**Zeitschrift:** ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

**Herausgeber:** Schweizerische Offiziersgesellschaft

**Band:** 175 (2009)

**Heft:** 04

**Artikel:** Auf der Suche nach dem Zentrum der Kraftentfaltung?

**Autor:** Braun, Peter

**DOI:** https://doi.org/10.5169/seals-282

# Auf der Suche nach dem Zentrum der Kraftentfaltung?

—

**Der Analyse von Zentren der Kraftentfaltung, von kritischen Befähigungen, Anforderungen, Verwundbarkeiten sowie von Schlüsselbereichen kommt im Rahmen der Operationsplanung eine grosse Bedeutung zu.**

Die aktuellen Führungsreglemente der Schweizer Armee erwähnen zwar diese Analyse, die entsprechenden Ausführungen sind aber ausgesprochen knapp und von hohem Abstraktionsgrad. Ziel dieses Artikels ist es, auf diesem zentralen Gebiet der Operativen Kunst einen klärenden Beitrag zu leisten.

Peter Braun

Dr.phil., Major. Kernprozessmanager Militärdoktrin im Planungsstab der Armee. Lehrbeauftragter für Geschichte an der Universität Zürich. Papiermühlestrasse 20, 3003 Bern. E-Mail: peter.braun@vtg.admin.ch

**Einleitung**

«The most important task confronting campaign planners [...] is being able to properly identify the adversary's [...] *Centers of Gravity* (GOGs), i.e. the sources of strength, power and resistence. [...] This process cannot be taken lightly, though; a faulty conclusion as to the adversary COGs because of a poor or hasty analysis can have very serious consequences. [...] In fact, detailed operational planning should not begin until the adversary's COGs have been identified. Identifying COGs is an analytical process that involves both art and science.»[1] Wie die Autoren der amerikanischen Führungsvorschrift *Joint Doctrine for Campaing Planning*, aus welcher dieses einleitende Zitat stammt, völlig zu Recht festhalten, kommt dem Identifizieren der «*kritischen Faktoren*»[2] (nicht nur der *Zentren der Kraftentfaltung*, wie die *Centers of Gravity* in deutschen, österreichischen und schweizerischen Vorschriften genannt werden,[3] sondern auch der *kritischen Befähigungen, Anforderungen, und Verwundbarkeiten* sowie der *Schlüsselbereiche*) im Rahmen der Operationsplanung in der Tat herausragende Bedeutung zu. So bezeichnete auch der preussische Kriegstheoretiker Carl von Clausewitz, auf dessen Gedanken das US Konzept in erster Linie basiert, das «Unterscheiden», sprich Identifizieren der so genannten *centra gravitatis* oder *Schwerpunkte* in seinem 1832–1834 posthum publizierten Standardwerk *Vom Kriege* als regelrechten «Hauptakt des strategischen Urteils».[4]

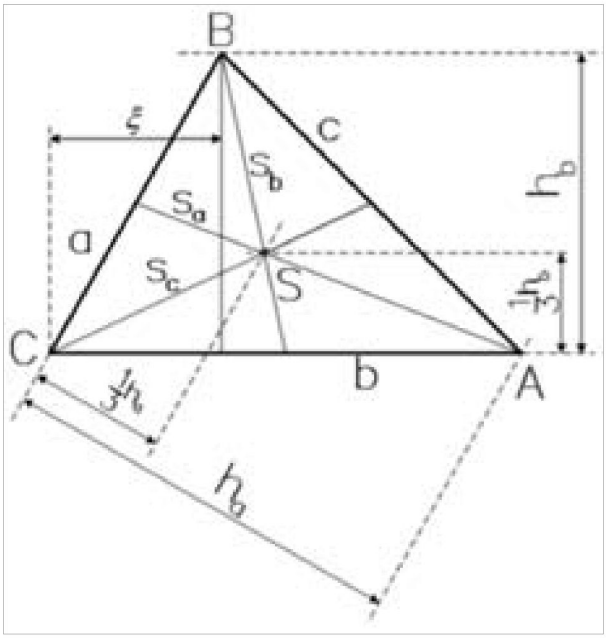
Auch die aktuellen Führungsreglemente der Schweizer Armee, namentlich die Operative Führung (OF) XXI, erwähnen die Analyse von Zentren der Kraftentfaltung im Rahmen der Operationsplanung.[5] Die entsprechenden Ausführungen sind allerdings ausgesprochen knapp und darüber hinaus von äusserst hohem Abstraktionsgrad. Ziel des vorliegenden Artikels ist es, auf diesem zentralen Gebiet der operativen Kunst einen kleinen, klärenden Beitrag zu leisten. Dabei soll zunächst gezeigt werden, was Clausewitz unter einem *centrum gravitatis* versteht. Im Anschluss wird erläutert, wie die amerikanischen Streitkräfte das Konzept in den vergangenen zweieinhalb Jahrzehnten im Rahmen ihrer *operational art* weiterentwickelt haben. In einem dritten Teil schliesslich soll gezeigt werden, wie das Konzept im Rahmen des aktuell intensiv diskutierten Effektbasierten Ansatzes zur Operationsführung (EBAO) fruchtbar gemacht werden kann.

**Clausewitz und das Centrum gravitatis**

Die Renaissance, die Clausewitz zurzeit in der angelsächsischen und in ihrem Fahrwasser auch in der schweizerischen Militärtheorie erlebt, hängt sehr wesentlich mit der Entwicklung der amerikanischen operativen Führungskunst seit Anfang der achtziger Jahre zusammen. Seit dem Vietnamkrieg haben die USA im Erarbeiten von Grundlagen der so genannten operativen Kunst *(operational art)* eine eigentliche Vorreiterrolle übernommen, wobei sie bei verschiedenen klassischen Militärwissenschaftlern (allen voran Carl von Clausewitz, dann aber auch Antoine Henri Jomini, Sun Tsu, Helmuth von Moltke und Giulio Douhet) einen reichen intellektuellen Erfahrungsschatz vorfanden, welchen sie systematisch auswerteten und für die Formulierung der eigenen Doktrin fruchtbar machten.[6] Die zuweilen etwas eklektisch anmutende Übernahme von teilweise jahrzehnte- und jahrhundertealten Prinzipien der Kriegführung führte allerdings gerade im Hinblick auf die Brauchbarkeit und praktische Umsetzbarkeit der Clausewitz'schen Lehre von den *centra gravitatis* bzw. den *Schwerpunkten* zu einem bis heute andauernden Streit zwischen verschiedenen Lehrmeinungen.

Das Problem ist vielschichtig, zum einen, weil der Blick der amerikanischen Experten nicht selten durch die jeweils benutzten englischen Übersetzungen von Clausewitz' Hauptwerk *Vom Kriege* getrübt ist, was oftmals allein schon aus sprachlichen Gründen zu inhaltlichen Missverständnissen führte und nach wie vor führt,[7] zum anderen aber auch, weil die Lektüre und erst

*[1]*




*[2]*

recht ein vertieftes Verständnis der Clausewitz'schen Gedanken auch für einen Leser deutscher Muttersprache eine beträchtliche intellektuelle Herausforderung darstellen. Hinzu kommt, dass *Vom Kriege* unvollendet geblieben ist und dass das hier interessierende Konzept, wie es in den Büchern 6 und 8 entwickelt wird, ausgesprochen schwierig auf den Punkt zu bringen ist.

Die heute im internationalen militärischen Schrifttum geläufige englische Bezeichnung *Center of Gravity* geht auf den von Clausewitz – allerdings nur ein einziges Mal – verwendeten lateinischen Begriff *centrum gravitatis* zurück. Ansonsten benutzt der preussische Theoretiker (insgesamt über fünfzig Mal) durchgängig das deutsche Wort *Schwerpunkt*. Unter einem *Schwerpunkt* ist ein bestimmter Punkt in einem festen Körper oder ausserhalb desselben zu verstehen, in dem die gesamte Masse des Körpers vereinigt gedacht werden kann[8] oder – anders ausgedrückt – derjenige Punkt, in welchem man einen Körper unterstützen muss, damit dieser unter Einwirkung der Schwerkraft in jeder Lage im Gleichgewicht ist. Wie die Begriffsbestimmung bereits deutlich macht, handelt es sich um einen aus der Newton'schen Physik stammenden Terminus.

## Tatsächlich machte Clausewitz zur Beschreibung seiner intellektuellen Konstrukte verschiedentlich Anleihen bei der mechanischen Wissenschaft, …

… wobei er diesbezüglich insbesondere von Paul Erman, einem Physikprofessor, der zusammen mit ihm an der Allgemeinen Kriegsschule in Berlin lehrte und mit dem er während Jahren freundschaftlichen Umgang pflegte, beeinflusst wurde.[9]

[1] Joint Publication (JP) 5-00.1, Joint Doctrine for Campaign Planning, Januar 2002, S. II–6f.

[2] Der Begriff «kritische Faktoren» (critical factors) als Sammelbezeichnung für *Centers of Gravity*, Critical Capabilities, Critical Requirements, Critical Vulnerabilities und Decisive Points stammt aus der amerikanischen Joint Doctrine for Campaign Plannig. Siehe JP 5-00.1, S. II–1.

[3] In der im Moment noch in Bearbeitung stehenden Operativen Führung der deutschen Bundeswehr wird der Begriff *Center of Gravity* allerdings nicht mehr mit Zentrum der Kraftentfaltung übersetzt, sondern mit Gravitationszentrum (Operative Führung von Einsätzen der Bundeswehr (OpFüBw), 2. Mitprüfungsentwurf, Mai 2004, S. 44). Die Verwendung des Begriffes Zentrum der Kraftentfaltung ist tatsächlich nicht unproblematisch, und zwar deshalb, weil dadurch leicht der (falsche) Eindruck entstehen könnte, es handle sich um eine Quelle, aus der sich eine spezifische Kraft entfaltet, während ein *Center of Gravity* - auch nach Clausewitz'scher Vorstellung und wie unten noch ausführlicher zu zeigen sein wird - nicht eine Quelle der Kraft ist, sondern die Kraft selber.

[4] Clausewitz, Carl von, Vom Kriege. Ungekürzter Text. Berlin 2003, 6. Buch, 27. Kap., S. 540.

[5] Regl 51.7, OF XXI, Ziff. 215, S. 45: «Als Zentren der Kraftentfaltung werden jene Elemente bezeichnet, die das entscheidende eigene bzw. gegnerische Leistungsvermögen ausmachen (z.B. Quellen der Handlungsfreiheit, Kampfkraft, Moral, Siegeswillen, Durchhaltevermögen) und von welchem das Ganze abhängt. Es ist materieller oder immaterieller Natur und weist eine strategisch-operative Dimension auf.»

[6] Vgl. dazu: Eder, Philipp, Die Entwicklung moderner operativer Führungskunst. In: ÖMZ 3 (2003), S. 1–23, hier S. 4–11.

[7] Siehe dazu v.a.: Vego, Milan, Clausewitz's *Schwerpunkt*. Mistranslated from German – Misunderstood in English. In: Military Review 1 (2007), S. 101–109.

[8] Vgl. Das digitale Wörterbuch der deutschen Sprache des 20. Jahrhunderts, Eintrag «*Schwerpunkt*». www.dwds.de [Zugriff: 07.03.2008].

[9] Echevarria, Antulio J., Clausewitz's *Center of Gravity*: Changing Our Warfighting Doctrine – Again! o.O. 2002, S. 8.

*[1]* Carl von Clausewitz (1780–1831), preussischer General, Militärtheoretiker und geistiger Vater der Center-of-Gravity-Analysis

*[2]* Der *Schwerpunkt* in der Geometrie als Schnittpunkt zweier Schwerlinien.

Besonders deutlich wird der Einfluss zeitgenössischer physikalischer Theorien im 27. Kapitel des 6. Buches, wo Clausewitz die Idee des *Schwerpunkt*es erstmals ausführlicher entwickelt. Wörtlich heisst es dort: «Der Wirkungskreis eines Sieges wird natürlich abhängen von der Grösse des Sieges und diese von der *Masse der besiegten Truppen*. Also gegen *den* Teil, wo die meisten feindlichen Streitkräfte beisammen sind, wird *derjenige* Stoss geschehen können, dessen glückliche Wirkungen am weitesten reichen; und wir werden dieses Erfolges am meisten gewiss sein, je grösser die Masse der eigenen Streitkräfte ist, die wir zu diesem Stoss verwenden. Diese natürliche Vorstellungsreihe führt uns auf ein Bild, in welchem wir sie klarer feststellen können, es ist die Natur und Wirkung des *Schwerpunkt*es in der Mechanik. So wie sich der *Schwerpunkt* [in der Physik] immer da findet, wo die meiste Masse beisammen ist, und wie jeder Stoss gegen den *Schwerpunkt* der Last am wirksamsten ist, wie ferner der stärkste Stoss mit dem *Schwerpunkt* der Kraft erhalten wird, so ist es auch im Kriege.»[10]

**Materielles oder immaterialles Center of Gravity**

Wie der amerikanische Militärwissenschaftler Antulio J. Echevarria verschiedenenorts zu Recht festgehalten hat, sind die von Clausewitz hier verwendeten Metaphern aus der Physik für ein inhaltliches Verständnis der Clausewitz'schen Grundidee zentral.[11] Denn wie aus der obigen Passage hervorgeht, handelt es sich beim *Schwerpunkt* vor allem um einen Faktor der Balance, d.h. letztlich geht es darum zu erkennen, wo die Kräfte im Gleichgewicht gehalten werden. Clausewitz selber gibt darauf folgende Antwort: «Die Streitkräfte jedes Kriegführenden, sei es ein einzelner Staat oder ein Bündnis von Staaten, haben eine gewisse Einheit und durch diese Zusammenhang; wo aber Zusammenhang ist, da treten die Analogien des *Schwerpunkt*es ein.»[12]

Was bei amerikanischen Theoretikern nun aber zu Verwirrung und zu einem regelrechten Forschungsstreit geführt hat, ist die folgende Passage, in der Clausewitz konkreter darauf eingeht, was diese «gewisse Einheit» und den «Zusammenhang» stiftet. «Es gibt [...] in diesen Streitkräften», so fährt er fort, «gewisse *Schwerpunkt*e, deren Bewegung und Richtung über die anderen Punkte entscheidet, und diese *Schwerpunkt*e finden sich da, wo die meisten Streitkräfte beisammen sind. So wie aber in der toten Körperwelt die Wirkung gegen den *Schwerpunkt* in dem Zusammenhang der Teile ihr Mass und ihre Grenze hat, so ist es auch im Kriege, [...]. Wie verschieden ist der Zusammenhang des Heeres *einer* Fahne, welches durch den persönlichen Befehl *eines* Feldherrn in die Schlacht geführt wird, und der einer *verbündeten Kriegsmacht*, die auf 50 oder 100 Meilen ausgedehnt oder gar nach ganz verschiedenen Seiten hin basiert ist! Dort ist der Zusammenhang als der stärkste, die Einheit als die nächste zu betrachten; hier ist die Einheit sehr entfernt, oft nur noch in der gemeinschaftlichen politischen Absicht, und da auch nur dürftig und unvollkommen vorhanden und der Zusammenhang der Teile meistens sehr schwach, oft ganz illusorisch.»[13]

Ausgehend von diesem Abschnitt entwickelte sich in den USA eine literarische Auseinandersetzung darüber, ...

> ... ob Clausewitz mit Schwerpunkt eher etwas Materielles (Streitkräfte, gegnerische Stärke)[14] oder eher etwas Immaterielles (innerer Zusammenhalt des Gegners)[15] meint.

Dabei ist Joe Strange und Richard Iron Recht zu geben, wenn sie festhalten, dass die drei von Clausewitz genannten Elemente *Zusammenhang*, *Einheit* und *gemeinschaftliche politische Absicht* (politische Interessenkongruenz) hier kaum als *Schwerpunkte* anzusehen sind. Vielmehr handle es sich um «factors that will determine which of the armies or components thereof, on each side, will function as 'the' or 'a' center of gravity.»[16] Clausewitz selbst bestätigt diese Auffassung im 28. Kapitel des 6. Buches, wo er schreibt: «Eine Hauptschlacht auf dem Kriegstheater ist der Stoss des *Schwerpunkt*es gegen den *Schwerpunkt*; je mehr Kräfte wir in dem unserigen versammeln können, um so sicherer und grösser wird die Wirkung sein.»[17] Das Zitat zeigt, dass der preussische Kriegsphilosoph hier of-

*[3]*

fensichtlich in der Tat zwei aufeinander treffende Armeen, also etwas Physisches, Konkretes, im Auge hatte und weniger zwei immaterielle Elemente. Konkret ist – wie aus dem Gesamtkontext deutlich genug hervorgeht – unter einem *Schwerpunkt* folglich der stärkste Teil innerhalb der gegnerischen Gesamtstreitmacht zu verstehen, gegen den der Hauptstoss (mit dem stärksten Teil der eigenen Streitmacht) geführt werden muss, damit das militärische Ziel, die Niederlage des Gegners, und dadurch der politische Zweck eines Krieges, ein dauerhafter Friede, erreicht werden können.

