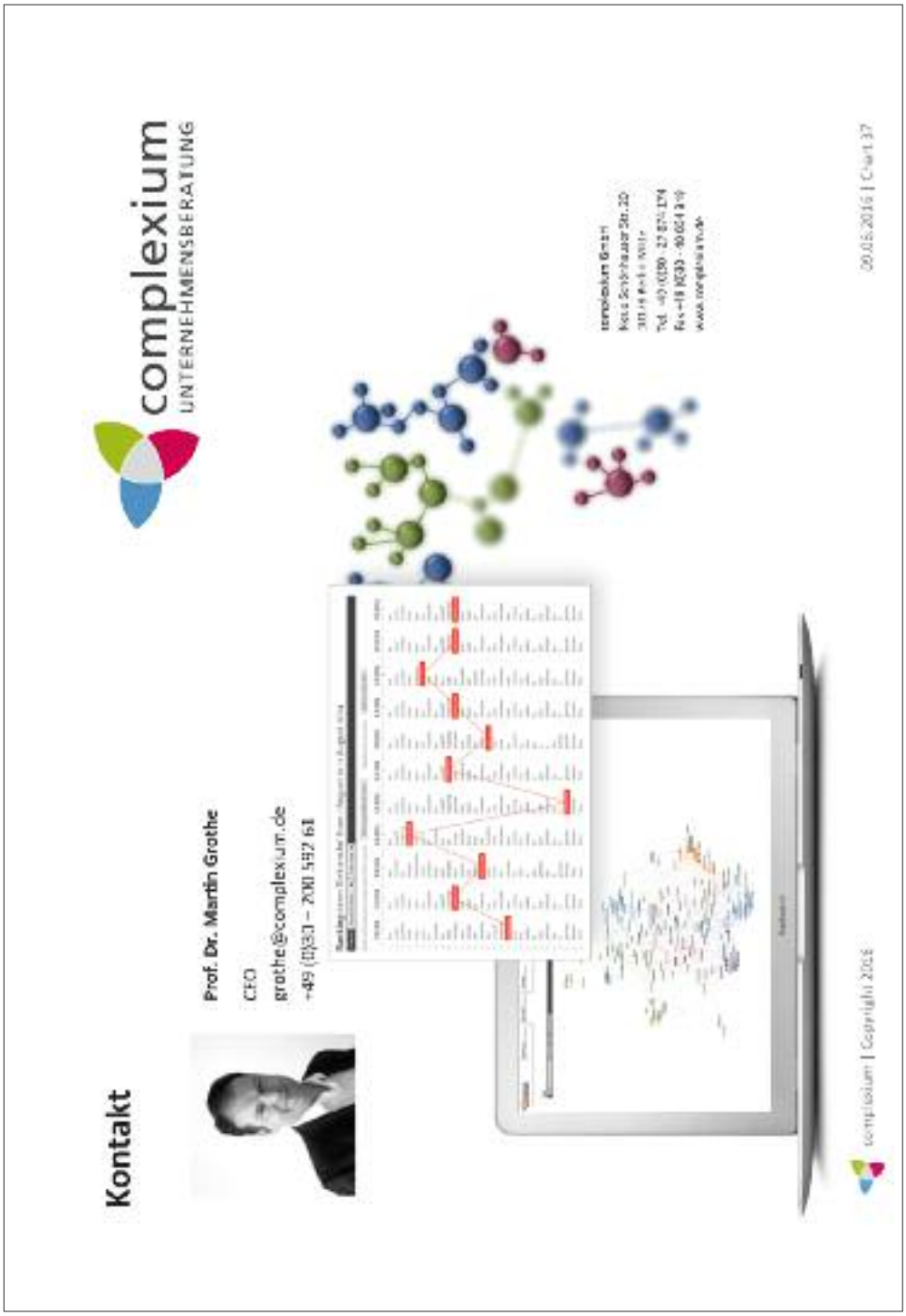
Im Repertoire von Wettbewerbern und Gegnern: Trolle, Sockenpuppen und Bots.

Wenn Ihr Gegner Social Bots gegen Sie einsetzt,
dann sollten Sie die Fähigkeiten zur Prävention und Detektion bereits breit in der Organisation verinnerlicht haben:
Sie können massiv unter Stress gesetzt werden.

Empfehlungen:

- Prävention durch Aufklärung, Verhaltensregeln und regelmäßige **Sichtbarkeitsanalysen.**
- Detektion von Meinungsmanipulation durch qualitatives **Social Listening** in Echtzeit.


COMPLEXIUM
COSMOS
KEYPLEX
GALAXY
MATRIX
Map
Beispiel: Energie-Klima-Diskussion.
Sozialökologisches Milieu.
Kontext.
Themenlandkarte.
Was wird aktuell diskutiert? Cluster?
Abb: GALAXY-Map (complexium)


Kontakt
complexium
UNTERNEHMENSBERATUNG
Prof. Dr. Martin Grothe
CEO
grothe@complexium.de
+49 (0)33 – 200 532 61
complexium | Copyright 2018
20.05.2016 | Chart 37

Das Zusammenspiel von Unternehmenssicherheit und Unternehmenskommunikation

Ronald Pofalla, Deutsche Bahn AG

Eine partnerschaftliche Zusammenarbeit zwischen den Sicherheitsbereichen der Unternehmen und den Sicherheitsbehörden ist heutzutage wichtiger denn je. Nur gemeinsam werden wir die vielfältigen und zahlreichen Angriffe auf die Sicherheit unseres Landes und unserer Unternehmen erfolgreich bewältigen können. Und nur gemeinsam können wir auch weiterhin für Kunden und Bürger einen hohen Sicherheitsstandard sicherstellen. Deshalb arbeitet die Deutsche Bahn AG bereits seit 2000 eng mit dem Bundesinnenministerium und der Bundespolizei in einer Ordnungspartnerschaft zusammen. Und das sehr erfolgreich! So ging im vergangenen Jahr die Kriminalität aufgrund unserer Sicherheitskonzepte um drei Prozent zurück. Und dieser Trend setzt sich weiter fort.

Gemeinsam mit der Bundespolizei arbeiten wir derzeit daran, die Bahnhöfe durch den Ausbau und die Erneuerung der Videotechnik noch sicherer zu machen. Bis 2023 investieren wir dafür gemeinsam mit der Bundespolizei 85 Millionen Euro – zusätzlich zu unserem Sicherheitsbudget von jährlich rund 160 Millionen Euro.

Bisher wurde der Mannheimer Hauptbahnhof und das Berliner Ostkreuz neu mit Videotechnik ausgestattet. In den Hauptbahnhöfen Bremen, Nürnberg, Hannover, Hamburg und einer Vielzahl Berliner Bahnhöfen wurde zudem mit dem Bau bzw. der Planung für die Videotechnik begonnen.

Außerdem werde ich in Kürze eine Taskforce Sicherheitstechnologie einrichten, die sich mit den neusten Software-Systemen beschäftigt. Ein Beispiel dazu:
Wird ein Koffer irgendwo am Bahnsteig länger abgestellt, wird das vom System automatisch erkannt. Wir können dann sofort reagieren und die Bundespolizei verständigen. Darüber hinaus werden wir Kriminalitätsschwerpunkte an unseren Bahnhöfen und in unseren Zügen durch die Auswertung statistischer Daten noch besser identifizieren. Das ermöglicht einen noch zielgenaueren Einsatz unserer Sicherheitskräfte.

Fest steht im Übrigen: Die Sicherheit in Zügen und auf Bahnhöfen ist weithin auf einem hohen Niveau – deutlich höher als im sonstigen öffentlichen Raum. Gleichwohl sehe ich mit Sorge auf Entwicklungen, die uns bereits jetzt und in der Zukunft mehr denn je beschäftigen werden.

