Ute Bernhardt

Das Imperium schlägt zurück

Information Warfare beschäftigt sich mit der Störung und Zerstörung von informationstechnischen (IT-) Systemen in Konfliktfällen. Ziel ist es, Schäden in zivilen und militärischen Systemen zu erzeugen, um damit eigene militärische oder politische Zwecke zu erreichen. Diese Sicht auf Risiken ist nicht neu. Schon vor Jahren wurde diskutiert, daß die Nutzung von IT-Systemen als Grundlage immer größerer Teile unseres Wirtschafts- und Gesellschaftssystems eine neue Qualität der gesellschaftlichen Verletzlichkeit herstellt.

> Diese neue Qualität führt den Gedanken an eine konventionelle Kriegsführung ad absurdum: Störende Einwirkungen auf IuK- Techniksysteme sind im Kriegsfall nicht auszuschließen, eher wahrscheinlich. Sie treffen den Lebensnerv der Industriegesellschaft und können schon nach kurzer Zeit ihren Zusammenbruch herbeiführen […] sie bedeuten — ob Sieg oder Niederlage — in jedem Fall die Vernichtung unserer industriellen Zivilisation.[1]

Wenn Militärs von Cyberwar reden oder Kommunikationsguerillas mit ihrer disruptiven Macht kokettieren, steckt dahinter bisweilen wenig mehr als modische Attitüde. Bisweilen jedoch verbirgt sich dahinter bereits ein Ansatz neuer Konflikte. In ihrer mittlerweile zum Klassiker avancierten Studie gruppieren John Arquilla und David Ronfeld unter die bei einem Netwar möglichen Konfliktparteien auch Menschenrechts- und Umweltgruppen.[2] Mittlerweile hat sich daraus das Bild der Cyber-Terroristen entwickelt, die den Zusammenbruch von Volkswirtschaften herbeiführen. Hacker mutieren in diesem Prozeß ebenso zu gefährlichen Terroristen wie in den 60er Jahren Unabhängigkeitsbewegungen zu Satelliten Moskaus und einer Weltrevolution, die nie stattfand.

Was darüber jedoch allzu leicht vergessen wird, ist der bittere Ernst der Sache. Naiv genug ist, wer Information Warfare für ein unblutige Sache hält. Schlimmer ist es, die Folgen eines solchen Konflikts auszublenden. Die Verletzlichkeit der IT-basierten Gesellschaft ist ein altes Thema gerade kritischer InformatikerInnen. Nun wollen Militärs diese Verletzlichkeit durch Information Warfare vorsätzlich und systematisch ausnutzen und zum Mittel der Konfliktaustragung machen. Wer IT-Systeme programmiert, kann da nur den Kopf schütteln und fragen, ob sie wirklich wissen, was sie tun. Schließlich sind wir froh, wenn unsere Systeme halbwegs stabil laufen — instabil sind sie von allein.

Ich möchte hier nicht die militärische Bedeutung von Information Warfare betrachten,[3] sondern dessen Folgen für die Informationstechnik und deren Einsatz.

Die Verletzlichkeit der Informationsgesellschaft findet in zivilen Zusammenhängen kaum Beachtung. Das Jahr 2000 wird dies an vielen Computersystemen vorführen. Dasselbe in militärische Kategorien übersetzt, tritt rege Aktivitäten los. Nicht verstanden blieb also offenbar die Bedeutung, IT-Systeme allein als Mittel zur Überlegenheit, zur Zerstörung, zu sehen. Was heißt es für die Informationsgesellschaft und ihre Infrastrukturen, zum Kriegsschauplatz zu werden? Was sind die Folgen einer solchen Militarisierung — kann es noch eine zivile Informationsgesellschaft geben? Und: Wie lassen sich Risiken von IT-Systemen ausnutzen und gleichzeitig für die eigene Seite ausschalten?

Zivilschutzübung 2000

Was ist eigentlich so schlimm, wenn die Informationsgesellschaft wegen des Ausfalls ihrer Computer einmal nicht stattfindet? Gut, wir kommen nicht ins Internet, aber das wird noch zu verkraften sein. Doch ohne Computer werden wir weder telefonieren, noch werden wir mit

Eisenbahn, Auto oder Flugzeug weit kommen. Geld geben weder Bankfilialen noch Bankautomaten heraus. Was sollten wir auch damit, denn die Computerkassen funktionieren ja ebensowenig. Die Medizin wird auf den größeren Teil ihrer Geräte verzichten müssen. Überhaupt läuft nichts, weil der Computercrash auch die Stromversorgung lahmgelegt hat. Wie gut Kernkraftwerke darauf vorbereitet sind, werden wir sehen müssen.