## Schwerpunkte (gegnerische und eigene) existieren nicht von sich aus, sondern sie stehen in einem spezifischen Verhältnis zueinander.

In der in der *Center-of-Gravity-Diskussion* wohl mit Abstand meistzitierten Passage, die – in einer allerdings nicht unumstrittenen englischen Übersetzung[18] – sogar wortwörtlich Eingang in die aktuellen NATO *Guidelines for Operational Planning* (GOP)[19] fand, schreibt Clausewitz dazu: «Es kommt darauf an, die vorherrschenden Verhältnisse beider Staaten im Auge zu haben. Aus ihnen wird sich ein gewisser *Schwerpunkt*, ein Zentrum der Kraft und Bewegung bilden, von welchem das Ganze abhängt, und auf diesen *Schwerpunkt* des Gegners muss der gesammelte Stoss aller Kräfte gerichtet sein.»[20] Das Zitat zeigt, dass der preussische Theoretiker hier einen dynamischen Ansatz verfolgt. Erst durch ihren jeweiligen Zusammenhang, durch ihr Zusammen- resp. Entgegenwirken werden die *Schwerpunkte* – wie Clausewitz an anderer Stelle festhält – zu «wirksamen Dingen»[21]. Joe Strange und Richard Iron erklären diesen Zusammenhang anhand eines anschaulichen Beispiels: 1991 seien die irakischen Republikanischen Garden ein *Center of Gravity* gewesen, nicht weil es sich um einen besonders gut ausgebildeten beträchtlich mechanisierten und dem Diktator Saddam Hussein treu ergebenen Verband ge-

[10] Clausewitz, Vom Kriege, 6. Buch, 27. Kap., S. 539.
[11] Echevarria, Antulio J., Clausewitz's *Center of Gravity*: It's Not What We Thought. In: Naval War College Review 1 (2003), S. 108–123, hier S. 110.
[12] Clausewitz, Vom Kriege, 6. Buch, 27. Kap., S. 539.
[13] Ebd.
[14] Siehe dazu v.a.: Strange, Joseph L. / Iron, Richard, *Center of Gravity*: What Clausewitz Really Meant. In: Joint Force Quarterly 35 (2003), S. 20–27, hier S. 21 und Strange Joseph L. / Iron, Richard, Unterstanding *Centers of Gravity* and Critical Vulnerabilities. Part 1: What Clausewitz (Really) Meant by *Center of Gravity*. o.O. u. o.J., Ms., S. 2f.
[15] Diese Meinung wird vor allem von Antulio Echevarria vertreten. Vgl. Echevarria, Antulio J., *Center of Gravity*: Recommendations for Joint Doctrine. In: Joint Force Quarterly 35 (2003), S. 10–17, hier S. 13: «For Clausewitz and his contemporaries, center of gravity represented the point where the forces of gravity converge within an object in the context of modern elementary physics. Striking an object with enough force will usually cause it to lose its equilibrium and fall. Center of gravity is therefore not a source of strength but a factor of balance. The strength of an infantryman, for example, can be attributed to his muscles, brains, or weapons in any combination, but it relates to center of gravity only so far as he needs to be balanced to use them. Conversely, a soldier might be physically frail, intellectually challenged, or lack for weaponry, but these conditions have little effect on his equilibrium.»
[16] Strange / Iron, Understanding, S. 6.
[17] Clausewitz, Vom Kriege, 6. Buch, 28. Kap., S. 542.
[18] Clausewitz, Carl von, On War. Hrsg. und übersetzt von Michael Howard u. Peter Paret. Princeton 1989, S. 595f.: «[…] one must keep the dominant characteristics of both belligerents in mind. Out of these characteristics a certain center of gravity develops, the hub of all power and movement, on which everything depends. That is the point against which all our energies should be directed.»
[19] Guidelines for Operational Planning (GOP), Januar 2000, S. 3–1: «COG […] are described as the hub of all power and movement on which everything depends, or the point against which all energies should be directed.»
[20] Clausewitz, Vom Kriege, 8. Buch, 4. Kap., S. 671.
[21] Ebd., 6. Buch, 28. Kap., S. 541.

*[3]* Gemäss Clausewitz findet sich der *Schwerpunkt* «da, wo die meisten Streitkräfte beisammen sind.» Diese Definition war freilich stark von Clausewitz' persönlichem Erfahrungshintergrund, der napoleonischen Kriegführung an der Wende zum 19. Jh. geprägt. Hier eine Darstellung von der Schlacht bei Auerstedt 1806.

handelt habe, sondern vielmehr aufgrund ihrer von der konkreten Situation (sprich dem Aufmarsch im Norden Kuwaits) abhängigen Möglichkeiten, auf das alliierte VII. Korps einzuwirken. Im zweiten Irak-Krieg vom Frühjahr 2003 wurden die Republikanischen Garden wiederum als *Center of Gravity* identifiziert, diesmal jedoch aufgrund der Befürchtung, dass sich der Verband nach Bagdad zurückziehen und den Amerikanern dort ein zweites Stalingrad bereiten könnte.[22]

**Das strategische Center of Gravity**

Während sich ein *Schwerpunkt* aufgrund einer isolierten Lektüre der Ausführungen im 6. Buch noch ohne grosse Schwierigkeiten als etwas relativ konkret Fassbares, nämlich als der jeweils stärkste Teil der gegnerischen resp. eigenen Streitmacht, definieren lässt, gewinnt die Sache erheblich an Komplexität bei einem Blick ins 8. Buch «Kriegsplan», wo Clausewitz die Bedeutung des *Schwerpunktes* – modern gesprochen – nicht nur auf der operativ-taktischen wie im 6. Buch, sondern auch auf der strategischen Stufe erläutert. Hier, so Clausewitz, stellen die Streitkräfte nur einen von verschiedenen mehr oder weniger physisch-materiellen *Schwerpunkt*en dar: «[B]ei Staaten, die durch innere Parteiungen zerrissen sind, liegt er [der *Schwerpunkt*] meistens in der Hauptstadt; bei kleinen Staaten, die sich an mächtige stützen, liegt er im Heer dieser Bundesgenossen; bei Bündnissen liegt er in der Einheit des Interesses; bei Volksbewaffnung in der Person der Hauptführer und in der öffentlichen Meinung. Gegen diese Dinge muss der Stoss gerichtet sein. Hat der Gegner dadurch das Gleichgewicht verloren, so muss ihm keine Zeit gelassen werden, es wieder zu gewinnen.»[23] In der etwas nebulösen Verwendung des Begriffes *Schwerpunkt* für zwei – zumindest auf den ersten Blick – an sich nicht völlig deckungsgleiche Dinge im 6. und 8. Buch von *Vom Kriege* liegt denn auch genau einer der Hauptgründe für die immer wieder zu beobachtende Konfusion in der aktuellen *Center-of-Gravity*-Diskussion. Der konkret fassbare, physische Aspekt des Konzeptes, wie wir ihn im 6. Buch noch beobachten konnten, tritt im 8. Buch nämlich stark in den Hintergrund. Was aber bei näherem Hinsehen immer noch gleich geblieben ist, ist die Tatsache, dass …

> Clausewitz mit Schwerpunkt analog der Definition im 6. Buch die hauptsächliche Stärke des Gegners meint, die auf strategischer Stufe indessen eher psychologisch-moralische Qualität aufweist und in der Regel immaterieller Natur ist …

(Hauptstadt als Zentrum der Macht, Zusammenhalt einer Allianz, Persönlichkeit des Führers, öffentliche Meinung).[24]

Zusammenfassend kann folgendes festgehalten werden. Unter einem *Schwerpunkt* versteht Clausewitz eine hauptsächliche eigene oder gegnerische Stärke, von der das Ganze abhängt, d.h. die auf den Verlauf einer Operation insofern einen entscheidenden Einfluss hat, als dass ihre Vernichtung das gesamte gegnerische System aus dem Gleichgewicht bringt, was zwangsläufig dessen Zusammenbruch zur Folge hat. Es handelt sich um dynamische, aktive Elemente («wirksame Dinge»), die untereinander in einem Interaktionsverhältnis stehen. *Schwerpunkte* lassen sich auf verschiedenen Stufen identifizieren; auf der operativ-taktischen sind sie in der Regel physisch vorhanden und konkret (an-)greifbar, auf der strategischen sind sie eher immaterieller Natur. Wie Joe Strange vor allem in seinen neueren Arbeiten mit Nachdruck festhält, sind *Schwerpunkte* bei Clausewitz nicht Quellen der Stärke (und schon gar nicht solche der Schwäche), sondern die Stärken selber.[25] Dieser feine Unterschied ist vor allem mit Blick auf die Darstellung des *Center-of-Gravity*-Konzeptes in den amerikanischen Führungsvorschriften von Belang, was im Folgenden kurz skizziert werden soll.

**Das Center of Gravity in der amerikanischen Militärdoktrin**

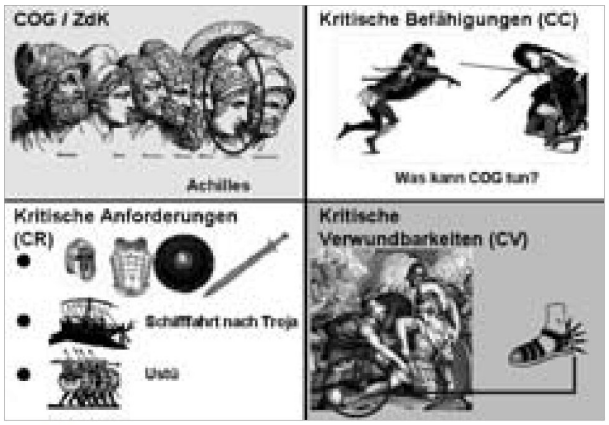
Wie bereits mehrfach erwähnt, ist die Geschichte des *Center-of-Gravity*-Konzeptes in der amerikanischen Militärdoktrin seit seiner erstmaligen Erwähnung (in der 1986er Ausgabe des FM 100-5) eine Geschichte von Falschinterpretationen der Clauswitz'schen Grundidee, von Missverständnissen und von konzeptionellen Richtungskämpfen zwischen den verschiedenen Teilstreitkräften. Entsprechend gross war (und ist) denn auch die Bandbreite von Definitionen in den jeweiligen Führungsreglementen der einzelnen Teilstreitkräfte, die von «strength» über «source of strength» bis hin zu «rather a critical vulnerability» reicht.[26] Man könnte das ganze relativ leichten Herzens als intellektuelle Wortklauberei abtun, hätte die praktische Umsetzung nicht derart handfeste (und durchaus schwerwiegende) Konsequenzen.

> So identifizierte beispielsweise der amerikanische Oberbefehlshaber im Golfkrieg von 1990/91, General Norman Schwarzkopf, drei Centers of Gravity[27], die Air Force deren zehn[28] und die Army – getreu ihrer Doktrin – nur eines[29].

Ein gewisser Ausgleich zwischen den Teilstreitkräften konnte mit der Doctrine for Joint Operations vom 10. September 2001 erzielt werden, worin ein *Center of Gravity* als «those characteristics, capabilities, or sources of power from which a military force derives its freedom of action, physical strength, or will to fight»[30] definiert wird. «At the strategic level COGs might include a military force, an alliance, national will or public support, a set of critical capabilities or functions, or national strategy itself. COGs also may exist at the operational level.» Wie Strange und Iron richtig beobachtet haben, findet sich in dieser Passage insofern ein Widerspruch, als dass eine Streitkraft zwar als Beispiel für ein *Center of Gravity* aufgeführt wird, dass sie aber aufgrund der Definition unmöglich eines sein kann, da dort gesagt wird, dass ein *Center of Gravity* eine Quelle der Kraft sei, aus welcher eine Streitmacht ihre Handlungsfreiheit, physische Stärke oder ihren Kampfwillen beziehe.[31] Dies steht nicht nur in Widerspruch zum Clausewitz'schen Konzept, der unter *Schwerpunkt* durchaus die Streitkraft selber verstand, sondern ist auch eine Quelle des Missverständnisses.

**Das CG-CC-CR-CV-Model**

Die Vorschrift *Joint Doctrine for Campaign Planning* vom 25. Januar 2002 brachte in Bezug auf die Definition von *Centers of Gravity* zwar keinen Fortschritt,[32] wohl aber in Bezug auf die




*[4]*

Analysemethode, indem das von Joe Strange Mitte der neunziger Jahre erstmals vorgestellte und seither in verschiedenen Aufsätzen weiterentwickelte CG-CC-CR-CV-Modell[33] ausführlicher erörtert wird. Ausgangspunkt der Überlegungen ist der in gewisser Weise paradoxe Umstand, dass *Centers of Gravity* (CG) zwar eine Hauptstärke darstellen, deren Vernichtung den Zusammenbruch des Systems herbeiführen kann, dass militärische Operationen in der Regel aber nicht auf gegnerische Stärken zielen, sondern – genau umgekehrt – wo immer möglich die Schwächen des Gegners auszunützen versuchen.

> Die Lösung dieses scheinbaren Widerspruchs liegt in der Erkenntnis, dass jeder Stärke normalerweise auch eine Reihe von kritischen Verwundbarkeiten (critical vulnerabilities – CV) innewohnt.

Dieser Zusammenhang lässt sich anhand zahlreicher militärgeschichtlicher Beispiele aufzeigen. So befand sich beispielsweise im Frankreichfeldzug 1940 die kritische Verwundbarkeit der französischen Armeegruppe 1 (aus deutscher Sicht das gegnerische operative *Center of Gravity*) in der schwachen Verteidigung an der Maas (was von den Deutschen durch ihren Panzerangriff durch die Ardennen gekonnt ausgenützt wurde) oder diejenige der 6. deutschen Armee bei Stalingrad (das gegnerische COG aus sowjetischer Sicht) in ihrer Abhängigkeit vom Flankenschutz durch schlecht ausgerüstete und wenig kampfkräftige rumänische, italienische und ungarische Divisionen (was sich der sowjetische General Georgij Schukow geschickt zunutze machte). Der Zusammenhang zwischen immenser Stärke und darin innewohnender Schwäche ist auch aus der griechischen Mythologie bekannt, und zwar in Form der Erzählung von Achilles, dem stärksten und wildesten Kämpfer im Trojanischen Krieg, der abgesehen von seiner Ferse unverwundbar war – eine Schwäche, dank der sein Kontrahent Paris – durch einen Pfeilschuss in die redensartlich berühmt gewordene «Achillesferse» – den Zweikampf zu seinen Gunsten entscheiden konnte.

Mit Hilfe einer von Joe Strange entwickelten Analysemethode kann der Zusammenhang zwischen einem *Center of Gravity* (im Sinne einer hauptsächlichen Stärke) und der ihr innewohnenden kritischen Verwundbarkeit systematisch herausgearbeitet werden.

