© BUNDESWEHR/BIER

Entladung in Bremerhaven und Verladung auf der Eisenbahn

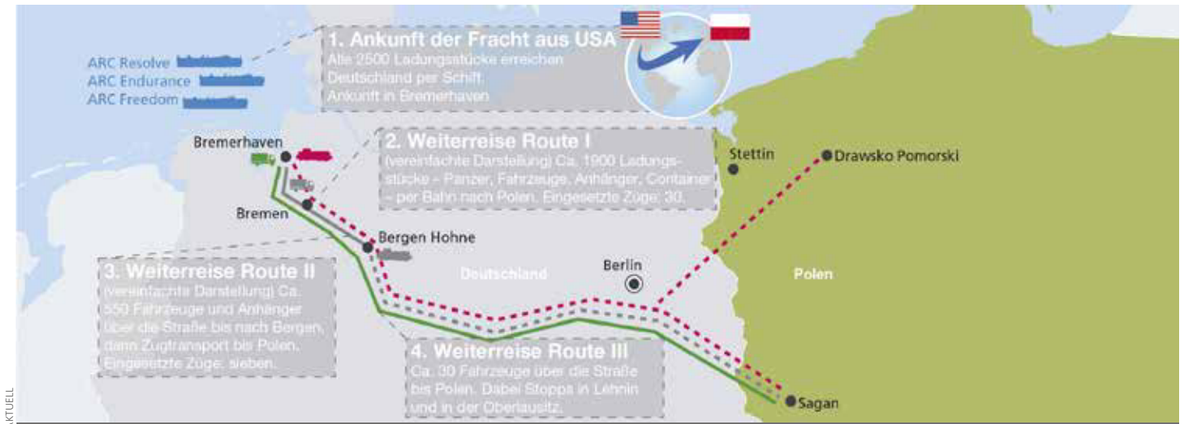
der baltischen Staaten mit dem polnischen NATO-Partner verbinden und das Territorium der russischen Exklave Kaliningrad von Weißrussland trennen.

/ Seit April 2014 haben die US-Streitkräfte verstärkt multinationale Trainings- und Sicherheitskooperationen mit Verbündeten und Partnern in Osteuropa durchführt.

/ Diese multinationale Trainings- und Sicherheitszusammenarbeit findet in Estland, Lettland, Litauen, Polen, Rumänien, Bulgarien und Ungarn statt. Diese Ausbildungsveranstaltungen verbessern die Interoperabilität, stärken die Beziehungen und das Vertrauen zwischen den alliierten Armeen, tragen zur regionalen Stabilität bei und sollen das US-Engagement gegenüber der NATO zeigen.

/ Über das Verhalten der Trump-Administration im Bereich der Atlantic Resolve kann derzeit nur spekuliert werden. Zwar meinte der US-Verteidigungsminister James Mattis beim Treffen mit seinen Amtskollegen in Brüssel: „Die USA stehen felsenfest zu Artikel 5 und zu unserem gegenseitigen Beistand." Doch noch am Vortag war sein Drängen auf höhere Verteidigungsausgaben der europäischen Bündnispartner vielfach als Drohung, gar als Ultimatum verstanden worden.

/ Die NATO verfolgt eine Doppelstrategie gegenüber Russland. Einerseits zeigt sie ihre militärische Stärke durch Truppenstationierungen und Manöver in den östlichen Bündnisstaaten und andererseits setzt sie auf Gespräche mit Moskau. Russland stationierte drei vollständig ausgestattete Brigaden, Flugabwehrsysteme S-400 „Triumph" und ballistische Raketen „Iskander-M" in Kaliningrad. (Red.)



© BW-AKTUELL

US-Army-Verlegung quer durch Deutschland

Internet der Dinge – Neue Herausforderungen für den Sicherheitssektor

MAJOR HERBERT SAURUGG, MSC

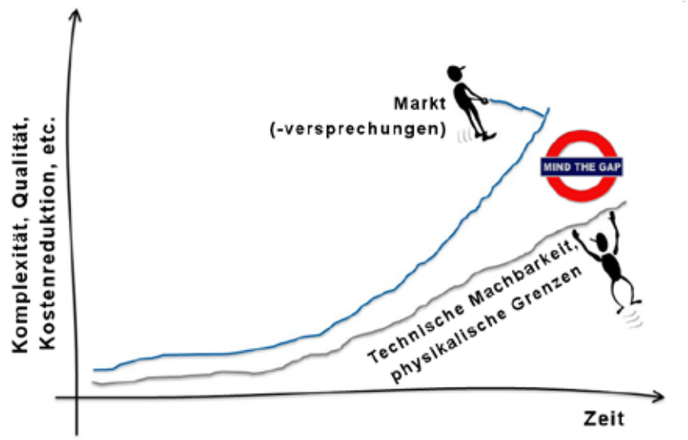
Digitalisierung, Internet der Dinge, Industrie 4.0, Smart Cities, Smart Grids, Smart Homes, Deep Learning, Predictive Maintenance, Big Data ... an neuen Schlagwörtern und damit verbundenen Versprechungen mangelt es nicht. Alles soll noch besser und umfassender vernetzt werden. Die genannten Zahlen, wie viele Dinge in den nächsten Jahren unter dem Schlagwort „Internet der Dinge" online gehen sollen, überschlagen sich laufend. Gleichzeitig eskalieren auch die damit verbundenen Sicherheitsprobleme mit erwartbaren weitreichenden Auswirkungen. Grund genug, um einmal hinter die Kulissen zu blicken und mögliche Ableitungen für den Sicherheitssektor zu treffen.

