Rüstung und Technik

Rohde & Schwarz: Erfolgreiches Familienunternehmen

In der Februar-Ausgabe 2014 stellten wir die Schweizer Niederlassung von Rohde & Schwarz, die Roschi & Schwarz AG vor. Am 20. Februar 2014 hatten wir Gelegenheit, uns am Hauptsitz des erfolgreichen Familienunternehmens in München umzusehen.

AUS MÜNCHEN BERICHTET OBERSTLEUTNANT PETER JENNI, RESSORTREDAKTOR

Ganz in der Nähe des Ostbahnhofes in München, nach einem kurzen Spaziergang von gut fünf Minuten, steht man auf dem für Schweizer Verhältnisse imposanten Gelände von Rohde & Schwarz. Dank der Nähe der Bahn verzichten viele Mitarbeitende auf die Anreise mit dem Privatwagen, Parkplätze sind auch hier rar.

Neben verschiedenen älteren Gebäuden umfasst die Anlage auch Neubauten, ein weiterer Ausbau vor Ort wäre möglich. Alles gesichert mit Eingängen, die nur mit Badges durchschritten werden dürfen. Das Kontrollpersonal macht trotz der frühen Morgenstunden und dem unfreundlichen Nebelwetter einen freundlichen, aber bestimmten und kompetenen Eindruck.

Drahtlose Kommunikation

Rohde & Schwarz steht nach eigenen Angaben seit über 80 Jahren für Qualität, Präzision und Innovation auf dem vielfältigen Gebiet der drahtlosen Kommunikationstechnologie. Das unabhängige Familienunternehmen ist nach wie vor in der Lage, das Wachstum aus eigener Kraft und ohne Banken zu finanzieren. Es ist somit auch keinem hektischen und kurzfristigen Quartalsdenken unterworfen und kann entsprechend langfristig planen. Das Unternehmen ist in mehr als 70 Ländern vertreten und beschäftigt rund 9300 Mitarbeitende, davon 5650 in Deutschland; am Standort des Hauptsitzes allein arbeiten 2500 Mitarbeitende.

Im vergangenen Geschäftsjahr erreichte der Umsatz rund 2 Milliarden Euro, davon flossen 15 Prozent in die Forschung und Entwicklung. Seit 2008 konnte der Umsatz von 1,5 auf nahezu 2 Milliarden Euro gesteigert werden, parallel dazu stieg die Zahl der Mitarbeitenden von 7400 auf 9300 und die Investitionen in Forschung und Entwicklung wurden von 227 auf 295 Millionen Euro erhöht.

75 Prozent der Belegschaft haben eine technische Ausbildung. Der Exportanteil am Umsatz beläuft sich auf 90 Prozent. 39 Prozent werden in Europa, nach Afrika und dem Nahen Osten geliefert, 43 Prozent nach Asien, Australien und Ozeanien sowie 18 Prozent nach Nord- und Südamerika.

Die Verantwortlichen legen Wert auf die Feststellung, dass die verkauften Geräte bis zu 30 Jahre im Einsatz stehen. Das bedingt eine hohe Qualität. Um diesem Anspruch zu genügen, findet die Produktion in firmeneigenen Betrieben überwiegend in Deutschland, Tschechien, Singapur und Malaysia mit einer grossen Fertigungstiefe statt.

Diese Unabhängigkeit erlaubt Flexibilität und Qualität. Die Variabilität der Fertigungsorganisation zur Bewältigung der grossen Produktevielfalt bei wechselnden Losgrössen garantiert eine schnelle Reaktion auf sich ändernde Marktanforderungen. Diese Philosophie erlaubt es, auf allen Arbeitsgebieten unter den international führenden Anbietern zu sein.

Gliederung

Rohde & Schwarz ist neben den zentralen Diensten in fünf Geschäftsbereiche gegliedert:

- Messtechnik: Rohde & Schwarz ist einer der weltweit grössten Hersteller von elektronischer Messtechnik.
- Rundfunktechnik: In mehr als 80 Ländern empfangen Fernsehzuschauer und Radiohörer Programme, die über Sender von Rohde & Schwarz verbreitet werden.
- Sichere Kommunikation: Das Münchner Unternehmen beliefert alle Truppengattungen mit interoperablen Funksystemen für den Einsatz am Boden, zu Wasser und in der Luft. Dank der komplexen Verschlüsselungsverfahren erfüllen die Systeme höchste nationale und internationale Sicherheitsstandards.
- Funküberwachungs- und -ortungstechnik: Die Empfänger, Funkpeiler, Signalanalysatoren, Antennen und massgeschneiderten Systeme erlauben dem Kunden, seine Aufgaben zuverlässig zu erfüllen.
- Mit dem weltumspannenden Service-Netz hilft Rohde & Schwarz den Kunden bei der Sicherung ihrer Investitionen.