[22] Strange / Iron, a.a.O., S. 9.
[23] Clausewitz, Vom Kriege, 8. Buch, 4. Kap., S. 672.
[24] Es zeigt sich, dass Clausewitz – zu Recht! – zunehmend davon abkam, Krieg nur in Abhängigkeit von physischen Faktoren und militärischen Gleichgewichten zu analysieren, und zwar in dem Masse, in dem er auch die Rolle metaphysischer Faktoren in seine Überlegungen einbezog. Siehe dazu: Heuser, Beatrice, Clausewitz lesen! Eine Einführung. München 2005, (Beiträge zur Militärgeschichte - Militärgeschichte kompakt; Bd. 1), S. 91–95 und Strachan, Hew, Über Carl von Clausewitz, Vom Kriege. Aus dem Englischen von Karin Schuler. München 2007, S. 97–100.
[25] Strange Joseph L. / Iron, Richard, Understanding *Centers of Gravity* and Critical Vulnerabilities. Part 2: The CG-CC-CR-CV Construct: A Useful Tool to Understand and Analyse the Relationship between *Centers of Gravity* and their Critical Vulnerabilities. o.O. u . o.J., Ms., S. 6: «*Centers of Gravity* (CG) are physical or moral entities that are the primary components of physical or moral strength, power and resistence. They don't just contribute to strength; they ARE the strength.»
[26] Siehe im Detail: Strange, Joseph L., *Centers of Gravity* & Critical Vulnerabilities. Building on the Clausewitzian Foundation So That We Can All Speak the Same Language. o.O. 1996, (Perspectives on Warfighting; Bd. 4), S. 27–42. Vgl auch: Echevarria, Antulio J., Clausewitz's *Center of Gravity*: It's Not What We Thought, S. 108f.: «Thus the U.S. Marine Corps, a relatively small force designed more for winning battles than fighting campaigns or wars, prefers to strike at enemy weaknesses. Accordingly, it initially equated enemy centers of gravity (CoGs) with key vulnerabilities. Recently, however, Marine Corps doctrine has distinguished between CoGs and critical vulnerabilities, considering them different but complementary concepts; CoGs, for the Marines, are now 'any important sources of strength'. By comparison, the U.S. Air Force, which takes a 'targeting' approach to warfare, sees centers of gravity as multiple strategic and operational critical points that it can attack with its bombing assets. Airpower theorists like John Warden, with his notion of 'concentric rings', have in fact identified so many CoGs as to reduce the concept to absurdity. In contrast, the U.S. Army, which has the role of fighting campaigns and winning wars, sees the enemy's center of gravity as his 'source of strength'. Accordingly, the Army tends to look for a single center of gravity, normally in the principal capability that stands in the way of the accomplishment of its own mission. In short, the Army considers a 'friendly' CoG as that element – a characteristic, capability, or locality – that enables one's own or allied forces to accomplish their objectives. Conversely, an opponent's CoG is that element that prevents friendly forces from accomplishing their objectives. Likewise, the U.S. Navy, as America's force for winning maritime wars, has a center-of-gravity concept that resembles that of the Army and the Marines. Like the Army, the Navy's doctrine states that a 'center of gravity is something the enemy must have to continue military operations – a source of his strength, but not necessarily strong or a strength in itself. There can only be one center of gravity.'»
[27] Saddam Hussein, die Republikanischen Garden, die irakischen ABC-Kapazitäten.
[28] Irakisches Regime, nationale Führung (C2), Elektrizitäts- und Ölversorgung, Rüstungsproduktion, Eisenbahnlinien, Flugstützpunkte, Häfen, strategische Luftabwehr, strategische chemische Kriegführungsfähigkeit.
[29] Republikanische Garden.
[30] Joint Publication (JP) 3-0, Doctrine for Joint Operations, September 2001, S. III–22.
[31] Strange / Iron, Understanding, Part 1, S. 1.
[32] Joint Publication (JP) 5-00.1, Joint Doctrine for Campaign Planning, Januar 2002, S. II–6: «Centers of gravity are those characteristics, capabilities, or sources of power from which a military force derives is freedom of action, physical strength, or will to fight.»
[33] Strange, Centers of Gravity & Critical Vulnerabilities, S.43–91; Strange / Iron, Understanding, Part 2, S. 6f.

*[4]* Abb. 4: Das COG-CC-CR-CV-Modell am Beispiel von Achilles, dem stärksten der griechischen Helden im Trojanischen Krieg.

Ausgehend vom *Center of Gravity* werden so genannte *kritische Befähigungen (Critical Capabilities – CC)* abgeleitet. Kritische Befähigungen werden in der amerikanischen *Joint Doctrine for Campaign Planning* als «those adversary capabilities that are considered crucial enablers for the adversary's GOG to function as such, and essential to the accomplishment of the adversary's assumed objectives»[34] definiert. Der dahinterstehende Gedanke ist der, dass jedes *Center of Gravity* über bestimmte Befähigungen verfügen muss, um in einer konkreten Lage überhaupt wirksam zu werden. *Kritische Befähigungen* machen eine Aussage darüber, was ein *Center of Gravity* machen kann (z. B. etwas *zerstören*, jemanden *abhalten*, seinen Auftrag zu erfüllen etc.).

Damit ein *Center of Gravity* seine kritische Befähigung erlangen und ausspielen kann, müssen gewisse entscheidende Bedingungen materieller oder immaterieller Natur erfüllt sein (z. B. bestimmte Witterungsverhältnisse während der Operation, Logistik, Flankenschutz, Verbindungen, Luftüberlegenheit während einer bestimmten Zeit usw. usf.). Diese Bedingungen werden in der amerikanischen Joint Doktrin *Kritische Anforderungen (Critical Requirements – CR)* genannt. *Kritische Anforderungen* sind gemäss Joint Doctrine for Campaign Planning «those essential conditions, resources, and means for a critical capability to be fully operational.»[35]

> Ohne *Kritische Anforderungen* kann ein *Center of Gravity* nicht erfolgreich funktionieren …

… und hört auf, eine hauptsächliche Stärke zu sein, welche kritische Befähigungen hervorbringt. Die obige Aufzählung von Beispielen *Kritischer Anforderungen* zeigt, dass zwar alle in einer bestimmten Lage benötigt werden, damit ein *Center of Gravity* seine Stärke überhaupt ausspielen kann, dass einige aber durchaus auch das Ziel eigener Handlungen sein können. Genau hier liegt der Link zwischen der hauptsächlichen Stärke und der ihr innewohnenden Schwäche, die Joe Strange und die amerikanische *Joint Doctrine for Campaign Planning Kritische Verwundbarkeit (Critical Vulnerability)* nennen. *Kritische Verwundbarkeiten* sind «those critical requirements, or components thereof, that are deficient, or vulnerable to neutralization or defeat in a way that will contribute to a center of gravity failing to achieve its critical capability.»[36] Oder einfacher ausgedrückt: Kritische Verwundbarkeiten sind kritische Anforderungen, die verwundbar sind und deshalb angegriffen werden können (resp. geschützt werden müssen).

Die Analyse der *kritischen Faktoren* hat immer sowohl die eigene als auch die gegnerische Seite zu umfassen – ganz im Sinne des Clausewitz'schen Diktums, dass es darauf ankomme, «die herrschenden Verhältnisse beider Staaten im Auge zu haben.»[37] Nur ein sorgfältiges Abwägen eigener und gegnerischer Stärken und Schwächen im Rahmen einer gesamtheitlichen Betrachtungsweise erlaubt eine erfolgreiche Umsetzung des in der *Joint Doctrine for Campaign Planning* beschriebenen Rezeptes, «to use force strength to undermine the adversary's strength by exploiting adversary's weaknesses.»[38]

**EBAO: eine Antwort auf die Komplexität des heutigen Komfliktumfeldes**

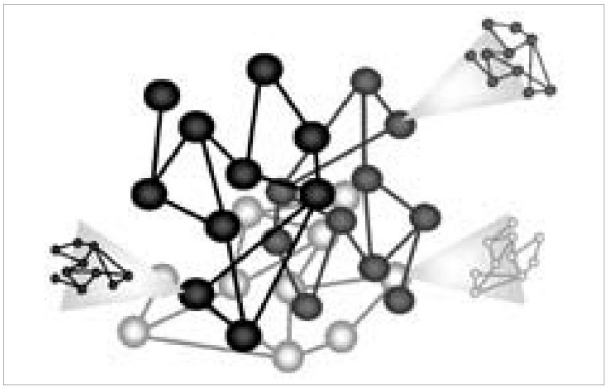
Bald 200 Jahre nach dem Tod des grossen preussischen Kriegsphilosophen bilden Clausewitz' Ideen ebenso wie seine Terminologie – ob sie nun korrekt angewandt wird oder nicht, bleibe dahingestellt – einen festen Bestandteil der militärischen und sicherheitspolitischen Literatur. Demgegenüber wurde immer wieder Kritik laut, seine Gedanken seien veraltet, insbesondere nach der strategischen Wende von 1989.

> Richtig ist, dass Clausewitz, was angesichts seiner persönlichen Prägung durch die napoleonischen Kriege in Mittel- und Osteuropa nicht weiter erstaunt, in erster Linie den zwischenstaatlichen Krieg vor Augen hatte.

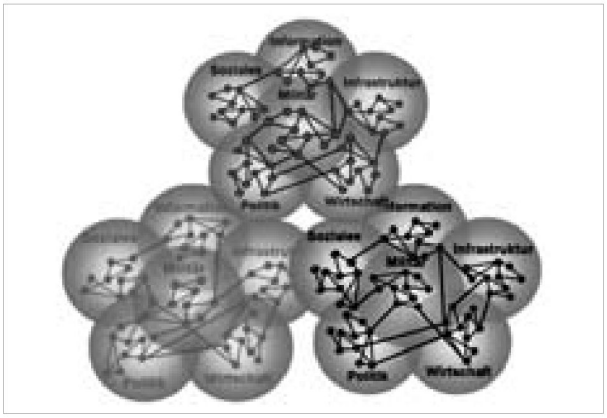
Seit dem Niedergang der Sowjetunion zu Beginn der 1990er Jahre sehen sich allerdings nahezu alle modernen Armeen mit anderen sicherheitspolitischen Herausforderungen konfrontiert. Einsätze von Streitkräften spielen sich heute in einem zunehmend komplexeren Umfeld ab und beinhalten – neben der klassischen Kampfaufgabe – zusätzlich ein breites Feld an Einsätzen zur Wahrung der inneren Sicherheit sowie diverse friedensfördernde und humanitäre Operationen. Die zunehmende Bedeutung derartiger Armeeeinsätze hängt nicht zuletzt zusammen mit der Entwicklung moderner nationaler und internationaler Gesellschaften als komplexe, bisweilen gar chaotisch anmutende Systeme mit zahlreichen untereinander abhängigen Subsystemen («Systems-of-Systems»). Die gleiche Feststellung gilt freilich auch für die Kräfte der Gegenseite, welche ebenfalls als komplexe, anpassungsfähige Systeme mit zahlreichen Subsystemen innerhalb der internationalen Gemeinschaft agieren und sich dabei die Anfälligkeiten eben dieser Systeme zunutze machen. Das eigene System, dasjenige von Partnern, unbeteiligten Dritten und Neutralen sowie dasjenige der Gegenseite bilden eine eng verschränkte Systemlandschaft mit zahlreichen Abhängigkeiten und Interdependenzen.

> Die klassische, stark von Clausewitz' Gedankengut geprägte militärische Operationsführung, welche – zumindest bis zum Ende des Kalten Krieges – vornehmlich darauf abzielte, das gegnerische Kampfpotenzial möglichst effektiv abzunützen oder zu zerstören, trägt dem gewandelten Konfliktbild kaum mehr angemessen Rechnung.

Mehr denn je geht es vor allem darum, durch wohldosierte Anwendung eigener militärischer, aber auch anderer staatlicher und nicht-staatlicher Fähigkeiten den Willen und das Verhalten von Akteuren in Einklang mit den von der politischen Führung festgelegten Zielvorstellungen zu beeinflussen resp. die gegnerischen Fähigkeiten nachhaltig zu beeinträchtigen und dabei eigene Verluste sowie Kollateralschäden wo immer möglich zu vermeiden. Die Kohärenz zwischen den definierten strategischen Zielvorstellungen und Endzuständen einerseits und dem taktischen Handeln im Einsatzraum andererseits wird durch die Festlegung von



*[5]*



*[6]*

«Effekten» sichergestellt. Aus diesem Grunde spricht man von einem *Effektbasierten Ansatz zur Operationsführung (EBAO)*, ein Konzept welches – basierend auf Überlegungen von John Warden (Fünf-Kreise-Theorie) und zunächst unter dem Namen *Effects-Based Operations (EBO)* – von den USA seit Anfang der neunziger Jahre entwickelt wurde.[39] Seit einigen Jahren wird der Ansatz auch innerhalb der NATO intensiv diskutiert, wobei man hier gemeinhin von einem *Effects-Based Approach to Operations* spricht. Trotz der zurzeit noch schwachen doktrinellen Ausgestaltung wird EBAO allenthalben als erfolgversprechend und zukunftsweisend bewertet und gilt international als einer der Haupttreiber der Streitkräftetransformation. Gemäss aktuell gültigen Richtlinien versteht die Nordatlantische Allianz unter einem Effects-Based Approach to Operations «the coherent and comprehensive application of the various instruments of the Alliance, combined with practical cooperation with non-NATO actors involved, to create effects necessary to achieve planned objectives and ultimately the NATO end-state.»[40]

Die Erzeugung zielgenauer Effekte, wie dies im Rahmen von EBAO angedacht ist, setzt zwingend die Fähigkeit voraus, das Umfeld als komplexes System von untereinander in Beziehung stehenden Elementen zu erfassen und diese Elemente in ihrer Bedeutung sowie in ihrer gegenseitigen Abhängigkeit und Beeinflussung zu verstehen.[41] Die Methode dazu ist die System-of-System-Analysis (SoSA), ein praktisch anwendbares Verfahren der Systemtheorie, welches es ermöglichen soll, Aussagen über vergangene und zukünftige Entwicklungen sowie über mögliche Verhaltensweisen eines Systems in bestimmten Szenarien zu machen. Die Analyse umfasst dabei nicht nur das System des Gegners (rot), sondern auch das eigene (blau) und dasjenige von Neutralen resp. unbeteiligten Dritten (grün). Zur Strukturierung der Analyse wird das System dazu in die so genannten PMESII-Domänen (Political, Military, Economy, Social, Infrastructur, Information) unterteilt. Kollaborative Informations- und Nachrichtenbeschaffung im Rahmen eines weit gefassten Nachrichtenverbundes, der Einbezug von Expertenwissen beispielsweise aus der Wirtschaft und Wissenschaft sowie der Einsatz moderner Informationstechnologie sind eine wesentliche Voraussetzung für eine möglichst umfassende System-of-System-Analysis.

[34] JP 5-00.1, S. II–7.
[35] Ebd.
[36] Strange / Iron, Understanding, Part 2, S. 7. Die Definition in der Joint Doctrine for Campaign Planning, die sich ansonsten eng an diejenigen von Strange anlehnt, weicht hier in geradezu fataler Art und Weise ab: «Critical vulnerabilities [...] are those aspects or components of the adversary's critical capabilities (or components thereof), which are deficient, or vulnerable to neutralization, interdiction, or attack in a manner achieving decisive or significant results, disproportionate to the military resources applied» (JP 5-00.1, S. II–7). Warum die Autoren der Vorschrift «critical requirements» durch «aspects» und «contribute to a center of gravity failing to achieve its critical capability» durch «in a manner achieving decisive or significant results, disproportionate to the military resources applied» ersetzten, ist nicht nachvollziehbar, denn dadurch geht genau die – von Strange bewusst gesuchte und damit entscheidende! – Systematik der Analysemethode (vom Center of Gravity über die Critical Capabilities und Critical Requirements) wieder verloren!
[37] Clausewitz, a.a.O., 8. Buch, 4. Kap., S. 671.
[38] JP 5-00.1, S. II–9.
[39] Zur EBAO-Thematik existiert mittlerweile eine kaum mehr überblickbare Flut von Literatur. Siehe insbesondere: Smith, Edward A., Effects Based Operations. Applying Network Centric Warfare in Peace, Crisis, and War. Washington DC 20002 und ders., Complexity Networking & Effects-Based Approaches to Operations. Washington DC 20002. Eine ausführliche Diskussion des Forschungsstandes findet sich bei: Jobbagy, Zoltan, Literatur Survey on Effects-Based Operations. A Ph.D. Study on Measuring Military Effects and Effectiveness. s'Gravenhage 2003.Vgl dazu auch den Beitrag «Effects based...What?» von Col EMG Sylvain Curtenaz in der Military Power Revue Nr 2 – 2008, Seiten 21 – 28.
[40] NATO Bi-Strategic Command Discussion Paper, Development of NATO's Effects-Based Approach to Operations, 02.07.2007, S. 1.
[41] Unter einem System ist eine funktional, physisch, sozial oder virtuell miteinander verbundene Gruppe regelmässig interagierender und interdependenter Elemente zu verstehen, die einen Gesamtzusammenhang (z.B.einen Staat oder eine bestimmte Organisation) darstellen.

*[5]* Graphische Darstellung des System-of-System-Ansatzes
*[6]* System-of-System-Analysis unter Berücksichtigung der PMESII-Domänen (Political, Military, Economic, Social, Information, Infrastructure).

Obschon in den letzten Jahren vor allem dank intensiven Arbeiten im Rahmen der vom US Joint Force Command geführten Multinationalen Experimente (MNE) bedeutende konzeptionelle Fortschritte erzielt wurden[42] und obwohl EBAO innerhalb der NATO (namentlich bei der ISAF in Afghanistan, wo die Grundprinzipien bereits seit einigen Jahren praktisch anwendet werden) allmählich zu einer gelebten Realität wird, …

… gelang es bis heute nicht, eine verbindliche EBAO-Doktrin festzulegen.

So konnten insbesondere die Konsequenzen des Denkansatzes auf die Führungsverfahren, Prozesse und Strukturen bis anhin noch nicht abschliessend abgeleitet werden.

