Chancen und Risiken in der digitalisierten Welt

Ein gewohnt gehaltvolles Programm bietet vom 20. bis 22. September 2013 die Gesellschaft der silbergrauen Offiziere an ihrem Forum im Bad Horn. Oberst Michael Kientsch, der kompetente Präsident, führt in das Thema ein: Chancen und Risiken in einer digitalisierten Welt. Naturgemäss dominieren dann die erheblichen, oft unterschätzten Risiken.

Kientsch begrüsst die Ehrengäste: an der Spitze den Thurgauer Regierungsrat Claudius Graf-Schelling; Korpskommandant André Blattmann, Chef der Armee; Divisionär Jean-Paul Theler, Chef FUB; Brigadier Willy Siegenthaler, Kdt LVb FU 30; Oberst Willi Bühn, Präsident der FU-Stiftung; und Oberst Thomas Hugentobler, ZSO Kdt Inf Br 7 (vertritt die Inf Br 7).

Datenpannen schaden

Kientsch: «Wir müssen die Vernetzung verantwortungsbewusst nutzen. Datenpannen wie bei Swisscom oder Vodaphone verunsichern die Bevölkerung. Der Ruf nach der Meldepflicht wird laut. Wer Daten verliert, der riskiert die Wettbewerbsfähigkeit und/oder seinen guten Ruf.»

- «Wissen wir, was den Daten widerfährt, wenn wir anrufen oder mailen?»
- «Weiss die KMU, dass ihre guten Ideen womöglich längst beim Konkurrenten sind?»
- «Sind wir uns bewusst, dass die Manipulation immer einfacher wird?»

Gehört zur Verteidigung

André Blattmann: «Die digitale Bedrohung ist allgegenwärtig. Cyber-Angriffe lösen Krisen aus. Der Finanzplatz Schweiz kann jederzeit via Cyber attackiert werden.» Die Schweiz müsse jeden Tag an ihrer digitalen Abwehrlinie arbeiten:

- *Cyber Defense* gehört integral zum Gesamtsystem Verteidigung.
- Die Einsatzbereitschaft ist jederzeit sicherzustellen, auch für die Zivilen.
- Die Miliz kommt zum Tragen. Ohne Miliz können wir nicht aktiv sein.
- *Cyber Defense* gehört zu den Basisleistungen der Armee. Das Einsatznetz Schweiz ist stets in Betrieb.
- Die Swisscom garantiert in ausserordentlichen Lagen die Verbindungen nicht. Darum braucht die Schweiz das geschützte Einsatznetz Verteidigung.

Temperamentvoll schildert Daniela Vorburger, Projektleiterin der Strategischen Führungsübung 2013, den Cyber-Angriff, den es in der Übung abzuwehren galt.

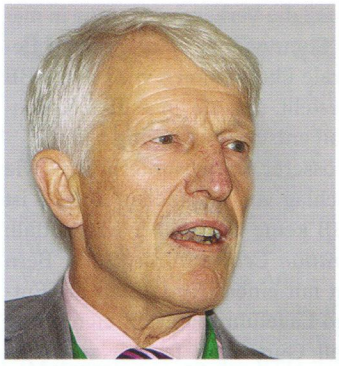
Cyber-Fachleute gesucht

Die Armee müsse sich selber schützen. So das Tor zur Kaverne in Meiringen: «Wenn wir fliegen wollen, müssen *wir* das Tor steuern, nicht der Gegner.»

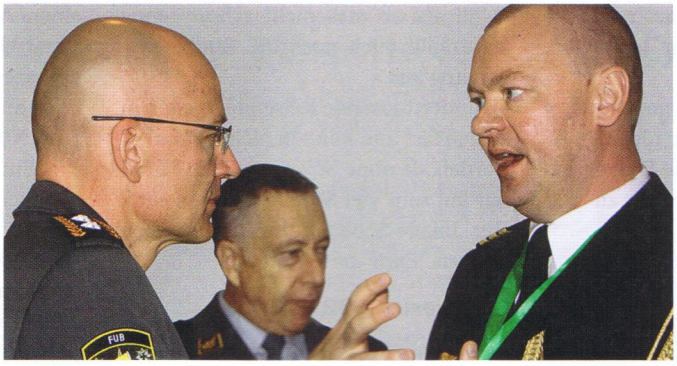
Wenn die zivile Infrastruktur zerstört sei, dann springe die Armee ein. Mit wem kann die Schweiz zusammenarbeiten?