Das alles kann auch die Folge von Information Warfare sein. Was Information Warfare für die Infrastruktur einer von Computern abhängigen Gesellschaft bedeuten kann, werden wir zum Jahrtausendwechsel hautnah erleben. Das Jahr 2000 wird uns eine Zivilschutzübung der Extraklasse liefern. Denn: Grundlage für Information Warfare ist nicht allein der Angriff auf militärische, sondern der auf die viel schlechter geschützten, aber bedeutsameren zivilen Infrastrukturen. Genauso wie beim Straßen- und Schienennetz kennt Information Warfare keine Trennung zwischen ziviler und militärischer Infrastruktur. Information Warfare findet im Telekommunikationsnetz ebenso statt wie im Internet. Wenn wir den Übergang ins Jahr 2000 überstanden haben, sollten sich Politiker und Militärs noch einmal gründlich die Konsequenzen überlegen, wenn sie Information Warfare ernsthaft zu einer Option der Konfliktaustragung machen. Es geht mir also um den Widersinn, die Verletzlichkeit unserer Gesellschaft durch Informationstechnik zu erhöhen und gleichzeitig noch Mittel zu erproben, diese Verletzlichkeit nicht systematisch zu verringern, sondern Sicherheitslücken als Kriegswaffen zu nutzen.

Neue Abschreckung

In der Pulverkammer mit der brennenden Lunte in der Hand herumzulaufen, war in vergangenen Zeiten auch bei Militärs kein Zeichen von Mut. Die Lunte hat heute anderen Formen der Selbstzerstörung Platz gemacht. Symbol dieses Fortschritts war in den letzten Dekaden die Atombombe. Sie stellte das Fortbestehen der Menschheit grundsätzlich in Frage. Entsprechend hoch war zum Glück die Selbstabschreckung, die Lunte zu legen und diese Waffen auch einzusetzen. Abschreckung basiert heute aber nicht länger auf Nuklearwaffen. Die USA sehen Information Warfare als geeigneten Nachfolger: die nuntiale Abschreckung löst die nukleare ab. Ausländischen Militärbeobachtern wird zu diesem Zweck reichlich Gelegenheit gegeben, die Manöver voll digitalisierter U.S.-Truppenverbände zu studieren. Der derzeitige Entwicklungsstand wird dabei mit der Frühphase der nuklearen Abschreckung verglichen.[4] Als Folge wird der Nuklearschirm der USA als Basis für Allianzen abgelöst: "Ebenso wie nukleare Dominanz der Schlüssel für eine Koalitionsführerschaft in der alten Ära war, so wird Informationsdominanz der Schlüssel im Informationszeitalter sein".[5]

Wer hier nur an den Zugang zu Satellitenbildern denkt, greift zu kurz. Information Warfare basiert auf der Nutzung des Technologievorsprungs in der Informationstechnik. Wäre jede Schwachstelle eines Computersystems allgemein bekannt, wäre der schöne Wissensvorsprung genauso dahin, wie zu dem Zeitpunkt, an dem jeder das Wissen hätte, sich gegen solche Angriffe zu schützen. Information Warfare basiert also auf Lücken in der IT-Sicherheit und dem wohlgehüteten Wissen darüber. Gäbe es denn Computersysteme, die keine Sicherheitslücken mehr hätten, wäre Information Warfare wertlos. Solange also Unternehmen aus den USA ihren Vorsprung im IT-Sektor halten und vor allem der Vorsprung an Know-how groß genug ist, macht Information Warfare zumindest für die USA Sinn.

Für die zivile Informationsgesellschaft hat dies bittere Konsequenzen. Als Austragungsstätte der Kampfhandlungen wird die Sicherheit von zivilen IT-Systemen vorrangig an strategischen und taktischen Maßstäben gemessen. Am Beispiel Kryptographie lassen sich einige der daraus folgenden Mechanismen verdeutlichen.