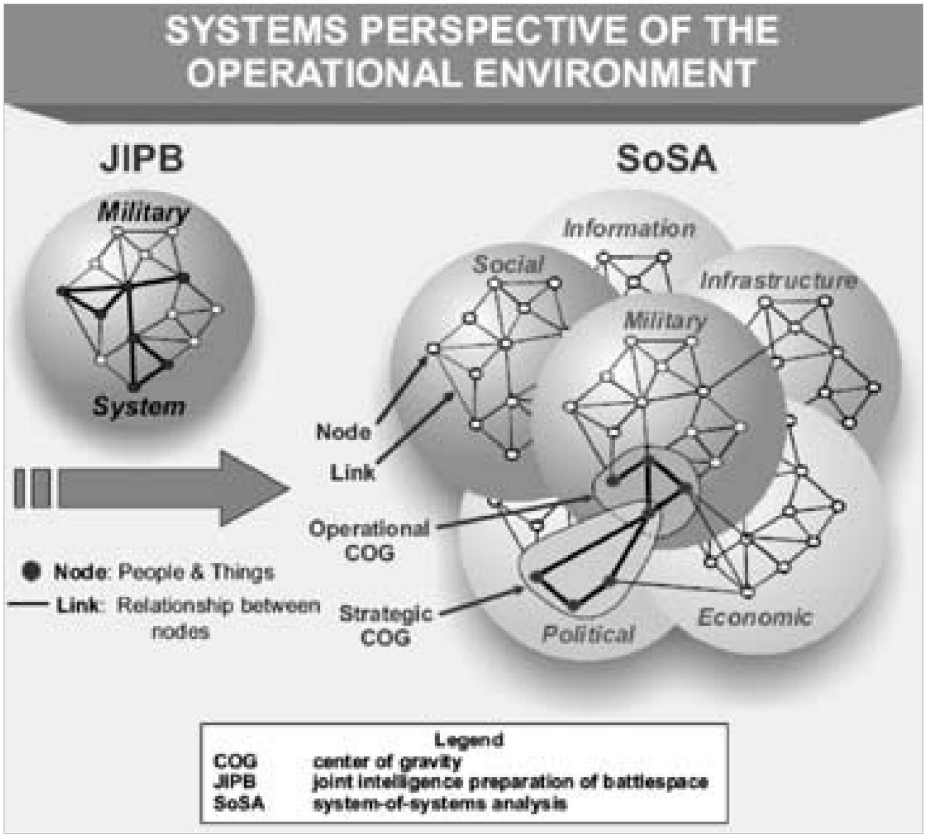
**Center of Gravity-Analysis versus Systemdenken**

Dissens besteht unter anderem auch und gerade in der Frage, inwiefern sich der Effektbasierte Ansatz mit der Vorstellung von einem *Center of Gravity* vereinbaren lässt. So bezeichnete beispielsweise Oberstleutnant im Generalstab Jörg Neureuther von der deutschen Bundeswehr das *Center of Gravity* im Rahmen einer jüngst durchgeführten EBAO-Konferenz wörtlich als «vom Aussterben bedrohte Art» und plädierte nachdrücklich dafür, inskünftig auf seine Verwendung im Planungsprozess zu verzichten, weil es in einem als System gedachten Umfeld – um mit Clausewitz zu sprechen – keine *Schwerpunkte* geben könne, deren Bewegung und Richtung über die anderen Punkte entscheide.[43] In eine ähnliche Richtung geht auch die Argumentation von William J. Olson, Professor für strategische Studien an der National Defense University in Washington. In einem Artikel mit dem bezeichnenden Titel *War Without a Center of Gravity* spricht er – ähnlich wie der israelische Militärhistoriker Martin van Creveld bereits zu Beginn der 1990er Jahre[44] – Clausewitz' Theorien die Relevanz für die so genannten postmodernen oder neuen, von internationalem Terrorismus und globalisierter Kriminalität geprägten Kriege grundsätzlich ab. Zwar hätten die USA ihre sich an klassischen Militärtheorien orientierte Fähigkeit, einen konventionellen Gegner innert kürzester Zeit aus dem Feld zu schlagen, im Irak und in Afghanistan eindrücklich unter Beweis gestellt; das längerfristige Resultat hingegen sei mehr als fragwürdig, was nicht zuletzt auf die Annahme von der Existenz eines alles entscheidenden, angreifbaren Elementes im gegnerischen System (nämlich Saddam Hussein bzw. die Taliban- oder Al-Qaida-Führung) zurückzuführen sei. «[In postmodern war] the enemy has no fixed address or easily discerned identities and markers.

The security environment has been globalized. The enemy has no center, no focal point.»[45]

Aus ganz ähnlichen Gründen riet Colonel Mark Cancian vom US Marine Corps schon Ende der 1990er, militärische Planer sollten sich besser an den übergeordneten Zielen orientieren, anstatt nach einem einzigen, alles entscheidenden Punkt im gegnerischen System zu suchen, denn solche Punkte würden in der Realität nur selten existieren. Das Problem bestehe nicht darin, dass Zentren der Kraftentfaltung schwierig zu identifizieren seien, wie verschiedenste Autoren suggerierten, sondern darin, dass sie schlichtweg nicht vorhanden wären.[46]

Die grundsätzliche Kritik dieser Anti-COG-Schule, dass nämlich das aus dem vorindustriellen Zeitalter stammende und allzu simplifizierende Clausewitz'sche Konzept militärische Planer letzten Endes für die komplexe und anpassungsfähige Natur des postmodernen Konfliktumfeldes eher blind mache, blieb freilich nicht unwidersprochen. Tim Keppler von der US Army beispielsweise, dessen Arbeit sich trotz einiger interessanter Ansätze insgesamt eher als wenig kritische Rechtfertigungsschrift der amerikanischen Politik im Kampf gegen den Terror liest, gab sich überzeugt, dass die Theorie nach wie vor ihre Berechtigung habe, obschon sie selbstredend kein Wunderheilmittel sei, mit deren Hilfe alle militärischen Probleme gelöst werden könnten.[47] Während sich Keppler über die theoretische Fundierung seiner Arbeit weitgehend ausschweigt, lieferte Oberstleutnant Dale C. Eikmeier schon vor bald einem Jahrzehnt in




*[7]*

einer am US Army Command and General Staff College in Fort Leavenworth verfassten Diplomarbeit zahlreiche, gerade auch mit Blick auf die aktuelle EBAO-Debatte durchaus stichhaltigen Argumente. Er betonte, dass eine moderne COG-Definition nicht zwingend mit dem «outdated linear-based Clausewitzian concept of the center of gravity as the essence of campaign design» identisch sein müsse, sondern durch eine mit dem Systemdenken kompatible Begriffsbestimmung zu ersetzen sei. Eine Kräftekonzentration, welche für Clausewitz noch den konkreten Erfahrungshorizont gebildet habe, bestehe heutzutage nurmehr selten. Die Vernetzung eines modernen Gegners könne nur mithilfe der Systemtheorie angemessen erfasst werden. Allerdings wäre eine systemische Analyse des Konfliktumfeldes ohne modernen COG-Ansatz ausschliesslich beschreibend und hätte keinen praktischen Nutzen, denn auch in einem System gebe es gewisse, im Hinblick auf eine Beeinflussung besonders lohnende Elemente und Beziehungen, welche identifiziert werden müssten, um die eigene Kraftanwendung zu fokussieren – und dies seien die *Centers of Gravity*. «It's only when the planner strays from the modern definition and uses the traditional Clausewitzian definition does he revert to a search for a concentration of power center of gravity that may not exist. However, system theory can explain where the elusive center of gravity is and how it works. Therefore, the further one gets from the nineteenth century definition of center of gravity and the closer to the modern definition the more compatible system theory [...] and the center of gravity become.»[48]

[42] Siehe z.B. Grossman-Vermaas, Robert, The Effects-Based Concept, MNE 3 and NMOs: an Experimental Analysis. Ottawa 2004; Turner, John, Multi-National Experiment 4. In: The Three Swords Magazine 5 (2006), S. 25–26; Neureuther, Jörg, Effects-Based Operations. In: Europäische Sicherheit 4 (2007), S. 73–76; Rüther, Christian, Knowledge Development im Einsatz. In: Europäische Sicherheit 1 (2008), S. 64–67.

[43] Neureuther, Jörg, EBO and the integration of Networked Security – a German perspective. Vortrag gehalten am 2nd Annual Effects-Based Operations Forum, Barcelona, 27./28. November 2007.

[44] Vgl. van Creveld, Martin, The Transformation of War. New York 1991.

[45] Olson, William J., War Without a Center of Gravity: Reflections on Terrorism and Post-Modern War. In: Small Wars and Insurgencies 18/4 (2007), S. 559–583, hier S. 581.

[46] Cancian, Mark, Centers of Gravity Are a Myth. In: Proceedings, September 1998, S. 30–34.

[47] Keppler, Tim, Center of Gravity Determination and Implications for the War Against Radical Islamic Terrorism. Carlisle 2005.

[48] Eikmeier, Dale C., The Center of Gravity Debate Resolved. Fort Leavenworth 1998, S. 11.

*[7]* Abb. 7: Das Center of Gravity im Rahmen einer systemischen Betrachtung des Konfliktumfeldes (aus: USJFCOM, Commander's Handbook for an Effects-Based Approach to Joint Operations, 24.02.2006, S. II-2)

Für Eikmeier basierte die ganze Auseinandersetzung zwischen Systemtheoretikern und COG-Verfechtern folglich auf einem begrifflichen Missverständnis …

… – eine These, die sich – gerade mit Blick auf den in den USA seit Anfang der 80er Jahr wuchernden Definitionsdschungel – wohl kaum von der Hand weisen lässt. Robert Umstead und David Denhard von der US Air Force beurteilten die Problematik – nun explizit mit Blick auf die EBAO-Thematik – denn auch ganz ähnlich. Um Verwechslungen mit dem Clausewitz'schen *Schwerpunkt* zu vermeiden, schlagen sie vor, künftig von einem «maximum influence node» anstatt von einem *Center of Gravity* zu sprechen.[49]

Vorderhand konnten sich sowohl in den USA als auch innerhalb der NATO diejenigen Fachleute durchsetzen, welche die Vorstellung von einem *Center of Gravity* mit der für EBAO konstituierenden systemischen Betrachtungsweise für vereinbar halten. So findet es sich – wenn auch zugegebenermassen eher am Rande und weit weniger prominent als in den amerikanischen Reglementen – auch im kürzlich erschienenen Pre-Doctrinal EBAO-Handbook der NATO[50], obschon die Beibehaltung – glaubt man Insiderstimmen – offenbar auch innerhalb der multinationalen Expertengruppe, welche das Dokument erarbeitete, nicht unumstritten war.

Auch in der offiziellen amerikanischen Militärdoktrin scheint das Konzept trotz kritischen Stimmen in der Fachliteratur immer noch grossmehrheitlich akzeptiert zu sein. Das im Februar 2006 erlassene *Commander's Handbook for an Effects-Based Approach to Joint Operations* unterstreicht die Bedeutung der *Center of Gravity-Analysis* im Rahmen der Festlegung des *operational Design* noch zusätzlich, indem es festhält, dass das Konstrukt gerade im Rahmen einer systemischen Betrachtungsweise dazu beitrage, eigene und gegnerische Hauptstärken und Verwundbarkeiten zu identifizieren, und zwar nicht nur im Bereich des Militärs, sondern in allen PMESII-Domänen.[51] Auch die 2006er Ausgabe des Reglements JP 5-0, *Joint Operational Planning*, welcher grundsätzlich ein effektbasierter Ansatz zugrunde liegt, …

… bezeichnet die Identifikation von *Centers of Gravity* nach wie vor als zentrale Aufgabe im Rahmen des operativen Planungsprozesses, …

… wobei ein COG allerdings – ganz im Sinne Eikmeiers – im Rahmen eines systemischen Ansatzes definiert wird, nämlich als ein «set of characteristics, capabilities, and sources of power from which a system derives its moral or physical strength, freedom of action, and will to act.»[52] Auch wenn es sich dabei nicht mehr um einen Clausewitz'schen *Schwerpunkt* im ursprünglichen Sinne handelt, sondern eher um ein Element, welches eine gewisse Struktur in die System-of-System-Analysis bringt, so ist es den Autoren der amerikanischen Vorschrift nichtsdestotrotz gelungen, ein bewährtes Element des operational Design mit dem für EBAO zentralen Systemdenken in Einklang zu bringen und dabei für den militärischen Praktiker einen Mehrwert zu schaffen. Allerdings dürfen auch die Grenzen eines derartigen, leicht mechanistischen Vorgehens nicht ausser Acht gelassen werden, indem sich nämlich insbesondere die psychologisch-moralische Dimension – wie oben gezeigt ein zentraler Aspekt der COG-Analyse auf strategischer Stufe – durch das im JP 5-0 beschriebene Verfahren vermutlich nicht angemessen abbilden lässt.[53]

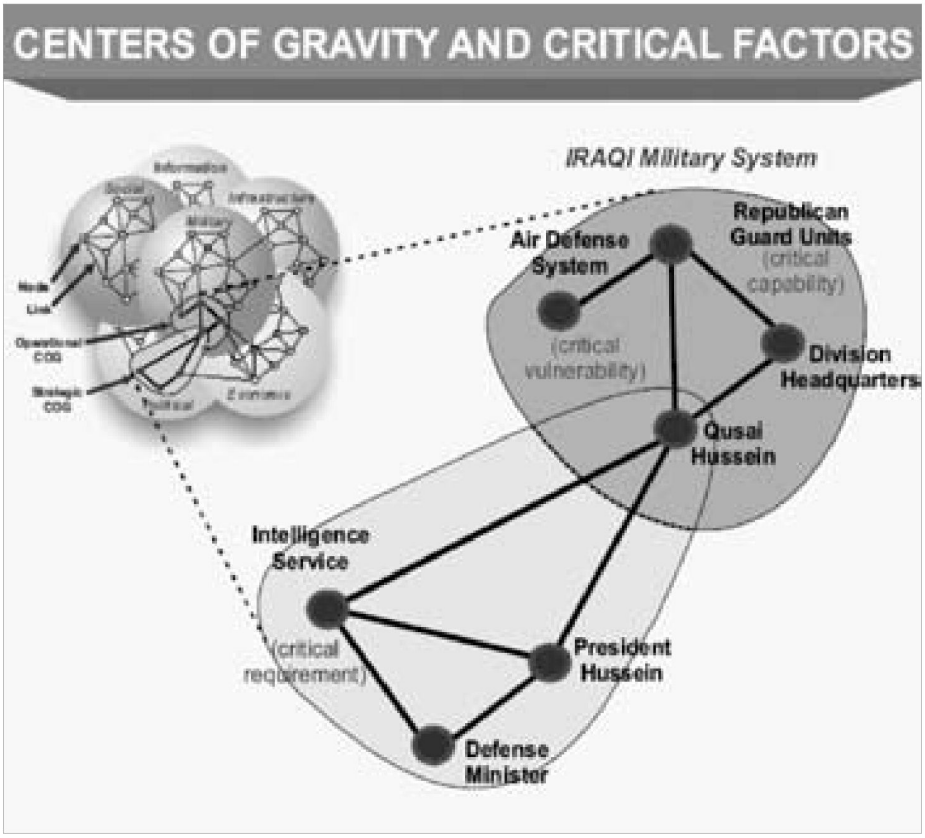
**Zusammenfassung und Ausblick**

Trotz dem gleichsam gebetsmühleartig wiederholten Pochen auf der Wichtigkeit der *Center of Gravity-Analysis* erwies sich der Ansatz seit seiner Einführung Mitte der achtziger Jahre in den amerikanischen Streitkräften und in ihrem Fahrwasser in praktisch allen westlichen Armeen vor allem als permanente Quelle des Missverständnisses und der Verwirrung. Nicht völlig zu Unrecht bezeichnete Major Seow Hiang Lee das Konzept in einer am amerikanischen Air and Staff College verfassten Arbeit als regelrechtes «Center of Confusion».[54] Ein Grossteil der Verwirrung hat seine Ursache wohl nicht zuletzt in einer bisweilen etwas allzu eklektischen Clausewitz-Rezeption, welche mitunter dazu tendiert, eigene Überlegungen mit Zitaten aus dem reichhaltigen intellektuellen Steinbruch des preussischen Kriegsphilosophen zu schmücken, anstatt den gesamten Gedankengängen des Autors von *Vom Kriege* zu folgen und zu versuchen, die jeweiligen Betrachtungen in ihrem grösseren Kontext zu verstehen.

Die Festlegung einer allgemein anerkannten COG-Definition ist denn auch bis heute nicht gelungen.

Immerhin: Vor allem dank den Arbeiten von Joe Strange verfügen wir heute über eine im Hinblick auf die praktische Umsetzung im Rahmen der Operationsplanung ausserordentlich nützliche Analysemethode, welche einen echten Mehrwert schafft. Dass sich die dazugehörige COG-Definition im Zuge der Forschung immer weiter von den Clausewitz'schen Grundideen entfernt hat, ist letztendlich von untergeordneter Bedeutung, war es doch bekanntlich noch nie ein Qualitätsmerkmal guter, d.h. praktisch anwendbarer Militärdoktrin, dass sie in allen Teilen mit den Reflexionen preussischer oder auch chinesischer Philosophen übereinstimmte. Denn mit dem Verlust an Kongruenz mit der Clausewitz'schen Begriffswelt ging unbestreitbar ein Gewinn an Kompatibilität mit dem für eine Analyse des heutigen komplexen Konfliktumfeldes unentbehrlichen Systemdenken einher. Ein *Center of Gravity* ist in diesem Zusammenhang nicht mehr zwingend «ein Schwerpunkt, dessen Bewegung und Richtung über die anderen Punkte entscheidet», vielmehr ein «maximum influence node», welcher dazu dient, die eigene Kraftanwendung auf die zentralen Systemelemente zu fokussieren, oder – etwas salopp ausgedrückt – ein Element, mithilfe dessen etwas Struktur in die ohnehin ausgesprochen komplexe System-of-System-Analysis gebracht werden kann.