Dank an den Sozialdemokraten Graf-Schelling

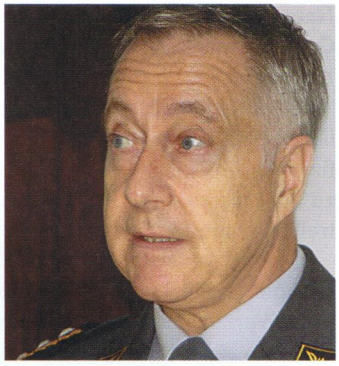
Schon im Abstimmungskampf hatte sich der sozialdemokratische Regierungsrat Claudius Graf-Schelling immer wieder kraftvoll für die Wehrpflicht eingesetzt. In Horn wiederholte er dieses Bekenntnis ausdrücklich. Armeechef Blattmann dankte Graf-Schelling für seine Position, die von der offiziellen SP-Linie abweicht.



General Jo Godderij (NL).



Div Jean-Paul Theler und Oberstlt Petersson, VA Schweden.



Blattmann: Jederzeit bereit.

Blattmann: «Da glaube ich nicht an die multilaterale Kooperation, jetzt weniger denn je. Es sind ausgesuchte, ganz wenige Staaten, denen wir vertrauen können. Ich jedenfalls würde dem *Cyber Center* Tallinn keine Info überlassen.»

Der Armeechef schliesst mit einem Aufruf: «Wer von Ihnen gute Cyber-Fachleute kennt, bitte melden Sie diese dem Obersten i Gst Vernez, unserem Delegierten für *Cyber Defense*.»

Info kann Leben retten

Einen rassigen Auftritt hat der niederländische F-16-Pilot und NATO-General Jo Godderij: «Wir führen den Krieg heute so vernetzt wie möglich.» Zu Beginn des Afghanistan-Krieges habe jeder sein eigenes Netzwerk mitgebracht. Heute stütze sich ISAF auf ein einziges Netz ab: «Das kann Leben retten.»

Das Führungskommando der Bundeswehr in Potsdam verfüge exakt über das Lagebild der deutschen Kommandanten vor Ort.

In der Datenanalyse habe die NATO gewaltige Fortschritte erzielt: «Es reicht nicht aus, *Big Data* zu besitzen und zu verarbeiten, wir müssen die Daten analysieren. Die NATO analysiert jeden Tag eine Datenmenge, die 90-mal dem Bestand der *National Library* der USA entspricht.»

Im Kampf gegen Verbrecher erlaube die Analyse Gegenmassnahmen: «In New York haben die Jets ein Heimspiel. Viele Häuser stehen leer. Wo ist die Gefahr am grössten? Dort patrouillen wir dicht.»

Direkt melden, Zeit gewinnen

Godderij erläutert englische Begriffe wie *virtual reality, artificial intelligence, universal translators* und *operational awarness*. Der letzte Begriff kann im Gefecht über Sieg oder Scheitern entscheiden.

Godderij: «Im Grunde ist es wie im Raumschiff *Enterprise*. Wer über alle Info in Echtzeit verfügt, der ist überlegen: in der Lagebeurteilung, der Entschlussfassung und der Führung im Kampf.»

Godderij, Vater eines Sohnes, der in den gefürchteten Spezialkräften der niederländischen Streitkräfte dient, nennt ein Beispiel: Eine Patrouille *Special Forces* entdeckt im Feindesland eine A-Bombe.

- Früher führte der Meldeweg die Hierarchie hinauf. Zeit ging verloren.
- Heute meldet der Patrouillenführer den Fund direkt dem *Component Commander*. Ohne Zeitverzug werden alle Chefs ins Bild gesetzt. Sofort wird entschieden, wie vorgegangen wird.