Dies betrifft zum einen die Verrohung eines Teils unserer Gesellschaft. Wir nehmen dies durch eine deutlich ansteigende Anzahl von Übergriffen -

plus 20% - gegen unsere Mitarbeiter wahr. Aber auch die zunehmenden Gewaltexzesse von Hooligans in unseren Zügen und Bahnhöfen machen uns Sorge. Diese Leute, die der Sport oft gar nicht interessiert, bekommen von uns die rote Karte gezeigt und werden damit vom Platz gestellt. Wir setzen hier klare Zeichen und begleiten dies mit einer gezielten und aktiven Medienarbeit.

Unsere Kunden sollen wissen, dass die Deutsche Bahn sich dieses Verhalten nicht länger bieten lässt. Deshalb werden wir auf die Belästigungen unserer Kunden und die teils stark beschädigten Züge mit Hausverboten und Beförderungsausschlüssen direkt vor Ort antworten, sobald die Bundespolizei einen Täter feststellt. Ebenso gehen wir gegen Personen vor, welche unsere Mitarbeiter angreifen.

Die Deutsche Bahn arbeitet daher gemeinsam mit der Bundespolizei und den Interessensvertretungen an weiteren Maßnahmen. Zum Beispiel am Ausbau von Deeskalations- und Verhaltenstrainings. Doch gegen die gesellschaftlichen Entwicklungen, die bei einem Teil der Menschen zu stärkerer Gewalt führen, müssen wir gemeinsam vorgehen. Dazu benötigen wir eine breite öffentliche Diskussion in der Gesellschaft.

Die DB unterstützt diesen Prozess. So haben wir zum Beispiel den unternehmensweiten Wettbewerb „Bahn-Azubis gegen Hass und Gewalt“ ins Leben gerufen. Seit Beginn konnten unsere Berufsanfänger in mehr als 1.000 Projekten deutliche Zeichen setzen. Für Toleranz, Zivilcourage und gegen Rassismus und Gewalt!

Ein weiteres Thema beschäftigt den DB-Konzern sowie alle Sicherheitsbehörden. Die Gefahren durch den islamistischen Terrorismus. Durch die zuständigen Behörden wird diese Gefahr weiterhin als abstrakt hoch für Deutschland eingeschätzt. Sie kann sich jederzeit in Form sicherheitsrelevanter Ereignisse bis hin zu terroristischen Anschlägen in Deutschland konkretisieren. Der Bahnverkehr und dessen Einrichtungen sind aufgrund des hohen infrastrukturellen und wirtschaftlichen Schadens sowie der hohen medialen Aufmerksamkeit besonders gefährdet.

Klar ist: Die Gefahrenabwehr ist Aufgabe der Sicherheitsbehörden. Aber selbstverständlich übernimmt auch die Deutsche Bahn ihre unternehmerische Verantwortung. Unsere Sicherheitsmaßnahmen für die Infrastrukturen und die Fahrzeuge sind gesamthaft konzipiert und auf das offene und integrierte Verkehrssystem Bahn ausgerichtet.

3.700 DB-Sicherheitskräfte und rund 5.000 Beamte der Bundespolizei sind täglich in vielen Bahnhöfen und Zügen präsent. Im Sicherheitszentrum Bahn arbeitet die Informationsstelle des Bundespolizeipräsidiums und das Lagezentrum der DB Tür an Tür und Hand in Hand. Alle Einsatzmaßnahmen der DB werden eng mit der Bundespolizei abgestimmt. Beide Seiten

profitieren vom Wissen des anderen.

Auch baut die DB ihre Objektschutzmaßnahmen für Bahnhöfe und Bahnanlagen in enger Abstimmung mit der Bundespolizei weiter aus. Darüber hinaus halten wir ein qualifiziertes Krisenmanagementsystem für die Bahnhöfe und Züge vor.

Ein drittes Thema, welches uns zunehmend beschäftigt, ist die Cyber-Sicherheit. Aktuell befassen sich konzernweit rund 260 Projekte mit der Digitalisierung. Kein Unternehmensbereich der DB ist davon ausgenommen. Die Digitalisierung wird alle Bereiche verändern: Produkte, Prozesse, aber auch die gesamte Arbeitswelt. Dabei überwiegen für uns als Mobilitäts- und Logistikdienstleister klar die Chancen.

Nehmen Sie unseren DB Navigator: Bereits jetzt ist für über die Hälfte unserer Kunden im Fernverkehr das Smartphone Fahrplanauskunft, Ticketschalter und Reisebegleiter in einem. Oder nehmen Sie unsere neueste ICE-Strecke zwischen Leipzig/Halle und Erfurt, die wir im Dezember in Betrieb genommen haben. Sie kommt vollständig ohne ortsfeste Signale aus! Züge, Fahrweg und Betriebszentrale kommunizieren vollautomatisch über Sensoren und eine digitale Datenverarbeitung.

Natürlich entstehen damit neben den Chancen auch Risiken. Für uns steht außer Frage: Weitere Erfolge werden entscheidend davon abhängen, wie gut wir die IT-Systeme und Kommunikationsnetze schützen.

Fakt ist: Die Deutsche Bahn ist auch auf dem elektronischen Weg ein potentiell gefährdetes Angriffsziel. Dem Know-how, den Erfahrungen und der Wachsamkeit des IT-Sicherheits-managements ist zu verdanken, dass wir bisher schnell und angemessen auf alle cyberkriminellen Angriffe reagieren konnten.

Was wir aber mit Sorge beobachten: Die Quantität und die „Qualität" der Angriffe nehmen zu. Bei den sogenannten DDoS-Attacken [Distributed Denial of Service], also Angriffen mit dem Ziel die Computer lahm zu legen, hat sich das Datenvolumen der Angriffe in den vergangenen fünf Jahren verzehnfacht. Cyber-Kriminalität ist mittlerweile hochgradig professionell organisiert. Das bedeutet für die DB, dass wir der Cyber-Sicherheit in jeder Hinsicht höchste Aufmerksamkeit widmen.

Unsere Abwehrmaßnahmen setzen daher auf allen Ebenen an: Innovative Sicherheitstechnik, eine moderne Organisation und funktionierende Prozesse. Technische Maßnahmen umfassen zunächst Maßnahmen zur Gebäudesicherheit wie Zäune oder Zutrittskontrollen mittels Kartenlesern. Die technischen Maßnahmen schließen aber auch das gesamte Spektrum ein, das unsere Server, Kommunikationsnetze und IT-Endgeräte schützt: Firewalls, Anti-Viren-Software, Werkzeuge zur aktiven Überwachung der