Informationstechnik als Kriegswaffe

Der Begriff "Kryptokontroverse" ist die Umschreibung der erbitterten Auseinandersetzung um die uneingeschränkte Nutzung von Verschlüsselungsmethoden. Bürger und Industrie wollen die Vertraulichkeit ihrer Daten auch gegen Ausspähung bei deren Übertragung sichern. Geheimdienste entwerfen Schreckensszenarien, sollte ihnen genau dies nicht mehr möglich sein. Kryptoverfahren sind heute schon das, was andere IT-Sicherheitstechniken erst noch werden: Kriegswaffen für Information Warfare. Noch dürfen sie in den meisten Staaten im Inland frei genutzt werden, beim Export sind sie jedoch seit Jahrzehnten Kriegswaffen gleichgestellt.[6] Nicht nur in der Bundesrepublik ist der Export von Kryptiersoftware dasselbe Vergehen, wie Plutonium und andere Massenvernichtungswaffen zu exportieren.

Wenn die Sicherheit von Daten ein ebenso großes Verbrechen ist wie der Bau von Atombomben, dann sollte dies für die Karriere von Information Warfare eine deutliche Warnung sein. Doch Kryptierverfahren sichern nicht nur Daten und deren Vertraulichkeit. Sie sind die Grundlage für digitale Authentisierung und Verbindlichkeit und weitere Konzepte. Wie die Atombombe die militärische Bedeutung einiger Länder neu definierte, so verändert die Kontrolle über Chiffrierverfahren die politische Landkarte. Die Exporteure von Chiffriersystemen haben — so Militärexperten — bei Verkäufen von Systemen an Drittländer die "strategische Kontrolle" über die geschützte Kommunikation ihrer Kunden.[7]

Die Entfesselung der Kryptographie als Wissenschaft, deren Früchte wir heute ernten, war eine Geschichte der Behinderungen und Einschüchterung durch militärische Interessensvertreter. In den achtziger Jahren sah es fast so aus, als ob das Pentagon den gesamten Wissenschaftszweig zum "Born Secret" erklären könnte. Erst der entschlossene, bisweilen verzweifelte Widerstand der Wissenschaftsgemeinde konnte dies verhindern.[8] Auch der Druck verschiedener Regierungen — zu denen trotz Dementis auch die Deutsche Bundesregierung gehört[9] — auf die internationale Standardisierungsorganisation ISO, die Normierung von Kryptosystemen zu unterlassen, hatte wenige Erfolg. Zwar hatte die ISO Beteiligten zufolge ihren Technical Committees die Normierung von Kryptieralgorithmen verboten. Damit wurde jedoch die Verbreitung eines Kryptier- Programms wie Pretty Good Privacy (PGP) keineswegs aufgehalten, sondern eher gefördert. Nun drängen die USA die ISO, sich an die Normierung zu machen, um dem Quasi-Standard PGP etwas entgegensetzen zu können. Mit der Kryptographie hat die zivile Welt eine Schlüsseltechnologie der IT-Sicherheit für sich geöffnet. Ob dasselbe mit der Vielfalt von Einzeltechniken zur Sicherheit von IT-Systemen gelingen wird, ist weniger klar auszumachen.

Mißtrauen

Die Kryptographie bietet auch ein Füllhorn von Beispielen für das aus der Konkurrenz ziviler und militärischer Interessen erwachsende Mißtrauen gegenüber staatlich geförderten Sicherheitsstandards. Schon bei der Entwicklung des 1977 zum Standard erklärten Data Encryption Standard (DES) wurde dessen Schlüssellänge als zu kurz kritisiert.[10] DES wurde 1984 für die Verschlüsselung des US-Bankenverkehrs vorgeschrieben.[11] In Konkurrenz zum asymmetrischen RSA-Verfahren entstand in den 70er Jahren auch eine auf anderen mathematischen Einwegfunktionen basierende Methode, das sogenannte Knapsack-Verfahren. Nach umfangreichen Entwicklungen wurde erst die fehlerbedingte Angreifbarkeit des Verfahrens bekannt. Erst zu diesen Zeitpunkt gab die NSA zu, diesen Fehler lange gekannt zu haben.[12] Sicher ist: Hätte sich das Knapsack- gegen das RSA-Verfahren durchgesetzt, wären der NSA einige Sorgen erspart geblieben. Vor kurzer Zeit schließlich sorgte die Nachricht für Aufregung, auch gut gesicherte Chipkarten könnten durch

entsprechende Behandlung und einer "differential fault analysis" ihren geheimen Kryptoschlüssel preisgeben. Doch wieder erklärten die staatlichen Kryptoexperten offiziell, die Gefahr sei nur theoretisch und gar nicht bewiesen.[13]