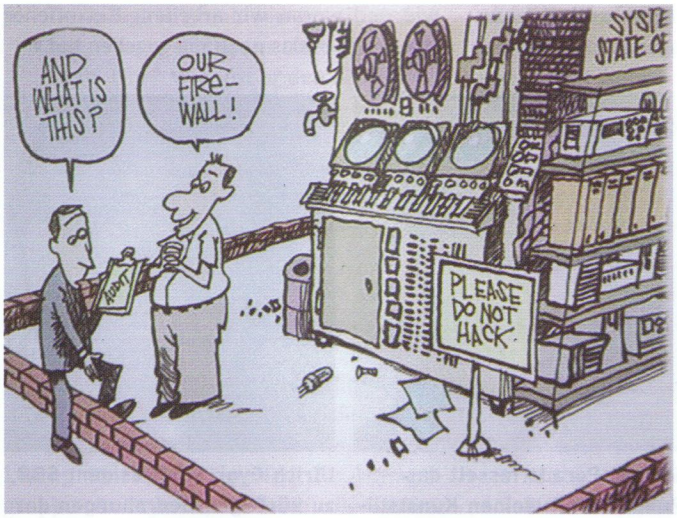
Godderij verschweigt die Gefahren nicht: «Wir sind mittlerweile total vernetzt. Wenn das System versagt oder wegen einer Schwachstelle ganz zusammenbricht, dann herrscht das Chaos.»

Gefährlicher USB-Stick

Als gefährlichen Gegner bezeichnet Godderij die Verräter: «50% der Daten gehen durch Verrat verloren.» Weiter nennt Godderij: Spione, die Organisierte Kriminalität, Hacker und Terroristen.

2008 brachen Hacker in die amerikanischen Streitkräfte ein. Diese benötigten ein volles Jahr, um die Schäden zu flicken. Die Operation Stuxnet, die Iran in der Atomrüstung um ein halbes Jahr zurückwarf, begann mit einem USB-Stick. Godderij: «Wäre ich oberster Chef, ich würde jeden Stick verbieten.»

Auch Verbündete könnten sich nicht durchwegs vertrauen: «In den AWACS-Maschinen der NATO fliegen stets mehrere



Auditor zur Mauer: «Was ist das?» Antwort: «Unsere Firewall.»

Präsident Kientsch, Oberst i Gst Vernez, der Cyber-Delegierte.

Nationen mit. Das führt automatisch zu Gefahren auch im *Cyber War*, der heute Realität ist.»

Godderij schliesst mit einer zuversichtlichen Note. Es gelte den Gegner zu identifizieren, die Gefahr zu verstehen, die Daten zu analysieren und Gegenmassnahmen zu treffen. Dann habe man Erfolg.

Am Beispiel der Olympischen Sommerspiele: «Peking 2008 hatte noch 90 kritische Vorfälle, London 2012 keinen mehr.» Godderij zitiert Albert Einstein: «Die Welt wird voller Idioten sein.» Das gelte jedoch nicht für Milizarmeen: «Soldaten aus dem Berufsleben bringen bestes Wissen mit.»

Gygi: Verletzbare SBB

Ulrich Gygi, VR-Präsident der SBB, konfrontiert die Zuhörer mit dem Jahr 2020: «Professionelle Hacker wetten, wer zuerst in eines der komplexen europäischen Bahnnetze eindringen kann.»

Ein Hacker geht auf die SBB los: «Beim Versuch, die Leittechnik der SBB zu hacken, findet einer eine Sicherheitslücke im Überwachungssystem eines Liftes und dringt so in das SBB-Netz ein.» Es folgt ein Horror-Szenario:

- «Voller Euphorie verändert der Hacker die im System hinterlegten Zugnummern, so dass alle Züge in der Schweiz dieselbe Nummer tragen.»
- «Es gelingt dem Hacker, die Steuerung der Energie und das SBB-interne Telecomnetz zu stören.»
- Die Folgen sind verheerend: «Innert kürzester Zeit wissen die Zugverkehrsleiter nicht mehr, welcher Zug sich wo befindet. Verschiedene Züge steuern im Bahnhof das gleiche Gleis an.»
- «Da sowohl das fixe als auch das mobile Telecomnetz gestört ist, können die Zugverkehrsleiter nur äussert schlecht Verbindung zu den Lokführern aufnehmen, um diese zu warnen.»
- «Und als ob dies nicht schon genug wäre, fällt auch noch die Energieversorgung aus.»
- «Hunderttausende Reisende stecken in Zügen fest und können nicht evakuiert werden, da ohne Strom auch die Türen nur mit sehr viel Mühe zu öffnen sind. Der Image-Schaden für die SBB ist immens. *Ende der Fiktion.*

Exponierter SBB-Fahrplan

Auch wenn die Geschichte nach einem *Science-Fiction*-Film töne: Die SBB seien verletzbar geworden. Noch vor 20 Jahren waren die Gefahren klar eingrenzbar: Energie- und Wasserversorgung, Verkehrswege und das Notfall- und Rettungswesen – plus Naturkatastrophen, Sabotage und kriegerische Angriffe. Die Schäden waren begrenzt.