Technische Meilensteine

In den dreissiger Jahren des vergangenen Jahrhunderts entstand bei Rohde & Schwarz die weltweit erste transportable

Das hochdatenratige Software Defined Radio (R&S(R)SDTR) funktioniert.

Das Technologie Zentrum von Rohde & Schwarz in München.

Bilder: Rohde & Schwarz

Quarzuhr, ein Jahrzehnt später Europas erster UKW-Rundfunkempfänger. In den fünfziger Jahren der Kurzwellenempfänger EK 07 und zehn Jahre später Europas erstes Fluglärmüberwachungssystem. In den 1990er-Jahren fand mit dem GSM-Systemsimulator der Startschuss in die digitale Welt des Mobilfunks statt.

Im neuen Jahrhundert entwickelten die Ingenieure die ersten softwarebasierten Funkgeräte für militärische Anwendungen und den weltweit ersten Spektrumanalysator von 0 bis 67 GHz. Vor wenigen Jahren wurde das erste Oszilloskop mit digitalem Trigger im Hause Rohde & Schwarz gebaut.

Neue Märkte

Die Produktion erfolgt nach wie vor in eigenen Werken in Deutschland. Um in den Besitz von wichtigen Technologien und Märkten zu gelangen, wurden in der Vergangenheit einzelne kleinere Firmen zugekauft. Dieses Vorgehen ist in der Regel effizienter als über den Aufbau einer neuen Organisation.

Neue Märkte werden gemäss Thomas Zeller, Leiter strategisches Marketing im Geschäftsbereich Funkkommunikationssysteme, erschlossen, indem man die operativen Herausforderungen des potenziellen Kunden analysiert und entsprechend optimierte Systeme und Produkte anbietet. Es geht ihm dabei zuerst um den Aufbau von Vertrauen. Die Qualität und das Vertrauen in die Firma dürften die wesentlichsten Gründe für den Unternehmenserfolg sein.

Sichere Kommunikation

Allgemein bekannt ist, dass die Armeen ihre Informationen sicher, zuverlässig und zeitnah austauschen wollen.

Davon hängt ein wichtiger Teil des Erfolgs nationaler und internationaler Missionen ab. Rohde & Schwarz beliefert alle Truppengattungen mit interoperablen Funksystemen für den Einsatz am Boden, zu Wasser und in der Luft. Dank wirksamen Verschlüsselungsverfahren erfüllen die Systeme nationale und internationale Sicherheitsstandards. Die neuen softwarebasierten taktischen Funkgeräte vom Typ R&S SDTR auf der Basis der SCA-Architektur erlauben den Einsatz in den Einsatzszenarien der Zukunft.

Auch die zivile Flugsicherung stützt sich in 80 Ländern an mehr als 200 Flughäfen und Flugleitstellen auf die Funksysteme von Rohde&Schwarz ab. Für Unternehmen, Behörden, Regierungsstellen, kritische Infrastrukturen und das Militär entwickelt das Münchner Unternehmen Verschlüsselungen zur geschützten Sprach- und Datenübertragung via Funk, Mobilfunk- und Verbindungen über das Festnetz.

Die Geräte von Rohde & Schwarz benötigen für die Nutzung dank der erwähnten Verschlüsselungen keine speziell ausgebildeten Funker. Der Wehrmann muss sich nicht mehr mit Verschlüsselungslisten abmühen. Er kann sich voll auf seine Aufgaben auf dem Gefechtsfeld konzentrieren.

Der Auftrag

Die Spezialisten von Rohde & Schwarz haben sich bezüglich der Lösungen für das Militär verpflichtet, den Militärs ein Partner zu sein, der ihre Bedürfnisse erkennt und Lösungen anbietet, die es ermöglichen, die Aufgaben auf dem Gefechtsfeld zu erfüllen. Dazu gehört unter anderem das Erreichen der gesicherten Informationsüberlegenheit. In den modernen Armee ist alles vernetzt, jeder Soldat ist eingebunden, und die Systeme und Geräte müssen verschlüsselt einen hohen Durchsatz von Daten gewährleisten.