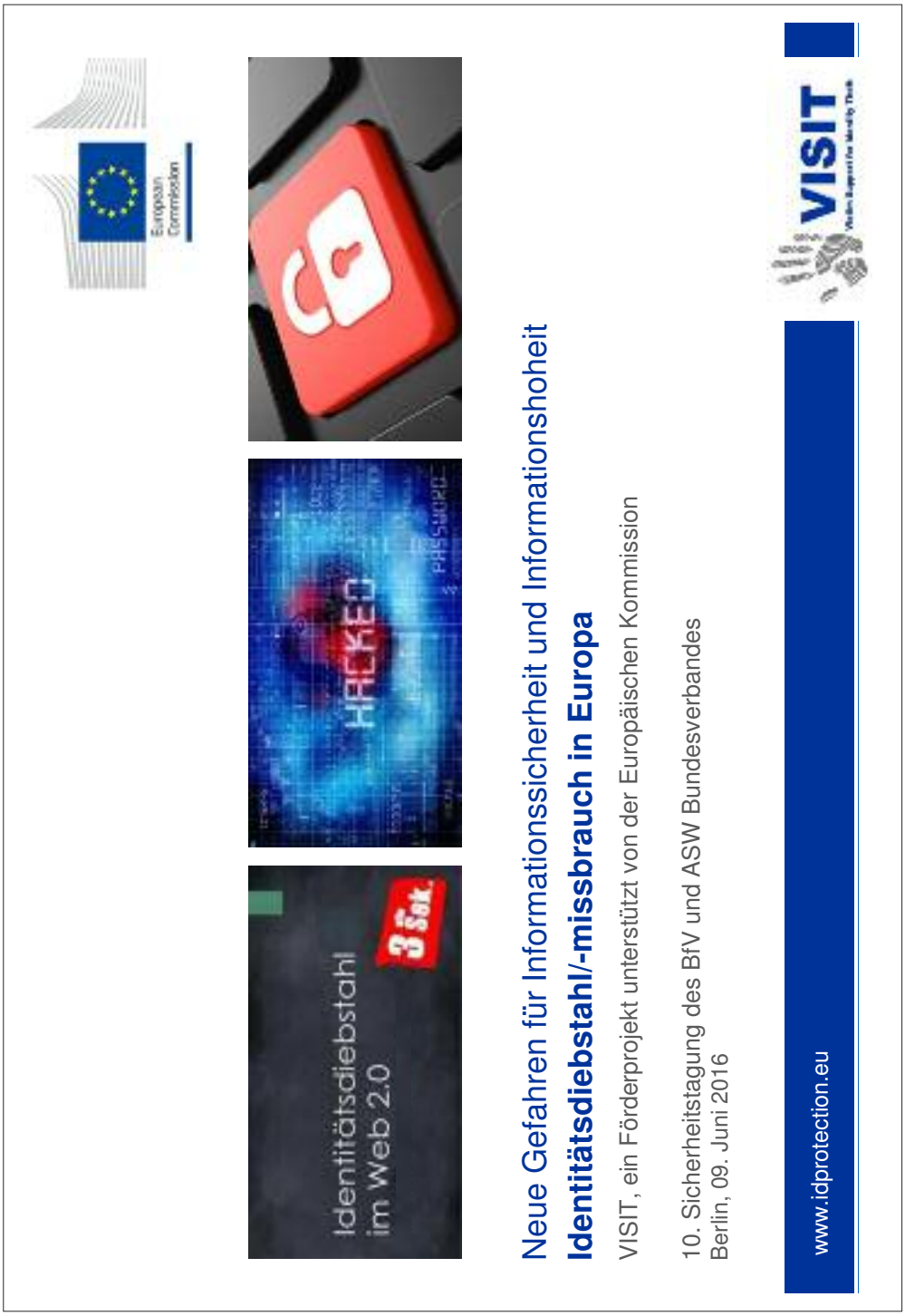
IT-Systeme oder Netze und Abwehr von Angriffen, Anti-Spam-Filter und vieles mehr.

Darüber hinaus sind wir gerade dabei, ein „Cybersecurity Incident Response Team“ aufzubauen – so etwas wie eine schnelle Eingreiftruppe. Dieses Team ist rund um die Uhr einsatzbereit, um bei Cyberangriffen schnell zu reagieren. Auch der Gesetzgeber hat erkannt, dass das Feld der Cyber-Sicherheit größer und komplexer wird. Er nimmt viele Unternehmen, so auch die DB, über das IT-Sicherheitsgesetz in die Pflicht. Dieses Gesetz ist für uns als DB Anforderung und Ansporn zugleich, unsere Infrastruktur zu schützen und uns bei der Cyber-Sicherheit kontinuierlich weiterzuentwickeln und zu verbessern. Das setzt voraus, dass wir das Thema Cyber-Sicherheit weiter gemeinsam angehen und aktuelle Entwicklungen unter allen Akteuren kritisch und konstruktiv diskutieren.

Wir, als Deutsche Bahn, wollen und werden diesen Dialog aus tiefster Überzeugung weiter suchen und fördern. Die Zusammenarbeit mit Unternehmen – und natürlich mit den Sicherheitsbehörden – ist aus unserer Sicht unabdingbar für die weiteren Fortschritte bei der Digitalisierung und für die Sicherheit.

Identitätsdiebstahl/-missbrauch in Europa

Jürgen Kempf, Result Group, Vertreter des EU-Projektes V.I.S.I.T.



AGENDA

- Kurzüberblick EU Projekt Identitätsdiebstahl
- Identitätsdiebstahl und Risiken online und offline
- Deliktsformen
- Schilderungen von Geschädigten
- 7 goldene Regeln zur Abwehr

www.idprotection.eu

DEFINITION IDENTITÄTSDIEBSTAHL

- Besser Identitätsmissbrauch (IDDM) – die unberechtigte Nutzung personenbezogener Daten (Identität) einer natürlichen Person durch Dritte
- Neben dem Namen werden eine Reihe persönlicher Daten wie Geburtsdatum, Anschrift, Führerschein- oder Sozialversicherungsnummern, Bankkonto- oder Kreditkartennummern genutzt, um die Feststellung der tatsächlichen eigenen Identität zu umgehen oder diese zu verfälschen.
- Identitätsdiebstahl ist eine der am stärksten zunehmenden Kriminalitätsformen in hochtechnisierten Ländern (Quelle Juraforum)
- Begehungsformen: Online, Offline und Misch-Versionen

VICTIM SUPPORT FOR IDENTITY THEFT

Das europäische Förderprojekt VISIT wurde am 1. September 2014 gestartet

Projekt-Leitung:

Result Group GmbH (DE)

Partner:

Universität Jyväskylä (FI), Guarda Nacional Republicana (PT), TU Lübeck (DE)

Aufgaben im Projekt:

Erfassen der Aktivitäten von Behörden und Institutionen, inkl. Wirtschaftsauskunfteien

Sammeln und Auswerten von ID-Diebstahlfällen sowie Modus Operandi

Erfassen und Analysieren von Schwachpunkten

Analyse, Verwertung und Weiterentwicklung bestehenden Präventionsmaterials

Entwicklung einer Webseite, zur Darstellung des Projekts und Berichtsplattform für Opfer

Erarbeiten eines eLearning-Programms für Bürger und Sicherheitsbehörden

Ausrichten von Veranstaltungen sowie einer finalen Konferenz Ende 2016

www.idprotection.eu

ERWARTETE ERGEBNISSE

- Übersicht und Analyse des Bedrohungspotentials durch IDDM
- Sensibilisierung zu IDDM in Gesellschaft und Verwaltung
- Erstellen einer Aufklärungskampagne - Erhöhung der Vorsicht bei Online Nutzung
- Identifizierung/Koordination von Aktivitäten mit einer vorgegeben Anzahl von natürlichen Personen, um ID-Betrug zu reduzieren
- Verbreitung und Integration des Strategieplans der EU, um ID-Diebstahl und -Betrug zu verhindern und zu bekämpfen sowie sicheres ID-Management zu fördern
- Entwickeln von sicheren ID-Managementtechniken für Behörden und staatliche Einrichtungen
- Einbinden von Nichtregierungsorganisationen (NRO) und Unternehmen zur Reduzierung von IDDM
- Fortlaufende Evaluierungen, um Fortschritte und Effekte zu analysieren und zu erfassen

AKTIVITÄTEN DEUTSCHLAND

Kommunikation, Kontakte und Kooperationen in Deutschland bis heute:

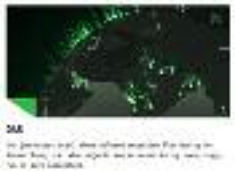
- Bayerisches Staatsministerium des Innern: Joachim Herrmann
- LKA Berlin: Wolfgang Volland und Präsident Klaus Kannst
- LKA Bayern – Zentrale Ansprechstelle Cyber Crime ZAC: Günter Younger
- LfV Bayern – Cyber Allianz Zentrum CAZ: Michael George
- Innenministerkonferenz unter Leitung: Klaus Bouillon/Saarland
- Weisser Ring: Roswitha Müller-Piepenkötter, Jörg Ziercke
- Bundesverband Mittelständische Wirtschaft: Mario Ophoven
- Allianz für Sicherheit in der Wirtschaft: Jan Wolter
- Bundesverband der Sicherheitswirtschaft: Harald Olschok
- Creditreform: Christian Wolfram
- SCHUFA: Michael Freytag
- Bundesdruckerei: Ullrich Hamann

www.idprotection.eu

CYBERTHREAT REAL-TIME MAP

https://cybermap.kaspersky.com

Frei drehbarer Globus - Jedes Land anklickbar- Anzeige der aktuellen Bedrohungslage



OAS on access scan
ODS on demand scan
WAV web anti virus
MAV mail anti virus
IDS intrusion detection
VUS vulnerability scan
KAS Kaspersky anti spam
BAD botnet activity

Datenbasis: Antiviren-Programme des Herstellers, deren Analysen live in die Karte integriert werden.