Heute sei mit Cyber-Angriffen auf Computer, Netzwerke und Daten zu rechnen. Das Werkzeug sei einfach zu beschaffen: «2008 baute ein Schüler in Polen die Fernbedienung fürs Fernsehen so um,dass er Weichen der Lodzer S-Bahn umstellte und Züge zum Entgleisen brachte.»

Exponiert sei die Fahrplanabfrage auf der SBB-Webseite: «Jeden Monat werden einige Millionen Fahrpläne abgefragt, konzentriert innerhalb weniger Stunden am Tag. Zwischendurch weisen die Systeme vermehrt angriffsartige Streumuster und Belastungen auf. Das kann die Abfrage stark verlangsamen oder verunmöglichen.»

SBB wappnen sich

Die SBB begegnen der Gefahr durch vielfältige Vorkehrungen: «Jedes Jahr werden Szenarien in Übungen durchgespielt, Notfallkonzepte für die Hauptstrecken und die grossen Knotenbahnhöfe erstellt, aktualisiert und geschult.»

Die vier neuen Betriebszentralen in Lausanne, Olten, Pollegio und Zürich-Flughafen sind so ausgestaltet, dass bei einem Ausfall die Verkehrssteuerung in maximal vier Stunden von einer anderen Betriebszentrale übernommen wird. Die SBB ist so aufgestellt, dass sie im akuten Krisen- oder Notfall entscheidungsfähig bleibt.

Ein grösserer Betriebsunterbruch – wie der Steinschlag von Gurtnellen 2012 – ist für die SBB keine Krise, aber ein Notfall: «Das *Operation Center* Infrastruktur Bern übernimmt mit einem Notfallstab die Entscheid- und Lageführung des Ereignisses.»

Im Fall Gurtnellen fanden zwei- bis dreimal täglich Telefonkonferenzen statt. Daran nahmen ein Geologe, rund zehn Leitstellen von in- und ausländischen Cargobahnen, die Personenleitstelle SBB, die Betriebszentralen der SBB, der italienischen und der deutschen Bahn teil.

Facebook öffnet Tor und Tür

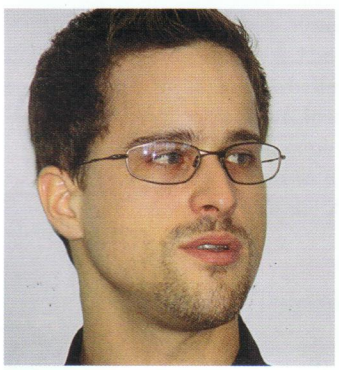
Christian Funk, *Senior Virus Analyst* Kapersky Lab, schildert packend die Angriffswaffe *Net Traveler* – unter dem Leitwort: Schnell rein, schnell raus, keine Spuren hinterlassen.

Opfer von *Net Traveler* seien Regierungen, Botschaften, Armeen, Rüstungsfirmen und Privatfirmen in den Bereichen *High Tech*, Raumfahrt, Laser. Die Weltkarte zeigt Schwerpunkte in Asien und Deutschland – nicht in der Schweiz.

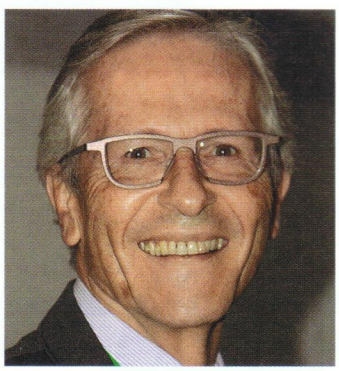
Net Traveler zeigt exemplarisch einen Angriff vom Eindringen bis zur Exfiltration der Daten. Das Eindringen erfolgt meist via Mail – unvergessen ist, wie viele Empfänger auf *I love you* hereinfielen.

Der Angreifer attackiert zielgerichtet: Welche Person offenbart Schwächen? Wie mache ich ihn oder sie neugierig? Worauf reagiert er?