Das aus solchen Verhaltensweisen erwachsende Mißtrauen gegen den Wahrheitsgehalt von Aussagen offizieller Institutionen ist naheliegend, wenn diese Institutionen entweder wie die NSA Geheimdienste sind oder wie das Bundesamt für Sicherheit in der Informationstechnik in der Bundesrepublik aus geheimdienstlichen Zusammenhängen erwachsen sind.[14] Die einzigen Institutionen mit großer Erfahrung zur unabhängigen Bewertung der Qualität von Sicherheitssystemen sind damit ausgerechnet dieselben, die Wege aufzeigen sollen, aus Sicherheitslücken militärischen Gewinn zu schlagen.

Sicherheitslücken im Zusammenhang mit kryptographischen Verfahren sind jedoch nur die Spitze eines Eisbergs. Zwar bleibt meist im dunkeln, welche Hintergründe zu bestimmten Sicherheitslöchern führten, doch sitzt das Mißtrauen gegenüber der Sicherheit von IT-Produkten aus anderen Ländern mittlerweile auch bei staatlichen Stellen so tief, daß bundesdeutsche Stellen vor der Verwendung bestimmter Systeme aus den USA warnen.[15]

Dort wird dagegen eifrig katalogisiert, welche Sicherheitslücken sich für Angriffe auf IT-Systeme anbieten. Das Joint Command and Control Warfare Center der US-Streitkräfte verfolgt die Sammlung aller verfügbaren Daten über Waffen- und C3I-Systeme eines potentiellen Gegners und deren Schwachstellen. Diese Daten werden aufbereitet und stehen Information Warriors in der sogenannten Constant Web-Datenbank auf einem über 67 Länder verteilten Netzwerk zur Verfügung.[16]

Wenn Militärs zu Hackern werden

Militärs, die in die Rechner von Bundesbehörden eindringen, demonstrieren nicht allein deren Verletzlichkeit. Sie arbeiten zugleich an Arbeitsbeschaffungsmaßnahmen für sich selbst. Denn wer ist besser in der Lage, die Sicherheit der nationalen IT-Infrastruktur zu schützen als eben jene, die diese Infrastruktur zum Kriegsgebiet machen wollen? Auf diese Weise verfremden Information Warriors die ursprüngliche Hackerethik vom Ausspähen anderer, um die Opfer auf die gefundenen Sicherheitslücken aufmerksam zu machen.

Was die Betroffenen bisweilen als moderne Variante der Schutzgelderpressung begreifen, wenden Information Warriors auf ganze Nationen an — ihre eigenen zuerst. Nachdem die Militärs einige Zeit gewisse Zuwächse an IT-Sicherheit hinnehmen mußten, erlaubt ihnen das Forcieren von Information Warfare als systematischer Steigerung der IT-Unsicherheit überdies ein Zurückdrängen nichtmilitärischer Lösungskonzepte: Das Imperium schlägt zurück. Im Gegensatz zu Gelegenheitshackern und professionellen IT-Sicherheitsberatern geht es bei Information Warfare eben nicht um die systematische Reduktion von Verletzlichkeit, sondern um deren selektive Nutzung. Wie das Beispiel Kryptographie zeigt, sind Militärs aber kein Faktor von Sicherheit, sondern von Unsicherheit. Ihre Interessen stehen in scharfem Kontrast zu denen der zivilen Gesellschaft.