/ Für viele Menschen und auch Entscheidungsträger haben die letzten beiden Jahrzehnte bereits genug Herausforderungen geschaffen, die vor allem auf die Verbreitung von Computern und die Vernetzung über das Internet zurückzuführen sind. Erst vor vier Jahren hat die deutsche Bundeskanzlerin gemeint, dass das Internet noch ziemlich Neuland für uns sei und somit auch so manche negative Überraschung berge. Bedenkt man, dass das für uns heute weitgehend selbstverständliche Smartphone gerade erst zehn Jahre alt geworden ist und welche Veränderungen damit verbunden waren, dann kann man sich nur schwer vorstellen, wie diese Entwicklung in den nächsten Jahren weitergehen könnte. Eines scheint jedoch fix: Die Geschwindigkeit bei den Veränderungen dürfte nicht abnehmen, ganz im Gegenteil.

Komplexitätslücken

Aus systemischer Sicht drängt sich hier leider der Vergleich mit einem medizinischen Krebs auf, dessen Wachstumserfolg zur Selbstzerstörung führt. Auch ein anderer Vergleich passt hierher: Aus der jüngsten Mayaforschung ist bekannt, dass wahrscheinlich die hochentwickelte (Wasserversorgungs-) Infrastruktur der Mayas ein Mitgrund für den Untergang dieser Hochkultur war, da es zu einer mehrjährigen Dürreperiode kam und es für diesen Fall keine Rückfallebenen gab und damit das hohe Niveau der (Infrastruktur-) Versorgung nicht aufrechterhalten werden konnte. Auch die Warnung vor steigenden Komplexitätslücken des in Wien lebenden Komplexitätsforschers John Casti, der unter anderem bei der Entwicklung des Internets in den 1970er Jahren mitgewirkt hat, verhallen weitgehend ungehört.

/ Komplexitätslücken entstehen, wenn Systeme unterschiedlicher Komplexität miteinander interagieren: etwa zwischen der steigenden technischen Vernetzung und Abhängigkeit sowie uns Menschen, mit den daraus resultierenden Folgen umgehen zu können. Jede Komplexitätslücke tendiert zum Ausgleich: entweder durch eine Komplexitätsreduktion oder -erhöhung, oder wenn das nicht ausreicht oder rasch genug erfolgt, durch Kollaps, Chaos und Neuorganisation („Schöpferische Zerstörung"). John Casti bezeichnet derartige strategische Schockereignisse als Extreme-Events (X-Events), von Menschen selbst geschaffene Ereignisse, die unser Zusammenleben nachhaltig verändern können, wie etwa durch ein Blackout oder einen weitreichenden Internetausfall (siehe hierzu auch die Beiträge in „Der Offizier" 3 und 4/2015).



... in the end, it was this very complexity which helped bring the system down

Dieser etwas heftigere Einstieg ist notwendig, um besser verstehen zu können, warum eine kritische Auseinandersetzung mit den eingangs angeführten Schlagwörtern und Hype-Themen notwendig ist. Denn mit all diesen Themen ist eine weitere Zunahme der Vernetzung und damit auch Komplexität verbunden, die wir kaum bzw. nur in Nischenbereichen wirklich verstehen. Während es jedoch in den vergangenen Jahrzehnten vorwiegend um ›

eine datentechnische und virtuelle Vernetzung gegangen ist, natürlich durchaus mit Auswirkungen im Alltag, führen die nächsten Schritte zu einer massiven Vernetzung von Infrastrukturen. Das bedeutet daher, dass sich mögliche negative Auswirkungen auch weit über den bisher bekannten Datendiebstahl oder aktuell der erpresserischen Datenverschlüsselung („Ransomware“) auswirken werden. Bereits 2014 kam die Studie „Beyond Data Breaches: Global Interconnections of Cyber Risk“ zum Schluss: „The way in which the complexity of interconnected risks is assessed is painfully similar to how financial risks were assessed prior to the 2008 crash … in the end, it was this very complexity which helped bring the system down.“ Nun könnte man auch meinen, dass es schon immer Mahner gegeben hat, man denke hier nur an die Aussagen von Sokrates über die Jugend. Aber was hat das mit dem Internet der Dinge zu tun?

