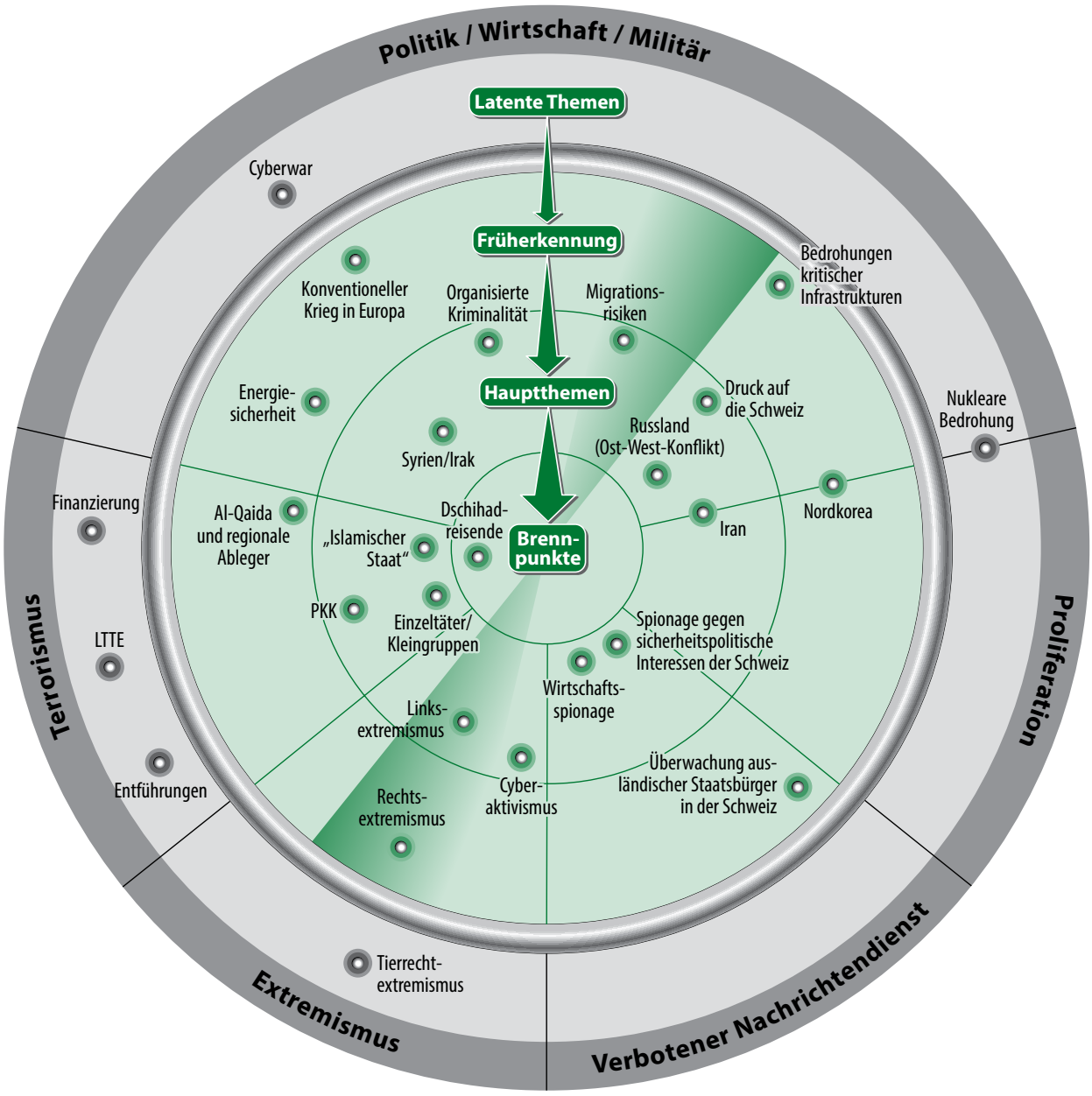
STA 60 info

Schweizerische Gesellschaft
Technik und Armee

Société suisse
Technique et Armée

Società svizzera
Tecnica e Armata

Societad svizra
Tecnica ed Armada



INHALT

03	STA-Herbstveranstaltung: «Weckruf gehört!»
05	Sicherheit in einer vernetzten Welt
11	60 Jahre Schweizerische Gesellschaft Technik und Armee (STA) – zweiter Teil: 1985-2014
14	Ein sicheres und autonomes IKT-Netzwerk für die Armee
19	Kurzgedanke: Big Data – Relevanz in allen Sphären
20	Industriespionage im digitalen Zeitalter

VORSTAND UND KONTAKTADRESSE

IMPRESSUM

Herausgeber	Schweizerische Gesellschaft Technik und Armee STA c/o Geschäftsstelle Kasernenstrasse 19, CH-3003 Bern
Layout	Esra Kunz
Druck	armasuisse
Kontakt	pascal.voeroes@ar.admin.ch
Auflage	600 Exemplare
Titelbild	Mit freundlicher Genehmigung des Nachrichtendienstes des Bundes (NDB) zeigt das Titelbild das Instrument Lageradar. Der NDB benützt dieses für die Darstellung der für die Schweiz relevanten Bedrohungen. Die abgebildete, öffentliche Version (vereinfacht und ohne vertrauliche Daten) führt die Bedrohungen auf, die im Arbeitsgebiet des NDB liegen, ergänzt mit den sicherheitspolitisch ebenfalls relevanten Punkten «Migrationsrisiken» und «organisierte Kriminalität». Zusätzliche Informationen finden sich im Lagebericht 2015 des NDB.

EDITORIAL

STA-Herbstveranstaltung: «Weckruf gehört!»

Leitgedanke der diesjährigen Industrieorientierung und STA-Herbstveranstaltung war «Sicherheit in einer vernetzten Welt». Der Anlass wurde dieses Jahr zum 13. Mal zusammen mit armasuisse, Swissmem und GRPM durchgeführt und verzeichnete mit über 200 Teilnehmenden einen Teilnehmerrekord.

Ein erneut hochkarätiges Referentenfeld aus Wissenschaft, Verwaltung und Armee führte aus, mit welchen Bedrohungen und Herausforderungen die Schweiz in einem vernetzten Umfeld zunehmend konfrontiert ist und wie diesen begegnet werden kann. Thematisiert wurden dabei die Anforderungen, welche eine zunehmende Digitalisierung und Vernetzung von Gesellschaft und Armee an die Technik und deren Benutzer stellt.

Einig waren sich im abschliessenden Podiumsgespräch alle Referenten: Es bedarf einer intensiven Information und Kommunikation, um die ganze Bevölkerung zum Thema «Sicherheit in einer vernetzten Welt» und vor allem deren Bedeutung bezüglich unserer Infrastrukturen wie Elektrizitäts- und Kommunikationsnetze, aber auch der ganzen logistischen Versorgung zu sensibilisieren. Ebenso klar wurde festgehalten, dass dabei der Armee als einziger strategischen Reserve eine zentrale Bedeutung zukommt.

Meine persönlichen Schlussfolgerungen des Tages:

- Das neue Nachrichtendienstgesetz wird dringend benötigt. Eigentlich unverständlich, dass eine in die Regierungsverantwortung eingebundene Partei das von verschiedenen Seiten erhobene Referendum massiv unterstützt.
- Es ist explizit festzuhalten, dass Europa seine digitale Souveränität verloren hat und hart an deren Wiedererlangung arbeiten sollte. Dass Europa heute sowohl in der Hardware als auch in der Software praktisch fremdbestimmt ist, hat sicher jeden Teilnehmer zum Nachdenken angeregt.
- Waren die 1990er und 2000er Jahre geprägt vom Glauben an eine hohe Friedensdividende nach dem Mauerfall, so wissen wir heute, dass uns wieder erheblich unruhigere Zeiten bevorstehen – nicht zuletzt geprägt durch den wiederaufflammenden Ost-/West-Konflikt, dem klaren Machtanspruch der Volksrepublik China sowie den grossen, zum Teil nicht mehr kontrollierbaren Migrationsströmen. Dem Statement eines der Referenten im Rahmen der Podiumsdiskussion, dass die in der Armee XXI angenommene Vorwarnzeit von 10 Jahren eventuell bereits abgelaufen sei, widersprach auf jeden Fall keiner der Anwesenden.

An dieser Stelle sei nochmals allen Referenten für ihre sehr engagierten und prägnanten Referate gedankt. Für mich waren sie effektiv ein Weckruf. Ich glaube die Teilnehmer haben ihn gehört.

Für mich erfreulich ist ebenfalls die Entwicklung bezüglich der Weiterentwicklung der Armee (WEA). In der gleichen Woche, in welcher die Herbstveranstaltung stattfand, beschloss die Sicherheitspolitische Kommission des Nationalrates mit sehr klarem Mehr, nun doch die Botschaft des Bundesrates vollumfänglich zu unterstützen. Ein Zahlungsrahmen von 20 Milliarden Franken und ein Bestand von 100 000 Armeeangehörigen kann nun mit sehr hoher Wahrscheinlichkeit umgesetzt werden.

Dies sind eindeutig positive Signale, dass man den Wert des Produktes Sicherheit wieder vermehrt zu schätzen beginnt. Vielleicht tragen dazu die aktuellen Situationen in der Ukraine, in Syrien und Irak mit dem Islamischen Staat (IS), aber auch die Anschläge des IS in Paris und generell die wachsende Terrorbedrohung in Europa zu diesem Umdenken bei. Sich rasch wandelnde Situationen zeigen, dass auch für die Schweiz folgende Prinzipien nach wie vor gelten:

- hohe Bereitschaft für verschiedenste Szenarien zeigen,
- robuste Mittel für rasche Interventionen zur Verfügung haben,
- nachrichtendienstlich à jour zu sein
- und last but not least, geschützte und gehärtete Kommunikationsnetze für alle Lagen zu haben.

Also heisst es jetzt, die Umsetzung der WEA mit den Kernelementen

- Erhöhung der Bereitschaft,
- Verbesserung der Kaderausbildung,
- Vollausrüstung der Einsatzverbände
- und Regionalisierung

zeitverzugslos an die Hand zu nehmen.

Sowohl als Staatsbürger als auch als Organisation wie die STA sind wir gefordert uns an diesen Diskussionen zu beteiligen und unsere Standpunkte nachhaltig zu vertreten.

