# Information Warfare : Chancen eines Kleinstaates

Autor(en): **Keller, Roger**

Objekttyp: **Article**

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

Band (Jahr): **167 (2001)**

Heft 6

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-67332

# Information Warfare – Chancen eines Kleinstaates

**Die Möglichkeit, dass wir Zeitzeugen einer neuen «Revolution in Military Affairs» (RMA) sind, ist nicht von der Hand zu weisen. Die rasante Entwicklung der Informationstechnologie hat längst in den Streitkräften Einzug gehalten und wird zweifellos die Struktur und den Einsatz künftiger Armeen massgeblich beeinflussen. Die Extremversion dieser Revolution stellt eine neue Art der Kriegführung, den sogenannten «Cyber War», ins Zentrum.**

Roger Keller

Nicht Soldaten bekämpfen sich auf dem Schlachtfeld der Zukunft, sondern ausgeklügelte Informationssysteme auf einer Digitalen Kriegsbühne.[1] Diese Art der Kriegführung wird landläufig als «Information Warfare» (IW) bezeichnet. Obwohl der Begriff sehr oft und meist militärisch gebraucht wird, existiert keine allgemeingültige Definition. Es geht in diesem Aufsatz darum, den Begriff Information Warfare mehr strategisch als militärisch zu beleuchten und aus den gewonnenen Erkenntnissen Chancen für einen Kleinstaat abzuleiten.

## Historische Grundlagen

Beschaffung, Interpretation, Kontrolle, Verbreitung und Verleugnung von Information war in der Geschichte schon immer ein Schlüssel zum Erfolg. Sun Tzu's Standardwerk, «The Art of War», ist gespickt mit Hinweisen, welche wir heute unter dem Begriff «Information Warfare» subsumieren würden: «All warfare is based on deception»; Know your enemy and know yourself and in hundred battles you will never be in danger.»[2] Die Lehren Sun Tzu's könnten über Griechen und Römer nach Byzanz geflossen sein. Als Wirtschaftsmetropole war Byzanz eng mit Europa und Asien verknüpft. Durch regen Handels- und Kulturaustausch gelangten die alten strategischen Schriften im 10. Jahrhundert möglicherweise nach Europa, aber auch nach Russland. In Westeuropa beschäftigte sich der italienische Philosoph Niccolo Machiavelli (1469–1527) mit den antiken strategischen Abhandlungen. In seinem Werk «Dell'Arte della Guerra» hat er der Kavallerie folgende Aufgaben zugewiesen: Aufklärung, Beunruhigung des gegnerischen Hinterlandes und Unterbrechung des gegnerischen Nachschubes. Dem Herrscher rät er in seinem Standardwerk «Il Principe», zur fundierten Kenntnis und immerwährenden Analyse der Innen- und Aussenpolitik. Im 19. Jahrhundert vertrat Antoine-Henri Jomini in seinem Buch «Précis de l'art de la guerre» unter anderem die These, dass die Kenntnis über den Gegner als Grundvoraussetzung der Strategie gelte. Ein effizienter Nachrichtendienst bildete die Basis hierzu.[3]

## Informationskrieg im 20. Jahrhundert

Währenddem die Strategie des 20. Jahrhunderts mit Schwergewicht auf Clausewitz' Lehren beruhte, verhalf die Technologie des elektromagnetischen Spektrums der Informationskriegführung zur neuen Blüte. Alle deutschen Panzer waren an der Ostfront mittels Funkgeräten verbunden. Dies gab ihnen eine Gefechtsfeldüberlegenheit, obwohl die sowjetischen Panzer zahlenmässig und technologisch überlegen waren, jedoch nur über Funkgeräte auf Kommandantenstufe verfügten. Es sei an dieser Stelle vermerkt, dass Guderian seine Karriere als Übermittlungsoffizier begann.[4] Es scheint, als haben die Alliierten es sehr gut verstanden, Information Warfare als Waffe gegen die Achsenmächte einzusetzen. Vor allem in der Täuschung waren sie wahre Meister. Sie bauten Geisterarmeen in Westengland auf und setzten Puppen als Fallschirmtruppen ein, um die Deutschen zu überzeugen, dass sie am Pas de Calais ihre Invasion durchführen würden und nicht in der Normandie. Die Entschlüsselung des ENIGMA Codes durch die Briten und die anschliessende Vertuschung dieser Tatsache trug massgeblich zum alliierten Sieg bei und stellt im Wesen nichts anderes als eine erfolgreiche Aktion im Rahmen von Information Warfare dar.