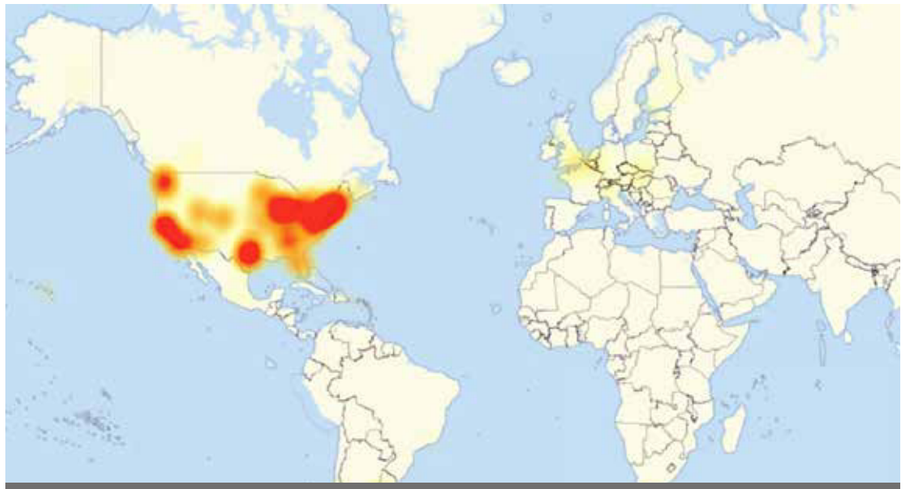
Das Internet der Dinge

Bisher kommunizierten vor allem Menschen mit anderen Menschen über Computer, auch wenn es etwa in der Automatisation oder im Infrastrukturbetrieb bereits eine Kommunikation Machine to Machine (M2M) gab. Computer waren noch irgendwie greifbar bzw. entsprachen unseren Vorstellungen von Computern. Durch die zunehmende Miniaturisierung von Computern verschwinden diese aber immer mehr aus unserem Blickfeld und verschmelzen mit den Gegenständen, daher spricht man auch gerne von Cyber-Physical-Systems oder vom Internet der Dinge (engl. Internet of Things, IoT). Hinzu kommt eine direkte Vernetzung mit dem Internet und damit auch, wenn keine gegenteiligen Vorkehrungen getroffen werden, eine weltweite Ansprech- und Manipulierbarkeit. Im positiven Fall kann damit die Heizung aus dem Büro eingestellt werden, im negativen Fall kann das auch jemand anderer tun.

/ Genau genommen sind dabei drei Ebenen im Spiel: Sensoren, wie etwa für die Temperaturmessung, dann die Steuerungsebene, welche im einfachen Fall eine Smartphone-App oder auch eine Big-Data- oder Cloud-Anwendung sein kann, und dann die Aktorik, also das Gegenstück, das auf die Steuerung in Folge der Sensorwerte reagiert, wie beispielsweise eine Heizung damit auf- oder abgedreht werden kann.

Predictive Maintenance

Warum Toaster und Kühlschränke mit dem Internet verbunden werden müssen oder sollen, erschließt sich wohl nur wenigen Menschen. Wo das Internet der Dinge aber auf jeden Fall Sinn macht, ist etwa im Bereich der Predictive Maintenance, also der vorausschauenden Wartung. Hier werden



© LEVEL 3

Die Karte des Netzwerkanbieters Level 3 zeigt zahlreiche Störungen am Freitag.

umfassende Daten gesammelt und Big-Data-Analysen durchgeführt, sodass man zukünftig die Wartung anhand konkreter Signale dann durchführen kann, wenn sie wirklich notwendig ist. Das bringt in gewissen Segmenten enorme Vorteile wie Kosten- und Ressourceneinsparungen. Auch im Infrastruktursektor, etwa bei der Erkennung von Lecks in Wasserleitungen, kann durch eine genauere Beobachtung und Auswertung viel Geld gespart werden. So gibt es mit Sicherheit eine ganze Reihe von sinnvollen und nützlichen Anwendungen, die trotz der in diesem Artikel sehr kritischen Betrachtung hervorzuheben und auch weiterzuverfolgen sind. Wie überall gibt es auch hier zwei Seiten, die es zu betrachten gilt. Daher richtet sich die Kritik auch nicht generell an diese Entwicklungen, sondern vielmehr an die unreflektierten Umsetzungen, die häufig nur vom Markt und Gewinnstreben getrieben werden.