EDITORIAL

Es muss uns gelingen, durch einen Schulterschluss von bürgerlicher Politik, Armee, Verbänden, Milizorganisationen und der Wirtschaft einer nachhaltigen und glaubwürdigen Sicherheitspolitik zum Durchbruch zu verhelfen.

Ich freue mich, Sie alle auch im Jahre 2016 an unseren Anlässen begrüssen zu dürfen.

Der Präsident der STA

Dr. Fritz Gantert

INDUSTRIEORIENTIERUNG UND HERBSTVERANSTALTUNG 2015

Sicherheit in einer vernetzten Welt

Am 5. November 2015 fanden die Industrieorientierung der armasuisse sowie die Herbstveranstaltung der Schweizerischen Gesellschaft für Technik und Armee statt. Über 200 Vertreter – ein neuer Teilnehmerrekord – aus Armee, Industrie, Forschung und Wissenschaft, Verbänden und Verwaltung waren der Einladung gefolgt. Als Gastreferentin wurde Frau Prof. Dr. Gabi Dreo Rodosek, Lehrstuhlinhaberin für Kommunikationssysteme und Netzsicherheit an der Universität der Bundeswehr München, eingeladen.

Rüstungschef Martin Sonderegger, Dr. Fritz Gantert und Prof. Dr. Gabi Dreo Rodosek während der Podiumsdiskussion.

Die Veranstaltung stand ganz im Zeichen des Themas «Sicherheit in einer vernetzen Welt». Anhand der eingeladenen Referenten wurde eine vielschichtige Diskussion des Themas erwartet. Die fortschreitende Globalisierung und Technologisierung lassen die Welt immer näher zusammenrücken. In den Referaten kam immer wieder klar zum Vorschein, dass sich die globale Vernetzung sowohl positiv wie auch negativ auswirken kann.

armasuisse als Schnittstelle

Um 9.15 Uhr wurde der Anlass mit der Rede des Rüstungschefs Martin Sonderegger eröffnet. Dem Publikum wurde aufgezeigt, wie stark die armasuisse vernetzt ist. Als Bundesamt für Rüstung befindet sich armasuisse an einer wichtigen nationalen und internationalen Schnittstelle. Auf nationaler Ebene ist nach wie vor die Armee der wichtigste Auftraggeber. Auf internationaler Ebene existieren aktuell 15 bilaterale Rahmenabkommen im Rüstungsbereich. Das armasuisse-Büro in Washington DC unterstützt Schweizer Unternehmen bei deren Geschäften in den USA. armasuisse steht zudem in regem Kontakt mit der Europäischen Verteidigungsagentur (EVA). Der Rüstungschef führte aus, dass das Beschaffungsvolumen sinkt. Damit verbunden sei die Gefahr, dass auch die sicherheitsrelevanten Kompetenzen abnehmen. Deshalb, so Sonderegger, gilt es, das in der Schweiz vorhandene Know-how zu sichern. Zudem müsse man sich bewusst machen, welche Fähigkeiten und Schlüsseltechnologien zwingend in den eigenen Händen gehalten werden müssen. Ausserdem gilt es zu klären, wie man mit nicht vorhandenen Fähigkeiten umgehen soll. In seinen Ausführungen machte Martin Sonderegger ferner auf die Bedeutung der Weiterentwicklung der Armee (WEA) aufmerksam und erörterte die beiden Rüstungsprogramme des laufenden Jahres. Er erklärte dem Publikum, dass 98 Prozent des beantragten Gesamtkredits des zusätzlichen Rüstungsprogramms 2015 – falls durch das Parlament genehmigt – bei der heimischen Industrie in Auftrag gegeben und als Konsequenz der Werkplatz Schweiz gestärkt werden würde. In der Folge gab er einen Überblick über den Prozess der beschleunigten Beschaffung, wobei hier der frühe und intensive Einbezug der Industrie eine entscheidende Rolle

Prof. Dr. Gabi Dreo Rodosek erklärt die Bedeutung von Cyber Defence.

spielt. Im Rahmen eines «Competitive Dialogue»-Prozesses soll zukünftig bei gemeinsamen Meetings alle Anbieter resp. Mitbewerber auf den gleichen Informationsstand gebracht werden. Damit herrsche einerseits Transparenz und andererseits würde somit der Aufwand von armasuisse nachhaltig reduziert werden. Martin Sonderegger nannte hier das Projekt BODLUV 2020 als Paradebeispiel.

Sicherheit ist nicht selbstverständlich

Korpskommandant André Blattmann, Chef der Armee, erläuterte die aktuellen globalen Krisen und Konflikte. Das sich rasch wandelnde geopolitische Umfeld kann sehr plötzlich Auswirkungen auf die Sicherheit der Schweiz haben. Diese Umstände gelte es mit einem wachsamen Auge zu beobachten. Deshalb sei die Armee als Gesamtsystem wichtig zum Schutz und zur Wahrung der Interessen der Schweiz. Weil die Sicherheit aber nicht selbstverständlich ist, forderte Blattmann dringend die Umsetzung der Weiterentwicklung der Armee. Die WEA sieht eine vollausgerüstete Miliz-Armee mit 100 000 Mann und einem jährlichen Budget von 5 Milliarden Franken vor. Insbesondere die Erhöhung der Bereitschaft (Wiedereinführung eines Mobilmachungssystems) und die Verbesserung der Kaderausbildung ermöglichen es künftig, die Armee rasch und flexibel einzusetzen. Zusätzlich soll die Armee wieder vermehrt regional verankert werden. Der Chef der Armee wies deutlich auf die Notwendigkeit der Anpassung der Strukturen in den grundlegenden Punkten Finanzierung und Bestände hin. Es gehe nicht darum, einzelne Verbesserungen umzusetzen, sondern wieder ein funktionierendes Gesamtsystem mit Blick auf moderne Bedrohungen und die gesellschaftliche Realität zu schaffen.

Der Westen hat gute Absichten, aber keine Mittel

Die Vortragsreihe des Vormittags wurde durch den Direktor des Nachrichtendienstes des Bundes (NDB), Dr. Markus Seiler, abgerundet. Er ging auf die Aufgaben des Nachrichtendienstes ein und strich die wichtigsten Kernkompetenzen heraus: Prävention, Früherkennung potentieller Bedrohungen sowie deren Analyse. Als aktuelles Beispiel führte er die zunehmende Gefahr durch den Terrorismus ins Feld. Auch die jüngsten Konfrontationen zwischen Russland und dem Westen ist gemäss Seiler schädlich für das weltpolitische Klima. Ein Problem sieht der NDB auch in der Tatsache, dass der Westen auf Dialog setzt und seine jährlichen Militärausgaben senkt, aber der Rest der Welt zeitgleich aufrüstet. Eine zusätzliche Brisanz erhält dieser Trend dadurch, dass der Westen ein wichtiger Exporteur von Terroristen (sog. «Foreign Fighters») nach Syrien und Irak geworden ist. In Bezug auf die Schweiz hielt er fest, dass der Terrorismus keine theoretische Bedrohung mehr sei, sondern eine reale. Daher sei eines der Hauptziele der Terrorismusprävention, die bereits laufenden Massnahmen verschiedener sicherheitsrelevanter Akteure zu verknüpfen.

Schliesslich machte Seiler auf die Sensoren und Funktionen eines Smartphones und das dahinter verborgene kriminelle Potential aufmerksam. Mit einem kurzen Einblick in das neue Nachrichtendienstgesetz (NDG) schloss der Direktor seine Ausführungen.

Das «smarte» Leben oder alles ist mit allem vernetzt

Zu Beginn des Nachmittages berichtete Frau Prof. Dr. Gabi Dreo Rodosek von ihrer Arbeit am Forschungszentrum für Cyber Defence (CODE) an der Universität der Bundeswehr München. In der heutigen Zeit sind immer mehr Komponenten unseres täglichen Lebens miteinander verknüpft: Smartphones, Smart Home, E-Health, vernetzte Autos etc. Sie hielt fest, dass zwar diese Welt das Leben vereinfachen kann, andererseits jedoch die vernetzte, digitale Welt einen endlosen Spielplatz für Hacker darstellt. Es war in der Vergangenheit sogar möglich, Insulinpumpen oder Herzschrittmacher, die mit drahtlosen Steuerungen ausgerüstet waren, zu hacken. Die Professorin wies auch auf die Problematik hin, dass ganze Elektrizitätsnetze über IT-Netze gesteuert werden. Ein wichtiger Diskussionspunkt war der Cyber War. Hier ist man schon so weit fortgeschritten, dass ein einzelner «Black Hat» (Hacker mit kriminellen Absichten) mit einem Laptop und Internetzugang mehr Schaden anrichten kann als eine Bombe.

INDUSTRIEORIENTIERUNG UND HERBSTVERANSTALTUNG 2015

Die schnelllebige Zeit und die damit verbundene Weiterentwicklung seien weitere Herausforderungen, welche sich heute der Gesellschaft stellen, so Rodosek. Die weltumspannende Interkonnektivität und der Austausch von Daten führen zu einer zunehmenden Angreifbarkeit. Das Forschungszentrum Cyber Defence der Universität der Bundeswehr arbeitet an Gegenmassnahmen sowie Lösungen und pflegt zu diesem Zweck auch eine strategische Partnerschaft mit dem Bundeskriminalamt (BKA). Zudem nimmt das Forschungszentrum regelmässig an Hackerkonferenzen teil. Ein Schwerpunkt in der Cyber Defence liegt in der Sensibilisierung der Bevölkerung und in der dezentralen Datenspeicherung.