Wenn es dennoch Sicherheitskonzepte gibt, ist deren Anwendbarkeit in zivilen Bereichen oft nicht recht angemessen. Alternativen etwa zur überholten Authentisierung per Paßwort sind biometrische Verfahren zur eindeutigen Identifikation. Finger- oder Handabdrücke, Iris- oder Thermo-Scans des vaskularen Systems der Blutgefäße im Gesicht werden als eindeutige biometrierbare Eigenschaften genutzt, um den Zugang zu allerlei sensitiven Systemen zu schützen. Aus militärischen Forschungsprojekten sind auch Vorhaben bekannt, in denen über

die Nutzbarkeit von GPS-gemessenen Ortsangaben und sogar implantierbaren Identifikationschips als Zugangskontrolle nachgedacht wird. Die implantierbare Hundemarke des Soldaten wird so zum Multifunktionsgerät. Am Ende steht die vollständige Transparenz der Aktivitäten im Internet. Alle diese Verfahren sind vielleicht in militärischen Szenarien durchsetzbar. Sie haben jedoch den gravierenden Nachteil, in zivilen Kontexten bestenfalls mit Mühen verfassungskonform zu sein.

Damit stellt sich die Frage, ob wir wirklich nur die Alternative haben zwischen einer vollends militarisierten Informationsgesellschaft oder viel zu geringer IT-Sicherheit. Besteht wirklich nur noch die Wahl zwischen einem aussichtslosen Verzicht auf IT-Einsatz zu sicherheitskritischen Zwecken und der Einordnung von IT-Sicherheit in militärische Kategorien?

Zivile Gegenkonzepte zu Information Warfare

Was wir auch unabhängig von Information Warfare benötigen, ist eine Reduktion der Verletzlichkeit der Informationsgesellschaft. Neben einer frühzeitigen Abschätzung der Risiken kann dazu vor allem eine Verbesserung der IT-Sicherheit beitragen. Mit dem Orange Book stammen die ersten IT-Sicherheitskriterien aus dem Pentagon, die mittlerweile mit den Common Criteria nur leicht zivilisiert wurden. Definition und Bewertung von IT-Sicherheit ist damit kaum je unter zivilen Gesichtspunkten entwickelt worden. Wenn die Zuverlässigkeit, die Sicherheit und die Verfügbarkeit der Infrastruktur der Informationsgesellschaft von Sicherheitsmaßnahmen abhängen, dann können wir deren Definition und Bewertung ernsthaft nicht Militärs oder Geheimdiensten überlassen. Die eigentliche Frage ist also die nach den zivilen Anforderungen für Bewertungskriterien und ihrer Bedeutung im Alltag.

Folgerung aus der Debatte um Information Warfare kann nur die konsequente Politisierung und Zivilisierung der IT-Sicherheit sein. IT-Sicherheit ist in zivile Hände zu legen und entsprechend ziviler Anforderungen zu entwickeln, statt sie weiterhin unter militärischen Aspekten zu sehen. Wir brauchen auch keine Militärs, um zu verdeutlichen, worin die Verletzlichkeit der Informationsgesellschaft liegt. Wie eingangs erwähnt, gab es schon vor der Erfindung des Begriffs "Information Warfare" eine rege Debatte sowohl um die Folgen fehlender Sicherheit als auch um Sicherheitslücken. Warum sollten aus Hackern erst Soldaten werden müssen, um diese Sicherheitslücken ernstzunehmen?

Die Sicherheit und der Schutz einer verletzlichen Informationsgesellschaft sind besser in den Händen ziviler Institutionen aufgehoben. NGOs und Berufsverbände waren es, die in den letzten 20 Jahren auf die Brisanz des Thema aufmerksam gemacht haben. Sie müssen auch in Zukunft an dieser Debatte beteiligt werden, statt die Sicherheit der Informationsgesellschaft staatlichen Institutionen mit zweifelhaftem Ruf und militärischen Interessen zu überlassen. Statt es als Risiko zu begreifen, Sicherheitslücken offenzulegen, sollten im Gegenteil Informationsbörsen ausgebaut werden, um die betroffenen Systemadministratoren zu unterstützen. Die Offenlegung von Standards und Sicherheitsfeatures schützt vor unliebsamen Überraschungen. NGOs wie zum Beispiel Menschenrechtsgruppen oder Netzaktivisten als Kriegsgegner in einem Netwar zu begreifen, geht in die falsche Richtung. Mit ihrer Arbeit der letzten Jahre bieten sie am ehesten die Gewähr dafür, die Informationsgesellschaft demokratischen und zivilen Prinzipien entsprechend zu entwickeln und deren Verletzlichkeit im Interesse der Allgemeinheit zu vermindern. Werden solche Aktivitäten nicht unterstützt und solche Gruppen nicht eingebunden, wird nicht die Sicherheit zunehmen, sondern allenfalls die Sicherung vor mißbräuchlicher Nutzung. Information Warfare nötigt uns daher die Entscheidung ab, ob das Ziel eine zivile Informationsgesellschaft sein soll oder nicht.