Die neuen softwarebasierten Geräte ermöglichen eine klare Übertragung, sind dank neuer Frequenzsprungverfahren schwierig zu stören, und der Kunde legt die Verschlüsselung selber fest. Vor dem Einsatz findet ein Abgleich der Systeme und Geräte in den Fahrzeugen und bei den Wehrmännern statt.

Nach eigenen Angaben ist Rohde & Schwarz in Deutschland auf diesen Gebieten Technologieführer und bietet Vertrauen, Zuverlässigkeit und Beständigkeit basierend auf den neusten Technologien, deutschem Ingenieurwesen, Zuverlässigkeit, Qualität und Produkten, die heutigen und künftigen Anforderungen gerecht werden.

Cyberkrieg in vollem Gang

Wenn die Clausewitz-Gesellschaft zum Berliner Colloquium ruft und zum Thema erst noch den Cyberkrieg erkürt, dann wartet sie auch mit erstklassigen Rednern auf. Abschliessende Antworten erwartete vom 18. bis zum 20. März am Colloquium 2014 niemand – rasend schnell breitet sich der Cyberwar aus. Konsens herrschte zur Tatsache: Der Cyberkrieg hat längst begonnen, und die gefährlichsten Akteure sind die staatlichen – von Ost und West.

AUS BERLIN BERICHTET CHEFREDAKTOR OBERST PETER FORSTER

So renommierte Referenten und Moderatoren wie

- General Klaus Naumann, ehemaliger Generalinspekteur,
- General Volker Wieker, amtierender Generalinspekteur,
- Generalleutnant Kurt Herrmann, Präsident der Clausewitz-Gesellschaft,
- Oberst i Gst Dietmar Bierkandt, Bundesnachrichtendienst, Technische Aufklärung,
- Professor Marco Gercke, Cyberkrime Research Institute, Universität Köln,
- Markus Kolland, Geschäftsführer Airbus Defence & Space,
- William Schneider, U.S. Defence Science Board,
- Botschafter Sorin Ducaru, NATO-Hauptquartier

boten eine derart dichte Fülle von Informationen, dass im Rahmen der vorliegenden Berichterstattung bestenfalls Schwerpunkte hervorgehoben werden können.

Angriff auf die Ukraine

Die Tagung begann am historischen 18. März 2014, am Tag, an dem Wladimir Putin – wie ein Gast in Anspielung auf 1938 und den Anschluss von Österreich ans Dritte Reich spöttisch anmerkte – vor der Geschichte die Rückkehr der Krim ins Russische Reich vermeldete. Wie Botschafter Hans-Dieter Heumann, der Präsident der Bundesakademie für Sicherheitspolitik, einleitend mitteilte, begann die Invasion der Krim durch Putins Geisterarmee mit rund 40 Cyberangriffen auf ukrainische Einrichtungen.

Zivile und militärische Anlagen seien mit einer Überfülle von Nachrichten derart eingedeckt worden, dass sie ausfielen. Wichtige Elemente der ukrainischen Abwehr lagen lahm.

Zweierlei Schlüsselgelände

Parallel dazu griffen russische Hacker unter dem Code «BERKUT» digital das NATO-Hauptquartier in Belgien an – BERKUT, Russisch für Königs- oder Steinadler, ist der Name der russischstämmigen Sondertruppe, die von der neuen Regierung in Kiew Ende Februar sofort aufgelöst wurde, ebenso die Bezeichnung für ein russisches Luftschiff von 1910 und das Kampfflugzeug Suchoi Su-47.

Zwei Grundprobleme kristallisieren sich im Verlauf des Colloquiums als «Schlüsselgelände» heraus:

- Sicherheit im Cyberraum. Mehrheitlich sprachen die Redner den Cyberraum nach Land, See, Luft und Weltraum als neue fünfte Dimension an.
- Der digital-wirtschaftlich-militärische Komplex, in Anlehnung an Präsident Eisenhowers Schlagwort vom industriell-militärischen Komplex. Heute besässen weltweit tätige Internet-Firmen eine singuläre Machtstellung. Botschafter Heumann sprach sogar von der Übermacht dieser Unternehmen – weit vor den staatlichen Instanzen.