Die Sicherheitsverbundsübung 2014 deckte Lücken auf

Im letzten Referat des Tages kam André Duvillard zu Wort. Er ist Delegierter des Sicherheitsverbundes Schweiz (SVS) und ging in seiner Rede auf die Sicherheitsverbundsübung 2014 (SVU 2014) ein. Das Übungsszenario sah eine mehrmonatige Strommangellage und eine Pandemiewelle für ganz Westeuropa vor. Die SVU 2014 sollte die Zusammenarbeit der verschiedenen politischen Ebenen sowie der koordinierte Einsatz von Armee, Zivilschutz, Polizei und zivilen Helfern auf ihre Machbarkeit prüfen. Die Übung legte ihre Schwergewichte auf vier Themenbereiche (Mobilität, Versorgung/Entsorgung, Gesundheitswesen, öffentliche Sicherheit) und drei Führungsbereiche (Information/Kommunikation, Koordination/Führung, Ressourcenmanagement). Während der SVU 2014 wurden verschiedene mögliche Auswirkungen wie die Kontingentierung des Stroms, Einschränkungen im Nationalstrassenbetrieb, Engpässe in der Trinkwasser- und Lebensmittelversorgung sowie eine verringerte Produktion durchgespielt.

Die SVU 2014 zeigte auf, dass die Schweiz für eine mehrmonatige Notlage unzureichend vorbereitet ist. Zwar war den Ausführungen Herrn Duvillards zu entnehmen, dass man kurz- und mittelfristig mit einem Drittel weniger Strom auskäme, einzig für die Industrie wäre es längerfristig kritisch. Auch die tägliche und «just-in-time» Belieferung der Detailhandelsfilialen mit Lebensmitteln würde zu einem Versorgungsproblem in der Bevölkerung führen. Dennoch wurden die Erkenntnisse der SVU 2014 positiv bewertet sowie die grosse Bereitschaft und der Einsatz der 24 teilnehmenden Kantone gelobt.

Schliesslich beendete Duvillard seine Erläuterungen mit der Frage ans Publikum, ob denn jemand noch Notvorräte lagere oder ein batteriebetriebenes Radio besitze…

Eine angeregte Podiumsdiskussion als krönender Abschluss

Die Vorträge gaben Anlass zur Diskussion, was anhand der über einstündigen Podiumsdiskussion klar zum Ausdruck kam. Rüstungschef Martin Sonderegger veranschaulichte die enorme technologische Entwicklung anhand des heutigen Smartphones, welches alleine bereits eine höhere Rechenleistung aufweist, als 1969 bei der ersten Mondlandung benötigt wurde. Der Rüstungschef sieht die Aufgabe der armasuisse darin, die auf dem Markt vorhandenen, für den Auftraggeber geeignetsten Technologien sinnvoll und stabil nutzbar zu machen. Von Seiten Armee wurde erneut die Wichtigkeit der WEA betont, da nur eine stabile Milizarmee ihren Vorteil – die Nutzung des Miliz-Know-hows – gewährleisten kann. Im Bereich der Cyber Defence ist die Armee heute vor allem darauf ausgelegt, primär ihre eigenen Systeme zu schützen. Frau Prof. Dr. Dreo Rodosek konnte die Fragen, wie gut die Aufklärung im Bereich der Cyberkriminalität funktioniere, durchaus positiv beantworten. Sie wies erneut darauf hin, wie wichtig es sei, die Anwender möglichst früh auf die Gefahren hinzuweisen. Zudem sollten in der gesamten Gesellschaft die digitalen Kompetenzen sowie die Prävention gestärkt werden. Hier hakte ein Vertreter des Nachrichtendienstes ein und betonte, dass selbst die beste Firewall nichts nütze, wenn jemand eine E-Mail eines unbekannten Absenders öffne. Die menschliche Komponente ist in der virtuellen Welt also nach wie vor der grösste Risikofaktor. Trotzdem oder gerade deswegen ist für die nachhaltige Sicherheit in unserer vernetzten Welt die Zusammenarbeit verschiedenster Akteure oder Nutzergruppen und deren Ausbildung äusserst wichtig.

Die nächste Ausgabe der Herbstveranstaltung findet am 3. November 2016 statt.

Brian Jost

Download Referate

Die Handouts aller Referate der Anlässe stehen zum Herunterladen auf der STA Webpage zur Verfügung unter:

http://www.sta-network.ch/ > Downloads > Herbstveranstaltung

IMPRESSIONEN DER INDUSTRIEORIENTIERUNG armasuisse UND DER STA-HERBSTVERANSTALTUNG 2015

IMPRESSIONEN DER INDUSTRIEORIENTIERUNG ARMASUISSE UND DER STA-HERBSTVERANSTALTUNG 2015

IMPRESSIONEN DER INDUSTRIEORIENTIERUNG ARMASUISSE UND DER STA-HERBSTVERANSTALTUNG 2015

STA-JUBILÄUM

60 Jahre Schweizerische Gesellschaft Technik und Armee (STA) – zweiter Teil: 1985-2014

Das 60-jährige Jubiläum der Schweizerischen Gesellschaft Technik und Armee (STA), ehemals Schweizerische Kriegstechnische Gesellschaft (SKG), bietet Gelegenheit für einen Blick in die Geschichte dieser Organisation. Die Fortsetzung des in der letzten Ausgabe des «STA-Flash» begonnen Rückblicks.

Sicherheitspolitisches Spannungsfeld

Die sicherheitspolitische Lage in Europa hat sich nach den ersten 30 Jahren des Vereinsbestehens im Jahre 1985 bis heute laufend verändert. Das Zusammenbrechen des Eisernen Vorhangs und die Wiedervereinigung Deutschlands führten unter anderem zur Armeereform «Armee 95» und damit zu sinkenden Mannschaftsbeständen sowie zu verkleinerten Budgets. Die Wertschätzung der Armee in der Bevölkerung verringerte sich. Zu spüren bekamen dies auch die Rüstungsbetriebe des damaligen Eidgenössischen Militärdepartementes (EMD), deren Auftragsvolumen stetig sank. Sie wurden 1998 unter dem Namen RUAG Schweiz AG in eine privatwirtschaftliche Aktiengesellschaft überführt.

Nach anfänglich friedlicher Koexistenz in Europa entstehen neue Bedrohungen. Populistische und radikale Gruppen erhalten Zuwachs und gewinnen immer mehr Einfluss in die politischen Entscheidungen. Die Flüchtlingsströme aus den Krisenregionen und die Gefahr von Terroranschlägen nehmen zu und stellen die Schweiz ebenfalls vor neue sicherheitspolitische Probleme.

Aus SKG wird STA

Die SKG/STA hat ihre Aktivitäten dieser stetig ändernden Entwicklung angepasst. Als neutrales Bindeglied im wehrtechnischen Beschaffungsprozess ist es den Verantwortlichen immer wieder gelungen, namhafte und gut vernetzte Persönlichkeiten aus der Politik, der Armee, der Industrie und der Wissenschaft sowohl für das Präsidium als auch für die Mitarbeit im Vorstand zu gewinnen. An regelmässig durchgeführten Veranstaltungen hatten die Mitglieder Gelegenheit, bestehende Kontakte zu pflegen und neue aufzubauen. An Seminaren wurden den Teilnehmern vertiefte Informationen durch ausgewiesene Referenten aus dem In- und Ausland zu aktuellen und zukunftsorientierten Themen weitergegeben. Unter den vielen Themen seien folgende herausgegriffen:

- 1985: Ein neutraler Staat als Auftraggeber von Wehrmaterial.
- 1987: Die Schweizerische Rüstungsbeschaffung aus der Sicht der Industrie.
- 1988: Informatik in Armee und Wirtschaft.
- 1990: Armee und Rüstung in einem sich wandelnden Umfeld.

In den letzten 30 Jahren wurde die SKG/STA von folgenden Präsidenten geleitet:

- 1971 – 1986: Herr Dr. Marcel Pfulg, Unternehmer
- 1986 – 1995: Herr Claude Thalmann, Direktor POLYTRONIC
- 1995 – 2003: Herr Dr. Peter Affolter, Delegierter der Konzernleitung der ASCOM AG
- 2003 – 2009: Herr Urs Ramseier, CEO ASCOM Systec AG
- Seit 2009: Herr Dr. Fritz Gantert, Unternehmer und unabhängiger Verwaltungsrat

Die Entspannung in Europa veranlasste den Vorstand der SKG einen dem Zeitgeist angepassten, neuen Namen zu geben. Nach diversen Vorschlägen und nach einer Urabstimmung wurde 1988 aus der SKG die STA, Schweizerische Gesellschaft Technik und Armee.

Internationale Zusammenarbeit

Trotzt der Globalisierung und Öffnung der Märkte ist der Zugang zu neuen Technologien im Sicherheitsbereich erschwert. Dies war einer der Gründe weshalb die STA Ende der 1980er Jahre in Europa Kontakt zu ähnlichen Organisationen suchte. Unter dem damaligen Präsidenten, Herr Claude Thalmann, und zusammen mit deutschen und französischen gleich gelagerten Organisationen, wurde in Genf im Jahr 1991 die European Federation of Defence Technology Associations (EDTA) gegründet. Die Statuten erarbeitete der STA-Vorstand. Mitgliedsländer der ersten Stunde waren neben der Schweiz, Deutschland, Frankreich, Italien, Spanien, die Niederlande, Dänemark und Griechenland. Erster Präsident der EDTA war Herr Claude Thalmann. Es folgte eine enge Zusammenarbeit mit den Agenturen der Mit-

gliedsländer, insbesondere mit der Deutschen Wehrtechnischen Gesellschaft (DWT). Regelmässig wurde jedes Jahr ein internationales Symposium mit Referaten und Diskussionen zu aktuellen sicherheitspolitischen Themen durchgeführt. Organisiert wurden die Symposien jeweils von einem andern Land. Referenten und Teilnehmer der Symposien waren ranghohe Persönlichkeiten aus Armee, Politik und Wirtschaft. Die STA führte unter anderem in der Schweiz die folgenden internationalen Symposien durch:

- 1993: Schweizerische Sicherheitspolitik in Europa
- 1998: Sicherheitspolitik und Rüstungstechnologie
- 2000: Rüstungspolitik wohin?

Aus Zeit- und Kostengründen konnten leider einige Länder die aufwändige Organisation nicht mehr übernehmen, so dass sich die internationale Zusammenarbeit seit 2005 auf Deutschland und Frankreich beschränkt. Es ist gut möglich, dass diese Kontakte wieder erweitert werden, sollte sich das sicherheitspolitische Umfeld weiterhin verschlechtern.