“IM NETZ” WDR 2013

https://www.youtube.com/watch?v=3_dN9SJrUy0

AKTUELLER DENN JE!

Sondereinsatzkommando der Polizei stürmt das Schlafzimmer einer Unternehmensberaterin Juliane Schubert. Die Beweise sind erdrückend.
Sie soll Wohnungen und Autos angemietet haben, die zur Vorbereitung eines terroristischen Anschlags dienen sollten.
Hat sich jemand Zugang zum Computer der Geschäftsfrau verschafft, ihre virtuelle Identität gestohlen und für kriminelle Zwecke missbraucht? Wie konnte es gelingen, dass ihre gesamten Konten leergeräumt wurden, ohne dass die Bank misstrauisch wird?

In ihr keimt der Verdacht, dass die Person, die ihr all das angetan hat, sich ganz in der Nähe befindet. Wem kann sie noch trauen?
Einmal ins Netz der Fahnder geraten, hat Juliane nur noch ein Ziel: Sie will ihr altes Leben zurück!

https://www.youtube.com/watch?v=3_dN9SJrUy0

BEGEHUNGSFORMEN OFFLINE

- Diebstahl von Geldbörsen, Ausweisen und Scheckbüchern
- Dumpster Diving – Müllauswertung
- Diebstahl von Informationen aus Wohnungen und Häusern
  - Rechnungen, vertrauliche Dokumente etc.
- Identitätsdiebstähle an Arbeitsplätzen
  - Kollegen, Besucher, Fremdpersonal
- Adressenbetrug - Adressen können geändert, Post umgeleitet werden
- Schulterblick und Abschöpfen von Informationen durch Mithören
- PIN-Nummer an Geldautomaten, Passwörter sowie andere Informationen auf Reisen

www.idprotection.eu

VISIT

BEGEHUNGSFORMEN ONLINE

- Phishing
  E-Mails, die von einer legitimen Person oder Organisation zu stammen scheinen
- Pharming
  Installation eines Codes, Weiterleitung auf gefälschte Webseiten
- Spyware und Trojaner
  Software, von Hackern installiert: Sammeln persönlicher Informationen, weiterleiten an gefälschte Webseiten, Änderung von Einstellungen, volle Kontrolle
- Spam, gesendet über Instant Messaging (IM) enthält Spyware, Keylogger, Viren etc.
- Nutzen Social-Networking-Webseiten
- Wardriving - Aufspüren und Nutzen ungeschützter WLAN-Netzwerke

ANDERE METHODEN

- Vishing/SMiSing
  - Funktioniert genau wie Phishing.
    Unterschied: Betrug erfolgt beim Vishing per Telefon, z.B. ein Anruf, der angeblich von Ihrer Bank kommt. “Abgleich” von Kontodetails
- SMiShing
  - Betrug erfolgt über SMS, enthält einen Link zu einer Webseite oder eine Telefonnummer, bei der ein automatisiertes System gestartet wird. Abfrage persönlicher Daten
- Skimming
  - Manipuliertes Geldausgabegerät; Hacker erhalten dadurch Zugriff auf Informationen, die im Magnetstreifen auf der Rückseite der Kredit- oder Geldkarte gespeichert sind
- Datenkompromittierung
  - Hacker greifen auf Kundeninformationen von Unternehmen zu

DATEN- UND FALLAUSWERTUNGEN

- Für 70 Prozent der Opfer war es schwierig oder fast unmöglich, negative Einträge wieder löschen zu lassen
- In fast die Hälfte aller Falle von Identitätsdiebstahl berichteten die Opfer, dass der Betrüger ein Freund, Familienmitglied, ehemaliger Lebensgefährte oder eine Person aus dem näheren Umfeld war, z.B. Arbeitskollege
- Der Diebstahl persönlicher Informationen mithilfe von Spam/Scam-E-Mails erlebt ein bisher nicht gekanntes Hoch
- Identitätsdiebstahl wird durch einfache Passwörter erheblich erleichtert
- Risikobewusstsein fehlt