Am Ende des Zweiten Weltkrieges war die Informationskriegführung auf taktischer, operativer und militärstrategischer Ebene angesiedelt. Es ist interessant, dass zu dieser Zeit die Ebene der «Grand Strategy» durch Information Warfare unberührt geblieben war. Dies änderte sich gegen Ende des 20. Jahrhunderts durch die rasanten Entwicklungen in der Informationstechnologie, welche zur sogenannten Globalisierung führte. Information oder Falschinformation kann heute als Waffe eingesetzt werden, welche in der Lage ist, ganze Organisationen oder Nationen zu lähmen. Die folgenden Beispiele sollen nicht als Recht oder Unrecht beurteilt werden, sondern lediglich aufzeigen, dass Information und vor allem gezielte Informationskriegführung auf der Ebene der «Grand Strategy» anzusiedeln ist. Die Schweiz wurde beispielsweise durch gezielte Informationsverbreitung über die Tätigkeit der Schweizer Banken während des Zweiten Weltkrieges massiv unter Druck gesetzt. Nebst einer Gefährdung des Handelsplatzes Schweiz sind Politiker, Diplomaten und Untersuchungskommissionen seit Jahren beschäftigt, und die Kosten sind nicht abzusehen. Der Fall Lewinski zeigte auf, dass sogar ein US-Präsident aufgrund von Informationen, welche gezielt verbreitet und gegen ihn verwendet wurden, an den Rand der Handlungsunfähigkeit gebracht werden kann. Das Bewusstsein, dass Information allgegenwärtig ist und jederzeit gegen einem verwendet werden kann, hat sich in den Köpfen vieler Politiker eingenistet. Es geht in der heutigen «Grand Strategy» meistens nicht mehr darum, einen strategischen Sieg zu erringen, sondern vielmehr darum, das politische Überleben zu sichern. Der NATO-Luftschlag gegen Jugoslawien zeigte diese Ohnmacht zweifelsfrei auf. Regierungschefs einiger NATO-Staaten kümmerten sich persönlich um die taktische Zielplanung und vernachlässigten die strategische Führung. Auf der anderen Seite verstand es der serbische Führer Milosevic hervorragend, Information als Waffe gegen das Bündnis einzusetzen. Diese Beispiele zeigen, dass Information jederzeit und gegen jeden eingesetzt werden kann. Der Schutz vor und die Führung von Information Warfare muss deshalb auf höchster Stufe (Landesregierung) angesiedelt werden.

## Was ist Information Warfare?

Ein US-Marineoffizier beschreibt IW als einen Konflikt, bei welchem Information die Ressource, das Ziel und die Waffe zur gleichen Zeit sei. Diese Definition limitiert IW auf den Bereich des Cyber War's, was nicht als richtig angesehen werden darf, da die Zerstörung einer wichtigen Informationsressource durchaus auch konventionell erfolgen kann. Der bereits zitierte Journalist James Adams definiert IW umfassender und vernetzter:

*«Information warfare therefore seems to break down into three distinct pieces: perception management where information is the message, systems destruction, where information is the medium, and information exploitation, where information is an opponent's resource to be targeted.»*[5]

Der US Joint Staff unterscheidet Information, Informationssysteme sowie die Netzwerke, welche beide verbindet. Die Definition sieht ein weites Spektrum von Massnahmen vor, die vom einfachen Einschleusen eines Virus bis zur Zerstörung ganzer Kommunikationszentren reichen. IW wird definiert als

*«action taken to achieve information superiority in support of national security by affecting adversary information, information systems and*

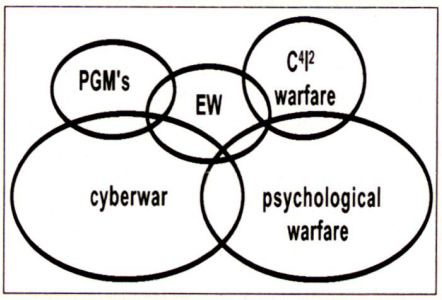
*computer-based networks while leveraging and protecting our information, information systems and computer-based networks.»*[6]

Interessant ist auch, dass die Amerikaner IW einen sehr hohen Stellenwert beimessen und auch den Schutz ihrer eigenen Systeme miteinbeziehen. Unter Präsident Clinton wurde die National Security Agency beauftragt, eine information warfare unit zu bilden und rund 1000 Spezialisten zu rekrutieren. Die Russen bekunden ebenfalls Mühe mit dem Begriff IW, unterschätzen aber keineswegs sein enormes Potenzial:

*«the possible catastrophic consequences of the use of strategic information warfare means by an enemy, whether on economic or state command and control systems or on the combat potential of armed forces… Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself.»*[7]

George Stein von der University of Pennsylvania sieht IW in einem völlig anderen Bereich angesiedelt. Für ihn hat IW damit zu tun, wie ein Mensch denkt oder Entscheidungen fällt. IW wird als Synonym für Beeinflussung und Manipulation des Gegners angesehen und ist somit im Bereich des «psychological warfare's» PSYOPS angesiedelt.