Rüstungsprogramme, Zusammenarbeit mit Swissmem und GRPM

Die jährlichen Rüstungsprogramme wurden ursprünglich jeweils in zwei Teilen präsentiert. Am Vormittag präsentierten die Beschaffungsstellen der Gruppe für Rüstungsdienste (GRD) den Industrievertretern die zu beschaffenden Vorhaben. Am Nachmittag hatten die Interessenten Gelegenheit, Details wie Beteiligungen, Lizenzvergaben, Umfang usw. der einzelnen Projekte zu erfragen und sich als Auftragnehmer zu empfehlen. Auf Initiative der STA wurde dieses Vorgehen in Zusammenarbeit mit Swissmem und GRPM durch die heute immer noch beliebten Herbstveranstaltungen abgelöst. Diese Veranstaltungen werden durch Referate zu aktuellen Themen der Sicherheitspolitik und der Wehrmaterialbeschaffung ergänzt.

Das gemeinsame Vorgehen führte dazu, dass die STA mit Swissmem und GRPM heute auch in anderen Bereichen eng zusammenarbeitet. Die von der STA angestrebte Plattform zur Förderung der Kontakte zwischen Armee, Wirtschaft und Politik findet hier seine Fortsetzung.

Sieben Thesen zur Sicherheitspolitik

Das Erfolgsrezept der STA ist sicher die seit der Gründung kaum veränderte und in den Statuten festgeschriebene Zielsetzung. Um dieser auch in Zukunft und in Zeiten erhöhter Bedrohung gerecht zu werden, braucht es vertiefte Leitsätze. Der Vorstand beschloss deshalb, ein Positionspapier auszuarbeiten. Unter der Leitung von Herrn Ueli Emch, Direktor Schweizerische Elektronikunternehmung AG, entstanden nach vielen Sitzungen, Besprechungen, Anhörungen und Vernehmlassungen sieben Thesen zur Sicherheitspolitik (siehe Kasten). Der Vorstand will damit zur sicherheitspolitischen Meinungsbildung beitragen.

Dass die STA seit 60 Jahren und bis heute nichts von ihrer Bedeutung im Beschaffungsprozess von Wehrmaterial eingebüsst hat, ist eine bemerkenswerte Erfolgsgeschichte. Es ist auch ein erfreuliches Bekenntnis zum Milizsystem und macht Hoffnung für die Zukunft.

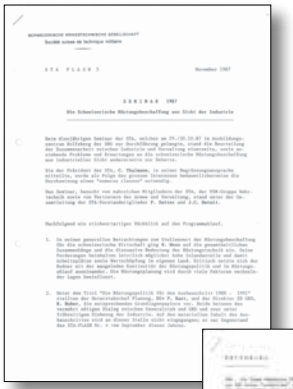
Heinz Hänzi

Die sieben Thesen der STA und ihre wesentlichen Aspekte:

- These 1: Die Sicherheits- und Rüstungspolitik muss an politischer, gesellschaftlicher und gesamtwirtschaftlicher Bedeutung gewinnen und langfristig ausgerichtet werden.
- These 2: Die nachvollziehbare Aufwuchsfähigkeit der Armee ist zwingende Voraussetzung und Grundpfeiler einer eigenständigen und glaubwürdigen Sicherheitspolitik. Dazu gehören der Erhalt von adäquaten Kapazitäten einer exportfähigen eigenen Rüstungsindustrie mit genügend breiter Technologiebasis.
- These 3: Ausrüstung, Bewaffnung, Ausbildung und Führung der Armee müssen auf einem hohen Stand sein.
- These 4: Der zukünftige Technologiebedarf der Armee erfordert eine intensive Zusammenarbeit zwischen Armee, Beschaffungsinstanzen, Wissenschaft und Industrie.
- These 5: Das wirtschaftliche Überleben der Schweizer Rüstungsindustrie erfordert eine Exportpraxis nach europäischen Rechtsstandards sowie internationale Kooperationen beim Rüstungsbeschaffungsprozess.
- These 6: Der Erhalt der industriellen Kernfähigkeiten in der Wehrtechnik ist sicherheitspolitisch und gesamtwirtschaftlich von Bedeutung.
- These 7: Die Finanzen dürfen nicht das bestimmende Element der Sicherheitspolitik sein.

STA-JUBILÄUM

Layoutveränderungen von STA-Flash und -Webseite im Zeitverlauf



1987

1996

2015

1990

2003

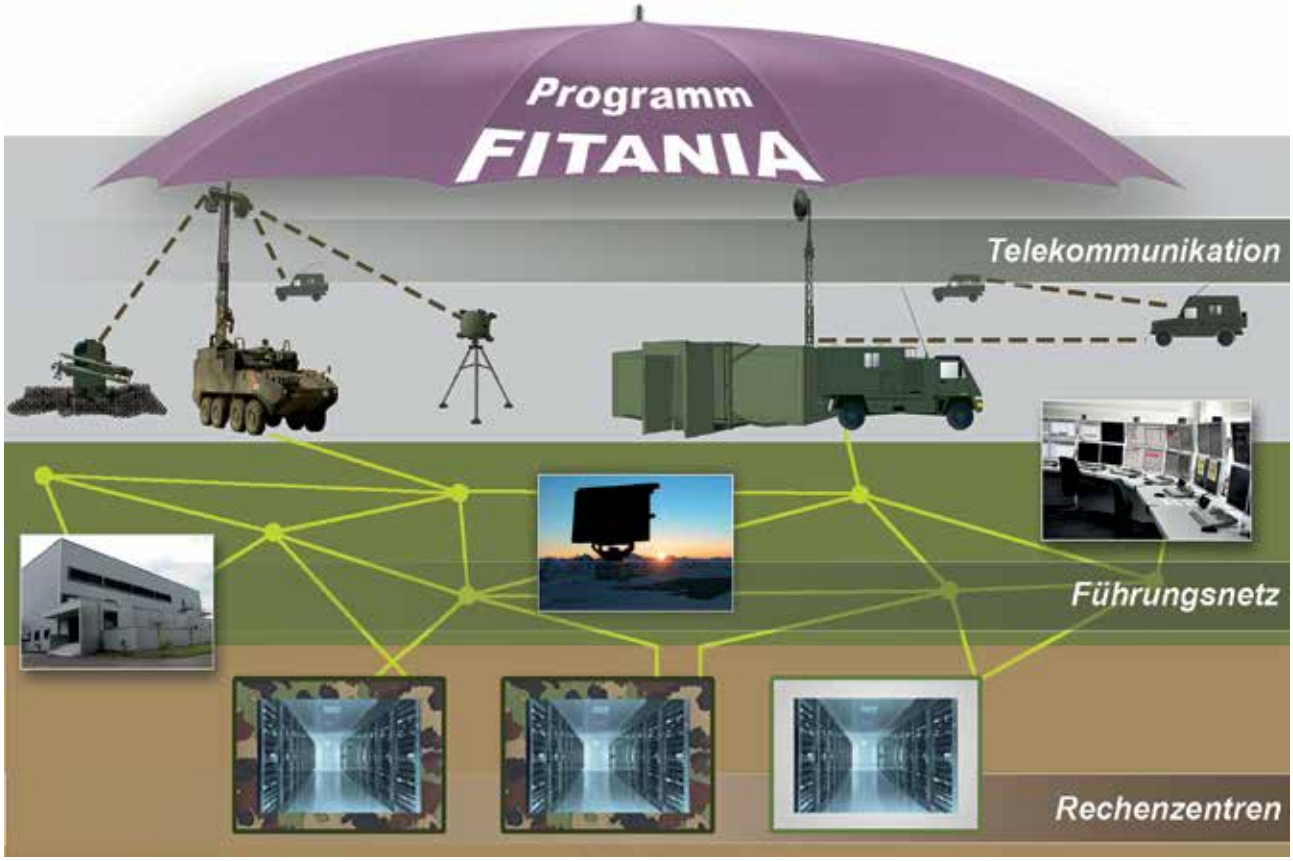
2005

2009

2015

Ein sicheres und autonomes IKT-Netzwerk für die Armee

Um ihre Führungs- und Einsatzfähigkeit gewährleisten zu können, müssen Streitkräfte heute über eine umfangreiche IKT-Infrastruktur verfügen. Die Schweizer Armee fasst ihre IKT-Systeme im Rahmen eines Programmes zu einem Netzwerk zusammen. Es trägt den Namen FITANIA, was als Abkürzung für die Bezeichnung «Führungsinfrastruktur, Informationstechnologie und Anbindung an die Netzinfrastruktur der Armee» steht. Dank FITANIA wird es möglich sein, Daten und Sprache von Rechenzentren über ein separates Übertragungsnetz bis hinaus zu den mobilen Endgeräten im Feld zu transportieren, und zwar sicher, permanent und autonom. Selbst bei einem Ausfall ziviler Provider und Stromlieferanten wird die Armee in der Lage sein, ihre Verbindungen aufrechtzuerhalten. Davon profitieren auch zivile Notfallorganisationen.



Schematische Darstellung des Programms FITANIA.

Die moderne Informations- und Kommunikationstechnik (IKT) hat auch in der Armee längst Einzug gehalten. Ohne IKT-Mittel fährt heute kein Panzer mehr los und hebt kein Kampfflugzeug mehr ab. Die IKT ist zu einem integralen Bestandteil der Führungsmittel geworden. Die Schweizer Armee verfügt über eine Vielzahl von Informations- und Kommunikations-Systemen. Teilweise laufen diese unabhängig voneinander und bauen auf unterschiedlichen Programmiersprachen und Technologien auf. Zudem sind die Daten in verschiedenen isolierten Rechenzentren gespeichert. Die Fähigkeiten und Mittel sind somit stark segmentiert.

Dieser Zustand rührt daher, dass die IKT-Mittel über die Jahre hinweg gestützt auf spezifische operationelle Bedürfnisse hin einzeln beschafft worden sind und folglich technisch verschiedenen Generationen angehören. Je nach System und Geräten können diese nicht weiterentwickelt oder zu Netzwerken zusammengefasst werden. Dadurch besteht einerseits erhöhter technischer Erneuerungsbedarf und anderseits ein grösserer

PROGRAMM FITANIA

Im Programm FITANIA wird die Rechenzentren-Infrastruktur konsolidiert.

Aufwand im Betrieb der verschiedenen Systeme, da eine zentrale Steuerung und Überwachung oftmals nicht möglich ist. Eine Lösung, die nicht nur einen grossen Personaleinsatz verlangt, sondern auch kostenintensiv ist.