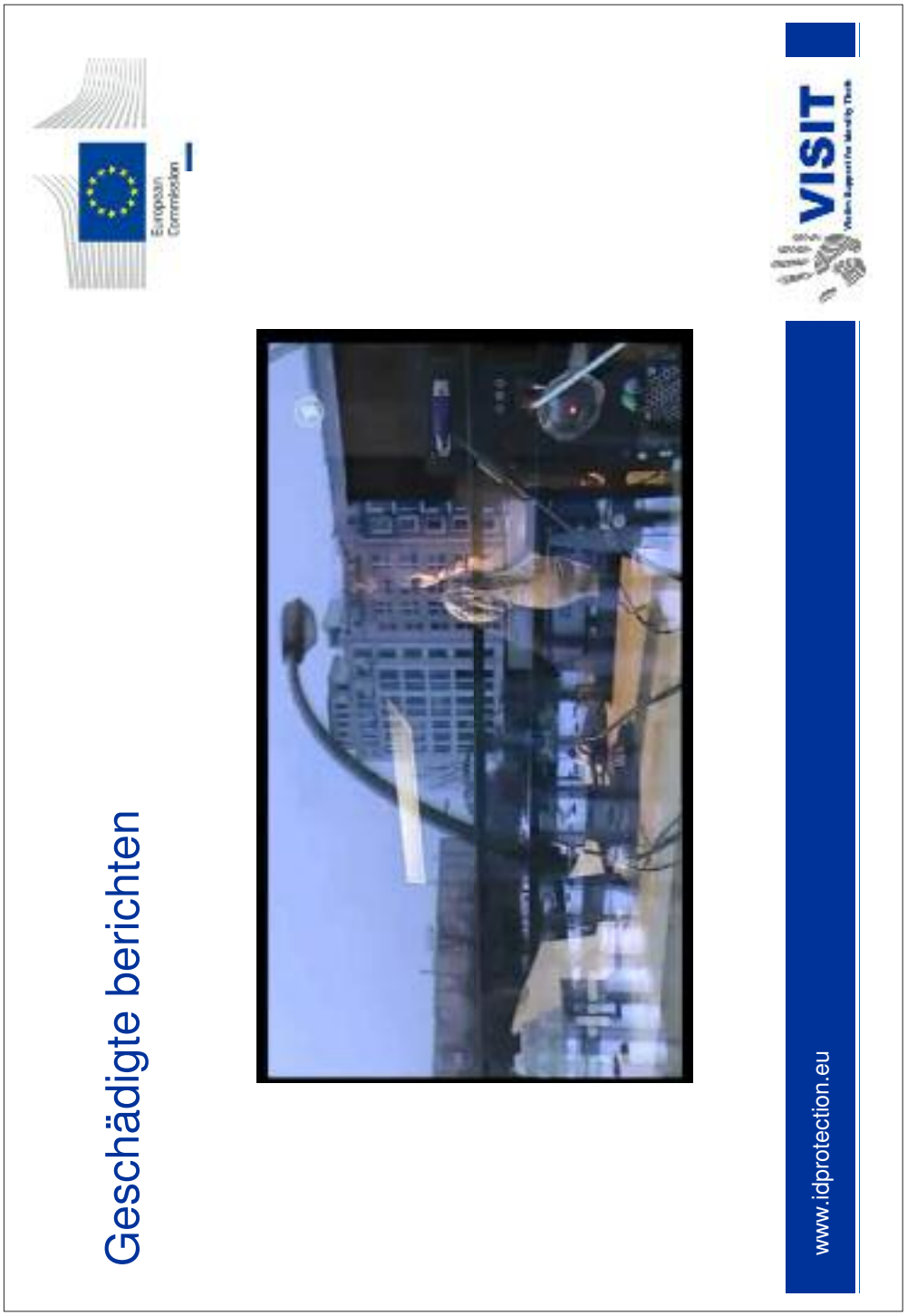
FESTSTELLUNGEN

- Problembewusstsein und Aufklärung tut Not
- Gesunder Menschenverstand kommt nicht immer zur Anwendung
- Es wird nicht auf die Umgebung und/oder Mitreisende geachtet
- Online- bzw. Virenschutz fehlt
- Schwache Passwörter werden verwendet
- Beim Surfen an öffentlichen Hotspots werden sensitive Datentransfers durchgeführt
- Wardriving bringt erhebliche Erfolge
- Kontobewegungen werden nicht zeitnah geprüft
- Sensitive Dokumenten werden nicht sicher aufbewahrt/vernichtet
- Sicherheitsbehörden erkennen IDDM nicht immer
- Kreditauskunfteien und Online Versandhäuser prüfen zu wenig (allerdings sind hier Sensibilisierungseffekte erkennbar)

www.idprotection.eu

DIE FOLGEN

- finanzieller Verlust
- geschädigte Kreditwürdigkeit
- Verlust rechtlicher Ansprüche
- Einträge in Strafregister
- erheblicher Aufwand für die Behebung des entstandenen Schadens
- Schwierigkeiten beim Wahrheitsbeweis
- Imageverlust


European Commission
VISIT
Geschädigte berichten
www.idprotection.eu

7 Regeln zur Prävention

- Sichere und unterschiedliche Passwörter - Passphrasen
  A96hieVbdA - Am 9.6. halte ich einen Vortrag bei der ASW
- Sicherungssysteme auf dem neuesten Stand (Firewall, Antivirus, Software updates etc)
- Vorsichtiger Umgang mit sozialen Netzwerken
- Shredder und Shredder Software benutzen
- Vorsicht bei “Super-Angeboten” im Netz
- Erstatten Sie Anzeige, lassen Sie sich nicht „abwimmeln“.
- Kontaktieren Sie Finanzinstitute/Unternehmen, bei denen Sie Konten oder Kundenkarten mit Bezahlfunktion haben und die betroffen sein könnten - aber Vorsicht:
  Denken Sie an KUNO

KUNO schiebt den Riegel vor!

KUNO - Abkürzung für "Kriminalitätsbekämpfung im unbaren Zahlungsverkehr unter Nutzung nichtpolizeilicher Organisationsstrukturen"

Ein simples aber wirkungsvolles Sperrsystem, von Polizeibehörden und Wirtschaft entwickelt wurde, um Zahlungen per Debitkarte im elektronischen Lastschriftverfahren – also mit Unterschrift – sicherer zu gestalten

Banken und Sparkassen informieren den Einzelhandel über gesperrte Karten seit Ende 2006 nur noch im Rahmen des Girocard-Verfahrens (Zahlung mit Karte und PIN)

Im Lastschriftverfahren können die gemeldeten Karten weiterhin zur Zahlung verwendet werden

Kontoinformationen polizeilich angezeigter Kartendiebstähle/-verluste werden von den Sicherheitsbehörden an eine zentrale Meldestelle übermittelt

Daten werden an die angeschlossenen Handelsunternehmen weitergegeben

www.idprotection.eu

Hacken - nicht's ist leichter

Hacken - nichts ist leichter

www.idprotection.eu


European Commission
VISIT
Victim Support for Identity Theft
SAVE THE DATE:
München, 3. November 2016
Internationale Konferenz zum Thema
Unsere Kontaktdaten:
Stephan Lehmann
Result Group GmbH
Head of Brussels Office
11, Square Ambiorix
1000 Brussels, Belgium
Mail: lehmann@result-group.com
Jürgen Kempf
Result Group GmbH
Head of Forensic Services
Am Grundwassersee 1
82402 Seeshaupt/Starnberger See
Mail: kempf@result-group.com
www.idprotection.eu
VISIT

Wie Drohnen die „Lufthoheit“ über Unternehmensinformationen bedrohen

Christian Janke, European Aviation Security Center

Was sind zivile „Drohnen“ heutzutage und was können sie leisten?

Zivile Drohnen

- Günstig und einfach zu erwerben
- Keine Pilotenausbildung notwendig
- Schnell, wendig und leistungsstark
- Zahlreiche Aufnahmefunktionen
- Echtzeitdatenübertragung
- Hersteller meist China und USA

Situation in Deutschland - **privat**

„Flugmodelle mit einer höchstzulässigen Startmasse über 25 Kilogramm; unbemannte Luftfahrzeuge, die in Sichtweite des Steuerers ausschließlich zum Zweck des Sports oder der Freizeitgestaltung betrieben werden" Luftverkehrs-Zulassungs-Ordnung (LuftVZO)

- Zahlreiche Hobby- und Freizeitflieger
- Offizielle und inoffizielle Flugplätze
- Häufig nicht über Privathaftpflicht abgedeckt
- Wenig Wissen über Rechtslage

Situation in Deutschland - **kommerziell**

- Sehr freies und liberales System – nur wenige Verbote
- Keine Pilotenlizenz, Zertifizierung des Geräts oder Firmennachweis erforderlich
- Bundesländer erteilen Aufstiegsgenehmigung
- **Fliegen nur ferngesteuert und in Sichtweite**
- Gefährdung ausschließen, z.B. nicht über Menschen

Drohnen und Missbrauch

Drohnen und Missbrauch

Privat oder kommerziell:

Industriespionage durch optische, akustische und EM- Aufklärung

Eindringen in den räumlich- gegenständlichen Bereich der privaten Lebensgestaltung Dritter (Persönlichkeit, Urheberrecht)

Organisierte Kriminalität:

Verbringung von Schmuggelware

Drogenkurierdienst

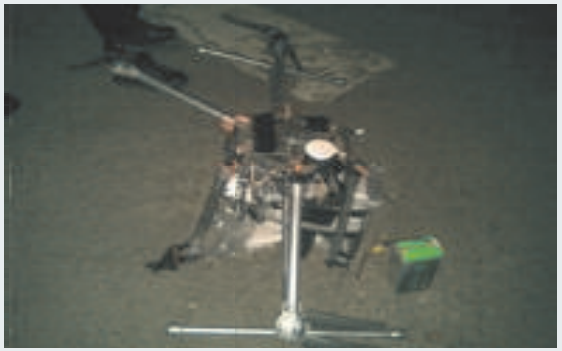
Einbringung von Gegenständen in Justizvollzugsanstalten

Terrorismus:

Verbringung von Gefahrstoffen in sicherheitsrelevante Bereiche (Sprengstoff)

Nutzung des RPAS als Rammelement (Luftverkehr)

Drohnen zur Lieferung



Neue Gefahren für Informationssicherheit und Informationshoheit

Wie groß ist die Gefahr?


Wie ist Schutz möglich?
easc
© 2016, EASC e.V.

Hochauflösende Kameratechnik

Extreme Miniaturisierung


DJI Phantom 3 III Professional Quadrocopter mit 4K Kamera inkl. Copter Card 3-Achs Gimbal 12MP
1399,90€
In den Warenkorb
NEUHEIT 2015
© 2016, EASC e.V.

Meldung vom April 2016

Wie kann man sich schützen?