Massiver Preisverfall und Miniaturisierung

Durch den massiven Preisverfall und die Miniaturisierung sind heute Anwendungen möglich, die noch vor wenigen Jahren nicht sinnvoll oder leistbar waren. Daher kommt es auch zu dieser rasanten bzw. exponentiellen Verbreitung von Geräten, wie digitalen Videorekordern, Web-Kameras, Heizungssteuerungen, Glühlampen, Fitness-Helfern bis hin zu Haushaltsgeräten wie Toastern, die mit dem Internet verbunden sind und weltweit angesprochen werden können. Hinzu kommt, dass hier zwar nicht besonders leistungsfähige Computer verbaut werden, sie aber kaum Sicherheitsmerkmale aufweisen, da sie ja einfach zu bedienen sein und andererseits nichts kosten sollen. Das führt dazu, dass wir nun zunehmend aus dem Internet ansprechbare Computer haben, die jedoch nicht wie in der Office-IT-Welt üblich upgedatet oder abgesichert werden können, weil weder die Hersteller (Kosten bzw. fehlendes Know-how) noch die Konsumenten (Einfachheit) ein Interesse daran haben. Jeder IoT-Computer ist für sich betrachtet auch nicht wirklich besonders sicherheitskritisch, sieht man von den möglichen Datenschutzverletzungen ab. Wenn es jedoch jemand darauf anlegt, wie im vergangenen Herbst bereits umfassend geschehen (siehe „Der Offizier“ 4/2016), und die Fähigkeit dieser Einzelcomputer bündelt, kann er eine sehr wirkungsvolle Waffe generieren und andere kritische Systeme zum Ausfall bringen. So kam es etwa an der Ostküste der USA zu teilweisen mehrstündigen IT-Ausfällen, durch eine Angriffsquantität, die man bisher noch nicht gesehen hatte.

/ Die Besitzer der Angriffswerkzeuge bzw. die Mitverursacher haben von dem wahrscheinlich nichts mitbekommen, außer vielleicht in Medienberichten über die Auswirkungen. Einmal mehr ein Beispiel für „kleine Ursache, große Wirkung“ oder „Nicht-Linearität“, zwei wesentliche Kennzeichen von komplexen Systemen.

Ihr Smart-Home wird zum Opfer

Die Manipulation kann aber auch im Kleineren passieren, wie zuletzt, wo bekannt wurde, dass neue Smart-TVs, also Fernsehen, die direkt mit dem Internet verbunden sind, von sogenannter „Ransomware“ oder Verschlüsselungs-Schadsoftware mit einer Lösegeldforderung lahmgelegt wurden.

© RANSOMWARE HTTP://WWW.SYSTEM-TIPS.NET/WP-CONTENT/UPLOADS/2013/06/LPD-BMI-VIRUS.JPG

/ In diesem Fall konnte der Hersteller eine Entsperrung vornehmen. Aber wie lange wird es dauern, bis findige Cyber-Kriminelle etwa Smart-Home-Anwendungen angreifen werden? Stellen Sie sich vor, Sie sind gerade auf Urlaub und die Smart-Home-Anwendung auf ›

© PIXABAY

© ANDREAS WASTIANY

ZUR PERSON

Herbert Saurugg, MSc, war 15 Jahre Berufsoffizier des Österreichischen Bundesheeres, zuletzt im Bereich IKT-/Cyber-Sicherheit. Seit 2012 beschäftigt er sich mit den möglichen Auswirkungen der steigenden Vernetzung und Komplexität, welche zu bisher kaum bekannten systemischen Risiken führen.
kontakt@saurugg.net,
www.saurugg.net

Ihrem Smartphone teilt Ihnen mit, dass sie gekapert wurde und Sie jetzt nicht mehr sicher sein können, was die Sensorik und Aktorik zu Hause wirklich macht. Sie haben aber die Möglichkeit, durch eine „kleine Spende" mit der virtuellen Währung Bitcoin den Spuk aufzuheben. Würden Sie zahlen? Wahrscheinlich würde der Angreifer sogar sein Versprechen einlösen. Würden Sie danach noch Ihrem Smart-Home vertrauen?

Ihr Infrastrukturbetreiber wird zum Opfer

Und jetzt stellen Sie sich das ganze Szenario so vor. Nicht Ihr Smart-Home wurde Opfer eines solchen Angriffs, sondern Ihr Infrastrukturbetreiber im Smart-Grid- oder Smart-City-Umfeld oder sogar das Krankenhaus, in dem Sie gerade versorgt werden. Das wäre zwar ein deutlich höherer Aufwand für den Angreifer, aber auch lohnender, und es ist nur eine Entwicklung, die konsequent weitergedacht werden muss. Die seit 2016 explosionsartige Zunahme von erpresserischen Verschlüsselungsangriffen auf Einzel-PCs verlagert sich gerade auf gezielte Angriffe von größeren Unternehmen und Netzwerken. So hat es etwa schon zahlreiche Krankenhäuser erwischt. Offenbar wurde mit den Massenangriffen das nötige Kleingeld für Weiterentwicklungen und den Zukauf von Experten erwirtschaftet.