In den aktuellen Führungsreglementen der Schweizer Armee, namentlich in der Operativen Führung XXI, wird sowohl der EBAO-Gedanke als auch die Systembetrachtung erwähnt[55] – allerdings nur in einer einzigen Ziffer und ohne dass die entsprechenden Ausführungen an anderer Stelle der Vorschrift ver-




*[8]*

tieft würden. Auch der Zusammenhang dieses systemischen Ansatzes mit der Center-of-Gravity-Analysis, wie wir dies oben skizziert haben, wird in der OF XXI eher vage angedeutet, indem festgehalten wird, dass es, um die Zentren der Kraftentfaltung zu definieren, unabdingbar sei, sowohl den Gegner als auch die eigene Seite als Gesamtsystem zu betrachten.[56]

> Solche und ähnliche theoretische und begriffliche Oberflächlichkeiten müssten im Rahmen der Überarbeitung der Führungsreglemente bereinigt werden, …

… und zwar unter Berücksichtigung neuester Erkenntnisse im Bereich der Systemtheorie. Ein gerade in Übersee oftmals vernachlässigtes Clausewitz'sches Diktum ist dabei allerdings stets im Auge zu behalten, das Diktum nämlich, dass jegliche Theorie, welche mit dem Geist in Opposition stehe, «diesen Widerspruch durch keine Demut gutmachen kann, und je demütiger sie ist, um so mehr wird Spott und Verachtung sie aus dem wirklichen Leben verdrängen.»[57]

[49] Umstead, Robert / Denhard, David R., Viewing the Center of Gravity through the Prism of Effects-Based Operations. In: Military Review 9/19 (2006), S. 90–95.
[50] Siehe NATO, Bi-SC Pre-Doctrinal Handbook (Effects-Based Approach to Operations), Final, 4.12.2007, S. 5–2f.: «Using the PMESII construct, systems analysis will provide the operational commander with an understanding of the engagement space and the strategic objectives and effects to be achieved/created. The operational commander will therefore use systems analysis to clearly understand the capabilities, behaviours and interactions of the main actors such that CoG(s) and objectives can be determined.»
[51] USJFCOM, Commander's Handbook for an Effects-Based Approach to Joint Operations, 24.02.2006, S. II-8f.
[52] JP 5-0, Joint Operation Planning, 26.12.2006, S. IV-8.
[53] Siehe dazu auch: Galvin, Thomas P., Assessing the New Joint Pub 5-0 Interpretation of «Center of Gravity»: Will it Help or Confuse Joint Planning. Arbeit im Rahmen eines Strategy Research Project. Carlisle 2006, S. 6–10.
[54] Lee, Seow Hiang, Center of Gravity or Center of Confusion – Understanding the Mystique. Alabama 1999, (Wright Flyer Paper; Nr. 10), S. 7–11.
[55] OF XXI, Ziff 57, S. 14: «Operative Führung orientiert sich am Potenzial aller beteiligten Kräfte. Der Erfolg einer Operation basiert daher auf umfassenden Kenntnissen sämtlichen Parameter, deren gegenseitige Abhängigkeiten sichtbar gemacht werden müssen. Diese Systembetrachtung ermöglicht eine gezielte Kraftanwendung auf erkannte gegnerische Schwächen. Ihr Ziel ist es, in der Folge eine Kaskade von Effekten zu generieren, um unter Einsatz minimaler eigener Mittel das gegnerische System zu lähmen (effektorientierte Operationen; international: effect based operations).»
[56] Ebd., S. 216.
[57] Clausewitz, Vom Kriege, 2. Buch, 2. Kap., S. 104.

*[8]* Analyse des Centers of Gravity und der Critical Factors im Rahmen einer systemischen Betrachtung am Beispiel des Golfkrieges 2003 (aus: USJFCOM, Commander's Handbook for an Effects-Based Approach to Joint Operations, 24.02.2006, S. II-9).

# L'information, zone de conflit et risque stratégique majeur

—

## Conséquences pour la politique de sécurité de la Suisse

La *guerre de l'information* est un de ces thèmes dont tout le monde parle mais qui semble-t-il ne se concrétise jamais. Depuis le dernier rapport sur la politique de sécurité en 1999, de nombreux événements ont pourtant eu lieu qui démontrent que l'information est un élément devant être pris très au sérieux en matière de politique de sécurité. Dans cet article, on va tenter de trouver le fil conducteur à partir de faits, à priori disparates, qui se sont déroulés depuis 2001 et qui l'attestent. On va montrer ensuite à quoi ressemble cette menace, quels sont ses acteurs, leurs motifs et les outils dont ils disposent pour attenter à la sécurité de la Suisse. Afin de cerner quelque peu cet immense domaine, une typologie est prés entée qui devrait, idéalement, constituer un dénominateur commun sur le sujet pour les discussions accompagnant la révision de notre politique de sécurité. Les conséquences de cette analyse sont ensuite résumées sous la forme de recommandations. L'article se termine sur la question *«Êtes-vous prêt à endosser la responsabilité si ça tourne mal?»* et son fil rouge est constitué des citations ci-dessous qui résument à elles seules tout ce qu'il faut savoir sur la question.

Gérald Vernez

Géologue et météorologue. Colonel EMG, chef d'état-major d'une brigade. A rejoint en 1996 le domaine des opérations au commandement de l'armée. Il s'est spécialisé dans la conduite et les opérations d'information. Il accomplit actuellement le MAS ETH Security Policy Crisis Management. Adresse: Etat-major de conduite de l'armée, Papiermühlestrasse 20, 3003 Berne. E-mail: gerald.vernez@vtg.admin.ch


### 1 Introduction

Depuis 1999, nous vivons au rythme du rapport de politique de sécurité 2000. Sa publication a entraîné de profondes transformations de notre appareil sécuritaire, mais notre esprit de défense est resté conventionnel, ce qui a engendré des lacunes. L'une de celles-ci est l'environnement informationnel et le but de cet article est d'apporter une vision d'ensemble sur ce domaine resté un parent pauvre de la sécurité.

#### Les environnements opérationnels

Lorsque l'on demande à un soldat, un policier, ou un chauffeur routier de mentionner dans quels environnements il se réfère à son quotidien et sa réponse est souvent «le sol et l'air». Pourtant, d'un point de vue global, cette subdivision est incomplète.

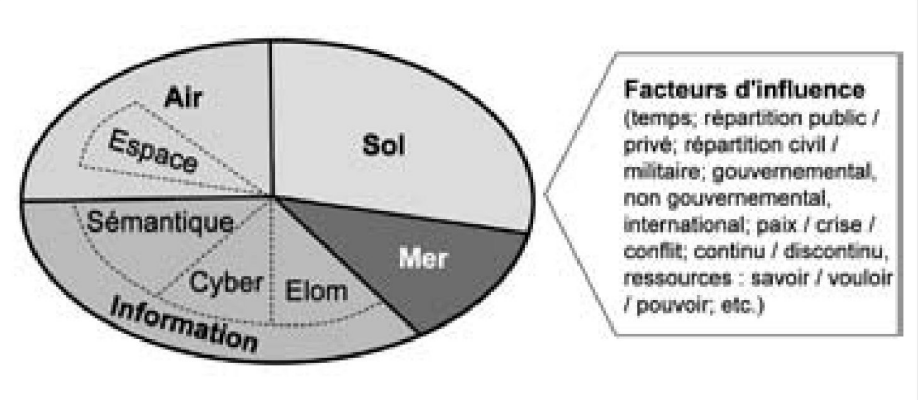
D'abord le terme «mer» manque à l'appel. La piraterie au large de la Somalie, l'aide lors du Tsunami, l'évacuation de nos concitoyens du Liban en guerre, ou notre politique d'approvisionnement en cas de crise désignent pourtant l'espace maritime comme un environnement[1] clé.

Ensuite, c'est le terme «information» qui fait défaut. Sans elle, nous ne pouvons ni appréhender la situation, ni planifier, ni diriger nos actions. Sans information les autres moyens sont donc inertes et inutiles.

Comme l'illustre la figure 1, l'environnement informationnel comprend trois parties:

- la dimension sémantique: c'est le monde des perceptions, de la signification et de la connaissance;
- la dimension technologique, divisée en cybernétique[2] (informatique) et électromagnétique[3] (éther).

Ces environnements ne sont pas invariables et il convient de considérer les facteurs d'influence qui les modifient et qui ainsi créent ou éliminent des options pour la politique de sécurité. Toute action dépend de la maîtrise de l'ensemble de ces




*[1]*

environnements en fonction des facteurs d'influence. Leur importance est telle qu'il ne viendrait à l'idée d'aucun stratège de prétendre que la protection de la nation ou une attaque couronnée de succès soient possibles sans maîtrise du ciel. En quoi cela serait-il concevable sans maîtrise de l'information?

Les conflits du Proche-Orient, de l'Afghanistan et de l'Iraq nous donnent la réponse. Ils nous montrent en effet que si la force sert à gagner la maîtrise des environnements air, sol et mer, le manque de maîtrise[4] de l'environnement informationnel rend toute victoire stratégique impossible. Les conflits ne trouvent alors pas d'épilogue.

Peu de généraux ont, mieux que Sir Rupert Smith[5], expliqué à quel point l'information est au cœur de la victoire. Il le résume d'ailleurs parfaitement par sa formule:

Capability = Means x Ways$^2$ x 3 Will.

On constate au quotidien, que nos réflexions capacitaires ont une fâcheuse tendance à se limiter à la question des moyens. Smith nous suggère ici de nous pencher sur l'art de réaliser les choses *(way)* et sur les perceptions *(will)*. Nous serions inspirés de suivre les conseils de ce grand soldat.

**L'environnement informationnel**

Dans la littérature traitant de l'information dans les conflits, le vocabulaire est variable et peu précis. Les expressions de *cyber-guerre et de guerre de l'information* induisent une approche militaire, informatique, ou guerrière, inadéquats pour les besoins de notre approche stratégique. En effet, ils occultent la complexité de la question et conduisent à des exagérations ou à des omissions. Pour corriger ce biais et répondre à nos besoins, on utilisera donc les expressions suivantes:

– Environnement informationnel: cette expression couvre tous les aspects techniques (vecteurs et contenants) et sémantiques (contenus et perceptions) de l'information; les termes *sphère* ou *domaine* ont été écartés, car ils suggèrent à tort l'existence de limites.

[1] JP 5-0, Joint Operation Planning, 26.12.2006, S. IV-8.
[2] La cybernétique est considérée (Wikipedia) comme l'étude des interactions entre systèmes gouvernants. «Cybernétique» vient du mot grec «kubernesis» signifiant au sens figuré «diriger» ou «gouverner». Le préfixe «cyber» désigne donc le monde de l'informatique.
[3] Désigne le monde des ondes et des transmissions ou, selon une notion plus ancienne de la physique, «l'éther», considérée comme la substance qui remplissait l'espace.
[4] Pour nous, au lieu de «maîtrise» il est plus réaliste de parler de «supériorité», ou la maîtrise limitée dans l'espace et dans le temps de certains éléments choisis.
[5] Rupert Smith. The Utility of Force - The Art of War in the Modern World. Penguin Politicy / History, 2005. Le général Smith a été commandant de la division blindée britannique lors de la guerre du Golfe (1990-1991), des forces de l'ONU en Bosnie (1995), des forces militaires en Irlande du Nord (1996-1999) et commandant suprême en second des forces alliées de l'OTAN en Europe (DSACEUR).

*[1]* Fig. 1: Les environnements opérationnels et les facteurs d'influence

– Menaces dans l'environnement informationnel: cette expression couvre tous les potentiels, intentions, organisations et acteurs susceptibles de s'en prendre à notre environnement informationnel.
– Conflits dans l'environnement informationnel: cette expression couvre toutes les activités conflictuelles dans, par et avec l'information.

S'agissant de l'information elle-même, précisons qu'elle n'est pas le but ultime, mais uniquement un moyen sur le chemin de la finalité. A travers l'information, on vise les savoirs, les perceptions, les actions qu'elle permet, les systèmes qui la contiennent, la transportent et la modifient.

> Sans contenu informationnel, le meilleur muscle reste immobile et n'effectue pas le mouvement prévu par le cerveau.

Ceci peut avoir plusieurs causes: l'ordre n'a pas été généré (le processus décisionnel a été perturbé) ou n'est pas parvenu au muscle (la transmission est perturbée); mais il peut aussi avoir été corrompu en chemin (manipulation, déception), ce qui peut engendrer un mouvement et des conséquences involontaires. Pour une machine comme pour un homme, cela peut aller jusqu'à son autodestruction. Pour un pilote de combat, il risque de détruire des objets non ciblés. Et cela s'applique aussi au chauffeur routier qui reçoit des informations falsifiées sur son téléphone mobile et livre des biens au mauvais endroit. Dans tous ces exemples, la finalité n'est pas l'information mais l'action qui en dépend: saboter une machine, manipuler une personne, faire manquer sa cible au pilote, faire perdre un client au camionneur.

**Faisons «la peau» à l'asymétrie**

Au travers de la formule du général Smith, on comprend que la capacité à vaincre est avant tout une affaire d'intelligence *(way)* et de courage *(will)*. Cela signifie que l'on attend du combattant qu'il trouve des manières originales pour vaincre son ennemi, même si ce dernier est plus fort. Faire la guerre n'est pas une activité de *gentlemen*. C'est sale et violent. Faire la guerre c'est vaincre l'ennemi par tous les moyens, par toutes les ruses, le plus vite possible, avec le moins de pertes et le plus de profit possible (tactique, politique, mais aussi économique quand il s'agit de piller les greniers de l'ennemi). Bien sûr qu'il faut, comme le dit le général Dufour *«sortir de cette lutte non seulement victorieux, mais aussi sans reproche»*. C'est pourquoi notre monde a établi des règles pour moraliser la guerre. Que nous les observions est tout à notre honneur et nous le ferons, mais s'attendre à ce que notre ennemi fasse de même et tout miser là-dessus relève de la naïveté coupable.

C'est pour indiquer que l'adversaire ne se tient pas à nos règles, que l'on a inventé le terme d'asymétrie, concept fourre-tout bien pratique qui a surtout permis, notamment aux américains, de vendre au monde la *guerre contre le terrorisme.*

> Tout ce qui n'est pas conforme à notre normalité se retrouve taxé d'asymétrie, …

… mais quelle réalité tactique justifie donc cette terminologie? Si on suit le raisonnement des chantres de l'asymétrie, alors il faut y classer également les armes nucléaires, chimiques et biologiques ainsi que les mines anti-personnel. Car tous ces moyens sont prohibés par notre morale et souvent aussi par le droit international. Pourtant personne ne les classe comme *asymétriques,* car même si elles sont épouvantables, ces armes font partie des arsenaux des grands Etats. Alors, bel euphémisme, on nous présente leur usage éventuel comme *ultima ratio!*

Dans la guerre tous les moyens sont bons, dès lors que celui qui les utilise le fait en fonction de ses règles. Et ce ne sont pas forcément les nôtres. Le vainqueur sera, indépendamment des rapports de force, celui qui réussira à emmener son adversaire sur un terrain où ce dernier est inférieur[6], pas présent[7], ou pas prêt[8]. Et c'est là que réside le génie stratégique. Parler d'asymétrie parce qu'on s'est fait piéger dans quelque chose auquel on ne s'attendait pas, c'est simplement avouer que nous ne sommes ni en mesure de nous adapter à l'ennemi, ni de le surprendre. C'est avouer que nous sommes otages de nos conventions et donc faciles à battre. Un tel aveu est plutôt inquiétant.

Dénoncer la monstruosité d'un adversaire qui, à notre sens uniquement, a commis quelque chose de moralement répréhensible dans le conflit à mort qui nous oppose, alimente peut-être une certaine rhétorique chère aux opérations psychologiques, mais ne nous protège pas. Au contraire, elle induit un dangereux biais dans nos raisonnements, ce qui est préjudiciable à notre préparation face aux vrais défis.

> Plusieurs auteurs[9] pensent que d'affronter la supériorité militaire occidentale est vain et que l'Occident doit être attaqué autrement.