Betrachtet man die diversen Definitionen, scheint es, als ob IW einerseits den Gebrauch von Informationen um gegnerische Informationen, Informationssysteme oder Netzwerke zu zerstören, zu verändern oder zu gebrauchen, aber auch den Bereich des direkten Angriffes auf die Entscheidfindung des gegnerischen Führers und der Bevölkerung vereint. Christopher Bellamy entwickelte den Begriff «PSYBERWAR», um auf diese spezielle Tatsache hinzuweisen. Sein Modell (Grafik 1) geht von der These aus, dass IW eine Mischung aus Cyberwar und psychologischer Kriegführung ist und deshalb als Teilmenge der RMA angesehen werden kann. Es tangiert die Bereiche der elektronischen Kriegführung sowie der Kriegführung gegen $C^4I^2$-Einrichtungen mittels Präzisionswaffen.




**Grafik 1: Information Warfare = PSYBERWAR.**

| | |
|---|---|
| Strategische Ebene | Verstand, Geist, Moral (Commanders Mind) |
| Operative Ebene | Informationssysteme |
| Taktische Ebene | Physischer Kampf |

**Grafik 2: die 3 Ebenen.**

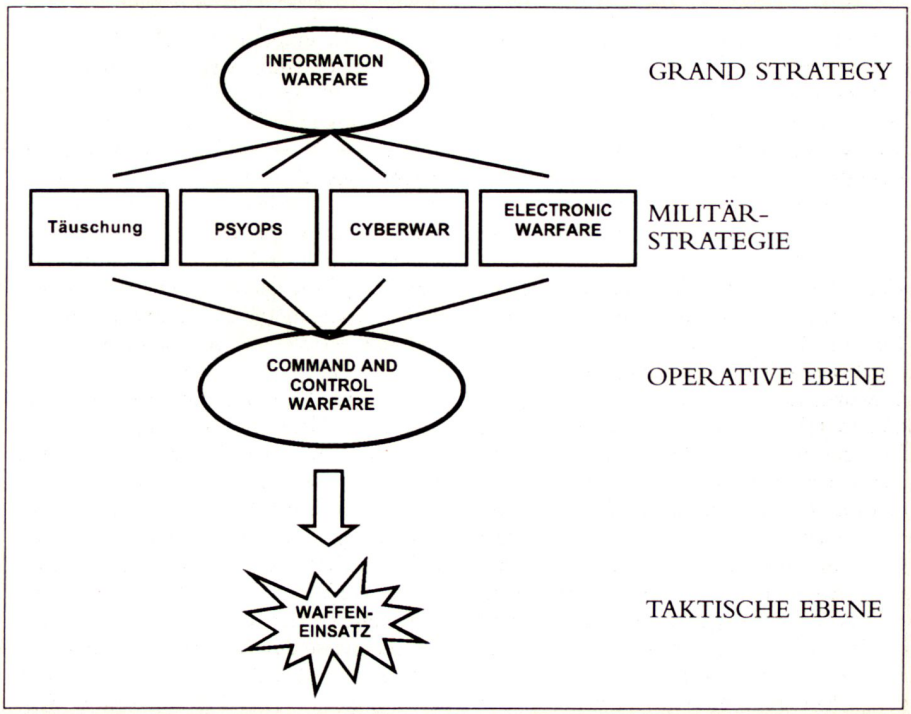
## Die drei Ebenen des Informationskrieges

Im Verlaufe unserer Geschichte war es immer schon ein primäres Ziel der Kriegführung, die gegnerische Führung zu verwirren, zu täuschen oder direkt anzugreifen. Dies hat sich bis heute nicht geändert. Einziger Unterschied ist die Anwesenheit von Informationssystemen. Historisch gesehen gab es zwei Stufen – strategisch und taktisch. Verbände wurden strategisch zur Schlacht geführt und kämpften taktisch. Während des Zweiten Weltkriegs wurden deutsche Städte bombardiert mit dem Ziel, den Willen der Bevölkerung und der kämpfenden Truppe zu brechen. Die Angriffe auf die Moral können als strategisch, jene der physischen Kampfeinsätze als taktisch bezeichnet werden. Zwischen diesen zwei Ebenen ist entsprechend der Entwicklung der Strategie die operative Ebene der Informationssysteme einzuführen (Grafik 2).