Paradigmenwechsel

Wie der bekannte IT-Sicherheitsexperte Bruce Schneier es kürzlich ausdrückte, findet gerade ein fundamentaler Paradigmenwechsel statt: „We no longer have things with computers embedded in them. We have computers with things attached to them." Wir bauen gerade eine „Weltmaschine", ohne dass wir uns dessen wirklich bewusst sind bzw. die richtigen Denkansätze dafür haben. Wir versuchen, den damit verbundenen Problemen weiterhin mit den bisherigen, nur bedingt erfolgreichen Lösungen in der Office-IT habhaft zu werden, was nicht funktionieren wird. Daher sollten wir uns einmal mehr Albert Einstein zu Herzen nehmen, dass man Probleme nicht mit derselben Logik lösen kann, mit der diese verursacht wurden. So wie ein Eurofighter heute ein fliegendes Netzwerk ist und völlig andere Rahmenbedingungen erfordert, als etwa der Draken, so benötigen wir auch im Infrastruktur- bzw. Sicherheitssektor komplementäre Ansätze und Lösungen.

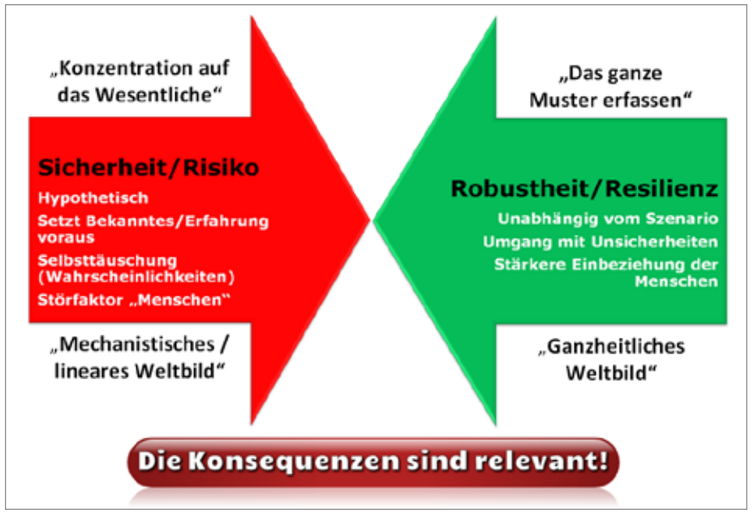
© PIXABAY

Fehlende Fachkräfte

Und hier scheitern wir derzeit vor allem an genügend Fachkräften. Denn wenn es schon schwierig ist, mangels entsprechender Fachexperten ein qualifiziertes Team für das Energie Computer Emergency Response Team (E-CERT), die sowohl die Office-IT als auch die Infrastruktur-IT verstehen, auf die Beine zu stellen, dann sind die Herausforderungen für eine nationale Cyber-Security oder Defence wohl um Dimensionen größer. Ganz abgesehen davon, dass das auch gleichzeitig bedeutet, dass es an den entsprechenden Fachkräften für den sicheren Betrieb mangelt, die eigentlich Zwischen- und Ausfälle verhindern sollten.

Cyber-Defence

Wer daher glaubt, dass diese Herausforderungen mit einer vermeintlichen Cyber-Defence bewältigt werden können, hat leider noch nicht verstanden, wie die neue Welt tickt. Man erinnere sich nur an das auch bei uns vor 15 Jahren intensiv diskutierte Thema „Network Centric Warfare" (NCW). Hat uns hier die Realität nicht auch von einer ganz anderen Seite eingeholt? Konnten wir unsere Überlegenheit irgendwo ausspielen? Zum Glück waren wir in keine kriegerischen Auseinandersetzungen involviert. Aber etwa die amerikanische Armee, der wesentliche Treiber hinter NCW, auch sie wurde durch missbrauchte Mobiltelefone in Form von Improvised Explosive Device (IED) überrascht. Wir wiederum wurden dafür von einer Migrationswelle überrumpelt, die in dieser Form ohne das Fluchtunterstützungstool „Smartphone" wohl nicht möglich gewesen wäre. Man denke nur daran, welche Fähigkeiten ein Smartphone heute mitbringt, von dem auch heute noch Soldaten oft nur träumen können. Aktuellstes Kartenmaterial, GPS, weltweite Kommunikationsfähigkeit, diverse Sensorik, Kameras, Echtzeit-Lagebild, und das alles zu geringen Kosten im Hosentaschenformat. Daher reicht es bei weitem nicht aus, wenn wir uns weiterhin in „Silos" organisieren, um mit einer vernetzten Realität und Angreifern zurechtzukommen.