Damit die Armee in der Krise funktioniert

Damit die Armee in Notlagen und Krisen einsatzfähig bleibt, ist sie darauf angewiesen, dass die IKT-Leistungen jederzeit, im benötigten Umfang und ohne Unterbruch zur Verfügung stehen. Denn in ausserordentlichen Lagen ist nicht mehr gewährleistet, dass die bestehenden Netze und Systeme von zivilen IKT-Providern noch funktionieren. Die Armee braucht eine IKT-Infrastruktur, die krisenresistent ist. Sie muss verfügbar sein, wenn ein grossflächiger und anhaltender Stromausfall eintritt, ein krimineller Angriff zivile Computersysteme lahmlegt, eine Naturkatastrophe zivile Verbindungen unterbricht, Systeme beschädigt oder zerstört, aber auch wenn gezielte militärische Schläge gegen die Schweiz ausgeführt würden.

Neben diesen Funktionalitäten soll FITANIA auch eine Vereinfachung und Uniformierung in der Systemlandschaft bringen. Anstatt weiterhin einzelne Silosysteme aufzubauen, werden die Elemente wo möglich und wirtschaftlich sinnvoll auf einer einheitlichen Plattform basieren. Durchgängige Kompatibilität der Systeme, einheitliche Applikationen und Programmiersprachen sowie eine gesamtheitliche Steuerung und Überwachung von Netzen und Anlagen sind weitere wesentliche Ziele des Programms FITANIA. Am Schluss soll ein Netzwerk aus einem Guss stehen. Damit werden der Betrieb und die Finanzierung der Infrastrukturen optimiert.

Auch zivile Behörden profitieren

Durch das neue krisenresistente IKT-Netzwerk wird die Armee jederzeit in der Lage sein, den Abruf und Austausch von Daten, welche für die Führung von im Einsatz stehenden Verbänden erforderlich sind, sicherzustellen. Daraus zieht nicht nur die Armee ihren Nutzen. Auch den zivilen Führungsorganen beziehungsweise dem Bundesrat dienen

die Infrastrukturen von FITANIA. Bereits heute sind sämtliche Kantone erschlossen und die Alarmierung der Bevölkerung (Sirenen für allgemeinen Alarm und Wasseralarm) stützt sich auf den Datentransport dieses IKT-Netzwerkes ab. Die zivilen Notfallorganisationen wie Polizei, Feuerwehr, Zivilschutz und Sanität werden durch einen noch im Detail zu vereinbarenden Einbezug weitere Dienste in Anspruch nehmen können.

Zudem wird angestrebt, Synergien zwischen den Elementen von FITANIA und einem geplanten neuen Datenverbundnetz der zivilen Krisenorganisationen auszuschöpfen, etwa indem wo möglich die gleiche Infrastruktur für den Transport von Daten verwendet wird. Dadurch können Funktionalitäten mehrfach genutzt und kostengünstigere Lösungen erreicht werden.

Weniger Plattformen, tiefere Kosten

Sicher, permanent und autonom: So lauten die heutigen Anforderungen der Armee an die IKT-Leistungen. Um diese Funktionalitäten langfristig sicherstellen zu können, geht es bei FITANIA um die Erneuerung der IKT-Systeme, die technologische Zusammenführung und eine bedarfsgerechten Anpassung der Infrastruktur. Das Programm FITANIA besteht aus drei Projekten:

- ein zusammenhängendes Übertragungsnetz, das Führungsnetz Schweiz;
- drei Rechenzentren (zwei militärisch vollgeschützte, ein teilgeschütztes zivil-militärisch genutztes), die über das Führungsnetz Schweiz verbunden sind und im Projekt Rechenzentren VBS/Bund 2020 realisiert werden;
- Verlängerung des Führungsnetzes Schweiz in die Mobilität und Ersatz der heutigen Funkmittel mit dem Projekt Telekommunikation der Armee.

Ziel der drei Projekte ist es, das gesamte Netzwerk stufenweise aufzubauen und die verschiedenen Systeme entweder zu integrieren oder – falls es technisch respektive von der Lebensdauer her nicht sinnvoll ist – durch neue, kompatible Komponenten zu ersetzen. FITANIA wird also nicht nur die Einsatzfähigkeit der Armee in jeder Lage gewährleisten, sondern bei den IKT-Plattformen die Standardisierung vorantreiben und zu einer Reduktion der Systemplattformen führen. Damit werden die heute vorhandenen Systeme koordiniert und aufeinander abgestimmt mit neuen Komponenten ersetzt und in die vorgesehene Struktur überführt.

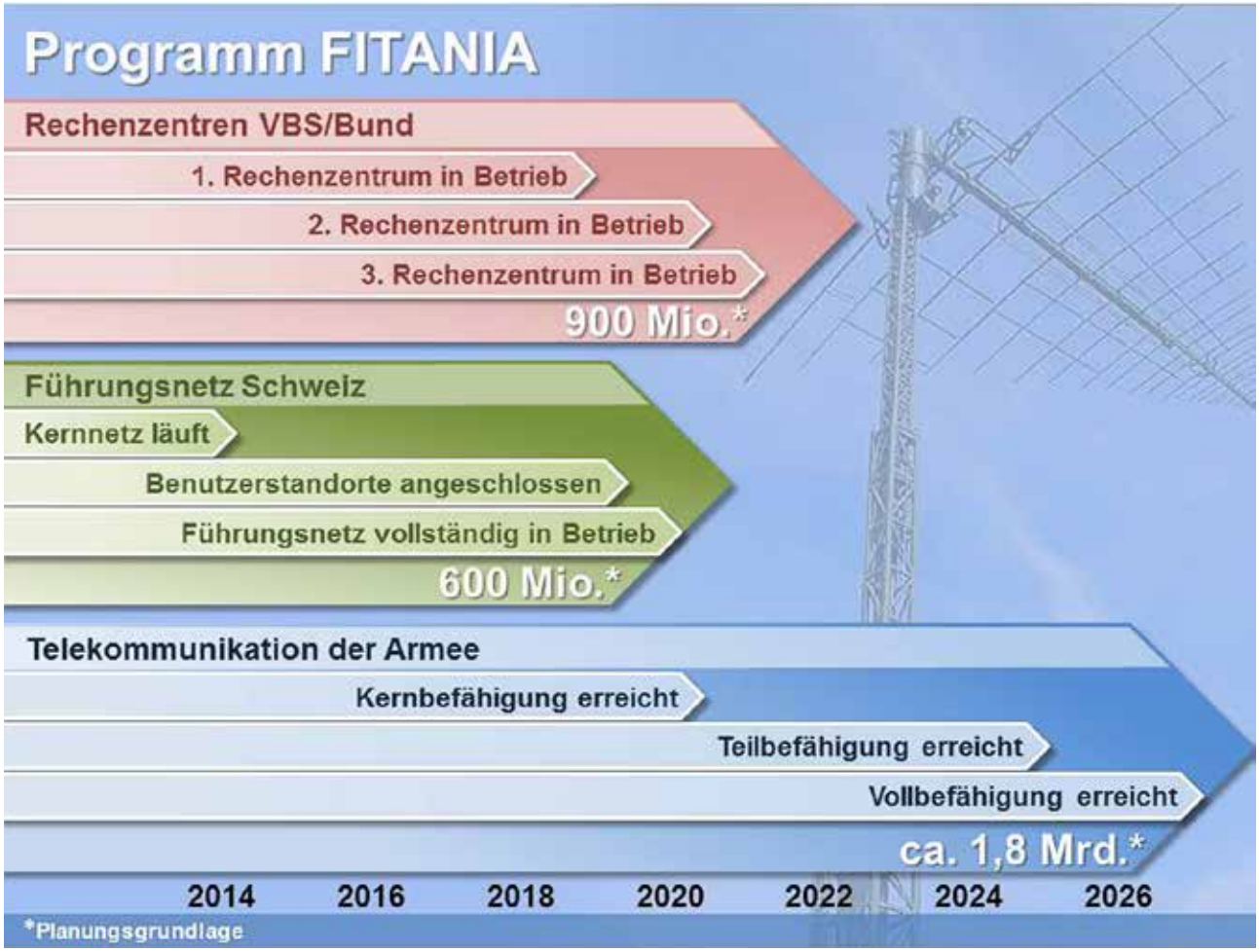
Radio Access Point Panzer der Schweizer Armee.

Sowohl der Betrieb als auch der Unterhalt der Systeme wird vereinfacht und die IKT-Kosten können bei gleicher Leistungsfähigkeit gesenkt werden. Nicht zuletzt wird die vereinheitlichte IKT-Landschaft dazu beitragen, dass die Führbarkeit der Armee in einem technisch zusehends komplexer werdenden Umfeld gewahrt bleibt. FITANIA wird somit die IKT-Infrastruktur der Armee auf lange Sicht prägen und dafür sorgen, dass diese zielgerichtet eingesetzt sowie effizient und sicher betrieben werden kann.

Drei Projekte, ein Ziel

Die drei Projekte, aus denen sich das Programm FITANIA zusammensetzt, sind so ausgelegt, dass auch die langfristigen Bedürfnisse der Armee an die Übermittlung von Gesprächen und Daten (Texte, Bilder usw.) erfüllt werden können. Aufgrund ihrer gegenseitigen Abhängigkeiten erfolgt die Koordination der Planung und Umsetzung der Projekte innerhalb von FITANIA. Das Programm stellt somit sicher, dass das Zusammenspiel der Systeme funktio-

PROGRAMM FITANIA



Aktuelle Planungssicht des Programms FITANIA.

niert und dass Synergien wo immer möglich genutzt werden können.

Redundante Rechenzentren

Um die umfangreichen Datenströme verarbeiten zu können, brauchen die Armee und die zivilen Führungsorgane inklusive des Bundesrats Rechenzentren mit ausreichend grossen Kapazitäten. Zudem müssen diese Zentren baulich erhöhte Schutzanforderungen erfüllen, damit sie auch im Katastrophenfall (bei physischen Einwirkungen oder Stromausfall) autonom von zivilen Einrichtungen weiter funktionieren. Überdies kann eine vollumfängliche Redundanz der Daten sichergestellt werden. Selbst wenn eines der Zentren komplett ausfallen sollte, bleibt der Zugriff auf die Daten in den anderen Anlagen möglich. Schätzungen gehen von einem Investitionsbedarf von knapp 900 Millionen Franken (inklusive Anteil der zivilen Departemente) für die drei Rechenzentren aus.