Les colonels Qiao Liang et Wang Xiangsui[10] pensent que la Chine doit éviter la confrontation directe et chercher à vaincre par d'autres moyens. Dans ce cas on en déduit que les armées ne serviraient qu'à consolider la victoire sur le plan opératif et tactique. Ainsi, les chinois semblent déterminés à utiliser l'environnement informationnel, notamment pour récupérer Taiwan. A cet effet ils envisageraient un volet technologique contre les infrastructures taïwanaises et contre la logistique des USA pour les empêcher d'intervenir et un volet psychologique contre cette île considérée comme moralement faible et sus-ceptible de tomber comme un fruit mûr[11].

Utiliser ces méthodes, ces ruses et l'environnement informationnel n'a donc rien d'asymétrique. Ce n'est que la conséquence logique d'une analyse qui conclut à l'impossibilité de vaincre de manière frontale par les armes, ce que suggère d'ailleurs Churchill dans la citation au début de cet article.

## 2 Crises et conflits significatifs

Jusque là, nous avons illustré à quel point l'information est une partie clé des conflits, au même titre que les autres environnements. Pour vérifier cette conclusion avec des exemples pratiques et en tirer des conséquences utiles, 6 cas sont discutés ci-après.

**Terrorisme et image de l'Amérique**

Après l'attaque simultanée contre les ambassades U.S. de Nairobi et Dar Es Salam (07.08.1998), puis l'attentat contre le destroyer USS Cole (12.10.2000), le 9 septembre 2001 marque le passage à un terrorisme dit *de masse.* Déployant une violence inégalée, cet acte va profondément secouer les USA et toucher la plus grande puissance dans son cœur. Les images de l'effondrement des tours du World Trade Center et du Pentagone partiellement en feu, passant en boucle sur toutes les télévisions des heures durant, vont induire un choc mondial. Le message d'Al Qaeda, *«on peut frapper où on veut, comme on veut, quand on veut»,* sera ressenti par les USA comme la provocation ultime, comparable à Pearl Harbour en 1941 et va déclencher la chasse planétaire contre les terroristes et leurs sponsors. Avec la *Global War On Terror,* les USA vont ouvrir deux conflits, non résolus à ce jour, en Afghanistan puis en Iraq. Mais alors que les USA avaient engrangé un fort capital de sympathie avec l'évènement du 9/11, ces guerres vont générer des images désastreuses pour eux, notamment à Abu Ghraib, à Guantanamo et avec les prisons de la CIA. Les soldats américains se sont admirablement battus, mais les dérapages et les mensonges sur les liens entre Saddam Hussein et le terrorisme ou au sujet des armes de destruction massive vont faire un tort considérable à l'Amérique. Son président va devenir un objet international de haine et la justification pour d'autres actes terroristes, surtout après son erreur de qualifier la lutte contre le terrorisme de *croisade.*


*[2]*

**Katrina ou l'impuissance du plus puissant**

L'ouragan Katrina aux USA en août 2006 mettra au grand jour les faiblesses de la *Federal Emergency Management Agency.* Surtout, l'Amérique va alors donner l'impression d'être incapable de prendre les bonnes décisions et d'acheminer à temps les secours à ses sinistrés. Avec une *National Guard* engagée en Iraq et ne pouvant que timidement aider sa propre population et *«Air Force One»* faisant des cercles à basse altitude sur la Nouvelle-Orléans pour permettre au Président de contempler le désastre, l'image d'impuissance de l'Amérique sera totale. Prise entre des conséquences annoncées, donc évitables, et les scandales politico-médiatiques qui en découleront, la popularité du Président, déjà au plus bas, atteindra un abîme historique, renforçant ainsi en même temps les détracteurs de l'Amérique.

**Estonie, Titan Rain et la vulnérabilité des infrastructures**

En mai 2007, l'Estonie va subir une attaque en règle. Durant plusieurs semaines et en plusieurs vagues, des attaquants, toujours non identifiés, vont faire payer à ce pays son audace de vouloir déplacer un symbole de l'ère soviétique. Partiellement retracées jusqu'en Russie, ces cyber-attaques seront attribuées au Kremlin; faute de preuves, cette accusation sera retirée. Mais tout cela n'est pas le fait de simples hackers et seule une organisation professionnelle a pu réaliser une opération de cette complexité. Première du genre à l'échelle d'une nation, cette attaque va réveiller les craintes de cyber-guerre et de cyber-terrorisme. Elle va aussi contribuer au lancement du *Cooperative Cyber Defense - Center of Excellence* de l'OTAN et justifier la place de ce problème en haut de l'agenda de l'Alliance.

Ces événements doivent être mis en perspective avec les dires d'un représentant de la CIA[12] en 2007 qui va révéler l'existence, hors des USA, d'attaques ayant pénétré des réseaux de distribution d'énergie. Ceux-ci auraient, une fois au moins,

[6] Voir le cas d'Israël au chapitre suivant.
[7] Actes terroristes là où de telles actions ne sont pas attendues, comme par exemple 9/11.
[8] Cas de l'attaque du destroyer USS Cole dans le port d'Aden (Yémen) le 20.10.2000.
[9] Comme le général Wang, fondateur des opérations d'informations chinoises (Toshi Yoshihara. Chinese Information Warfare: a Phantom Menace or Emerging Threat. Strategic Studies Institute, U.S. Army War College, 2001)
[10] Qiao Liang et Wang Xiangsui. Unrestricted Warfare. Beijing: People's Liberation Army Literature and Arts Publishing House, 1999. Dans la catégorie des non-military war operations ils considèrent les guerres commerciale, financière, écologique, une nouvelle forme de terrorisme de masse, psychologique, de fraude, médiatique, de la drogue, des réseaux, technologique, de fiction, des ressources, de l'aide économique, de la guerre culturelle, des lois internationales.
[11] James C. Mulvenon, Director, Advanced Studies and Analysis, DGI Center for Intelligence Research and Analysis. Chinese Information Operations Strategies in a Taiwan Contingency. Testimony before the U.S.-China Economic and Security Review Commission Hearing, 2005.
[12] Andy Greenberg. Cyber Crime - Hackers Cut Cities' Power. Forbes.com, 2008.

*[2]* Fig. 2: Le Président géorgien Saakachvili assimilé à Hitler par les propagandiste russes.

causé une panne de courant généralisée affectant plusieurs villes. En raison de l'état déplorable des infrastructures[13] donc de leur faible sécurité et stabilité, le terrain est fertile pour des tentatives d'extorsion et un responsable du *US Department for Homeland Security*[14] déclare à la même période que la criminalité informatique supplante désormais le marché mondial de la drogue avec un chiffre d'affaire annuel supérieur à 100 milliards $.

Lors du DefCon 2007, la conférence annuelle des hackers, un conférencier démontrera comment attaquer les systèmes SCADA[15] et la preuve de la vulnérabilité de ces systèmes sera apportée par le *Department for Homeland Security* au travers d'une démonstration rendue publique à fin 2007[16]. Parmi d'autres réalités, citons le cas[17] de l'une des plus grandes compagnies européennes de télécommunications gérant 120 millions de mails par jour, dont 92% sont des spams et qui consacre 10% de ses capacités à lutter contre des attaques de déni de service.

En 2005, des agences américaines de sécurité lancent l'alerte pour des attaques contre les réseaux de la Défense. Lancée de Chine et baptisée Titan Rain[18], cette attaque touche aussi la Grande Bretagne, la France et l'Allemagne. Le gouvernement chinois a toujours nié toute implication. Il s'agit de *«hackers isolés se servant des réseaux chinois comme couverture».* Mais ces dénégations sont contredites par de nombreux experts accusant le gouvernement chinois (et aussi russe), de sponsoriser le cyber-terrorisme et de rendre impossible le combat contre les agresseurs en refusant de les poursuivre ou de les extrader.

**Le conflit russo-géorgien**

Dans les médias, ce conflit va déclencher une vague de titres sur la *guerre de l'information.* Même si dans les faits la Géorgie a peu souffert d'attaques informationnelles, en raison certainement de son faible développement dans ce domaine, on aurait tort de ne voir là qu'un épiphénomène. Peu après son agression contre les troupes russes en Ossétie du Sud, la Géorgie va rapidement être contrainte de poursuivre le conflit en évidente infériorité. Le pays se réfugie alors derrière l'image d'un président faisant tout pour apparaître pro-occidental et s'affichant devant le drapeau européen pour invoquer sa protection face à ce qu'il décrit comme une *«intolérable agression russe».* Malgré les tentatives géorgiennes de prendre le monde à témoin, ni l'Europe ni les USA ne se hasardent à s'en mêler directement et jouent plutôt la carte de l'apaisement et de la solution politique.

Il est intéressant de constater que le message géorgien a été bien relayé par les médias occidentaux, alors que le message russe n'a pas été entendu. Ce qui a fait grand bruit et a été vivement dénoncé en Europe, c'est la propagande anti-géorgienne et les actions de défiguration de sites internet par des *cyber-patriotes* russes. Pour les services en ligne (information, banques, services gouvernementaux) qui ont été perturbés, certains ont déménagé leur portail dans des serveurs étrangers[19] pour assurer la continuité de leurs activités. En apparence inoffensive, cette solution pose néanmoins des questions légales. Quel est le comportement et les responsabilités qu'un Etat tiers endosse en offrant de tels services à un Etat en guerre surtout s'il en résulte des pertes économiques, des dégâts physiques, ou encore des pertes humaines ? Vaste question, mais les sites ainsi délocalisés n'ont plus été ennuyés, preuve peut-être que les attaquants se sont aussi posé ce genre de question.

> Comme en Estonie, il est impossible de dire si la Russie officielle se cache derrière ces attaques.

Toutefois, la réaction rapide et bien coordonnée qui a accompagné les opérations militaires ne laisse pas beaucoup de place à une *réaction populaire spontanée.* Comme pour la Chine, il semble évident que Moscou tolère ces activités sur son sol et en profite.

**Israël et le conflit du Proche-Orient**

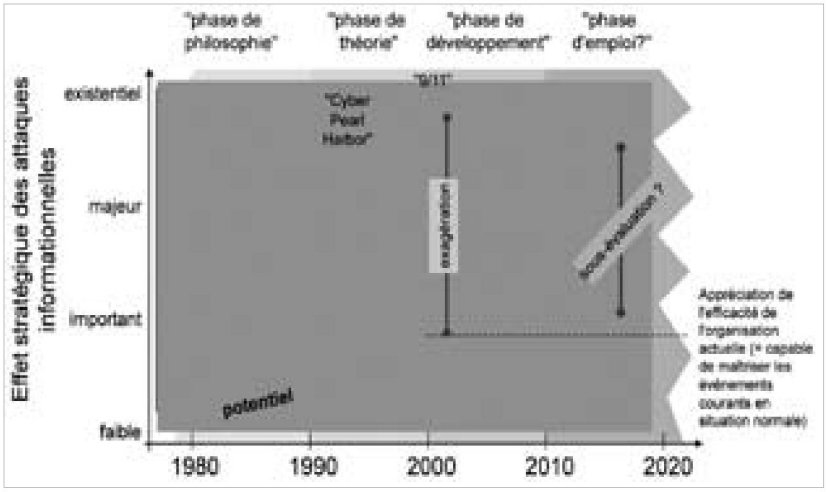
Au Proche-Orient, la bataille des perceptions fait constamment rage. Dans les technologies de l'information, la supériorité de Tsahal est complète. Même la prise de contrôle des canaux ennemis de radios et de télévision pour y diffuser ses propres messages est maitrisée. Les opérations psychologiques sont un standard et Israël a répandu plus de 17 millions de tracts en 47 missions durant la campagne de 2006 au Liban. Un autre vecteur utilisé régulièrement est le téléphone mobile qui permet de délivrer des messages très personnalisés et très efficaces, directement aux combattants ennemis identifiés ou à leur entourage direct.

Si sur le plan militaire, Israël ne craint personne, stratégiquement cela semble mal engagé, car son image se détériore irrémédiablement et ses soutiens diminuent. Ses ennemis ont en effet compris que pour vaincre l'Etat hébreu, il faut conquérir le cœur du monde en le poussant à la faute. Et le mécanisme est bien rôdé. Israël est provoqué quotidiennement par des enlèvements, des attentats et d'incessants missiles s'abattant sur son sol. Si cela ravive d'abord une certaine sympathie à son égard, cela l'oblige surtout à intervenir. Il s'ensuit alors des combats urbains très durs[20] nécessitant des moyens lourds[21]. En combattant systématiquement au milieu des populations, derrière les ONG et l'ONU, le Hamas et Hezbollah savent qu'ils vont invariablement provoquer des «affaires» médiatiquement destructrices pour Israël. Les exemples s'appellent Mohamad al Dura, Jenin[22], Cana[23], le bâtiment de l'ONU à Gaza il y a quelques semaines[24] ou encore la position de l'UNIFIL au Sud Liban en 2006.

Plus globalement, il faut encore ajouter la lutte entre l'Iran et le monde occidental au sujet de la volonté des mollahs de se doter de l'arme nucléaire et de leurs réitérées menaces de raser Israël dès qu'ils le pourront. Le risque que ce genre d'arme arrive dans des mains terroristes agit alors comme un levier peut-être capable de pousser Israël à des frappes préventives en Iran. De telles rumeurs de ces possibles bombardements réapparaissent régulièrement.

**Crise et crime économiques**

La crise actuelle apporte aussi ses enseignements. Il y a tout d'abord le *fonctionnement en temps réel de l'économie globalisée* et ses réactions à chaque rumeur, indépendamment de l'heure et du lieu. Ensuite, il y a la *gestion de crise,* élément critique où le dicton *«la parole est d'argent et le silence est d'or»* ne tient plus; le silence gêné n'est en effet pas une stratégie et les exécutifs doivent être prêts à gérer l'information dans des délais toujours plus brefs, face à des publics toujours plus agressifs.




*[3]*

## Il y a aussi la *virtualisation* d'une finance qui génère des valeurs sans fabriquer de biens; …

… mais au contraire des jeux vidéo où l'on peut ressusciter, les sommes sont bien tangibles, surtout pour ceux qui les perdent! Dans l'affaire de la Société Générale en France c'est la question de l'insider qui contourne le dispositif de sécurité (coût: 4.9 milliards d'€). Dans le même registre humain, le cas Madoff qui trompe tout le monde (coût: 50 milliards $), ou l'ingénierie sociale[25] permettant à Rifkin en 1978 de soutirer 10 millions $ en une observation et deux coups de téléphone à la Security National Bank de Los Angeles. Einstein disait *«Deux choses sont infinies: l'univers et la bêtise humaine, en ce qui concerne l'univers, je n'en ai pas acquis la certitude absolue.»* Avec cette citation et les exemples précédents au sujet du secteur bancaire, il faut comprendre que tout n'est pas affaire de technologie et que le facteur humain est central.

Il est aisé de pénétrer dans les systèmes informatiques pour des organisations criminelles toujours plus professionnelles. Pour les agresseurs moins sophistiqués qui manqueraient de savoir-faire, les armes à cet effet peuvent être acquises en ligne sur Internet . Si à la malveillance, la vengeance, l'appât du gain, les affaires de chantage, on ajoute la négligence , ces attaques peuvent tourner à la catastrophe pour les cibles.

**Pour conclure ce tour d'horizon**

Ces cas montrent qu'une lecture complémentaire des crises est nécessaire. Au Proche-Orient, le droit ne joue qu'un rôle subordonné. Avoir raison ne sert à rien. Seules les perceptions comptent. Et à quoi sert la meilleure préparation militaire si le pays est paralysé psychologiquement ou sur le plan logistique à cause de la mise hors service de son infrastructure vitale? Et l'ennemi ne doit pas forcément disposer des meilleurs hackers du monde pour y parvenir; cela aide, mais il peut aussi les louer sur Internet. Et tout cela, c'est sans compter les armes à impulsion électromagnétique[28] qui réduisent tout ce qui contient de l'électronique en matière inerte en une fraction de seconde.

[13] En 2008, l'ancien ministre US de l'énergie déclarait au sujet du réseau américain «a super-power with a third-world electricity grid» (Larry Walsh. Hackers Gain Real Power Over Electric Grid. Baseline Security, http://blog.baselinemag.com/security, 2008)

[14] Assessing the Cyber Security Threat. Security and Defense Agenda, Bruxelles, SDA Monthly Roundtable, 2008.

[15] Supervisory Control And Data Acquisition qui sont les systèmes permettant de contrôler à distance tous les processus industriels, la distribution des fluides, la gestion du trafic, mais aussi la distribution d'électricité, etc. Anciennement isolés, ces systèmes, de conception ancienne et d'un faible niveau de sécurité, se retrouvent tout-à-coup dans le réseau, atteignables depuis Internet et donc très vulnérables.

[16] Connu sous le nom de Aurora Generator Test, il s'agissait de démontrer la faisabilité de l'attaque par voie informatique d'un générateur. Le résultat de ce test peut être vu dans une vidéo. www.youtube.com/watch?v=fJyWngDco3g

[17] Exposé du Dr. Thomas Ramsauer (Ministère allemand de l'intérieur) à la conférence Cyber Warfare 2009 à Londres.

