Krieg im Informationszeitalter : was ist neu?

Autor(en): **Müller, Niklaus**

Objekttyp: **Article**

Zeitschrift: **Schweizer Soldat + MFD : unabhängige Monatszeitschrift für Armee und Kader mit MFD-Zeitung**

Band (Jahr): **71 (1996)**

Heft 11

PDF erstellt am: **19.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-716478

Krieg im Informationszeitalter: Was ist neu?

Von Oberst Niklaus Müller, Muri

Der Autor hat in der März-Nummer des «Schweizer Soldat» die Force XXI vorgestellt, die erste Truppe des Informationszeitalters. Nun befasst er sich grundsätzlich mit den neuen Möglichkeiten der Kriegführung im Informationszeitalter. Er will aber damit nicht sagen, in Zukunft werde nur noch mit dem Computer Krieg geführt: die verschneite, glitschige Strasse über den Mount Igman in Bosnien beispielsweise hat deutlich gemacht, dass die ganze Realität noch lange nicht im Informationssystem gespeichert sein wird.

Einleitung

Seit dem Golfkrieg 1991 ist der Faktor Information endgültig zur operativen Bestimmungsgrösse avanciert und hat den «schöpferischen Akt der instinktiven Eingebung des Feldherrn» zunehmend transparenter gemacht. Klagen über die «vermeintliche» Einschränkung der Handlungsfreiheit des militärischen Führers spiegeln nicht zuletzt die Angst vor dem Tag wider, an dem mehr Soldaten Computer als Waffen bedienen werden.

1993 erschien das Buch «War and Anti-War» von Alvin und Heidi Toffler. Es zeigte auf, dass das Industriezeitalter auch im Bereich des Militärs Vergangenheit ist und dass angesichts der Personalreduktionen und der immer knapperen Mittel nur der Schritt ins Informationszeitalter die Armeen davor bewahren kann, in die Bedeutungs- und Wirkungslosigkeit abzusinken.

In bezug auf die Bedeutung und Verwendung von Informationen unterteilen die Tofflers die Geschichte der Menschheit in die nachstehend dargestellten drei grossen Zeitalter.

Was ist Information Warfare?

Die wahrscheinlich am weitesten verbreitete und akzeptierte Definition ist diejenige der US Army: *«Actions taken to achieve information superiority by affecting adversary information, information based processes, and information systems, while defending one's own information, information based processes, and information systems.»* Sie bedeutet, frei übersetzt, Handlungen, welche die Überlegenheit im Bereich der Information wie folgt sicherstellen sollen; einerseits Beeinträchtigung der Information, der auf Information basierenden Tätigkeiten und der Informationssysteme des Gegners und andererseits Verteidigung der eigenen Information, auf Information basierenden Tätigkeiten und Informationssysteme. Diese Definition deckt nur den militärischen Teil ab.

Es gibt Autoren, die auch den Einsatz von – wahren oder falschen – Informationen gegen Einzelpersonen, Firmen und Verbände als Informationskrieg bezeichnen. Andere betrachten den Informationskrieg erst dann als gegeben, wenn man durch die Zerstörung kriegs- oder lebenswichtiger Informationen den Gegner handlungsunfähig machen kann und gar keine Massenvernichtungswaffen des Industriezeitalters mehr einsetzen muss. Die Technologie des Informationskrieges würden in diesem Fall die bisherigen Waffen nicht wirkungsvoller machen, sondern ersetzen. Autoren, die diese Ansicht vertreten, betrachten die Einsätze im Golfkrieg gegen Kommandoposten und Kommunikationsnetze und auch die Verwendung der Information durch die geplante Force XXI nicht als erste Beispiele von Informationskriegen, sondern als Kampfwertsteigerung von Waffen und Geräten des Industriezeitalters durch Aufpfropfung von Mitteln der Informationstechnologie.