Zwei der Zentren werden mit einem militärischen Vollschutz ausgestattet, das heisst sie werden unter Tag realisiert und weisen eine erhöhte Resistenz gegenüber elektronischen und physischen Einwirkungsversuchen auf. Die Kapazität der Rechenzentren kann modular ausgebaut werden, entsprechend dem Bedarf der Nutzer. Die Arbeiten am einen der beiden vollgeschützten Rechenzentrum sind im Gang, die zivil-militärisch genutzte Anlage befindet sich in Planung. Dieses gemeinsam betriebene Rechenzentrum wird in Frauenfeld entstehen; die Botschaft für den Bau soll im nächsten Jahr ins Parlament kommen. Der Baubeginn für die Anlage auf dem Waffenplatz Auenfeld in Frauenfeld ist auf 2017 geplant.

Das erste, rein militärisch genutzte Zentrum soll im Jahre 2019, das zivil-militärisch genutzte Zentrum im Jahr 2020

und das zweite militärisch genutzte Zentrum im Jahr 2021 in Betrieb genommen werden. Gleichzeitig mit der Inbetriebnahme der drei Zentren werden die über die gesamte Schweiz verteilten kleineren Rechenanlagen ausser Betrieb genommen.

3000 Kilometer Führungsnetz

Das Führungsnetz Schweiz ist ein standortgebundenes, fixes Transportnetz auf der Basis von Glasfaserkabeln und Richtstrahl-Verbindungen. Basis für das Führungsnetz bildet ein bestehendes Kern-Netz (Backbone), das bereits weite Teile der Schweiz erschliesst. Um die Verfügbarkeit hoch zu halten, werden die Verbindungen redundant aufgebaut. Im Endausbau wird das Netz eine Länge von knapp 3000 Kilometern und rund 300 Benutzerstandorte umfassen. Das ausgebaute Netz wird es erlauben, Daten verschlüsselt zu transportieren, und zwar zwischen jedem einzelnen Standort. Es erfolgt also nicht nur eine Verschlüsslung der Daten zwischen den Geräten von Sender und Empfänger, sondern auch zwischen den einzelnen Knoten innerhalb des Netzes. Dadurch wird ein nochmals erhöhtes Mass an Sicherheit erreicht.

Gemäss Schätzungen wird das Führungsnetz Schweiz rund 600 Millionen Franken an Investitionen kosten. Es soll nicht nur der Armee zur Verfügung stehen, sondern auch zivilen Organisationen mit sicherheitsrelevanten Aufgaben.

Ergänzend zum bestehenden Kern-Netz werden in einzelnen Ausbauschritten weitere Standorte angeschlossen. Damit wird auch die Redundanz dieser Lokalitäten gewährleistet. Zudem werden in den nächsten Jahren sämtliche Standorte und auch die Kern-Netzknoten, von denen aus die einzelnen Standorte erschlossen werden, mit einem erweiterten Schutz ausgerüstet, das heisst mit baulichen Massnahmen gegen physische Einwirkungen verstärkt. Mit dem Abschluss sämtlicher Arbeiten am Führungsnetz Schweiz ist bis 2021 zu rechnen.

Telekommunikation der Armee als Systemverbund

Um die für den Einsatz relevanten Daten und Informationen von den fixen Standorten beziehungsweise ab dem Führungsnetz Schweiz hinaus zu den mobilen Teilen der Armee zu transportieren und um die Sprachkommunikation sicherzustellen, ist ein eigenes, gesichertes Telekommunikationsnetz vonnöten. Dieses wird als Ersatz von bisherigen, technologisch in die Jahre gekommenen und isolierten Systemen ebenfalls als Plattform konzipiert und aufgebaut. Telekommunikation der Armee wird als Systemverbund betrachtet, dessen Realisierung in mehreren Etappen erfolgt. Jede zur Umsetzung frei gegebene Etappe bringt für sich bereits eine Teilleistung. Nachfolgend realisierte Etappen bauen auf den vorausgehenden Modulen auf und erweitern so die Funktionalität. Die geschätzten Investitionen für die Erneuerung der Telekommunikation der Armee belaufen sich auf cirka 1,8 Milliarden Franken.

Im Projekt Telekommunikation der Armee sind derzeit verschiedene konzeptionelle Arbeiten im Gang. Sie sollen sicherstellen, dass die verschiedenen Systeme dereinst miteinander kompatibel sind. In einem ersten Realisierungsschritt ist der Kauf einer Tranche neuer Richtstrahlgeräte vorgesehen. In einem folgenden Schritt wird es in etwa zwei bis drei Jahren um die Beschaffung neuer taktischer Funkgeräte und Zubehör gehen. Es folgen später die teilmobile Anbindung an das Führungsnetz und die teilmobilen Sende- sowie Empfangsanlagen. Der Aufbau des gesamten Systemverbundes Telekommunikation der Armee wird sich voraussichtlich bis Mitte der 2020-er Jahre erstrecken.

Gestaffelte Realisierung

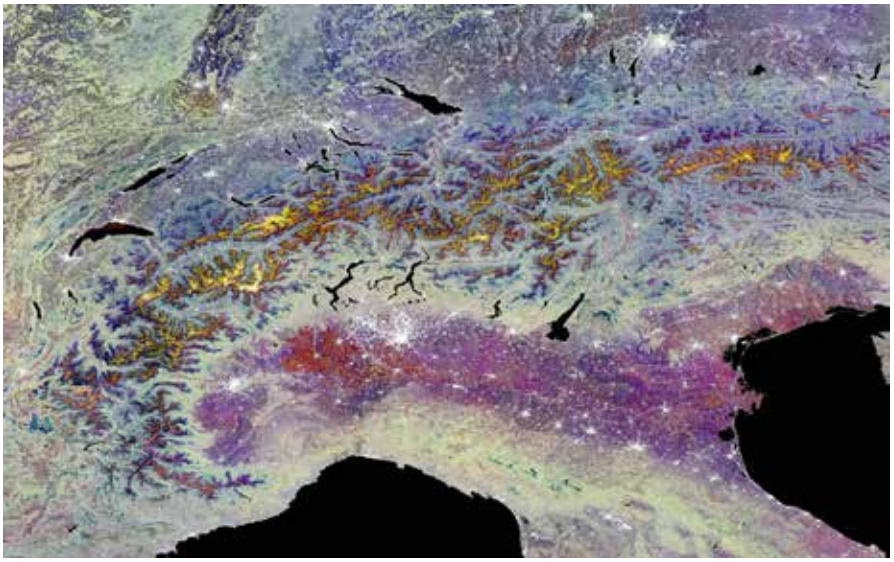
Die drei Projekte sind inhaltlich und damit auch terminlich voneinander abhängig. Ihre Umsetzung erfolgt zeitlich gestaffelt, dies unter Berücksichtigung des Lebensendes von bestehenden Systemen. Als erstes wird das Führungsnetz Schweiz um das Jahr 2020 herum vollständig in Betrieb sein, den Abschluss bildet Telekommunikation der Armee zwischen 2025 und 2027. Mit diesem Fahrplan von FITANIA wird sichergestellt, dass die Armee ein konsolidiertes und zukunftstaugliches IKT-Netzwerk erhält. Es wird dazu beitragen, dass die Führungs- und Einsatzfähigkeit der Armee zugunsten von Land und Leuten in jeder Lage gewährleistet bleibt.

Justus Bernold

BIG DATA

Kurzgedanke: Big Data – Relevanz in allen Sphären

Die Erhebung und Analyse von grossen Datenmengen, verbunden mit den heutigen Rechnerkapazitäten, ermöglichen eine Interaktion in Echtzeit, respektive zeitverzugsarm, zwischen Menschen, Gegenständen, Diensten und Systemen. Dies gilt in allen Sphären.



Der Sentinel-1 Erdbeobachtungssatellit der ESA eröffnet neue Blickwinkel auf die Erde

Doch was ist genau «Big Data»? Big Data ist ein breiter Begriff für Datensammlungen welche so umfangreich sind, dass diese mit herkömmlichen Methoden kaum verarbeitet werden können. Big Data kann entlang der folgenden vier Eigenschaften charakterisiert werden:

- Volumen: Die Grösse der Datenmengen übertrifft die Kapazität von herkömmlichen Computern.
- Geschwindigkeit: Daten ändern sich rasch und müssen in Echtzeit verarbeitet werden.
- Vielfalt: Daten sind semantisch heterogen und müssen integriert werden.
- Glaubwürdigkeit: Die Qualität der verwendeten Daten (Konsistenz, Vollständigkeit, Genauigkeit) muss sichergestellt werden.

Dabei ist festzuhalten, dass der kritische Faktor heute weniger im Datenvolumen steckt sondern vielmehr in der Datenvielfalt. Eine Konsequenz daraus ist, dass der Festlegung von Standards eine zentrale Bedeutung zukommt.

Dieser Punkt kann anhand des Beispiels von heutigen Erdbeobachtungssatelliten illustriert werden. Der Satellit Sentinel-1 des europäischen Erdbeobachtungsprogramms Copernicus zur Überwachung von Umwelt und Sicherheit liefert grosse Datenmengen – obwohl diese noch signifikant kleiner sind als zum Beispiel die Datenmengen die im Bereich TV bzw. Filmgeschäft übermittelt werden. Allerdings müssen Satellitendaten mit einer Vielfalt von Daten und Diensten auf der Erdoberfläche kombiniert werden. Es ist also zwingend notwendig, heute die Standards zu beeinflussen, denn diese werden die Entwicklung der Märkte von morgen mitgestalten.

Unser Land verfügt heute über einen bedeutenden industriellen Sektor, der fast 20 Prozent zum Bruttoinlandprodukt beisteuert. Für die kommenden fünf bis zehn Jahren zeichnen sich jedoch bereits neue Technologien und Verfahren ab, deren Beherrschung für den Erfolg der Schweizer Industrie fundamental sein dürfte. Dabei werden unter anderem die Entwicklungen in Informations- und Kommunikationstechnologien (IKT) eine noch zentralere Rolle spielen.