Sabotage, Spionage

Einig waren sich die Redner über die umfassende Umschreibung des Begriffs Cyberwar. Demnach umfasst der Cyberkrieg die gesamte Vernetzung der Welt. Das Internet gehört zu den kritischen Infrastrukturen und ist anfällig auf

- Sabotage,
- Spionage,
- Manipulation,
- Verweigerung.

Der Cyberwar ist in vollem Gange. Staatliche und nichtstaatliche Akteure nehmen die Bevölkerung als Geisel. Cyberangriffe können jederzeit und sofort ausgelöst werden. Sie haben ein gewaltiges Schadenpotenzial.

Wir wissen nicht einmal, was wir nicht wissen können. Möglicherweise kennen wir Cyberattacken nicht, die längst gegen uns geführt wurden.

Snowden: Hochverrat

Edward Snowden darf nach Ansicht der Cyber Community keinesfalls als Held angesprochen werden.

Er gilt vielmehr als Verräter, nach amerikanischem Recht sogar als Hochverräter, der seinem Land und Volk unendlich schadete. Fachlich ist er ein Administrator, kein Analytiker. Er konnte die gestohlenen Dokumente weder richtigen einordnen noch gültig bewerten.

Soziale Medien

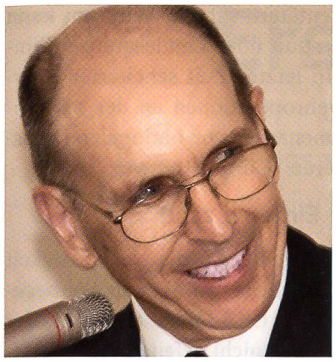
Die sozialen Medien werden in der Cyberszene durchaus als zu beachtende Grösse wahrgenommen.

Sie gelten als Treiber auch der politischen Umwälzung – siehe Arabien, siehe die Türkei, siehe Ukraine. Auch der internationale Terror bedient sich der sozialen Medien, die allein schon durch ihren Multiplikationseffekt genau betrachtet werden müssen.

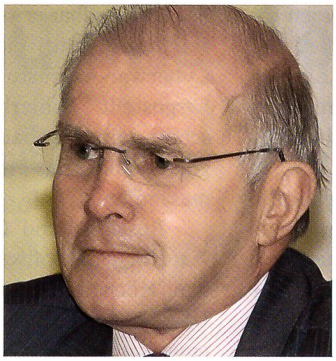
Überrumpelte Dienste

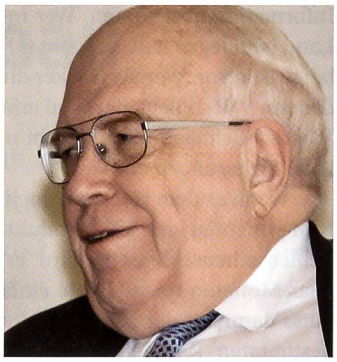
Putins Coup vom 1. März 2014 überrumpelte die westlichen Geheimdienste.

Wohl stellte deren Satelliten-Aufklärung Truppenbewegungen fest. Aber es fehlte dem Westen HUMINT, die Spionage über Menschen, die Streitkräfte, deren Absichten, Aufmarschräume und Kommandozentralen ausspähen. So überraschte Putins Gespensterarmee den Westen auf der Krim kalt.


GenLt Kurt Herrmann, Präsident Clausewitz-Gesellschaft.


Oberst i Gst Dietmar Bierkandt vom Bundesnachrichtendienst.


Gen Klaus Naumann, Ex-Generalinspekteur der Bundeswehr.


William Schneider vom U.S. Defence Science Board.

In Analogie zur früheren gegenseitigen atomaren Fähigkeit zur vollständigen Zerstörung müsse man heute von der gegenseitigen digitalen Abhängigkeit im Netz reden. Rund 100 Staaten besitzen defensive und offensive Kapazitäten zum Cyberwar.

Ungelöst sind die Fragen nach dem rechtlichen Status von handelnden Zivilpersonen, von handelnden Militärs und der Neutralen (Schweden und die Schweiz).

Deutsche Firmen im Visier

Cyberoperationen berühren nicht nur Armeen. Nein, sie ziehen die gesamte Gesellschaft in Mitleidenschaft. In Deutschland verursachen Cyberattacken Schäden in Milliardenhöhe, namentlich in der Wirtschaft. Deutsche Weltfirmen zählen mit ihren Erfindungen und Patenten zu den begehrten Zielen der Cyberspionage.