Streitkräfteplanungsentscheide von heute oder morgen entfalten ihre volle Tragweite mit Schwergewicht in 15 oder 20 Jahren. Die nachfolgenden Ausführungen befassen sich deshalb mit denjenigen Chancen und Gefahren, welche die Leser des «Schweizer Soldat» während der Zeit ihrer Einteilung in der Armee erleben werden, das heisst vor allem mit Mitteln des Informationskrieges, welche die Wirksamkeit von Waffen und Geräten des Industriezeitalters erhöhen beziehungsweise die Wirkung der gegnerischen Waffen und Geräte reduzieren sollen.

Übersicht über die drei Zeitalter

Zeitalter	1	2	3
Art des Zeitalters	landwirtschaftlich, vorindustriell	industriell	informationsbasierend
Physische Sicherheit	Kriegerkaste, Söldner, Volksheer	professionelle Soldaten	informationsbewusste Führer
Dominierende soziale, politische, wirtschaftliche Kräfte	Familie, Stamm, Stadt, Staat	Nationalstaat, Fabrik	multinationale Firmen
Wirtschaft charakterisiert durch	Handel	Geld	Symbole (z.B. in Datenbanken)
Krieg charakterisiert durch	repräsentative Kämpfe	Massenheere, grosse Verluste	Informationsangriffe, minimale Verluste
Stärkste zerstörerische Kraft	Schiesspulver	weltweite gegenseitige Zerstörung (AC-Waf)	Zerstörung essentieller Informationen
Führung	hierarchisch	viele Hierarchiestufen, starke Arbeitsteilung	flache Strukturen, Kompetenz auf unteren Stufen
Krieg basierend auf Informationen	ja	ja	ja
Informationstechnologie im Kriegseinsatz	nein	ja	ja
Informationskrieg	nein	nein	ja

Einsatzformen des Informationskriegs

Die sehr lesenswerte Schrift «What is information Warfare», herausgegeben von der US amerikanischen National Defense University, unterscheidet die folgenden Einsatzformen des Informationskriegs:

Führungskrieg

Im militärischen Bereich ist der Führungskrieg die wichtigste Komponente des Informationskrieges. Er soll bewirken, dass die feindlichen Kommandanten nicht wissen, wo ihre Truppen sind, und die Truppen nicht, welches ihre Aufträge sind, und gleichzeitig sicherstellen, dass die eigenen Kommandanten und Truppen wie beabsichtigt kommunizieren können.

Nachrichtenkrieg

Die Tätigkeit der Nachrichtendienste ist die traditionelle Komponente des Informationskriegs; es ist jedoch notwendig, ihre Einsatzgrundsätze dem breiteren Spektrum des heutigen Informationskrieges anzupassen, Sensoren systematisch einzusetzen und die Erkenntnisse der Aufklärung nicht nur dem Führungssystem, sondern auch – und möglichst verzugslos – den eigenen Feuerleitsystemen zur Verfügung zu stellen.

Elektronische Kriegführung

Die elektronische Kriegführung hatte bis jetzt die Aufgabe, das elektromagnetische Spektrum abzudecken und zu beherrschen; in Zukunft muss sie auch die Informationssysteme und die auf Information basierenden Prozesse schützen.

Psychologische Kriegführung

Psychologische Kriegsführung bedeutet Kampf um Gedanken und Gefühle. Im Rahmen des Informationskrieges geht es darum, dass sie die neuen technischen Möglichkeiten ausnützt und so ihre Wirkung verstärkt. So haben beispielsweise die Amerikaner vor dem Einsatz in Haiti detaillierte Marktfor-

schung betrieben, die Propaganda auf über 20 spezifische Bevölkerungsgruppen zugeschnitten und dann mit verschiedenen Technologien jede Gruppe mit der für sie vorgesehenen Propagandabotschaft bearbeitet.

Hacker-Krieg

Der Hacker-Krieg umfasst Angriffe auf Informationssysteme mit Hilfe von Computerprogrammen. Er ist typischerweise ein nicht militärischer Teil des Informationskrieges; er nützt die modernsten Technologien aus und erzielt, weil er noch so exotisch ist, die grössten Schlagzeilen in den Medien.