Aus einer sicherheitspolitischen Perspektive stellen sich Fragen nach der Positionierung der Schweizer Rüstungsindustrie, um dieser neuen Herausforderung zu begegnen, sowie nach der Integration dieser Thematik in die Teilstrategie IKT der Schweizer Armee.

Die Relevanz der Thematik betrifft jeden Sektor, sei er zivil oder militärisch. Ganzheitliche Ansätze sind umso gefragter. Es geht um die Wettbewerbsfähigkeit der Unternehmen in der Schweiz genauso wie um die effektive und effiziente Umsetzung der vernetzten Operationsführung. Die partnerschaftliche Zusammenarbeit zwischen Unternehmen, akademischen Akteuren, Armee und Regulierungsbehörden ist auch hier gefordert.

Daniel Neuenschwander

Industriespionage im digitalen Zeitalter

Geschäftsprozesse sind heute massgebend durch die IT unterstützt. Der Schutz digitaler Daten ist daher wesentlicher Bestandteil im Sicherheitskonzept von Unternehmen. Neben dem technischen Schutz entscheidet aber das Verhalten der Mitarbeiter über die Qualität der Informationssicherheit. Firmen sind gefordert, die Angestellten auf die Gefahren von Industriespionage zu sensibilisieren.

Die zunehmende Digitalisierung und Vernetzung bringen eine erhöhte Anfälligkeit für Cyberattacken mit sich.

Die Digitalisierung ist heute allgegenwärtig und nimmt kaum einen Lebensbereich mehr aus. Smart-Watches kartographieren unsere Laufstrecken, messen unsere Schritte und den Puls und melden dem Arzt automatisch, wenn etwas ungewöhnliches in Erscheinung tritt. Autos navigieren uns nicht nur auf dem kürzesten Weg zum Ziel, sondern fahren bereits heute streckenweise gleich selbst. Unsere Hauselektronik können wir über das Smartphone steuern und der Kühlschrank meldet uns, wann die Milch nachgefüllt werden muss. Das Internet der Dinge – die Vernetzung von Alltagsgegenständen also – steht vor der Tür und verspricht der Wirtschaft neue Absatzmärkte und Optimierungspotential in Fertigung und Betrieb. Das private und öffentliche Leben steht mitten in der dritten digitalen Revolution. Cloud Computing, soziale Netzwerke, Internet of Things und Big Data prägen die neuen Businessmodelle von Unternehmungen. Daten sind das «schwarze Gold» und damit lässt sich Geld verdienen.

Während Privatanwender noch weitgehend selbst entscheiden können, ob sie neuen Technologien Zugriff auf persönliche Daten geben wollen, können sich Unternehmen, Behörden und Organisationen kaum der Technisierung entziehen. Sie sind auf eine ausgebaute IT-Infrastruktur angewiesen. PCs, Laptops, Tablets und Smartphones sind aus dem Geschäftsleben nicht mehr wegzudenken. Das Internet hat die Prozesse beschleunigt und Lieferanten, Dienstleister sowie Kunden global vernetzt. Es ist zu einem zentralen Instrument von Wirtschaft und Gesellschaft geworden. Die fortschrei-

IT-SICHERHEIT IN UNTERNEHMEN

tende Digitalisierung und Vernetzung bringen aber eine erhöhte Anfälligkeit für Cyberattacken mit sich. Die Anzahl der Viren, Trojaner und sonstiger Schadsoftware nimmt rasant zu und mit ihr die Frequenz von Hackerangriffen. Während die Mehrzahl der Fälle auf Angriffe durch kriminelle Organisationen, konkurrierende Firmen oder Einzelpersonen zurückzuführen sind, nimmt die Spionage durch ausländische Nachrichtendienste ebenfalls laufend zu. Aus den 2013 durch Edward Snowden publik gewordenen Informationen zu den Spionageprogrammen der NSA wurde deutlich, dass Industriespionage auch von befreundeten Staaten ausgehen kann.

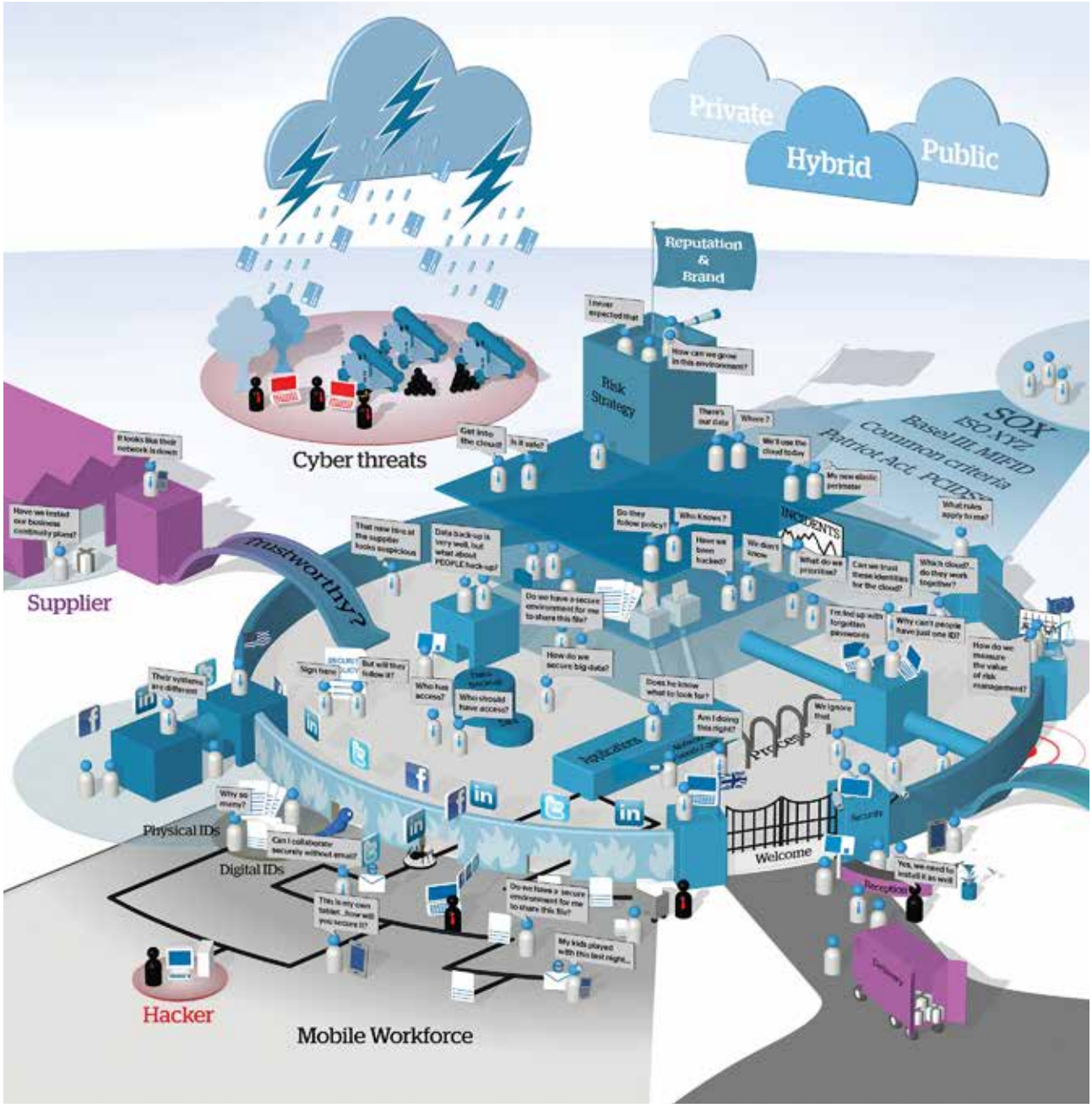
Industriespionage heute

Mit der Digitalisierung sind Unternehmen mehr denn je Spionageangriffen ausgesetzt und noch verwundbarer geworden als in der Vergangenheit. Die Bedrohung ist real, wie eine 2014 durchgeführte Studie von Corporate Trust zeigt: In Deutschland sind fast die Hälfte aller befragten Unternehmen schon einmal Ziel eines Spionageangriffs geworden. Besonders gefährdet sind dabei innovationsstarke Unternehmen aus dem Mittelstand. Allen voran wird der Maschinenbau mit 22,5 Prozent der Fälle am häufigsten getroffen. Aber auch die Pharmaindustrie, der Schiffsbau oder die Luftfahrtindustrie sind oft Ziel von Angriffen. Wie eine Attacke erfolgt ist, lässt sich oft nicht feststellen. Knapp 50 Prozent der betroffenen Unternehmen gaben laut der Studie aber an, dass ein Hackerangriff auf Server, PCs, Laptops, Tablet oder Smartphones registriert wurde. 41 Prozent der Geschädigten vermuteten, dass E-Mails oder Faxnachrichten mitgelesen wurden.

Industriespionage kann bei Unternehmen, die von einem Angriff betroffen sind, grossen Schaden anrichten. In Industriesektoren, die viel in Forschung und Entwicklung investieren, sind die finanziellen Verluste kaum abschätzbar: Wird beispielsweise das Patent für ein neues Medikament gestohlen, an dem seit vielen Jahren geforscht wurde, ist nicht nur die Arbeit einzurechnen, die in die Entwicklung investiert wurde. Auch der mögliche Gewinn geht verloren, der aus dem Verkauf hätte erzielt werden können. Die aus einem Angriff resultierenden Kosten sind beträchtlich. Laut einer Studie von Kaspersky, einem Anbieter von Sicherheitssoftware, kann ein ernsthaftes Sicherheitsleck ein KMU um die 50 000 Dollar kosten. Bei einem grossen Unternehmen belaufen sich die Kosten im Schnitt auf 649 000 Dollar. Wird eine Firma jedoch Opfer eines erfolgreich durchgeführten zielgerichteten Angriffs, kommt das Grossunternehmen sehr viel teurer zu stehen: Durchschnittlich entstehen direkte und indirekte Kosten von 2,4 Millionen Dollar. Ein gezielter Angriff auf ein KMU bedeutet im Schnitt einen Verlust von 92 000 Dollar. Auf etwas tiefere Werte kommt die Studie von Global Trust: In Deutschland lag der Schaden bei einem Grossteil der Firmen zwischen 10 000 und 100 000 Euro. 4,5 Prozent der Unternehmen mussten sogar einen Schaden von über 1 Million Euro in Kauf nehmen. Die Diskrepanzen in den beiden Studien machen deutlich, dass verlässliche Zahlen zu den Kosten von Industriespionage sehr schwierig zu erheben sind. Aus beiden Szenarien wird aber deutlich, dass der Verlust für die Gesamtwirtschaft eines Landes in die Milliarden geht.