Namentlich Schwellenländer aus der ganzen Welt greifen deutsche Firmen gezielt an. Sollten diese Attacken Erfolg haben, dann droht der deutschen Wirtschaft die Einbusse ihres derzeit noch erheblichen Vorsprungs an Wissen und Können. Das könnte der Bundesrepublik in jeder Hinsicht gewaltige Probleme bringen.

Wie Naumann berichtete, schlug im Kosovo-Luftfeldzug in der NATO das Militär vor, Milosevic auch digital offensiv gegenüberzutreten. Um Himmels Willen nein, habe der NATO-Rat geantwortet.

In Taiwan erfuhr Naumann, dass Rotchina eine 50 000 Mann starke Cyberwar-Truppe aufbaute – mit dem Ziel, Nationalchina im Jahr 2015 strategisch zu lähmen. Taiwan soll dann den Festlandchinesen wie ein reifer Apfel in den Schoss fallen.

Der Amerikaner William Schneider korrigierte die Zahl 50 000 dann auf über 100 000. Die Cybertruppe unterstehe in Peking weder der Armeeführung noch dem Verteidigungsministerium, sondern direkt der Kommunistischen Staatspartei. Seit einem Jahrzehnt berät Marco Gercke, angestammt Professor für Straf- und Völkerrecht in Köln, die NATO und westliche Regierungen. Er schliesst nicht mehr aus, dass ein strategischer Paradigmenwechsel weg vom kinetischen Krieg zum Cyberwar führen könnte – weg von der physischen Vernichtung hin zur digitalen Lähmung. Zugegeben: eine kühne These.

Gercke bestätigte die Anfälligkeit des NATO-Hauptquartiers, im Jugoslawienkrieg und jetzt wieder im Kontext der Krim. Werde jemand angegriffen, sei es ihm zuerst egal, wer angriff: Das System ist lahm, die Verbindungen sind zerstört, das Opfer ist erst einmal hilflos.

Dennoch dürfe die Hoffnung nicht aufgegeben werden, dass das Netz eines Tages eingegrenzt werde. Das sei indessen nur in Kooperation aller staatlichen Akteure möglich – auch das am Tag nach Putins Triumphrede im Kreml ein mutiger, zuversichtlicher Ansatz.

Gibt es ein Rotes Kreuz?

Gibt es im Cyberwar das Schutzzeichen des Roten Kreuzes? Seit Henri Dunant schützt das Rote Kreuz auf weissem Grund Ärzte, Krankenschwestern, Verwundete und Kranke. Kommt im Cyberkrieg ein Rotes Kreuz für medizinische Einrichtungen? Könnten sich die Akteure darauf verständigen, Spitäler, Operationssäle und die Verwundetenlogistik nicht anzugreifen?

Nach wie vor setzen die staatlichen Akteure auf Verschleierung. Die Besetzung der Krim vom 1. März 2014 zeige: Wer Abzeichen von der Uniform entfernt und Nummernschilder von Fahrzeugen abschraubt, der stiftet Verwirrung und Unsicherheit. Ebenso gehen Staaten im Cyberkrieg vor. Der Code «BERKUT» für den Angriff auf die NATO gehört noch zu den harmlosen Streichen.

Die deutsche Telekom stellt für Hacker Honigtöpfe auf. Der Honigtopf zeigt ihr, wer wo wann mit welchen Mitteln angreift. Freilich gibt es keinen 100-prozentigen Schutz. Staaten und Firmen richteten ihre Aktivitäten in der Regel zu 70 Prozent auf die Abwehr aus. Sie kommen aber nicht umhin, die restlichen 30 Prozent der Offensive zu widmen.

Schliche und Tricks

Wer nicht angreifen kann, der kann nicht verteidigen – in der amerikanischen Doktrin: *If you want to play defence, first learn offence*. Jede militärische Übung kenne das Red Team, die Opfer, die Markeure. Wer sich im Cyberwar verteidige, der müsse die Schliche und Tricks der Angreifer kennen und beherrschen.

Kann ein Hacker den Bahn- und Luftverkehr eines Landes lähmen? Die Deutsche Bahn nimmt für sich die Fähigkeit in Anspruch zu verhindern, dass zwei Züge aufeinander zurasen. Das sei jedoch nicht die Absicht des Hackers: Er lasse den Zug mitten auf der Strecke stehen und blockiere so den gesamten Verkehr.