Der Angreifer muss nur einmal erfolgreich sein ...

Und zu all dem kommt noch hinzu, dass ein Angreifer nur einmal, der Verteidiger aber jedes Mal erfolgreich sein muss. Und der Angreifer kann sich noch dazu alle Rahmenbedingungen selbst aussuchen, Zeit, Ort, Ziel ... denn er muss sich nicht an alte Denkmuster und starre Regeln halten bzw. die gehärteten Systeme angreifen, da auch wir völlig von den weniger geschützten zivilen Infrastrukturen abhängig sind (siehe Beitrag in „Der Offizier" 4/2016). Unsere rechtlichen und ethnischen Grenzen lassen sich nur bedingt ändern, da wir zum Glück in einem Rechtsstaat leben, aber die Denkmuster lassen sich ändern und es ist die einzige Chance, um mit den neuen Herausforderungen zurechtzukommen.

Asymmetrische Herausforderungen verlangen Maßnahmen auf Augenhöhe

Hier sollten wir von der dunklen Seite der Macht lernen, die in den letzten Jahren sehr augenscheinlich gezeigt hat, wie man durch Vernetzung und Kooperation sowie durch Flexibilität und Agilität sehr erfolgreich werden kann. Hier würde auch gleich das Thema „Fake News" und „Cyber-Manipulationen" dazupassen, was aber diesen Beitrag sprengen würde. Grundsätzlich ist das alles nicht neu, neu ist jedoch der Skaleneffekt durch die Vernetzung und die damit verbundene Geschwindigkeit und Dynamik. Neu ist auch, dass man sich nicht nur mehr auf den Einbrecher/Gegner aus der „Nachbarschaft" vorbereiten muss, sondern auf den besten Einbrecher, der von überallher kommen kann und einen auch noch dazu zum Mittäter machen kann.

Breite Angriffsflächen

Wir dürfen uns daher nicht wundern, wenn wir eine so breite Angriffsfläche bieten, dass diese auch ausgenutzt wird. Zu allem Überdruss kommt noch hinzu, dass die von uns geschaffene Komplexität nicht einmal mehr einen Angreifer benötigt, um uns selbst zu schaden. Leider waren wir bisher auch erfolgreich darin, immer erst dann Sicherheitsmaßnahmen zu ergreifen, wenn es bereits konkrete Vorfälle und Schäden gab. Man erinnere sich nur an die Hochwässer der vergangenen Jahre, Lawinenkatastrophen oder auch die Migrationswelle, immer haben wir zugewartet und nachher teuer repariert. Bei den absehbaren zukünftigen Infrastrukturausfällen könnte das jedoch fatal enden (siehe auch „Der Offizier" 3 und 4/2015).

Regeln und Regulation

Mit diesem Beitrag wurde versucht, das Wettrüsten zwischen Angreifer und Verteidiger, sofern solche überhaupt auszumachen sind, im Bereich Internet der Dinge etwas näher darzustellen. Nachdem weder die Hersteller / der Markt noch die Konsumenten wirklich ein erkennbares Interesse daran haben, für mehr Sicherheit zu sorgen, wird hier eine Regulierung bzw. die Vorgabe von Mindeststandards unumgänglich sein. Was derzeit für viele nur schwer vorstellbar ist, wird sich spätestens nach dem ersten schweren Zwischenfall ändern. So waren etwa viele Maßnahmen, die nach 9/11 gesetzt wurden, zuvor auch nicht vorstellbar gewesen. Klüger wäre es jedoch, sich bereits vorher mit diesem Thema auseinanderzusetzen und nicht dann im Schockzustand überzureagieren und das Kind mit dem Bad auszuschütten, wie wir das leider immer wieder erleben. Klar ist auch, dass eine nationale Regulierung völlig unzureichend ist und daher ein breiter internationaler Ansatz erfolgen muss. Das erfordert jedoch auch umfangreiche Fachexpertisen und vernetztes Denken, sonst könnte der Schuss leicht nach hinten losgehen.

/ Dieser Beitrag hat hoffentlich auch die Aussagen und Einwände in den bisherigen Beiträgen („Der Offizier" 3 und 4/2015 bzw. 4/2016) weiter untermauert bzw. die Notwendigkeit von einem neuen Sicherheitsdenken, das vor allem auf Robustheit und Resilienz fokussiert und eine bessere Vernetzung über Systemgrenzen hinaus vorsieht, verdeutlicht.