Wirtschaftlicher Informationskrieg

Der wirtschaftliche Informationskrieg umfasst die Möglichkeiten der Kriegsparteien, gegenseitig ihre Volkswirtschaften zu beeinflussen. So könnte zum Beispiel Japan den japanischen Firmen befehlen, all ihr Geld unverzüglich aus den amerikanischen Märkten abzuziehen; der Geldabfluss würde dank den modernen technischen Möglichkeiten so rasch vor sich gehen, dass die amerikanische Wirtschaft gelähmt wäre, bevor die Behörden der USA eine Chance hätten zu reagieren.

Cyberwar (Netzwerkkrieg u a)

Cyberwar ist der «Science-fiction»-Teil des Informationskriegs und umfasst diejenigen Aktivitäten, die sich vorläufig in keiner der anderen, klar definierten Gruppen von Tätigkeiten einordnen lassen.

Diese sieben Einsatzformen decken ganz verschiedene Aktivitäten ab, und nur drei sind, vor allem für einen offensiven Einsatz, schon klar genug definiert Es sind dies:

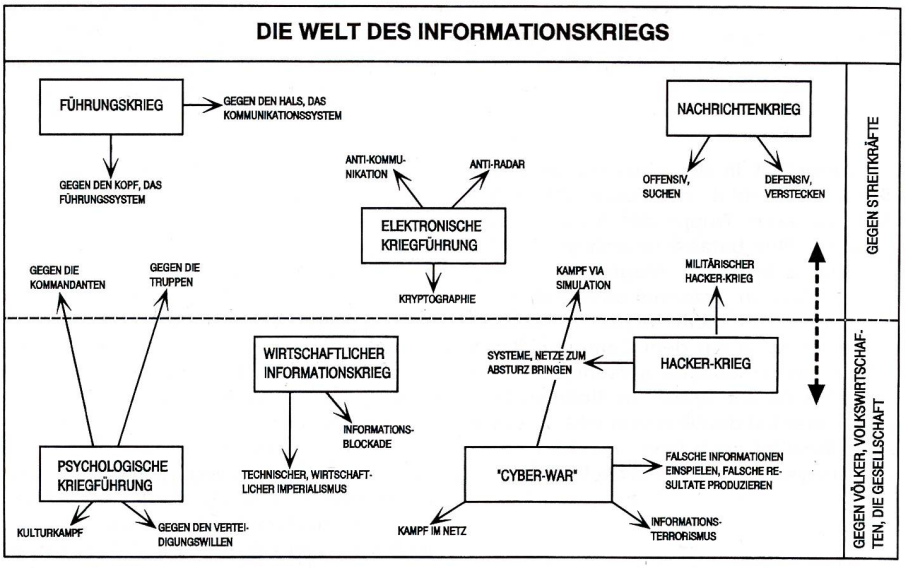
- der Führungskrieg und die elektronische Kriegführung mit dem Ziel der Zerstörung der gegnerischen Führungssysteme.
- der Nachrichtenkrieg, verstärkt durch Nachrichteninformationssysteme und
- die psychologische Kriegführung mit dem Ziel, die Beurteilung der Wirklichkeit durch den Gegner und die Einstellung der gegnerischen Bevölkerung zu beeinflussen.

Einsatzgrundsätze des Informationskrieges

Die Einsatzgrundsätze des Informationskrieges können wohl allgemein formuliert, müssen aber dann durch jede Armee ihrer spezifischen Bedrohungslage angepasst werden. Die nachstehenden acht Forderungen, gruppiert in vier Kategorien, könnten eine Diskussionsgrundlage dazu bilden.