Im Bereich der Spionage wollen viele Hacker einen Staat nicht lähmen, sie wollen nur möglichst viel militärische, politische, wissenschaftliche und ökonomische

Malaysia: Nur Gerücht

Während des Clausewitz-Colloquiums machten Zeitungsmeldungen die Runde, wonach zwischen dem Cyber und dem Verschwinden der Boeing 777 der *Malaysian Airlines* ein Konnex bestehe.

Der Flug MH370 sei via Mobiltelefon zum Absturz gebracht worden.

Diese Theorie wurde als unhaltbares Gerücht entlarvt. Wohl könnten Mobiltelefone grossen Schaden anrichten; aber es sei schon technisch unmöglich, via Mobiltelefon ein derart grosses Flugzeug wie die Boeing 777 der *Malaysian Airlines* zum Absturz zu bringen.

Information abschöpfen. Wer indessen ein Land lahmlegen will, der geht raffiniert und langfristig vor. Wer als Hacker die Laufbänder von VW stilllegt, der wird erfahren, dass VW den Schaden rasch behebt und zusätzliche Sicherungen einbaut.

Wenn es dem Hacker jedoch gelingt, in Komponenten der VW-Produktion digital Fehler einzuschleusen, wird er nach ein paar Monaten reiche Ernte einfahren: VW muss dann auf der ganzen Welt von einem bestimmten Typ Zehntausende von Automobilen zurückrufen, in denen der Fehler durchschlägt – eine Katastrophe für das Werk, eine Kalamität für Heerscharen von Kunden.

Berlin muss nachziehen

Auch in der NATO schaffen Bündnispartner von Deutschland offensive Kapazitäten. Deutschland muss nachziehen, auch Deutschland muss offensiv operieren können. Dazu braucht es im Rechtsstaat Deutschland den rechtlichen Rahmen. Nur das NATO-Handbuch reicht dazu nicht. Deutschland kann im Cyberwar nur mit einer starken Abwehr und einer gründlichen Offensivstrategie bestehen.

Die Vereinigten Staaten gehen offensiv subtil vor. Ihre Dienste schrecken nicht davor zurück, auch Verbündete anzugreifen. Die amerikanischen Angreifer schöpfen selbst in befreundeten Staaten Informationen bis ins Detail ab.

Estland das erste Opfer

Der erste umfassende Cyberangriff der noch jungen Geschichte des World Wide Webs galt der Republik Estland. Die Attacke legte den baltischen Staat eine Woche lang partiell lahm. Über den Umfang der Lähmung gingen auf dem Colloquium die Meinungen auseinander. Von einer teilweisen Lähmung kann indessen mit einiger Sicherheit gesprochen werden.

Die USA gingen in der Frühphase des Cyberwars eher zufällig vor. Während ihrer militärischen Offensiven gegen Grenada (1983) und Panama (1989) setzten sie Cybermittel ein. Systematisch attackieren die Vereinigten Staaten seit den 1990er-Jahren. Die amerikanische Führung erkannte, dass

- der Cyberkrieg im Vergleich zu allen anderen Kriegsarten extrem kostengünstig ist;
- der Cyberkrieg schnelle, nachhaltige Erfolge erlaubt;
- der Cyberkrieg eine gute technologische Forschung voraussetzt, weil die technische Entwicklung auch operativ und taktisch den Ton angibt.

Als verwundbar erweist sich im Westen die Nachschubkette. Viele Komponenten der Cyberwar-Ausrüstung werden in China hergestellt. Fehlerhafte Software kann schon dort eingebaut werden. Das Pentagon erkannte das Problem und traf Gegenmassnahmen.

Russland und China verkaufen Malware, Schadensoftware, an kriminelle Banden. Höchste Alarmstufe herrschte in den USA, als die Chinesen eine prominente amerikanische Firma angriffen, die schadhafte Software eingesetzt hatte. Es war ein Unternehmen aus der Rüstungsbranche, das Zugriff zu Geheimdokumenten besass. In der Abwehr gilt es, die wirklich kritischen Daten zu definieren und diese und nur diese mit allen Mitteln zu schützen.

Absolut sicher? Nein!

Oberst i Gst Bierkandt, der Spezialist vom Bundesnachrichtendienst in Pullach, nannte als Ziel der deutschen Abwehr, die Risiken aus dem Cyberraum seien auf ein vernünftiges Mass zu reduzieren. Damit gestand er: Absolute Sicherheit besteht nicht. Vor dem Internet sei die Abwehr recht einfach gewesen. Telefon, Telefax und Telex liessen sich leicht überwachen. Von 2002 an wurden mehr Daten digital als analog gespeichert. 2002 gilt als das Geburtsjahr des digitalen Zeitalters.