/ Es wäre auch nicht das erste Mal, dass der Gegner bzw. neue Technologien unterschätzt würden, was ja gerade zum kürzlich begangenen 150-Jahre-Jubiläum „Königgrätz 1866" passt. Daher zum Schluss eine auch für diesen Bereich gültige Weisheit von Sun Tzu: „Wenn du dich und den Feind kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten. Wenn du dich selbst kennst, doch nicht den Feind, wirst du für jeden Sieg, den du erringst, eine Niederlage erleiden. Wenn du weder den Feind noch dich selbst kennst, wirst du in jeder Schlacht unterliegen." ⚔

Eurofighter: Strafanzeige gegen zwei Airbus-Unternehmen

Das Bundesministerium für Landesverteidigung und Sport hat bei der Staatsanwaltschaft Wien eine Strafanzeige wegen des Verdachts auf arglistige und betrügerische Täuschung gegen die Airbus Defence and Space GmbH (vormals EADS Deutschland GmbH) und die Eurofighter Jagdflugzeug GmbH eingebracht. Die Republik Österreich, vertreten durch die Finanzprokuratur, hat sich dem Strafverfahren gegen die beiden Airbus-Unternehmen als Privatbeteiligte angeschlossen. Grundlage für die Sachverhaltsdarstellung mit Privatbeteiligtenanschluss sind die Ermittlungen der im Verteidigungsministerium 2012 eingerichteten „Task Force Eurofighter".

/ Aufgrund der Untersuchungen der „Task Force Eurofighter" geht das Ministerium in seiner Strafanzeige davon aus, dass die beiden angezeigten Airbus-Unternehmen die Republik Österreich seit 2002 sowohl über den wahren Kaufpreis als auch über die wahre Lieferfähigkeit und wahre Ausstattung der Eurofighter-Abfangjäger in betrügerischer Absicht getäuscht haben.

/ Verteidigungsminister Doskozil: „Ohne die betrügerischen Täuschungshandlungen der beiden Airbus-Unternehmen hätte sich die Republik Österreich im Jahr 2003 nicht für den Ankauf der Eurofighter entschieden. Auch der Vergleich vom Juni 2007 wäre nie zustandegekommen."

Republik Österreich fordert Schadenswiedergutmachung

Wolfgang Peschorn, Präsident der Finanzprokuratur: „Die Republik Österreich hat sich dem Strafverfahren gegen die beiden Airbus-Unternehmen angeschlossen." Der Schaden der Republik errechnet sich aus der Summe aus dem bezahlten Kaufpreis für 15 Eurofighter zuzüglich der Differenz aus den bislang angefallenen Betriebskosten für die Eurofighter im Vergleich zu hypothetischen Betriebskosten eines alternativen Flugzeuges abzüglich des heutigen Zeitwerts der 15 österreichischen Eurofighter. Der heute bekannte Schaden kann daher bis zu 1,1 Milliarden Euro betragen. Er steht jedenfalls mit zumindest 183,4 Millionen Euro fest, die die beiden Airbus-Unternehmen im Rahmen ihrer listigen Irreführung in den Kaufpreis eingepreist haben. Hinzu kommt der Schaden aus den zukünftig entstehenden Mehraufwendungen für den Betrieb des teureren Eurofighters, der heute noch nicht beziffert werden kann.

Betrug durch Täuschung über den wahren Wert des Kaufgegenstandes

Die Sachverhaltsdarstellung belegt, dass die beiden angezeigten Airbus-Unternehmen die Republik Österreich nie darüber aufgeklärt haben, in den Kaufpreis von 1,959 Milliarden Euro fast 10 Prozent, exakt 183,4 Millionen Euro, für Gegengeschäftskosten eingepreist zu haben. Dies, obwohl die Republik Österreich bereits in den ersten Ausschreibungsunterlagen von 2001 eindeutig verlangt hat, Kosten für die Abwicklung der geforderten Gegengeschäfte gesondert auszuweisen. Tatsächlich wurden die arglistig eingepreisten 183,4 Millionen Euro für legale, aber auch für kriminelle Gegengeschäftskosten verwendet. Sowohl die Staatsanwaltschaft München als auch die Staatsanwaltschaft Wien ermitteln in diesem Zusammenhang bereits seit Längerem.

Betrug durch Täuschung über den Kaufgegenstand

Die Beweislage der „Task Force Eurofighter" legt weiters nahe, dass die beiden angezeigten Airbus-Unternehmen der Republik Österreich seit 2002 die Lieferung eines Kaufgegenstandes versprachen und vertraglich zusicherten, obwohl sie zu dessen vertraglich vereinbarter Lieferung weder in der Lage noch willens dazu waren. Der 2007 abgeschlossene Vergleich zwischen der Republik Österreich und den Airbus-Unternehmen ändert nichts an der Strafbarkeit dieser Täuschungshandlungen.