Detektion

- akustische oder optische Sensoren
- Radar
- Frequenzbandüberwachung
- Laserschranken
- Achtsamkeit des Personals

Passive und aktive Abwehrmaßnahmen

- Bauliche Maßnahmen (Netze)
- Technische Verfahren
- Signal- Jamming, GPS Spoofing, Abfang-Drohnen
- zahlreiche weitere Möglichkeiten aus dem militärischen Bereich
- Kontrollierte Zwangslandung (Rechtsgüterabwägung)
- Gefahr am Boden durch Absturz

Anforderungen an Schutzsysteme

1. zivile Dimensionen in den Parametern Leistungsaufnahme, Emissionsrate im EM Spektrum, Gewicht, Mobilität und Preis (!)
2. Sensor-Fusion
3. Compliance mit Datenschutzgesetzgebung (Bildaufnahmen)
4. Verfügbarkeit und Funktionalität

- Zahlreiche Anbieter bereits auf dem Markt vorhanden
- Qualität und Funktionalität muss getestet werden

Kann man Drohnen auch sinnvoll nutzen?

Nutzung von Drohnen durch Unternehmen

- Erstellung von Echtzeit – Lagebildern
- Detektion von Bewegungen
- Baufortschrittsdokumentation
- Detektion von langfristigen Soll-Ist Veränderungen
- Transport innerhalb des Werksgeländes
- Brandschutz
- Notfalleinsatz

Unbequeme Wahrheiten

- Zivile Drohnentechnologie hat militärische längst erreicht
- Auch günstige Geräte können autonom und weit fliegen (5-10 km)
- Live-Bild-Datenübertragung zur Bodenstation oder direkt ins Internet möglich
- es gibt keine Registrierung von Kauf, Verkauf oder Inbetriebnahme
- Kaum Vorwarnzeit
- Gegenmaßnahmen müssen abgewogen werden
- Wirtschaftliche Nutzung von Drohnen wird voranschreiten
- Neubetrachtung von Datenschutz, Privatsphäre und Informationssicherheit

Vielen Dank für Ihre Aufmerksamkeit!

Christian Janke

Ausblick

- Kennzeichnung oder Registrierungszwang?
- Europäische Harmonisierung
- Information der Bürgerinnen und Bürger über aktuelle und geplante Flüge
- Neuerfindung von Datenschutz und Privatsphäre
- Forschungsprojekte zu Gefahrenabwehr

Andere Ideen...

Der deutsche Journalismus: Auf der Suche nach der Wahrheit oder einer möglichst großen Quote

Paul Elmar Jöris, WDR

Anrede

Es ist in den letzten Monaten Mode geworden, die Medien – Zeitungen, Zeitschriften, Radio und Fernsehen - pauschal als „Lügenpresse“ zu beschimpfen. Daran werde ich mich nicht beteiligen. Es geht auch überhaupt nicht um das bewusste Verbreiten unwahrer Meldungen, also um das „Lügen“, es geht ebenfalls nicht um Meinungsmache oder Manipulation. Alle, die glauben, dass es in den Verlagshäusern oder Rundfunkanstalten irgendwelche Finsterlinge gäbe, die im Geheimen die Drähte ziehen, damit ihre geknechteten Redakteurinnen und Redakteure die Unwahrheit und nichts als Unwahrheit berichten, allen, die das glauben, denen kann ich leider nicht helfen. Abseits dessen aber gibt es sie tatsächlich, die Berichterstattung, die unzufrieden macht, die mehr Fragen aufwirft, als Antworten gibt. Die oberflächlich ist und Tiefe vermissen lässt.

Ich bin ja beides: Journalist und Medienkonsument. Und es geht mir da – vielleicht wie vielen von Ihnen – mir fehlt immer häufiger etwas. Es geht mir vor allen Dingen darum, auf einige strukturelle Schwächen in den Medienunternehmen hinzuweisen, die zu einer unbefriedigenden Berichterstattung führen. Dies ist vor allen Dingen immer dann der Fall, wenn es um komplizierte Sachverhalte geht.

Ich hätte Ihnen im Gegenteil gerne von gut ausgestatteten Redaktionsstäben berichtet, von Archiven, die komplett digitalisiert sind und auf Stichwort alles Wissen in Schrift, Ton oder Bild liefern können. Ich hätte ihnen auch gerne erzählt, wie viel Zeit ein Fachredakteur darauf verwenden kann, sich ausschließlich mit seinem Thema zu befassen und schließlich hätte ich gerne von der unerschöpflichen Größe der Reise- oder Sachmitteletats geschwärmt. Aber leider ist die Wirklichkeit nicht nur viel prosaischer, sondern die Wirklichkeit sieht vollkommen anders aus.

Ich will hier nicht auf die Ursachen eingehen, denn hier geht es nicht um Medienpolitik, sondern ich will eine Skizze entwerfen, wie es um die fachpolitische Berichterstattung bestellt ist. Sämtliche Medien erlebten seit den 90er Jahren des vergangenen Jahrhunderts eine Reihe von Sparwellen. Kosten mussten gesenkt und Stellen eingespart werden. Die Etats für Recherchen wurden drastisch beschnitten. In schwindendem Umfang haben die Redaktionen genügend Personal, um sich kontinuierlich und intensiv mit den wichtigen politischen, wirtschaftlichen und gesellschaft-

lichen Entwicklungen zu befassen. Die Arbeit in den Redaktionen ist in einem ungeheuer großen Maß verdichtet worden. Früher war es üblich, dass jeder Redakteur nicht nur seine „Seite“ oder seine Sendung machte, sondern auch sich kontinuierlich mit einem Thema beschäftigte. Die Beratungsfirmen, die die Arbeit in den Redaktionen rationalisieren sollten, haben abgebaut, so ließen sich Stellen sparen. Auch bei den Reportern und Korrespondenten, die die Berichte liefern, wurden Stellen gestrichen. Ein Reporter muss jetzt über zwei oder drei höchst unterschiedliche Themen am Tag berichten. Er hat nicht mehr die Zeit sich in jedes Thema wirklich einzuarbeiten.

Wenn ein Thema plötzlich dominant wird, sei es die Banken- und Finanzkrise, Fukushima oder Terrorismus, dann wird durch Handauflegung ein Kollege zum „Experten“ ernannt. Folge der Sparmaßnahmen ist eindeutig ein Rückgang der Kompetenz.

Mittlerweile gibt es eine Reihe von Rechercheverbünde oder Expertenpools. Wenn ich beispielsweise an die Veröffentlichung der Panama-Papers denke, so komme ich zu dem Ergebnis, dass diese Veröffentlichungen zeigen, was Aufgabe von Journalisten in einer Demokratie ist, aber mir geht es nicht um solche Skoops, sondern ich will, dass die regelmäßige Berichterstattung über das politische und gesellschaftliche Geschehen ausführlicher und auch kritischer ist. Weniger Sensation, aber mehr tagtägliche Substanz.

Woran liegt das? Das hat etwas mit Konkurrenz zu tun. Die privaten Hörfunk- und TV-Sender haben vorgemacht, wie man mit seichten, preisgünstigen Sendungen, Geld machen kann.