Fast jeder trägt heute mit seinem Mobiltelefon sein eigenes Überwachungsgerät mit sich. Die technische Aufklärung kann jederzeit feststellen, wo sich der Mensch aufhält.

Spam jeder Art

Der Haupttrend besteht im enormen Zuwachs an Informationen – durchsetzt von Spam jeder Art, wie jeder weiss. Die enorme Fülle von Daten stellt die Geheimdienste vor riesige Probleme: Was ist herauszufiltern? Was ist für die Sicherheit relevant? Wollen wir den gläsernen Menschen?

Damit der BND in der enormen Datenmenge erfolgreich arbeitet, muss er «aus ganzen Fischschwärmen den richtigen Fisch fangen». Der Dienst benutzt Suchbegriffe. Er überwacht Absender und Empfänger und setzt Suchwörter an.

Der Einsatz von Suchbegriffen geht nicht so simpel vonstatten, wie sich das die Dampfplauderer vom Dienst vorstellen. Mit Wörtern wie «Bombe» oder «Angriff» wäre der BND hoffnungslos überfordert.

Mehr Erfolg versprechen zum Beispiel chemische Begriffe, wie sie für Schmuggel- oder Sprengstoffdelikte angewendet werden. Chemische Formeln können zu potenziellen Attentätern führen. Wirksam kann die Kooperation über Landesgrenzen hinweg sein. In letzter Zeit scheiterten allerdings Abwehroperationen an der schlechten Zusammenarbeit von nationalen Diensten über deren «Gärten» hinweg.

Jeder Einzelne zählt

Schaden richtet oft die Nachlässigkeit einzelner Mitarbeiter an. Wer als Werbegeschenk wahllos USB-Sticks annimmt, der ist vor Trojanern nicht gefeit. Geschäftsreisende werden in aller Welt in teuren Hotels ausgespäht. Wer Mails mit unbekanntem Absender öffnet, kann schon verloren sein. Allein schon das Öffnen solcher Mails kann den eigenen Computer verseuchen.

Scheinbar spurlos verschwinden Datenträger auch aus gut geschützten Unternehmen und Amtsstellen. Spionagesoftware ist heute derart raffiniert ausgestattet, dass Firmen oft jahrelang nicht merken, dass sie ausgespäht werden. Das Opfer weiss nicht, dass es Opfer ist.

Mafia am Werk

Kriminelle Organisationen kommen vor allem vom russischen Territorium. Doch überall, wo die organisierte Kriminalität am Werk ist, schlagen mafiöse Banden zu, auch in Südeuropa, auch in Afrika, in Latein- und Nordamerika und natürlich in Ostasien (die Triaden, die Yakuza).

Nichtstaatliche Akteure zeichnen für das Gros der Attacken verantwortlich. Islamische Terroristen nutzen das Internet für ihre diabolische Propaganda.

Die grösste Gefahr geht von staatlichen Akteuren aus. Sie besitzen mittlerweile immense Kapazitäten. Stuxnet, die erfolgreiche Operation gegen iranische Rechner im Bereich der atomaren Rüstung, überstieg die Fähigkeiten nichtstaatlicher Players. Es waren Staaten, welche die iranische Rüstung um ein halbes Jahr zurückwarfen. Wer an der Levante sucht und auch in Nordamerika, der wird nicht weit daneben liegen.

Fazit: Vieles liegt im Argen

- Im Cyberraum schreitet die Entrechtlichung kräftig voran. Im Gegensatz zum kodifizierten Recht entsteht Völkerrecht nur durch Handeln. Im Cyberwar liegt da vieles im Argen.
- Der Staat wird Tag für Tag, Minute für Minute angegriffen. Ohne eine starke Abwehr und die Fähigkeit zum offensiven Handeln erleidet die Gesellschaft unermesslichen Schaden.
- Der Staat muss handeln, will er Schaden abwenden.

Ersatz, Aufbau und Abbau

Das Rüstungsprogramm 2014 (RP 14) enthält erstmals nicht nur neues Gerät, sondern auch eine Liste über geplante Ausserdienststellungen. Letztere werden noch zu Diskussionen Anlass geben.