Social Engineering

Einen vollständigen Schutz vor Industriespionage gibt es leider nicht. Unternehmen können aber die Risiken so weit wie möglich minimieren. Sich auf den Schutz der elektronischen Daten und des Kommunikationsnetzwerks zu konzentrieren, greift allerdings zu kurz. Denn immer noch stellt der «Faktor Mensch» das grösste Sicherheitsrisiko dar. Spektakuläre Fälle wie der Verkauf von Steuerdaten mit den Namen von Bankkunden haben weltweit für Aufmerksamkeit gesorgt. Doch meistens wird der Datendiebstahl gar nie publik oder schlimmstenfalls nicht einmal bemerkt. Treten Mitarbeiter aus dem Unternehmen aus, besteht immer auch das Risiko, dass sie dem neuen Arbeitgeber vertrauliche Daten und Informationen weitergeben. Kaum ins öffentliche Bewusstsein rücken Fälle, in denen Mitarbeiter Informationen an Dritte preisgeben, ohne dies zu beabsichtigen. Nicht selten kann im Terminal am Flughafen oder im Flugzeug beobachtet werden, wie auf einem Laptop geschäftsrelevante Informationen für jedermann einsehbar sind, weil ein Mitarbeiter zum Beispiel gerade die aktuellen Finanzzahlen seines Unternehmens bearbeitet. Besonders gefährlich sind Werbegeschenke wie Computermäuse oder Webcams die an ein internes Gerät angeschlossen werden. Der Fantasie der Angreifer sind dabei keine Grenzen gesetzt. Werden in der Nähe des Unternehmensgeländes USB-Sticks verteilt, finden sich immer Mitarbeiter, die das Gerät dann auch benutzen und so unwissentlich einen Trojaner auf ihrem Laptop installieren. Zu denken, dass solche Methoden nicht von Organisationen genutzt werden, um an Informationen zu gelangen, unterschätzt die kriminelle Energie, die in das Auspionieren von Unternehmen investiert wird. Laut der Studie von Global Trust bemerkten 38 Prozent der Unternehmen Versuche, gezielt über einzelne Mitarbeiter an Informationen zu gelangen. Dabei wurden



Wirksamer Schutz vor Industriespionage ist ein komplexes Unterfangen.

Mitarbeitende teils über soziale Netzwerke, teils auf Messen oder sogar im privaten Umfeld angesprochen und ausgefragt. Tatsächlich haben die zielgerichteten Angriffe über die letzten Jahre massiv zugenommen. Dabei kommen verschiedene Methoden zum Einsatz. So werden Mitarbeiter beispielsweise telefonisch oder per Mail kontaktiert, wobei der Angreifer vorgibt, ebenfalls Mitarbeiter des Unternehmens zu sein (Identity Theft). Dabei wird versucht, die Hilfsbereitschaft der Mitarbeiter auszunutzen, um Sicherheitsschranken zu umgehen. Oder es wird versucht, mit gezielten Phishing-Mails Schadsoftware auf den Unternehmensrechnern zu installieren (Spear Phishing). Im Unterschied zu Phishing-Mails, die massenhaft an beliebige Adressen versendet werden, sind gezielte Phishing-Mails viel schwieriger zu erkennen, da sie auf den Mitarbeiter abgestimmt sind, der angegriffen wird. Solche Attacken werden vom US National Institute of Science

IT-SICHERHEIT IN UNTERNEHMEN

and Technology (NIST) als Advanced Persistent Threat (APT) bezeichnet. Damit werden Angriffe durch Organisationen bezeichnet, die über tiefgreifendes technisches Wissen und erhebliche Ressourcen verfügen. Das erlaubt es ihnen, ihre Ziele durch den Einsatz unterschiedlicher Angriffsvektoren zu erreichen. Dazu gehören neben Cyber-Angriffen auch Methoden, wie sie zu Zeiten des Kalten Krieges eingesetzt wurden: Mitarbeiter werden unter Druck gesetzt, Mittelsmänner eingeschleust oder sogar Konferenzräume verwanzt. Bei einer solchen Attacke ist der Angreifer bemüht, so lange wie möglich unentdeckt zu bleiben und über einen längeren Zeitraum kontinuierlich Informationen zu sammeln.

Sicherheitskultur im Unternehmen fördern

Während sich auf technischer Seite Daten und Informationen relativ gut schützen lassen, bleibt die Gefahr bestehen, dass Mitarbeiter wissentlich oder unwissentlich geschäftsrelevante Informationen an unbefugte Dritte weitergeben und damit die technischen Sicherheitsschranken umgehen. Teils, weil Angestellte Sicherheitsstandards und Auflagen nicht einhalten, diese nicht kennen oder schlimmstenfalls gar keine vorhanden sind. Teils, weil sie gezielt angegriffen und als Informanten genutzt werden oder aus eigenem Antrieb Informationen weiter geben. Nicht selten sind sich die Mitarbeiter und selbst das Management nicht der Risiken bewusst, denen sie ausgesetzt sind. Ein wirkungsvoller Schutz sensitiver und geschäftsrelevanter Daten und Informationen muss daher beim Top-Management ansetzen und von dort über alle Hierarchiestufen des Unternehmens getragen werden. Viele Unternehmen haben mittlerweile die Stelle des Chief Information Security Officers (CISO) geschaffen, um der Bedrohung aktiv zu begegnen. Unternehmen, die besonders wertvolle Informationen haben, beschäftigen nicht selten eine ganze Abteilung, die sich dem Schutz der Daten widmet. Beim Erstellen von Sicherheitsvorschriften gilt es immer auch abzuwägen, wie wertvoll die Informationen sind, die allenfalls gestohlen werden könnten, welche Risiken überhaupt vorhanden sind, wie gross die Wahrscheinlichkeit eines Angriffs ist und welche Kosten für den Schutz anfallen. Mit technischen Massnahmen lassen sich Daten bereits schützen. So sollte beispielsweise die Computerfestplatte der Mitarbeitenden mit Passwörtern geschützt sein, die den üblichen strengen Vorschriften entsprechen. Ein ausgebautes und robustes Identity und Access Management (IAM) muss den rollenbasierten Zugriff auf Daten und Applikationen sicherstellen und damit die individuellen Berechtigungen aller Mitarbeiter regeln. Hier gilt es sicher zu stellen, dass die Angestellten nur auf diejenigen Daten und Applikationen Zugriff haben, die sie auch für ihre Arbeit benötigen. Technische Massnahmen sind aber nur die eine Seite einer unternehmensweiten Compliance Strategie. Mit Informationsmaterial, Fragebogen oder Workshops gilt es die Mitarbeiter im Umgang mit Daten zu schulen und für die Risiken zu sensibilisieren.

Fazit

Industriespionage ist eine reale Gefahr für Unternehmen. Einen vollständigen Schutz gibt es dabei nicht. Die Risiken sollten aber so weit wie möglich reduziert werden. Dazu gilt es eine unternehmensweite Sicherheitskultur zu etablieren, die über die technischen Möglichkeiten hinaus die Mitarbeitenden in das Sicherheitskonzept einbezieht. Eine sichere IT lässt sich nur dann realisieren, wenn die Mitarbeiter auch sicherheitsbewusst handeln und über die möglichen Gefahren informiert sind. Während grosse Unternehmen bereits viel in ihre Sicherheitskultur investiert haben, sind insbesondere KMUs heute noch in vielen Fällen kaum geschützt und wenige sind sich der Gefahren bewusst, denen sie ausgesetzt sind.

Walter Kägi

Weiterführende Informationen:

Kaspersky 2013: «Global Corporate IT Security Risks: 2013», heruntergeladen von https://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf

Corporate Trust 2014: «Studie: Industriespionage 2014. Cybergeddon der deutschen Wirtschaft durch NSA & Co?», heruntergeladen von https://www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf

STA - VORSTAND

Titel	Name Vorname	Ressort	Funktion / Institution	E-Mail
Dr.	Fritz Gantert	Wirtschaft	Unabhängiger Verwaltungsrat / Unternehmer	fbg@bluewin.ch
	Urs Breitmeier	Wirtschaft	CEO / RUAG Holding AG	urs.breitmeier@ruag.com
	Peter Huber	Wirtschaft	President / Meggitt Sensing Systems	peter.huber@ch.meggitt.com
	Walter Kägi	Wirtschaft	CEO / Atos Schweiz AG	walter.kaegi@atos.net
	Giovanni Giunta	Wirtschaft	Stiftung KMU Next	giovanni.giunta@bluewin.ch
	Martin Sonderegger	Beschaffung & Technologie	Rüstungschef / armasuisse	martin.sonderegger@armasuisse.ch
Dr.	Thomas Rothacher	Beschaffung & Technologie	Leiter KB Wissenschaft + Technologie / armasuisse	thomas.rothacher@armasuisse.ch
KKdt	André Blattmann	Armee	Chef der Armee / Departamentsbereich Verteidigung	andre.blattmann@vtg.admin.ch
Div	Hans-Peter Walser	Armee	Chef Armeestab / Departamentsbereich Verteidigung	hans-peter.walser@vtg.admin.ch
Div	Daniel Baumgartner	Armee	Chef LBA / Departamentsbereich Verteidigung	daniel.baumgartner@vtg.admin.ch
	Daniel Neuenschwander	Wissenschaft	Leiter Raumfahrt / Staatssekretariat für Bildung, Forschung & Innovation	daniel.neuenschwander@sbfi.admin.ch

AUSBLICK STA 2016

Rüstungsmaterialpräsentation 2016
15. April 2016, Frauenfeld

Generalversammlung
21. Juni 2016, tbd

Herbstveranstaltung
3. November 2016, Mannschaftskaserne Bern