Fußnoten:

[1] Klischewski, Ralf; Rolf, Arno: "Informationstechnische Vernetzung und Kriegsunfähigkeit in hochentwickelten Industriestaaten". In: Bernhardt Ute, Ruhmann Ingo (Hg.): Ein sauberer Tod. Informatik und Krieg. Marburg, 1991, 268—282, 282

[2] Arquilla, John; Ronfeldt, David: Cyberwar is Coming! In: Arquilla, John; Ronfeldt, David (Hg.); RAND: In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica 1997. Deutsche Übersetzung siehe S. 24—56 im vorliegenden Band

[3] vgl. dazu: Bernhardt, Ute; Ruhmann, Ingo: "Der digitale Feldherrnhügel. Military Systems: Informationstechnik für Führung und Kontrolle". In: Wissenschaft und Frieden. Heft 1/97, Dossier Nr. 24, 1—16

[4] "Information Dominance Edges Toward New Conflict Frontier". In: Signal. Aug 1994, 37—40, 39

[5] Nye, J. S., Jr.; Owens, W. A.: "America's Information Edge." In: Foreign Affairs. March/April 1996, 20—36, 27. [Original: "Just as nuclear dominance was the key to coalition leadership in the old era, information dominance will be the key in the information age"]

[6] Die USA regeln das Exportverbot leistungsfähiger Kryptiersysteme in der International Traffic in Arms Regulation (ITAR), die Bundesrepublik in der Ausfuhrliste Teil I C Abschnitt 5 Teil 2 gemäß Außenwirtschaftsverordnung. Ausfuhren begutachten und damit genehmigen in allen westlichen Staaten die Chiffriergeheimdienste wie die NSA oder das BSI; vgl. die Antwort der Bundesregierung auf die Kleine Anfrage von Dr. Manuel Kiper "Sicherheit der Informationstechnik und Kryptierung", Drs. 13/4105, Frage 6

[7] Witt, Mike: "Tactical Communications". In: Military Technology. Nr. 5, 1991, 19—25, 22

[8] vgl. Ruhmann, Ingo: "Politik der Chiffren". In: FIfF-Kommunikation 3/96, 45—49

[9] vgl. Antwort der Bundesregierung auf die Kleine Anfrage des Abg. Dr. Manuel Kiper "Sicherheit der Informationstechnik und Kryptierung", Drs. 13/4105, Frage 11

[10] Diffie, Whitfield; Hellman, Martin: "A Critique of the Proposed Data Encryption Standard". In: Communications of the ACM. March 1976, 164—165

[11] Myers, Edith: "Speaking in Codes". In: Datamation. Dec. 1, 1984, 40—45

[12] Shamir, Adi; Adleman, Len ("S" und "A" des Akronyms RSA) stellten Mitte 1982 auf der Konferenz Crypto ’82 zwei verschiedene Verfahren zum Brechen der Knapsack-Verschlüsselung vor, vgl.: Kahn, David: "The Crypto ’82 Conference". In: Cryptologia. Jan. 1983, 1—5. Kurz darauf erklärte der damalige NSA-Chef Inman, den Fehler gekannt, aber nicht vor der Nutzung gewarnt zu haben, so: Kolata Gina: "NSA Knew of Flaw in "Knapsack" Code"; In: Science. 24.12.82, 1290

[13] vgl. Antwort der Bundesregierung auf die Kleine Anfrage des Abg. Dr. Manuel Kiper "Lage der IT-Sicherheit in Deutschland", Drs. 13/7753

[14] Bernhardt, Ute; Ruhmann, Ingo: "Der militärische Maßstab der Computersicherheit — Das Bundesamt für Sicherheit in der Informationstechnik"; In: dieselben (Hg.): Ein sauberer Tod. Ibid., 252—267

[15] Antwort der Bundesregierung auf die Kleine Anfrage des Abg. Dr. Manuel Kiper "Sicherheit der Informationstechnik und Kryptierung", Drs. 13/4105, Frage 10

[16] "Informations Dominance Edges Toward New Conflict Frontier", ibid., 38ff