1. Kategorie: **Verhinderung**

- Enthauptung bedeutet, dass – bildlich gesprochen – der Kopf und der Hals des Gegners (das heisst das Führungssystem und das Übermittlungssystem) vom Körper (das heisst der Truppe) getrennt werden:
  Führungssysteme, Computerprogramme zur Unterstützung der Entscheidfindung und Übermittlungssysteme sind die wichtigsten Ziele des Informationskriegs;
  Priorität der Sensoren sagt aus, dass alle gegnerischen Sensoren unterdrückt oder zerstört sein sollten, bevor man mit einem Angriff beginnt.



2. Kategorie: **Kampfkraftsteigerung**

- Das Prinzip des Wissens sagt aus, dass alle am Kampf Beteiligten über alle Informationen verfügen müssen, die sie für ihren Einsatz brauchen, und dass es auch keine Engpässe im Übermittlungssystem geben darf.
  Die Forderung nach zeitgerechter Information ist abgeleitet aus der Tatsache, dass im modernen Krieg Informationen ihren Wert in Sekunden oder Minuten, nicht mehr in Stunden oder Tagen verlieren können.

3. Kategorie: **Überlebensfähigkeit des Systems zur Lageerfassung und des Führungsinformationssystems**

- Überlebensfähigkeit postuliert, dass die strategischen Entscheide zentral gefällt werden, dass aber die Durchsetzung der geplanten Massnahmen dezentral geplant und ausgeführt wird; dies soll es dem Gegner so schwierig wie möglich machen, die Stäbe, welche Einsätze planen, und die Kommandanten, die diese Einsätze leiten, anzugreifen. Das Prinzip der Interoperabilität verlangt, dass die Datenkommunikationssysteme und die Systeme zur Verarbeitung und Speicherung dieser Daten so ausgelegt sein müssen, dass ein maximaler Informationsaustausch auf kürzestem Weg möglich ist. Der Kommandant eines Spitzenverbandes am Boden muss direkt mit dem über ihm fliegenden Piloten eines Erdkampfflugzeugs verkehren können, nicht auf Umwegen über die Computer der Luftwaffe und der Armee. Diese Forderung zielt darauf ab, dass eine ganz wesentliche Schwäche der beispielsweise im Golf eingesetzten Systeme eliminiert wird.

4. Kategorie: **Ebenen**

- Das Prinzip der Hierarchie der Mittel verlangt, dass alle, auch die modernsten verfügbaren Mittel eingesetzt werden, auch wenn man der Ansicht ist, der Gegner besitze nur Waffen des Industriezeitalters. Die Unterschätzung des Gegners und seiner Ressourcen kann katastrophale Folgen haben.
  Der Grundsatz der Intensität verlangt, dass Einsätze des Informationskrieges auf der untersten Stufe, die über die notwendigen Mittel verfügt, entschieden und dann mit allen verfügbaren Mitteln geführt werden.
  Es darf nicht sein, dass man auf das grüne Licht einer hohen Stelle warten muss, bevor man den lokalen Informationskrieg eskalieren kann. Der Entscheid einer solchen unbeteiligten Stelle und die Informationswege zu ihr und zurück zum lokalen Kommandanten stellen unnötige Engpässe dar.

Im Bereich des reinen Informationskriegs (ohne Blutvergiessen?) geht es vor allem um Diebstahl, Modifikation oder Zerstörung von Information oder um die Zerstörung der Informationsinfrastruktur, das heisst der Informationssysteme; und die als Computerviren bekannten Programme können verursachen, dass ein Computer Informationen verliert, Informationen oder Programme falsch verarbeitet, dass er fehlerhaft oder gar nicht mehr funktioniert.