Luftraumüberwachung gesichert

Unabhängig von der strafrechtlichen Aufarbeitung der Vergangenheit sei es aber die erste und wichtigste Aufgabe als Verteidigungsminister, die Sicherheit des Landes zu garantieren, so Doskozil.

/ Der Minister: „Die Luftraumüberwachung durch das Österreichische Bundesheer ist weiterhin sichergestellt. Unsere Luftstreitkräfte und unsere Piloten machen einen hervorragenden Job. Dazu brauchen sie leistungsfähige Abfangjäger. Ich bekenne mich zu 100 Prozent zur Aufgabe der Luftraumüberwachung durch das Österreichische Bundesheer." (Quelle: BMLVS)

© BUNDESHEER/ZINNER

Abfangjäger sichern den Luftraum über Westösterreich.

© BUNDESHEER/MILLER (2)

Die Radarstation am Salzburger Kolomansberg ist Teil des „Goldhaube"-Systems.

Luftraumüberwachungsoperation „Dädalus 2017"

Vom 17. bis 20. Jänner 2017 fanden in Davos-Klosters, Schweiz, die jährlichen Veranstaltungen des World Economic Forum (WEF) statt. Hierbei kommen international führende Politiker, Wirtschaftsexperten, Intellektuelle und Journalisten zusammen, um über aktuelle globale Fragen zu diskutieren. Den internationalen Standards entsprechend werden auch für diese Großveranstaltung Sicherheitsmaßnahmen in der Luft und am Boden vorgenommen. Da Davos nahe der österreichischen Grenze liegt, erging seitens der Schweiz das Ersuchen, den Luftraum in Österreich abzusichern. Zur Absicherung der jährlichen Veranstaltung führte das neu aufgestellte Kommando Luftstreitkräfte die Operation „Dädalus" durch. Entsprechend der bilateralen Vereinbarungen übernahmen die österreichischen Luftstreitkräfte die Überwachung des im österreichischen Luftraum liegenden Sektors der Flugverbotszone über Tirol und Vorarlberg.

/ Damit dies funktioniert, müssen die Militärluftfahrzeuge, technischen Systeme und das Fachpersonal reibungslos zusammenarbeiten.

Diese 5 Komponenten sorgten für einen sicheren Luftraum:

1) Die Eurofighter-Abfangjäger

Die Eurofighter sind die schnellsten und modernsten Flugzeuge der Luftstreitkräfte. Als „Polizei in der Luft" stellen sie in kürzester Zeit Sichtkontakt zum Eindringling her und beurteilen die Situation. Wenn nötig, fangen sie den Flieger ab, eskortieren ihn aus der Zone oder erzwingen seine Landung.

2) Das Radarsystem „Goldhaube"

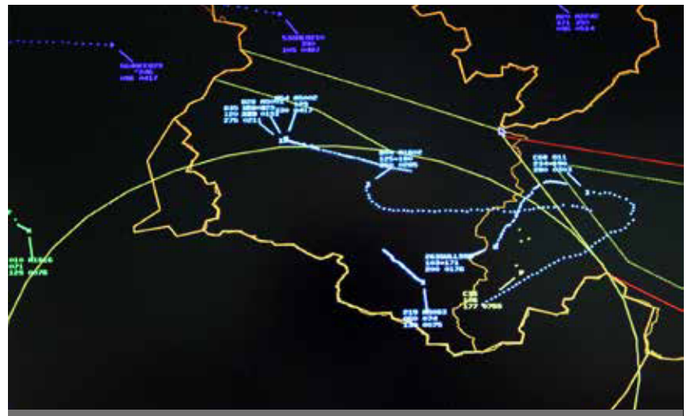
Das Luftraumbeobachtungs- und Führungssystem „Goldhaube" stellt sicher, dass eindringende Luftfahrzeuge geortet, identifiziert und gegebenenfalls abgefangen werden können. Mehrere Radarstationen blicken dabei weit über den heimischen Luftraum hinaus und erkennen Flugzeuge bereits lange, bevor sie über Österreich sind.

3) Flächenflugzeuge und Hubschrauber für Langsamflieger

Nicht jedes Privatflugzeug fliegt hoch und schnell. Flächenflugzeuge wie die PC-7 „Turbo Trainer" und Hubschrauber des Bundesheeres kümmern sich um Flieger, die langsam und oft in geringer Höhe in das Flugbeschränkungsgebiet eindringen.

4) Radarleitoffiziere

Die Soldaten des Radarleitdienstes beobachten den Luftraum rund um die Uhr. Von der Luftraumüberwachungszentrale aus führen sie mit Hilfe von Radar und Funk alle eingesetzten Flugzeuge. ›



Das Flugbeschränkungsgebiet über Tirol und Vorarlberg wird in verschiedene Sektoren unterteilt.