Zunächst waren die privaten Rundfunk- und Fernsehveranstalter sehr erfolgreich und nahmen den öffentlich rechtlichen viele Hörer und Zuschauer ab. Dabei konzentrierten sich die Privaten auf ein Publikum bis zu einem Alter von 49 Jahren. Das hängt mit der werbenden Wirtschaft zusammen, die an einem Publikum unter 50 Jahren interessiert ist. Im Hörfunkbereich reagierte man darauf mit einer strengen Formatierung der Programme. Ich will Sie hier nicht mit Einzelheiten langweilen. Nur die Folge für den Berichterstatter, den Reporter oder Korrespondenten ist, dass er fast in keinem Programm Platz hat, um ein Thema ausführlich darzustellen. ARD-Sammelangebote, also ein Beitrag, der von einem Sender der ganzen ARD zur Verfügung gestellt wird, das ist das tägliche Brot der aktuelle Berichtssendungen im Hörfunk, dieser Beitrag hat eine Länge von maximal 2 Minuten und 30 Sekunden. (das sind ungefähr 2.500 Zeichen mit Leerzeichen also anderthalb Normseiten). Für Korrespondentengespräche räumt eine Redaktion auch schon einmal 3 – 4 Minuten ein. Mehr meint man heute einem Hörer und seiner Konzentrationsfähigkeit nicht

zumuten zu können. Für die Printmedien und das Fernsehen gelten die gleichen Überlegungen. Nachrichten im Internet dürfen nicht länger als drei oder maximal fünf Zeilen sein. Wer mehr lesen will muss die die Meldungen anklicken.

Der Erfolg einer Redaktion wird ausschließlich an der Quote gemessen. Das gilt für alle. Entscheidend ist, wie viele Menschen eine Zeitung lesen oder eine Sendung hören oder sehen. Das wird ständig geprüft und führt auch sehr schnell zu Konsequenzen. Bei Nachrichtenagenturen wird beispielsweise Tag für Tag ermittelt, inwieweit sich die Meldung eines Korrespondenten durchgesetzt hat. Wer immer wieder Meldungen verfasst, die weniger abgedruckt werden, als die des Konkurrenten, wird nicht lange auf seinem Posten bleiben.

Diese Entwicklungen sollten Sie im Hinterkopf haben, wenn Sie z. B. über das Thema Medien und internationaler Terrorismus reden. Die Zahl der Journalisten, die sich regelmäßig und immer wieder mit dem Thema befasst, ist geringer geworden. Vielmehr als ein Dutzend finden Sie in den deutschen Medien nicht. Dazu gehören dann auch die „Terrorismusexperten". Ich berichtete für den ARD-Hörfunk über die Terrorismusprozesse in Düsseldorf (Kofferbomberverfahren, Sauerlandverfahren, sowie den NSU-Prozess in München). Bei der Prozesseröffnung in Düsseldorf, bei den Plädoyer und der Urteilsverkündung war die Pressebank voll. An allen anderen Tagen, waren die Agenturen vertreten – die Kollegen mussten spätestens mittags gehen, weil sie noch über andere Prozesse berichteten. Der Kölner Stadtanzeiger und die Bildzeitung war dort vertreten, die Süddeutsche Zeitung schickte häufig einen Korrespondenten, Spiegel online war da und sonst niemand. Die Düsseldorfer Büros der Landeskorrespondenten sind so verkleinert worden, dass sie einen so langen Prozess nicht mehr wie früher verfolgen können und Berichte über die einzelnen Prozesstage bekommen sie nur ins Blatt oder ins Programm, wenn etwas „passiert". Eine Reihe der Berichterstatter arbeitet auf Honorarbasis. Das bedeutet, dass sie nur für abgelieferte Beiträge bezahlt werden. Allein aus diesem Grund müssen sie so zuspitzen, dass sich – wenn ich bei dem Beispiel bleiben darf – die Aussage eines der Angeklagten im Düsseldorfer Sauerlandprozess durchsetzen kann.

Das Publikum der öffentlich-rechtlichen Fernsehveranstalter wird immer älter. Zuschauer unter 49 Jahren schalten diese Programme immer seltener ein. Die Jüngeren schauen private Programme und zunehmend gar kein Fernsehen. Wenn sie sich informieren, dann im Internet. Dazu werde ich gleich noch etwas sagen.

Das Vordringen der privaten Rundfunk- und Fernsehveranstalter führte zu einer Änderung der Berichterstattung aller Medien. Es gibt überall eine

eindeutige Entwicklung zu einem Boulevardjournalismus. Das bedeutet im Einzelnen:

1. Politik gilt allgemein als langweilig. Eine Emnid-Untersuchung im Auftrag des Bayrischen Rundfunks zeigt übrigens, dass diese Annahme gar nicht stimmt. Das Publikum will informiert werden. Das gilt übrigens über alle Altersgruppen.
2. Die Berichte werden kürzer. In den Zeitungen gibt es immer wieder neue Layouts, die „luftiger" und damit „leserfreundlicher" werden und zur Folge haben, dass die einzelnen Berichte oder Kommentare kürzer werden.
3. Die Darstellung wird zugespitzt. Als berichtenswert gilt eigentlich nur der Skandal. Ich mache mir keine Illusionen über die Qualität des öffentlichen Dienstes und der privaten Wirtschaft. Da läuft immer wieder etwas schief, was Medien aufgreifen müssen, aber es läuft nicht so viel schief, dass Sie jeden Tag einen wirklichen Skandal haben. Da muss man dann etwas „Gas" geben und so kommt es dann zum Alarmismus der Medien. Dabei findet dann auch eine schleichende Umbewertung der Ereignisse statt. Dazu ein Beispiel: In der Theorie werden unterschiedlichen gesellschaftlichen Interessen, im parlamentarischen Prozess zum Kompromiss ausgeglichen. Das ist der positive Kern des Parlamentarismus. Doch wie stellen wir diese Suche nach dem Kompromiss dar? Zunächst einmal hat der Begriff „Kompromiss" allein schon einen schalen Beigeschmack und die Suche nach ihm, wird in allen Medien als „Streit" bezeichnet. Das, was die Stärke unseres parlamentarischen Systems ausmacht, wird mit einem negativen Vorzeichen versehen.
4. Man konzentriert sich auf das Ereignis eines Tages.
   Ich will ihnen das einmal an einem konstruierten Beispiel erklären. Wenn der Präsident des Bundeskriminalamtes ein Pressegespräch über die Gefahren des internationalen Terrorismus macht, dann konzentriert sich die Berichterstattung auf diesen einen Punkt. Und der wird zugespitzt: *Wie gefährlich ist heute S-Bahn-Fahren? Terroristen wollen deutsche Züge in die Luft sprengen. Sind die Behörden machtlos?* Wenn drei Tage später der Bundesbeauftragte für den Datenschutz am BKA-Gesetz Kritik übt, konzentriert sich die Berichterstattung auf seine Kritik: *Wie sicher sind meine persönlichen Daten? Kann ich mein Tagebuch noch im Computer speichern?* Eine Verbindung zwischen den Themen „Sicherheit" und „Datenschutz" wird nicht mehr hergestellt. Eine Abwägung findet kaum statt.

> Die Konzentration auf ein einzelnes Ereignis führt dazu, dass Zusammenhänge nicht mehr erkannt werden. Im Sommer vergangenen Jahres berichteten sämtliche Zeitungen – in den elektronischen Medien sah das ähnlich aus – auf der ersten Seite darüber, dass das Bundesamt für Verfassungsschutz nun Haushaltsmittel bekommt, um die sozialen Netze verstärkt zu beobachten. Dies wurde problematisiert und in einigen Fällen skandalisiert. In denselben Ausgaben gab es weiter hinten im Blatt Berichte, – sie gingen auf eine Information des Bundesamtes zurück – dass man festgestellt habe, dass der IS mittlerweile über die sozialen Netze gezielt Nachwuchswerbung betreibt. Dies wurde mit konkreten Beispielen belegt. Nur eine Verbindung zwischen den beiden Themen – verstärkte Überwachung sozialer Netzwerke und gezielte Nachwuchswerbung des IS in den sozialen Netzwerken wurde nicht gezogen.