Einschränkungen, grundsätzliche Risiken

Der grundsätzliche Widerspruch im Bereich des Informationskriegs besteht darin, dass die hochentwickelten Nationen, die ihn am besten führen können, gleichzeitig auch am verwundbarsten sind. Wirtschaft, Verwaltung und Militär verwenden die modernen Mittel der elektronischen Kommunikation und des computergestützten Informationsaustauschs. Ein Angreifer kann die wichtigsten Knoten und Verbindungen mit vergleichsweise geringem Einsatz von Mitteln sabotieren.
Die Gründe für diese Verwundbarkeit sind vielfältig: moderne Geräte sind auf der ganzen Welt (für Freund und Feind) erhältlich, und die Angreifer können dank raffinierter Software in die Systeme eindringen.
Die Abwehr solcher Angriffe ist u a deshalb schwierig, weil viele Chefs die Gefahren des Informationskriegs noch nicht erkannt haben, weil die Informatikabteilungen zu wenig personelle und materielle Mittel gegen die Sicherheitsrisiken einsetzen und weil es nicht möglich ist, ein System absolut sicher zu machen.
Die Waffen des Informationszeitalters in den Händen moderner Staaten sind aber wirkungslos gegen Partisanen und vorindustrielle Heere; und sie haben nur eine beschränkte Wirkung gegen Armeen des Industriezeitalters.
Es ist deshalb durchaus möglich, dass sich in

näherer Zukunft eher Terroristen als reguläre Armeen solcher Waffen bedienen. Anstatt zum Beispiel eine Bombe in einem Flugzeug zu verstecken, könnte man mit viel weniger persönlichen Risiken alle Verbindungen des Kontrollturms eines Flughafens lahmlegen und so Unfälle verursachen.

Zur Strategie des weiteren Vorgehens

Das Informationszeitalter und der Informationskrieg konfrontieren uns mit neuen Risiken. Es geht darum, diese Risiken in eine ganzheitliche, vorausschauende Lageanalyse und Frühwarnung einzubeziehen und allenfalls zusätzliche sicherheitspolitische Zielsetzungen und neue Mittel zur Erreichung dieser sicherheitspolitischen Zielsetzungen zu formulieren. Die Tatsache, dass auch Terroristen die Söldner des Informationskriegs anheuern und sie gegen unseren Staat und unsere Wirtschaft einsetzen könnten, zeigt, dass nicht nur EDA und EMD, sondern auch die anderen Departemente der Bundesverwaltung sich mit dieser Aufgabe befassen müssen.
Der Informationskrieg kann nicht improvisiert werden. Es geht darum, rechtzeitig klare Ziele zu setzen und die notwendigen Massnahmen aufzuzeigen und anschliessend die neu erarbeitete oder ergänzte sicherheitspolitische Strategie mit aller Konsequenz in die Tat umzusetzen.

Schlussbetrachtungen

Im Interesse der aktiven, ausgreifenden Verteidigung ist es notwendig, dass man die Informationsarchitektur der potentiellen Gegner kennt, zum Beispiel, wie werden ihre Entscheide durch Nachrichten und Informationsmedien beeinflusst, wie ist ihre Kommandostruktur, ihre Kommunikationsinfrastruktur usw. bis hin zu den Details ihrer Informationssysteme und der Software, die darauf installiert ist.
Am erfolgreichsten ist man im Informationskrieg dann, wenn ein Konflikt gar nicht erst ausbricht, weil der eigene Informationsschutz oder die Informationsdominanz so stark ist, dass man gar nicht angegriffen wird.
Die nationale Kommunikationsinfrastruktur muss sicher und zuverlässig funktionieren und gegen Angriffe von innen und aussen geschützt sein.
Selbstverständlich muss auch der gesetzliche Rahmen für die vorgesehenen Massnahmen des Informationskrieges rechtzeitig vorhanden sein.
Damit sich ein Land im Informationskrieg erfolgreich verteidigen kann, muss auf allen Stufen und bei allen potentiellen Opfern eines solches Krieges das Bewusstsein für diese Kriegsform vorhanden sein. Der Nutzen einer öffentlichen Diskussion über dieses Thema ist gross; und die Gefahr, dass Hacker, Terroristen und mögliche gegnerische Staaten etwas über unsere offene Gesellschaft lernen, was sie nicht schon wissen, sehr klein.