[18] Franck Ebel. La Chine accusée de soutenir le cyberterrorisme. www.acissi.net et The Guardian (top story), 06.03.2008.

[19] En Pologne notamment, qui s'est mise spontanément à disposition.

[20 Les combattants du Hamas et du Hezbollah sont très bien entraînés et bien équipés.

[21] Il s'agit d'une guerre ou Israël doit protéger ses soldats et ne peut pas accepter une symétrie des pertes pour que ses actions soient «médiatiquement acceptables».

[22] Jenin est cette localité rasée pour les uns par Tsahal en 2002, alors que pour d'autres seules quelques dizaines de maisons (5% de la localité, au préalable évacué) ont été détruites pour en extirper des combattants ennemis.

[23] A Cana, les palestiniens ont accusé Tsahal d'avoir tué près de 60 personnes dans un bombardement (femmes, enfants et vieillards innocents … et aucun combattant !). Selon les officiels israéliens, le bâtiment était utilisé pour stocker des explosifs et beaucoup d'observateurs estiment qu'il y a eu mise en scène des palestiniens. Le même jour, le journal 24 Heures couvre cet événement par une pleine page; pour 60 fillettes massacrées dans leur école au Sri-Lanka, il consacre 15 cm2, soit 100 fois moins !

[24 Il s'agit à nouveau d'enfants morts, image ravageuse en matière de perceptions.

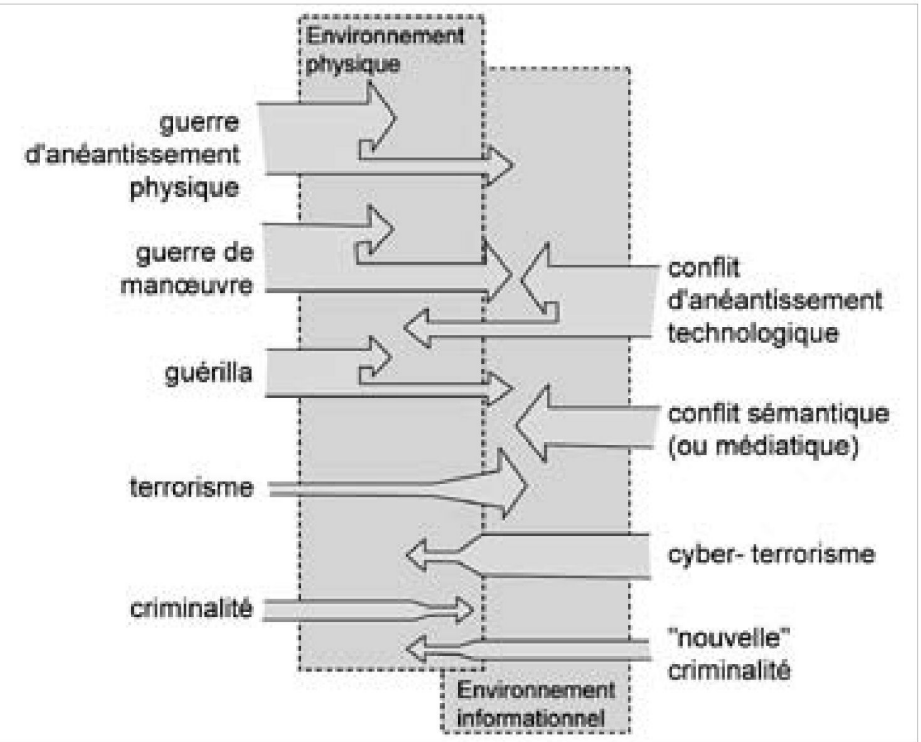
[25] Kevin D. Mitnick. The Art of Deception - Controlling the Human Element of Security. John Wiley and Sons, 2002.

[26] Selon Pedro Bueno, de McAfee Avert Labs (www.pcinpact.com), les tarifs courants sont les suivants: déni de service distribué (DDoS): entre 500 et 1500 $; virus spécialement conçu pour cibler une entreprise de votre choix: 50 000 $; virus modifié pour éviter la détection de signature: 200 $; 10 millions d'adresses email: 160 $; numéro de carte de crédit: de 2 à 6 $; numéro de carte de crédit avec son code: de 20 à 60 $; location d'un portable contrôlant un réseau botnet (5 à 10 000 ordinateurs): 100 $/jour; kit de phishing (hameçonnage): de 700 à 1000 $. En 2007, les internautes américains ont ainsi perdu 3,2 milliards de dollars du fait du phishing.

[27] Wade H. Baker, C. David Hylender, J. Andrew Valentine. 2008 Data Breach Investigations Report. Verizon Business Risk Team, 2008. De nombreux cas résultent de failles pour lesquelles des correctifs existaient depuis 6 mois. De plus, selon ce rapport, près de 20% des incidents et la majorité des pertes sont imputables à des insiders. Si ces derniers disposent en plus de droits d'administrateur, ils laisseront des souvenirs très désagréables!

[28] Des versions de ces armes sont disponibles sous plusieurs formes, notamment en tant que charge utile pour missile, obus de 155mm et attaché-case.

*[3]* Fig. 3: Appréciation générale de la menace dans l'environnement informationnel




*[4]*

## 3 Que faut-il comprendre et redouter?

de ce qui précède, il s'agit d'établir un profil général servant ensuite à la détermination de mesures possibles.

**Etat et développement de la menace**

L'évolution de la menace est résumée dans la figure ci-dessous.

- Phases: depuis que Toffler a décrit en 1980 l'évolution du monde en trois vagues[29], l'information est devenue une dimension à part entière dans l'analyse des conflits. Dans les années 90, on passe de la philosophie à la théorie et les doctrines militaires s'en emparent. Durant les années 2000, les concepts se précisent et des essais sont conduits dans les conflits en cours. L'évolution actuelle montre que la prochaine décennie sera celle de l'opérationnalisation de l'information qui pourrait prendre le pas sur les effets cinétiques.
- Capacités effectives et supposées: une certaine hystérie a régné durant les années 90, avec une culmination en 2001. Des ministres ont même craint un prochain *Cyber Pearl Harbor.* La menace reste difficile à mesurer[30], mais il semble qu'elle ait été clairement surévaluée. Les exagérations ont alors conduit beaucoup de gens à douter de cette réalité et beaucoup de décideurs l'ont alors ignorée, même si le sujet revenait dans chacun de leurs discours. Les derniers développements technologiques et faits concrets indiquent cependant que nous sommes désormais dans la situation où nous sous-estimons le danger, même si il est toujours impossible à mesurer. En effet, au contraire des chars, avions, bateaux, soldats et missiles, la menace informationnelle n'est pas quantifiable et c'est ce qui la rend si dangereuse car l'effet de surprise sera maximal.

**Internet et la cybernétique: lien et lieu de tous les problèmes**

Internet, source indéniable de prospérité et icône de la globalisation, est en passe de devenir la principale source de nos maux. C'est le vecteur d'une grande partie des attaques cybernétiques. Tout notre savoir et tous nos processus en dépendent. Grâce à ce «monstre», le voleur est dans nos maisons, l'espion dans nos laboratoires et le soldat ennemi dans nos rues. D'ailleurs, comment peut-on raisonnablement penser en déployant des produits informatiques en provenance de Chine dans nos infrastructures vitales et classifiées, que ceux-ci soient sûrs ? Et il en va de même pour les produits *Made in USA*[31]. Combien de lignes de codes et de transistors recevons-nous en bonus dans nos commandes ? Nous ne pouvons pour ainsi dire pas nous y opposer sauf à démonter chaque machine et y vérifier chaque ligne de code, option impraticable et ridicule. Mais couper une liaison, c'est comme stopper le sang qui entre dans un membre, cela revient à le condamner ou à l'immobiliser. Et laisser circuler le sang, c'est prendre le risque que la maladie pénètre dans le corps. Voilà un dilemme intéressant.

**Caractéristiques de l'environnement informationnel**

La liste ci-après tente de cerner les avantages et risques liés à l'information.

- Accessibilité à n'importe quel acteur: même si on observe partout une augmentation des budgets et une professionnalisation, l'environnement informationnel reste accessible à n'importe qui avec de faibles moyens et des connaissances restreintes.
- Rapport coûts / bénéfices attractif: en comparaison avec d'autres moyens, une *Task Force Information* coûte peu, intervient partout sans se déplacer physiquement et l'efficacité du *Information-Warrior* est très supérieure à celle d'un *Kinetical Warrior.*
- Insensibilité au temps et effet de surprise: contenus et cibles

| Type de l-attaque / Buts | Acteurs (nombre, budget) | Type 1 technologique (organisationnel – fonctionnel) | Type 2 sémantique (cognitif – psychologique) | Type 3 combiné (cognitif – psychologique – organisationnel – fonctionnel) |
|---|---|---|---|---|
| **Politique** (inclus les motifs religieux et ethniques sous-jacents) | • Etats<br>• Organisations terroristes (opérationnel)<br>• Nationalistes<br>(quelques dizaines) | X ? | X ↓ aussi amis **X** | X ↓ aussi amis **X** |
| **Profit** | • Criminalité (organisée et internationale)<br>• Terroristes (fonctionnel)<br>• Economie<br>(centaines de milliers) | **X** | X | |
| **Pathologique** | • Extrémistes<br>• Frustrés<br>• Joueurs<br>• Désœuvrés<br>• Vengeances<br>• "Murphy"<br>(dizaines de millions) | **X** problème = masse | X | |

*[5]*

sont disponibles et atteignables instantanément et en permanence. Si les préparatifs d'une attaque n'ont pas été détectés, l'effet de surprise est total. Quant l'attaque est avérée il ne reste d'autre choix que de gérer, contenir l'extension des dommages et revenir à la situation normale le plus rapidement possible.

- Insensibilité aux distances et disparition des frontières: les cibles sont atteignables quelles que soient les distances. Les technologies spatiales, cybernétiques et médiatiques permettent un suivi en temps réel. Les frontières politiques ne freinent bientôt plus que les poursuites judiciaires!
- Discrétion et déception: les préparatifs d'une attaque sont quasi indétectables; on peut aussi faire croire à la culpabilité d'un tiers, faire circuler des informations manipulées, etc. Camouflage et déception sont les maîtres mots et l'identification d'un agresseur souvent impossible.
- Impunité des acteurs: un Etat ou un groupe criminel peut utiliser des tiers pour commettre ses attaques et échapper à ses responsabilités. Si l'Etat protège ces acteurs, refuse de les poursuivre pénalement, de les extrader ou fait traîner les procédures, il rend toute contremesure légale impossible. Les criminels peuvent en outre passer d'un Etat à l'autre et profiter des lacunes juridiques.
- Des guerriers sans uniformes: il est impossible de déterminer le statut des acteurs. Souvent ce sont des civils et les mots *guerre* et *uniforme* sont alors inapplicables.
- L'environnement informationnel est un arsenal: développer des armes informationnelles est complexe et parfois hors de portée de petites organisations ou d'individus; mais il suffit alors d'acheter ces outils sur Internet. Faire circuler une rumeur ou une fausse information est simple avec de l'imagination, la compréhension du monde des médias et quelques logiciels de traitement d'image et de vidéo. Internet permet en outre de trouver la plupart des informations nécessaires[32].
- Forum de dénonciation et de désobéissance mais aussi de manipulation: grâce aux médias, plus aucune information ne peut être gardée secrète. Tout dérapage par rapport aux normes est découvert et dénoncé, renforçant ainsi la démocratie. Mais à travers les médias on peut aussi affaiblir la démocratie, attiser la désobéissance ou encore lancer toutes sortes d'attaques et de rumeurs.
- L'homme, ce maillon faible: comme dit Mitnick[33], *«vous pouvez dépenser autant que vous voulez pour la sécurité, tant que le facteur humain n'est pas maîtrisé, vous êtes vulnérable».* L'ingénierie sociale est certainement un des fléaux les plus efficaces dont on se méfie le moins.

[29] Alvin Toffler. The Third Wave. Bantam Books, 1980. Selon sa théorie, les sociétés se déclinent en trois vagues: de l'agriculture, de l'industrialisation, de l'information.

[30] Il existe peu d'articles sur ce sujet; voir par exemple Giampiero Giacomello (Measuring «Digital Wars»: Learning from the Experience of Peace Research and Arms Control. IWS –The Information Warfare Site, 2003).

[31] Basé sur les accusations régulière d'interférence portées contre le FBI (cas du CARNIVO-RE et du DCS 100) ou la NSA (cas de ECHELON et des backdoors dans Lotus Notes par exemple).

[32] On parle alors de OSINT ou Open Source Intelligence. De nombreux spécialistes estiment que par ce biais plus de 80% du renseignement peut être trouvé sans difficulté.

[33] Kevin D. Mitnick. The Art of Deception - Controlling the Human Element of Security. John Wiley & So, 2002.

*[4]* Fig. 4: Types de conflits et leur relation et poids relativement aux environnements physiques et informationnels

*[5]* Fig. 5: Typologie des menaces dans l'environnement informationnel

**Typologie des actions dans l'environnement informationnel et motifs**
En s'inspirant des suggestions de Wilson[34] et en poursuivant la discussion précédente, on voit que les conflits génèrent des effets dans l'environnement physique (air - sol - mer) et dans l'environnement informationnel. La figure ci-après présente les typologies de conflits ou de violences. Elle illustre le fait que l'environnement informationnel peut être atteint par l'environnement physique et inversement et ce à des intensités et pour des finalités variables.

- La guerre[35] d'anéantissement (ou d'attrition) vise à détruire le potentiel guerrier ennemi, si nécessaire sa nation toute entière, ou à s'en emparer; les armes de destruction massive appartiennent à cette catégorie dont les effets informationnels sont secondaires.
- La guerre de manœuvre (ou guerre moderne) vise à contrôler l'ennemi en maîtrisant ses points clé sans devoir lui infliger de destructions extensives. La guerre du Golfe en 1991 ou d'Iraq en 2003 appartiennent à ce type de conflit qui influence la manière dont on constitue les armées aujourd'hui. C'est une modernisation de la guerre d'anéantissement rendue possible par la technologique. Le point d'entrée est physique, mais l'information est un effort principal.
- La guérilla (ou petite guerre) vise à user l'ennemi, le tenir éloigné ou encore garder le contrôle partiel de biens ou de territoires; les violences urbaines durant le G8 en 2003, des banlieues françaises en 2005, ou de Grèce en décembre dernier s'y apparentent. Moyens et effets sont avant tout physiques, même si la composante psychologique (démoralisation de l'adversaire) en fait partie.
- Le terrorisme est une variation de la guérilla mais sans limites géographique ou de violence. Son but est essentiellement psychologique; il s'agit de terroriser, pousser l'autre à la faute, obtenir des concessions, etc. Le terroriste n'a pas pour but le gain ou la possession de territoire et son mariage avec les armes de destruction massive est le scénario le plus redouté.
- La criminalité (conventionnelle) a pour but de s'approprier des biens. Grâce à l'environnement informationnel, on enregistre un fort développement international.
- Le conflit d'anéantissement technologique est rendu possible par la globalisation et les réseaux. L'idéal est d'éliminer l'ennemi et de s'emparer de ses biens sans destructions, uniquement en agissant dans les environnements cybernétiques et électromagnétiques. Les effets et destructions physiques sont des sous-produits, mais les démonstrations récentes montrent qu'il faudra toujours plus s'attendre à des dégâts considérables.
- Le conflit sémantique ou médiatique est favorisé par la circulation de l'information et la multiplication des médias. Il n'y a pas d'effets physiques directs. C'est le domaine de la guerre psychologique qui précède et accompagne toute forme de conflit armé afin de faciliter les autres opérations et d'éviter ou de réduire les conséquences physiques.
- Le cyber-terrorisme est une variation du terrorisme classique. La plupart des experts estiment cependant que les terroristes ont trop besoin d'Internet pour leur propagande et comme instrument de conduite de leurs opérations pour se risquer à le détruire. En revanche, avec le rajeunissement[36] de leurs troupes, formées non plus dans les camps en Afghanistan, mais sur Internet, les terroristes développent leur savoir-faire technologie et il faut s'attendre à ce qu'ils en fassent usage. Si le but psychologique reste au premier plan, alors ces actions viseront des symboles ou des infrastructures particulièrement rentables, parmi lesquelles l'industrie des transports ou de l'énergie.
- La «nouvelle» criminalité peut désormais s'approprier des biens et des valeurs sans passer par la sphère physique. Son but est le gain, mais les caractéristiques de l'environnement informationnel sont telles, que la police et la justice sont souvent impuissants.