Womit wir, wie ich Ihnen schon angekündigt habe, im Internet gelandet sind. Mit der wachsenden Bedeutung des Internets als Massenmedium haben sich die Probleme in mehrfacher Hinsicht verschärft. Die Verlage haben noch keinen wirklich überzeugenden Weg gefunden, mit dem Internet Geld zu machen. Es wird insgesamt schwieriger mit gutem Journalismus Geld zu verdienen. In den USA kann man die dramatischen Folgen beobachten. Renommierte Redaktionen müssen Leute entlassen, ganze Regionen haben keine Zeitungen mehr. Geld wird im Internet mit den Suchmaschinen verdient, nicht mit den Inhalten. Journalisten waren immer die Schleusenwächter der Informationsflut: Durch Auswahl der Nachrichten und Berichte und ggf. die Kommentierung boten sie eine Orientierung. Im Internet übernehmen Suchmaschinen diese Aufgabe. Die nachwachsenden Generationen informieren sich fast ausschließlich im Netz. Das trifft ganz bestimmt für die unter 29jährigen zu. Die Fachleute sind sich einig, dass das Medium der Zukunft die sogenannten Streaming Dienste sein werden. Eine Umfrage im Jahr 2015 hat laut Chip Online gezeigt, dass 76 Prozent aller Deutschen ab 14 Jahre zumindest gelegentlich Videos per Stream gucken. Und gezeigt hat sich auch, wer sich hauptsächlich im Netz informiert, will keine ausführlichen Darstellungen, sondern die aktuellsten Meldungen, die nicht länger als vier oder fünf Zeilen sind.

Und noch etwas: Die sozialen Netzwerke sind unschlagbar schnell, wenn es darum geht über ein Ereignis zu berichten. Allerdings sind sie unzuverlässig und fast nie überprüfbar. Zutreffende Beobachtungen von Augenzeugen stehen neben Gerüchten und verbreiten sich gleich schnell. Bei internationalen Konflikten haben das die Konfliktparteien längst erkannt und sind dazu übergegangen, Journalisten wirkungsvoll auszuschließen. Da bleiben Berichte von Unbekannten im Netz. Was sie berichten ist fast

nie nachprüfbar. Grundsätze eines professionellen Journalismus spielen keine Rolle: Es gibt kaum eine Unterscheidung zwischen Berichten und Kommentaren. Vom korrekten Zitieren will ich gar nicht reden oder von der Angabe von Quellen. Es wird anonym berichtet, Bilder gefälscht oder falsch zugeordnet. Gleichzeitig geraten die professionellen Medien unter Druck. Sie können nicht stundenlang den Wahrheitsgehalt überprüfen, wenn diverse Quellen im Internet mit Berichten auf dem Markt sind.

Wenn ich alles zusammenfasse, komme ich zu dem Ergebnis: Die Medien bilden heute das Geschehen, die Wirklichkeit nicht mehr angemessen ab. Dies gilt für die Berichterstattung über Terrorismus, Katastrophen oder Auslandseinsätze der Bundeswehr wie für alle anderen Fachgebiete der Politik.

Lassen Sie mich zum Schluss dieser sehr pessimistischen Darstellung, einen Blick in die Zukunft werfen. Geht das so weiter? Ja! Nur wenn eine hinreichend große Zahl von Menschen bereit ist, für gute Informationen auch gutes Geld zu bezahlen, kann sich das Blatt wenden. Dies kann ich allerdings derzeit nicht erkennen.

Pressemitteilung

Neue Gefahren für Informationssicherheit und Informationshoheit

10. Sicherheitstagung des Bundesamtes für Verfassungsschutz (BfV) und der Allianz für Sicherheit in der Wirtschaft e.V. - ASW Bundesverband in Berlin

Zahlreiche Experten aus den Sicherheitsbehörden und der Wirtschaft diskutieren heute auf der 10. Sicherheitstagung des BfV und des ASW Bundesverbands in Berlin über verschiedene Aspekte des Wirtschaftsschutzes. Im Fokus steht in diesem Jahr die Themen Desinformation im Internet, Identitätsdiebstahl, Drohnen und das Zusammenspiel von Unternehmenssicherheit und Unternehmenskommunikation.

Dazu erklärt der Vizepräsident des BfV Thomas Haldenwang:

„Heute geht es um die übergeordnete Frage, ob und wie wir in Zeiten von Digitalisierung und Globalisierung die Herrschaft über unsere Informationen behalten können.

Die zunehmende elekronische Vernetzung der Wirtschaft, Stichwort Industrie 4.0 und Internet der Dinge, eröffnet nicht nur der deutschen Wirtschaft, sondern auch fremden Nachrichtendiensten neue Chancen und Perspektiven. Deshalb brauchen wir eine neue „risk map" für die Gefahren des Cyberraums – einen Wirtschaftsschutz 4.0.

Ein Zusammenwirken von Staat und Wirtschaft ist hierbei unverzichtbar. Wir haben ein gemeinsames Ziel: ein höheres Schutzniveau für die deutsche Wirtschaft. Ein Baustein bildet die langjährige und vertrauensvolle Partnerschaft von BfV und ASW Bundesverband, die wir weiter intensivieren wollen."

Der Vorsitzende des ASW Bundesverbandes Volker Wagner unterstreicht:

„Unternehmenssicherheit und Informationssicherheit sind untrennbar miteinander verknüpft. Mit der wachsenden Vernetzung wachsen auch die Angriffsflächen und Schwachstellen. Unternehmen können sich diesen Herausforderungen nicht mehr erfolgreich alleine stellen. So müssen sich die Unternehmen untereinander enger austauschen und gleichzeitig besser mit den Behörden vernetzen.

Uns liegen dabei besonders kleine und mittelständische Unternehmen am Herzen. Diese müssen stärker sensibilisert und ihnen müssen dann auch Hilfestellungen geboten werden. Hierfür wollen wir – das Bundesamt für Verfassungsschutz und der ASW Bundesverband – unsere Aktivitäten noch enger verzahnen.

Ein zentrales Projekt ist dabei das Grundschutzhandbuch Wirtschaftsschutz, das im Sommer dieses Jahres fertiggestellt wird.

Gemeinsam arbeiten wir auch in der Initiative Wirtschaftsschutz zusammen und treiben die Internetplattform www.wirtschaftsschutz.info voran."

Weitere Informationen:

www.verfassungsschutz.de/Wirtschaftsschutz
www.wirtschaftsschutz.info
www.asw-bundesverband.de

Ihr Ansprechpartner im BfV:

Für Firmen, Verbände und Institute: wirtschaftsschutz@bfv.bund.de

Bildmaterial

Dr. Emily Haber, Staatssekretärin Bundesministerium des Innern

Volker Wagner, Vorstandsvorsitzender ASW Bundesverband

Thomas Haldenwang, Vizepräsident Bundesamt für Verfassungsschutz

Jan Wolter, Geschäftsführer ASW Bundesverband

Bodo Becker, Referatsleiter Wirtschaftsschutz, Bundesamt für Verfassungsschutz

Dr. Burkhard Even, Abteilungsleiter Spionageabwehr und Geheimschutz,
Bundesamt für Verfassungsschutz

Ronald Pofalla, Deutsche Bahn AG

Jürgen Kempf, Result Group, Vertreter des EU-Projektes V.I.S.I.T.

Christian Janke, Europen Aviation Security Center

Paul Elmar Jöris, WDR

Prof. Dr. Martin Grothe, CEO complexium GmbH

Mitarbeiter (-innen) Referat Wirtschaftsschutz Bundesamt für Verfassungsschutz

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Referat Wirtschaftsschutz
Merianstraße 100
50765 Köln

Tel.: +49 (0) 221/792-3322
Fax: +49 (0) 221/792-2915

wirtschaftsschutz@bfv.bund.de
www.verfassungsschutz.de
www.wirtschaftsschutz.info

Gestaltung und Druck
Bundesamt für Verfassungsschutz
Print- und MedienCenter

Bildnachweis
© Nmedia- Fotolia.com
© ASW Bundesverband und BfV

Stand
Oktober 2016

initiative
wirtschaftsschutz

Gemeinsam. Werte. Schützen.

www.wirtschaftsschutz.info