Informationssysteme bieten die Möglichkeit, Aktionen auf beiden Levels gleichzeitig vorzunehmen. Ein Lahmlegen der Computersysteme unseres Banksystems, der Telekommunikation sowie der Stromversorgung würde zwar unmittelbar niemanden töten, könnte aber unsere Nation genauso lähmen wie ein Angriff mit einer taktischen Nuklearwaffe. Historisch gesehen wurden neue Waffensysteme immer zuerst strategisch eingesetzt und erst später als taktische Waffe des Gefechtsfelds. Vor diesem Hintergrund scheint es, dass IW eine strategische Waffe ist. IW wird jedoch meist im Zusammenhang mit dem Erreichen operativer militärischer Ziele verwendet. Der Autor ist der Meinung, dass IW vor allem auf strategischer Ebene anzusiedeln ist und nicht den Taktikern auf dem Gefechtsfeld überlassen werden darf. Es ist Aufgabe des Staates, diese Waffe für den Angriff und die Verteidigung nationaler und supranationaler Infrastruktur einzusetzen. Der Schutz von bzw. der Angriff auf militärische Informationssysteme wird im englischen Sprachgebrauch als command and control warfare bezeichnet und ist nur ein Element von IW (Grafik 3).

## Chancen für einen Kleinstaat?

Einleitend wurde die These aufgestellt, dass gezielte Informationen oder Fehlinformationen sowie Attacken auf die Informationsinfrastruktur einem Land beträchtlichen Schaden zufügen können. Für einen Kleinstaat wie die Schweiz haben




**Grafik 3: IW als strategische Waffe.**

Schutzmassnahmen gegenüber diesen Gefahren eine absolute Priorität. Eine zentrale Rolle hat für den Kleinstaat der strategische Nachrichtendienst. Seine Aufgabe ist es, Informationsattacken, Irreführung und Täuschung frühzeitig zu erkennen und der politischen Führung geeignete Gegenmassnahmen vorzuschlagen. Ferner muss er aktive Informationsbeschaffung über Schwächen möglicher Kontrahenten betreiben. Die Zusammenarbeit mit der Wirtschaft in diesem Bereich ist von zentraler Bedeutung und dient der Festigung der Wirtschaft des Kleinstaates.

Zum Schutze der Informationsinfrastruktur sollte der Kleinstaat seine technische Überlegenheit benutzen und eine Zusammenarbeit mit Hochschulen, Forschungsanstalten und der Wirtschaft anstreben. Die Forschungen auf diesem Gebiet dürfen nicht nur Verteidigungscharakter haben, sondern müssen auch eine offensive Komponente beinhalten. Die technische Unterstützung der Informationsbeschaffung und die Vorbereitung von Informationsattacken gegen mögliche Kontrahenten sind permanente Aufgaben. Es können dazu auch Mittel der Wirtschaft, aber auch des Verteidigungsbudgets eingesetzt werden.

## Beurteilung

IW beinhaltet nebst technischer Möglichkeiten auch eine starke psychologische Komponente. Es reicht heute nicht mehr, die militärischen Mittel gegen Informationsattacken zu schützen, da die Angriffe auf der strategischen Ebene beginnen. Durch Irreführung, Täuschung und gezielte Falschinformation kann ein Land wirtschaftlich unter Druck gesetzt und ohne den Einsatz militärischer Mittel politisch seiner Handlungsfähigkeit beraubt werden. Ein Kleinstaat wie die Schweiz hat aufgrund des hohen Technologiestandes und der fundierten Ausbildung seiner Bevölkerung gute Möglichkeiten, im Gebiete von IW eine aktive Rolle zu spielen. Die kommenden Entwicklungen im Bereich der Informationstechnologie werden die Risiken und Auswirkungen von IW noch mehr verstärken.


[1] James Adams: *The Next World War, The Warriors and Weapons of the new Battlefields in Cyberspace,* Arrow Books Ltd, London, 1998.

[2] J. H. Huang: *Sun Tzu, The Art of War, the new translation,* Quill, New York, 1993.