OBERSTLEUTNANT PETER JENNI, RESSORTREDAKTOR

Mit dem RP 14 beantragt der Bundesrat dem Parlament die Beschaffung von Rüstungsgütern für 771 Millionen Franken.

Um die Informations- und Kommunikationstechnologie-Infrastruktur (IKT) zu vereinheitlichen und gleichzeitig die Sicherheit zu erhöhen, soll das in der Immobilienbotschaft VBS 2013 bewilligte Bauvorhaben mit neuer IKT-Infrastruktur ausgerüstet und ins Führungsnetz Schweiz eingebunden werden. Dazu wird ein Kredit von 120 Millionen Franken angefordert. Die Beschaffung soll zwischen 2016 und 2021 erfolgen.

Für 32 Millionen Franken sollen Laserschusssimulatoren beschafft werden, mit denen Kommandopanzer und geschützte Transportfahrzeuge eine realitätsnahe Ausbildung betreiben können.

Für 440 Millionen Franken wird eine erste Tranche eines leichten und geländegängigen Motorfahrzeuges vom Typ Mercedes-Benz G 300 CDI 4×4 beantragt. Es soll die vor 25 Jahren eingeführten Puch-Fahrzeuge ablösen. Die Beschaffung der 3200 Wagen soll im Zeitraum 2016 bis 2022 stattfinden.

Schliesslich beantragt der Bundesrat für 179 Millionen Franken die Anschaffung von zwölf Brückenlegesystemen. Das zu beschaffende System befähigt die Truppe unter taktischen Einsatzbedingungen zum Überwinden von Hindernissen bis zu 25 Metern Breite. Es können Fahrzeuge mit bis zu 84 bzw. 73 Tonnen über die Brücke fahren.

Werkbild

Um eine realistische Ausbildung mit den geschützten Mannschaftstransportfahrzeugen zu ermöglichen, wird die aufgebaute Waffenstation mit Lasersendern (Aktivsystem) und einem Passivsystem (Ziel erkennt die Treffer) versehen.

Ausserdienststellungen

Im zweiten Teil des RP 14 beantragt der Bundesrat die Ausserdienststellung von umfangreichem Rüstungsmaterial. Bis 2016 sollen die derzeit noch im Einsatz stehenden F-5-Tiger-Kampfflugzeuge verkauft oder verschrottet werden. Das heisst ebenfalls, dass die Patrouille Suisse nicht mehr in der heutigen Form existieren wird.

Dazu kommen 96 Pz 87 Leo A4. Sie werden voraussichtlich zwischen 2015 und 2020 ausser Dienst gestellt. Ferner sollen 162 Pz Hb M109 KAWEST im gleichen Zeitraum verkauft oder verschrottet werden.

Widerstand

Gegen diese Pläne des Bundesrates hat sich bereits massiver Widerstand formiert. In einer Eingabe an die Mitglieder der Sicherheitspolitischen Kommission des Ständerates haben sämtliche Milizverbände der Schweiz gegen die «voreilige Verschrottung von Rüstungsmaterial» protestiert. Die Organisationen wollen zuerst die verbindlichen Entscheide zur Weiterentwicklung der Armee abwarten (WEA).

Der Bericht zur Vernehmlassung der WEA stösst ebenfalls auf Widerstand. So hat unter anderem der Verein Sicherheitspolitik und Wehrwissenschaft dazu in einer ersten Stellungnahme festgehalten: «...ein weiteres Beispiel für Inkompetenz in der Verwaltung und für eine fortgeschrittene Denaturierung des Vernehmlassungsverfahrens: Mit Akribie wird aufgeführt, wer was zu den einzelnen Punkten gesagt hat.

Eine Gewichtung nach Referendumsmacht, Expertise und Relevanz findet nicht statt. Die Positionen werden brav gezählt wie Erbsen; dabei geraten Kraut und Rüben durcheinander – von Kantonen über Bundesratsparteien zu Splittergruppen bis zu Stimmen von Einzelmasken. Die Absicht ist klar: Unübersichtlichkeit, das hilft, den eigenen Kurs möglichst ungestört durchzuziehen. Damit die Armee ihre Rolle als Machtmittel des Staates wahrnehmen kann, muss sie über eine klare Doktrin sowie über ausgewiesene Fähigkeiten verfügen. Die Armee (muss) zum Know-how-Erhalt als Ganzes einsetzbar bleiben, was derzeit weder führungsmässig noch mit der geplanten WEA gegeben ist.»