> Battles are won by slaughter and maneuver. The greater the general, the more he contributes in maneuver, the less he demands in slaughter.
>
> (Winston Churchill)

On peut réduire ces formes de violence à 3 motivations[37] fondamentales:

- politique: les motifs découlent d'une idéologie, d'une envie de pouvoir, ou du besoin d'obtenir une visibilité et une reconnaissance médiatique;
- profit: s'approprier des valeurs, des biens, des territoires;
- pathologique: lorsque la violence n'est plus ni à but politique ni pour le profit; on entre alors dans le domaine des fanatismes religieux, des idéologies, des croyances et vengeances ainsi que *du chaos pour le chaos;* un acculement (disparition de toute alternative) conduit à ce genre de comportement irrationnel et par nature difficile à maîtriser.

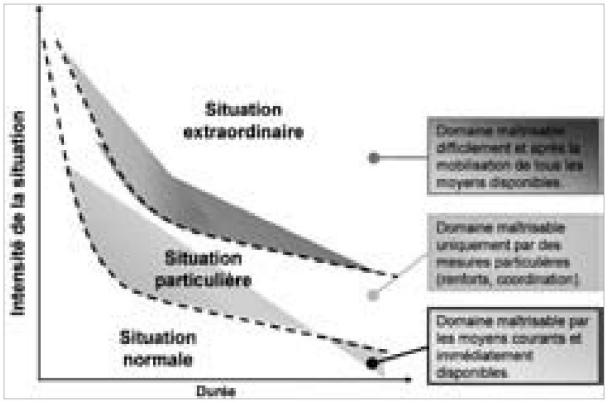
Mais «*Murphy*» aussi doit être considéré car de nombreux risques sont liés à la fragilité intrinsèque de la société. Il suffit de voir la réaction des gens à une simple tempête de neige pour s'en convaincre. Voilà un événement pourtant banal qui devient dans les médias et dans la tête des gens une catastrophe. Il s'agit donc de prendre en compte les soubresauts de notre environnement et les catastrophes qui perturbent notre mode de vie. Les blackouts d'Amérique du Nord et de Scandinavie en 2003, ou en Italie en 2005, sont là pour nous le rappeler. A la liste des conflits mentionnés ci-dessus, il faut ajouter les catastrophes naturelles et les catastrophes d'origine humaine.

**Typologie des attaques dans l'environnement informationnel**
On peut réduire les attaques informationnelles aux trois types suivants

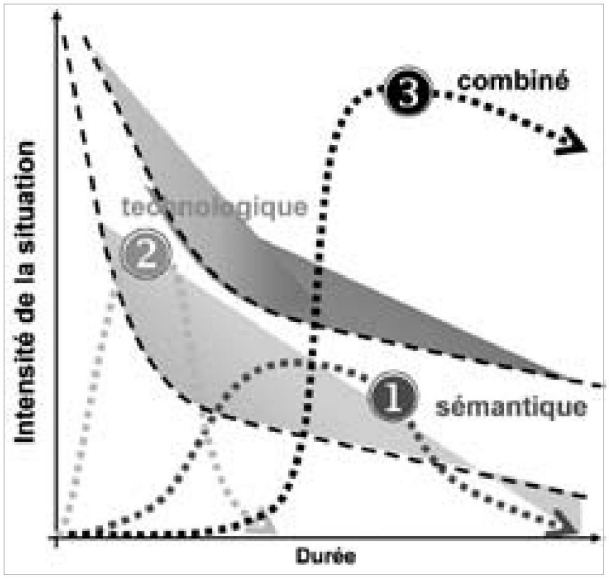
1. sémantique: au sujet des contenus (aspects cognitifs) et/ou des perceptions (aspects psychologiques);
2. technologique: au sujet des processus (aspects décisionnels) et toutes les infrastructures de l'information (aspects fonctionnels);
3. combiné: sémantique et technologique en même temps.

Vu sous l'angle des menaces contre notre Etat, la figure suivante présente une vision d'ensemble des types, buts et acteurs ainsi que de l'importance relative des actions (selon la taille des croix).

- Les motifs politiques concernent un nombre restreint d'acteurs puissants ayant des raisons de nous agresser. Mais il faut aussi considérer les amis susceptibles de nous influencer[38] ou de nous espionner[39], surtout en ces temps critiques le monde est en crise et où ressurgissent les réflexes nationalistes pour trouver des ressources ou quelqu'un à accuser de ses maux. Le terrorisme mentionné ici est «opérationnel» (commandement et réalisation d'actes de terreur).




*[6]*




*[7]*

- Les motifs de profit (criminels) sont le fait d'un grand nombre d'acteurs ayant des motifs matériels. Les risques sont importants du fait de l'industrialisation et de la professionnalisation du secteur. Les effets psychologiques concernent avant tout des objectifs de propagande au profit du terrorisme ou de chantage. La partie du terrorisme mentionnée ici est «fonctionnelle» (pour son financement, donc proche ou confondu avec la criminalité et ses activités de recrutement et de formation en ligne).
- Les motifs pathologiques qui englobent tous les autres acteurs sont un souci stratégique en raison de la masse des 1.5 milliards d'internautes. Si un 1% se comporte mal, cela fait 15 millions d'individus à problèmes. Les exemples de scénarii de réactions de masse sont celui du P3-Orion[40] en avril 2001, du bombardement de l'ambassade chinoise à Belgrade en 1999, ou de l'Estonie en 2007. A ces occasions on a constaté un mouvement plus ou moins spontané[41] d'un grand nombre de personnes parties à l'assaut des USA, de l'Europe et de l'Estonie via Internet.

**Situation normale, particulière, extraordinaire**

Dans le RAPOLSEC 2000, le Conseil fédéral a introduit la notion de situation normale, particulière et extraordinaire. A la lumière de ce qui précède, cette classification reste pertinente, mais quelques corrections sont nécessaires. En effet, on comprend qu'à chaque intensité de crise correspondent des moyens particuliers et que si le passage entre une situation et l'autre est floue, elle est relativement linéaire.

Toutefois, dans l'analyse des menaces informationnelles, le facteur temps représente une rupture de pensée qui induit des modifications des autres facteurs opératifs (force, espace et information). La figure suivante a donc été développée afin d'intégrer cette notion.

Cette représentation suggère, quelle que soit l'intensité de la crise, que la situation devient plus critique au fur et à mesure que la crise se prolonge. Ainsi une crise très intense mais très courte dans ces effets devra être considérée comme une situation normale, réglée uniquement avec les moyens courants. Cette représentation est cohérente avec la modification de la définition classique du risque[42] dont la formule devient …

[34] Michael Wilson (2002). IWAR Threat Model. Decision Support Systems, Inc.
[35] La guerre est comprise en tant que conflit conduit avec des armes (cinétiques).
[36] Exposé de Yael Shahar (Directrice, Database Project Institute for Counter-Terrorism, IDC Herzliya) à la conférence Cyber Warfare, Londres, 2009.
[37] Michael Wilson. Waging Iwar. Decision Support Systems, Inc., 2002.
[38] Nancy Snow. U.S. Public Diplomacy Its History, Problems, and Promise. Garth S. Jowett and Victoria O'Donnell (eds.): Propaganda and Persuasion: New and Classic Essays, 2005, au sujet de l'Office of Global Communications (OGC), dont la première publication en 2003 a été Apparatus of Lies: Saddam's Disinformation and Propaganda 1999–2003 pour obtenir le soutien public international pour une guerre contre l'Iraq sous la conduite des USA.
[39] Cas de ECHELON et de FRENCHECHELON.
[40] Avion de guerre électronique américain forcé à atterrir en Chine après une collision avec un chasseur chinois.
[41] En référence au comportement à chaque foi ambigu des autorités russes et chinoises?
[42] La formule classique est: risque = probabilité d'occurrence x ampleur des dommages.

*[6]* Fig. 6: Subdivision entre situation normale, particulière et extraordinaire sous la pression du facteur temps
*[7]* Fig. 7: Scénarii d'attaque informationnelle contre la Suisse

… risque = probabilité d'occurrence x ampleur des dommages x temps.

**Trois scénarii d'attaques informationnelles contre la Suisse**

Avant de tirer des conclusions applicables uniquement à des situations passées ou présentes, essayons de décrire également la forme des attaques informationnelles auxquelles notre Pays pourrait être confronté. Sur la base de la figure 6, trois scénarii se détachent.

- Le scénario sémantique: un adversaire privé / criminel a pour but de dégrader durablement l'image de la Suisse pour l'écarter de la course économique; à cet effet, il conduit une longue campagne de dénigrement par tous les moyens, y.c. chantages, attaques contre des personnes, attentats; la durée est d'une année et l'intensité moyenne.
- Le scénario technologique: des terroristes infligent des dommages à la Suisse pour la punir de la position de quelques citoyens par rapport à une autre culture ou religion; ils sont aidés par des mafias et de organisations criminelles voulant se venger des bons résultats de notre justice; la Suisse subit un roulement d'attaques technologiques et sémantiques visant à infliger des dommages et dérober des valeurs, en Suisse et à l'étranger; l'Etat, l'économie, la logistique sont particulièrement touchés; la durée est de quelques semaines et l'intensité forte.
- Le scénario combiné: un Etat, dans le cadre d'une guerre généralisée contre l'Europe, veut anéantir la capacité de défense et de résistance de la Suisse pour ne pas gêner ses opérations et pour se saisir des ressources utiles à son effort de guerre; il conduit une attaque combinée (y.c. avec des moyens cinétiques) pour briser moralement et technologiquement la nation; l'opération commence comme une surprise stratégique, concerne tous les pans de la société et dure plusieurs années; les dégâts qui en résultent sont irréversibles et l'intensité de l'action est très forte.

Il n'y a que deux puissances au monde, le sabre et l'esprit, à la longue le sabre est toujours vaincu par l'esprit.

(Napoléon)

## 4 Consequences et solutions pour faire face aux menaces dans l'environnement informationnel

Pour développer une nouvelle politique de sécurité, seule une approche globale *(comprehensive approach)* et comprenant tous les piliers et partenaires est réaliste. Une solution partielle ne conduirait, sur le plan opérationnel (conduite, synchronisation des mesures, etc.) et pratique (investissements, personnel, etc.), qu'à des solutions insulaires, coûteuses et inefficaces. Une telle discussion dépassant largement le cadre de cet article, on se contentera de proposer ci-dessous des éléments utiles aux travaux et réflexions en cours.

**Infrastructures vitales**

Cet élément clé nécessite une approche de *défense en profondeur* partant d'une analyse détaillée des risques. La stratégie requise doit être flexible et continûment adaptable à l'évolution des menaces. Sachant que la maîtrise de l'informatique est une solution sans issue, il s'agit pour la Suisse d'être au moins propriétaire de sa sécurité et d'y investir fortement. Les atteintes électromagnétiques doivent recevoir une attention particulière. La capacité à durer et de résilience est centrale.

**Bases légales**

Sur ce plan notre pays est plutôt bien armé. Des lacunes subsistent notamment pour permettre aux services de sécurité de prévenir les délits. Sur le plan international une coordination est nécessaire. Toutefois, tant que des Etats auront un avantage à ce que l'environnement informationnel serve leurs objectifs politiques et militaires, il ne faut pas attendre d'avance significative ni rapide. La question de la neutralité doit être approfondie.

**Assurer le développement continu de la société**

Même la meilleure réaction ne pourra pas nous protéger de tous les effets. Une attaque stratégique aura, dans les trois scénarii présentés, le potentiel de dégrader fortement et durablement le développement de la Suisse. Des préparatifs (planifications, organisations, réserves, etc.) visant à augmenter notre résilience sont indispensables.

**Communiquer et informer**

«*La première victime d'une guerre c'est la vérité*»[43] et la terreur a besoin des médias (et inversement). Notre capacité à gérer une crise sémantique est donc un facteur critique de succès. Il faut distinguer *informer* (mettre à disposition des contenus informationnels) de *communiquer* (adresser des contenus informationnels). Ces tâches impliquent un effort en diplomatie publique (image de la Suisse dans le monde) et en affaires publiques (images des forces de sécurité en Suisse). Du fait du brassage des populations dans notre société, l'intelligence culturelle doit être fortement augmentée.

**Disponibilité élevée**

Les attaques informationnelles sont caractérisées par leur effet de surprise. La paralysie d'une part importante de notre société peut signifier le débordement rapide des moyens. Si les chaînes logistique et financière sont paralysées, la Suisse aura faim après une semaine et les violences prendront rapidement le dessus. Des attentats ciblés (notamment avec des armes électromagnétiques) et la rumeur pourraient alors considérablement compliquer la situation. Cela implique que nos instruments doivent disposer de la capacité et du savoir-faire pour parvenir, même dans des conditions informationnelles très dégradées, à mobiliser rapidement et à opérer avec efficacité. Une défense psychologique efficace doit en outre être rétablie pour aider à maitriser les effets de la peur et éviter que des messages faux ou défaitistes ajoutent à la panique.

Il faut sortir de cette lutte non seulement victorieux, mais aussi sans reproche.

(Général Dufour, ordre du jour des 4 et 5 novembre 1847)

**Education du citoyen et recherche**

Le plus gros facteur à problèmes est l'humain. Avec la technologie actuelle nous avons mis des *grenades dégoupillées* dans les mains des gens. Mais personne ne leur apprend à les employer. Pourtant, pour acheter une voiture et la conduire, il faut un permis et une assurance. Voilà une énorme lacune de notre société et ce n'est pas la fondation InfoSurance, à l'abandon, qui la comblera. Un effort est aussi nécessaire pour faire renouer les professions des médias avec leur éthique et pour produire des professionnels en suffisance dans les hautes écoles pour gérer la sécurité. Enfin, la recherche fondamentale est nécessaire pour maintenir nos avantages concurrentiels et sécuritaires en identifiant aussi les tendances à temps.

**Conduire la manœuvre**
La Confédération doit conduire l'ensemble des initiatives requises par la menace informationnelle. Il s'agit d'une politique partielle devant être coordonnée avec les autres politiques (information, économie, éducation, infrastructures vitales, affaires étrangères) et entités (canton, secteur privé, partenaires internationaux, etc.). Il s'agit donc de créer des fonctions de haut niveau, à l'échelon stratégique, mais aussi au sein des départements notamment, avec des personnes endossant ces responsabilités. Il doit s'agir de spécialistes de la politique de sécurité et non d'informaticiens, capables de piloter la gestion des risques et de faire adopter à temps les mesures découlant de l'appréciation de la situation. Il s'agit d'établir l'image de l'état du système «Suisse» au profit des organes exécutifs.

**Défense combinée dans la profondeur**
Il s'agit d'élever, partout où cela est possible (techniquement et économiquement), le niveau de base. L'élévation du savoir du public et des professionnels, ainsi que la multiplication de points de protection, doivent réduire notre susceptibilité aux attaques. Une anticipation (donc un renseignement de qualité, aussi dans cet environnement) et une réactivité accrues doivent être atteintes par la mise en place d'une véritable défense, donc une approche dynamique combinant l'anticipation, la prévention, la dissuasion, la protection et l'intervention.

## 5 Conclusion

Comme dit Wilson[44] *«si vous ne voulez pas me croire, c'est votre choix; et je vous souhaite bonne chance; si vous me croyez, alors cessez de perdre du temps et mettez-vous tout de suite à la tâche, car chaque minute de perdue et une opportunité de plus pour les attaquants !»*

La solution parfaite, nous ne l'aurons jamais. Mais aussi longtemps que l'on se chamaillera pour des détails, que l'on tolérera les discussions de chapelle autour d'intérêts particuliers et que l'on restera sans agir, on laissera la porte de notre société ouverte à tous les i-criminels, i-voleurs et i-guerriers.

> Il est plus que temps que nous prenions la mesure de l'importance de l'information et que nous investissions dans la défense de la colonne vertébrale de notre Pays.

Il est plus que temps que tous les intervenants, indépendamment de leur origine et de leur couleur politique comprennent que la défense est une science de pointe et pas une *«orgie entre brutes».*

Si nous cessions d'invoquer Clausewitz comme une excuse pour ne concevoir que la guerre conventionnelle, nous aurions compris depuis longtemps, comme Smith et les chinois, que la masse du feu n'est pas la meilleure manière d'atteindre la victoire. Ne serait-il pas l'heure d'un vrai changement de paradigme face à la guerre?

L'histoire a montré que celui qui n'avait pas sa propre armée sur son territoire devait subir celle d'un autre. Ce dicton s'applique aussi à l'environnement informationnel et il est de notre devoir de concevoir une politique de sécurité où chaque environnement opérationnel est traité conformément à la menace et non en fonction de nos habitudes et de nos organigrammes.

A ceux qui auraient encore des doutes quant à la nécessité d'agir ou qui préfèrent attendre que la menace se matérialise vraiment pour s'assurer qu'elle existe, il suffit de demander simplement: «Êtes-vous prêt à endosser la responsabilité si ça tourne mal ?»

[43] selon la déclaration fait en 1917 le sénateur américain Hiram Johnson.
[44] Michael Wilson. Waging Iwar. Decision Support Systems, Inc., 2002.