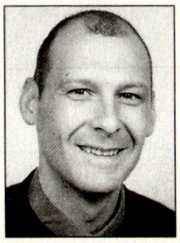
[3] Albert A. Stahel: *Klassiker der Strategie – eine Bewertung,* Strategische Studien Band 6, vdf, Zürich, 1995.

[4] John Arquilla and David Ronfeldt: *«Cyberwar is coming!»* International Policy Department, RAND Corporation, Santa Monica, 1993.

[5] James Adams: *The Next World War.*

[6] Cdr William Rohde, USN: *What is Info Warfare,* US Naval Institute Proceedings 122, No 2, USA, 1996.

[7] Timothy Thomas: *Deterring Information warfare: a new strategic challenge,* Parameters, Vol 26, No 4, Winter 1996–97. ■

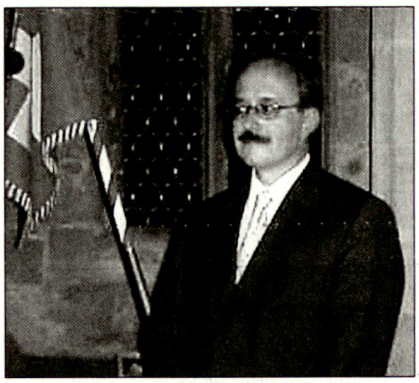

**Roger Keller, Berufsoffizier LW, Major i Gst, CFO, F Div 6, 5737 Menziken.**


# Bundesrat Samuel Schmid wirbt auf der Lenzburg für die Militärvorlagen vom 10. Juni 2001

Der laue Frühlingsabend vom 3. Mai und das ganz spezielle Ambiente des Schlosses Lenzburg boten einen würdigen Rahmen für den ersten offiziellen Auftritt von Bundesrat Schmid im Aargau. Der Einladung der Aargauischen Offiziersgesellschaft in den Rittersaal auf Schloss Lenzburg folgten gegen 400 Personen.

In seinem Referat verteidigte der Chef VBS die Militärvorlagen vom 10. Juni dieses Jahres engagiert und durchaus volksnah. In der nachfolgenden Diskussion, in welcher auch kritische Stimmen laut wurden, blieb Schmid zuversichtlich und hatte die grosse Mehrheit der Besucher klar auf seiner Seite.

Im Falle einer Ablehnung der Teilrevision des Militärgesetzes könne das Projekt für die Armee XXI rein organisatorisch durchaus weitergeführt werden, jedoch hätte die Ablehnung der beiden Initiativen in Bezug auf die Qualität und die Glaubwürdigkeit unserer Soldaten eine grosse Auswirkung, weil unsere Ausbildungsmöglichkeiten weit weniger optimal sein würden, so Schmid.



Ausserdem, erklärte der Bundesrat, hätte ein «2x NEIN» auch einen Einfluss auf die Glaubwürdigkeit unserer wichtigen humanitären Tradition. Was seit Jahrzehnten aufgebaut worden sei, wäre künftig nur sehr eingeschränkt, mittel- oder längerfristig vielleicht überhaupt nicht mehr möglich. Dies aber wäre unserem internationalen Ansehen und Respekt sowie unserer Neutralität sicher nicht förderlich.

Text und Foto: Maya Frey

# Armee XXI – Kantone wollen mitreden

Innere und äussere Sicherheit seien untrennbar miteinander verbunden, stellte die St. Galler Justiz- und Polizeidirektorin, Regierungsrätin Karin Keller-Sutter, in ihrem Referat an der Generalversammlung der Offiziersgesellschaft des Kantons St. Gallen fest. Berührungspunkte zur Armee machte sie beim Grossprojekt USIS (Überprüfung des Systems der inneren Sicherheit der Schweiz) aus. Kantonale Hoheiten seien zu achten und die Armee nur dann beizuziehen, wenn die zivilen Kräften nicht ausreichen würden. Vor diesem Hintergrund zeigte sich die Referentin rund um die Bestimmungen von «Schengen» und «Dublin» besorgt über die kantonale Polizeihoheit. Nationalrat Peter Weigelt stellte den Stand der Armee XXI aus politischer Sicht fest. Der Kommandant der Felddivision 7, Divisionär Peter Stutz, zeigte den militärischen Blickwinkel im Umbau der Armee. Trotz verschiedenen Auffassungen und Konflikten sei das Projekt Armee XXI insgesamt positiv zu werten. An der Generalversammlung waren auch Wahlgeschäfte traktandiert. Oberstleutnant Jürg Gygax löste Hans Bütikofer als Präsident der kantonalen Offiziersgesellschaft ab. (dk)