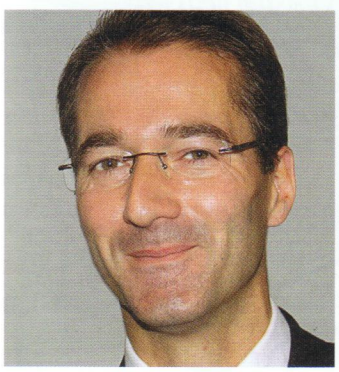
Zu Hilfe zieht der Angreifer *Facebook* oder *Twitter*. Funk: «Was geben wir da alles von uns preis! Unsere Vorlieben, wo, wie und woran wir arbeiten. Ein offenes Buch, wie es das noch nie gegeben hat.»



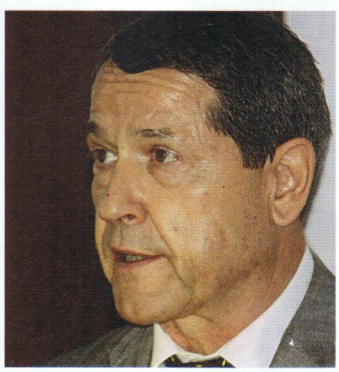
Christian Funk, von der Firma Kapersky Lab: Wie ein Angriff von Net Traveler abläuft.



Regierungsrat Claudius Graf-Schelling erhält Dank für sein Eintreten pro Wehrpflicht.



Gunnar Porada fesselt das Publikum mit seinen Kunststücken wie ein Zauberer.



Ulrich Gygi, VR-Präsident SBB, zu künftigen Bedrohungen der Bahnen.

Oberst i Gst Gérald Vernez ist der Delegierte des CdA für Cyber Defence

Seit Anfang 2013 amtiert Oberst i Gst Gérald Vernez als Delegierter des Chefs der Armee für Cyber Defence.

Seine umfassende zivile und militärische Ausbildung und seine reiche Erfahrung prädestinieren den 51-jährigen Waadtländer für dieses Amt.

Vernez studierte in Lausanne (Geologie), bei METEO France in Strasbourg (Meteorologie), an der ETH Zürich (Master of Advanced Studies in Security Policy and Crisis Management) und am Institut des hautes études de défense nationale. Er ist Gst Of und diente als Kdt eines Geb Inf Bat, als SC Geb Inf Br 10 und des FST A. Er arbeitete als Geologe und *Risk Manager*, bevor er 1996 in den Bundesdienst trat. 2001 realisierte er die Konzeption zum Führungssystem A XXI. Unter seiner Leitung entstand die erste und bisher einzige umfassende Konzeption zu den Informationsoperationen: mit *Cyber War* und *Psychological Operations*.

Von 2010 bis 2012 arbeitete Vernez als stellvertretender Direktor des nationalen Projektes Cyber Defence. Im Januar 2013 wurde er zum Delegierten des CdA für Cyber Defence ernannt.

Der Waadtländer Oberst Gérald Vernez.

Das Eindringen erfolgt in der Regel über den Anhang zum Mail. Beliebt sind dabei *Microsof-Office*-Dokumente, denen die Schadenware eingefügt wird. So verbindet sich *Net Traveler* mit der angegriffenen Stelle, deren Netz er in aller Ruhe durchsucht, ohne dass das Opfer den Angriff bemerkt.

Beispiel: die Attacke auf Exil-Tibetaner. Der Angreifer brachte die Exilanten dazu, einen Mail-Anhang zu öffnen, worauf die Schadensoftware placiert wurde.

Angriff auf «Wasserstelle»

Eine Spezialität ist die *Watering Hole Attack*, zu deutsch: der Angriff auf die Wasserstelle.

Der Angreifer fragt: Auf welchen Seiten treibt sich das Opfer gerne herum? Jeder hat seine Vorlieben – ein Sportclub, eine Kinoseite, eine bestimmte Zeitung. Immer wieder schlägt er die Seite auf – und öffnet dem *Net Traveler* Tür und Tor.

Der Angreifer kennt den Gegner:

- Wieviel leistet dessen Festplatte?
- Wo hat er Schwächen?
- Dann legt er genau den Angriffsbefehl fest: Wann schlägt er zu? Exakt um 11.08 Uhr? Wie löst er den Schadstoff aus? In kleinen Häppchen?
- Und wie wirken falsche *Domains* am besten, wenn sie echten ähnlich sehen: zum Beispiel *Facebok* statt *Facebook*.

Anonymus greift Schweiz an

Voller Schwung schildert die Projektleiterin Daniela Vorburger die Strategische Führungsübung (SFU) vom 23./24. Mai 2013. Thema der SFU war ein politisch motivierter Cyber-Angriff auf die Schweiz.

Sogar der Bundesrat nahm an der Übung teil. Der Angreifer, die Hackergruppe Anonymus, forderte alle sieben Departemente und die Bundeskanzlei heraus. Anonymus drohte mit der Lahmlegung aller Systeme und knackte das Online-Portal von *Post Finance*.

In der SFU ging es darum, die interdisziplinäre Kooperation zu verifizieren. Die Departemente, die Verwaltung und Ad-hoc-Krisenstäbe mussten gut zusammenwirken, um den Angriff abzuwehren.

Der Zauberer am Werk

Nun betritt der Magier die Bühne: Der Ex-Hacker Gunnar Podala, der in Walchwil die Firma *InnoSec* betreibt.

Er bietet mit drei Computern und einer Kamera die perfekte Hacker-Schau. Er dringt in das Spendenkonto der deutschen CDU ein, das den stolzen Betrag von 6,4 Millionen Euro aufweist. Dann fragt er das Publikum: Wem sollen wir spenden? Einer Kinderschutzorganisation! Gesagt, getan – 1,2 Millionen Euro wechseln die Hand.

Und eine Anekdote gefällig? Porada: Entsetzt ruft ein Wiener General aus: «Um Himmels willen, ich habe eine russische Botschaft auf dem Mobiltelefon.» Porada winkt ab, das komme vor. Darauf der General: «Ja schon, aber es ist mein streng geheimes Handy, keiner hat die Nummer.»

Noch nicht dort, wo wir...

Nun wieder ernsthaft. Den Höhepunkt der Tagung bildet das Referat von Gérald Vernez. Wie immer redet der Waadtländer Generalstabsoberst ehrlichen Klartext:

«Aus meiner Sicht sind wir als Nation in Sachen Abwehrmittel noch nicht dort, wo wir sein sollten.» Dann zeigt Vernez die fünfstufige Pyramide der Gefahren:

- Stufe 1: Anwender von *Hacking Tools*.
- Stufe 2: Entwickler von Verwundbarkeiten, motivierte Hacker.
- Stufe 3: Professionelle Organisationen Cyber-Kriminelle.
- Stufe 4: Gezielte und unerkennbare Bedrohungsagenten.
- Stufe 5: Die Top 5. Die gefährlichste Bedrohung kommt von Staaten.

Wie schlimm kann es werden? Vernez nennt: 1982 die sibirische Gaspipeline; 1999 Serbien; 2004 Libanon; 2007 den Aurora-Text; 2008 Georgien; 2009 Conficker; 2011 RQ 170; und natürlich den (israelischen) Klassiker Stuxnet 2010/2011.

Angriffe abwehren

Vernez zitiert die Absicht der Armee: «Um ihre Einsatzfähigkeit und Handlungsfreiheit jederzeit und über alle Lagen sicherzustellen, ist die Armee permanent in der Lage, Cyber-Bedrohungen zu erkennen, sich vor Angriffen zu schützen und diese abzuwehren.»

Dies geschieht durch Führung, Antizipation, Prävention und Reaktion – im Rahmen von Politik und Recht, Nationaler Zusammenarbeit, resilienten Leistungserbringern und internationaler Zusammenarbeit. Vernez schliesst seine magistrale Rede mit der Feststellung: «Nur integrale Cyber Defense ist gute Cyber Defense.»

Den Schluss macht informativ der Zukunftsforscher Andreas Walker mit dem Referat «Chancen und Risiken in der digitalen Welt. Wo geht die Reise hin?» *fo.*

*

Der SOG FU gebührt Dank für eine dichte, informative Tagung zu einem brennenden Thema. Besonderer Dank geht an Oberst i Gst Hanspeter Steiner für die vorzügliche Organisation und an Major Peter Hochuli für die kompakte Moderation.

Unsere älteren Leser bitten wir um Verständnis für die vielen englischen Begriffe – für die meisten gibt es nicht einmal eine Übersetzung!