Zürcher Beiträge

zur Sicherheitspolitik und Konfliktforschung Nr. 64

Myriam Dunn

Information Age Conflicts

A Study of the Information Revolution and a Changing Operating Environment

Hrsg.: Kurt R. Spillmann und Andreas Wenger
Forschungsstelle für Sicherheitspolitik
und Konfliktanalyse der ETH Zürich

Inhaltsverzeichnis

Preface

The basic conditions in which international relations operate have undergone some fundamental changes in the past decade. Most experts agree that the information revolution is an important component of this ongoing transformation. The unity of the state, of society, and of the economy can no longer be taken for granted: Geographic boundaries have lost in importance, and the boundaries between conventional political spaces have become blurred. The spaces in which power and influence are created and from which they are exerted no longer comprise only the „hard" spheres of territory, the military, and resources, but now also include the „soft" spheres of information, technology, and flexible institutions.

Although there is a general belief that the information revolution is causing a widespread restructuring of the international system, it is difficult to pinpoint the exact nature of these changes. Academics are still struggling to understand the often contradictory and volatile developments and the increasing complexity brought about by the information revolution. A variety of theories and concepts have been proposed in the past few years by scholars attempting to grasp the theoretical and practical impacts of recent developments and to explain the changes to international politics induced by the information revolution. One important aim of the present study is to review these fragmentary theories and to fuse them into theorems that will help us to describe the changing environment in the information age and that will further the development of new conceptual paradigms.

This study focuses on a potential new form and class of war, which the author terms „information age conflict" (IAC). The information revolution has dramatically increased the importance of information in the strategic world, alongside existing traditional physical military capabilities, and the information domain has moved to center stage in combat. As a consequence, new forms of warfare are being created. IACs are conducted according to new doctrine papers that describe the ways in which information operations are conducted, with substantial consequences for military affairs, politics, and society as a whole.

Using a model derived from the aforementioned theorems and illustrated by the situation that arose during Operation Allied Force in Kosovo, the author, Myriam Dunn, identifies factors in the emerging operating environment that substantially influence the successful managing and waging of IACs, as well as factors that are likely to pose problems for decision-makers. Dunn describes the effects of the information revolution on international relations in general and on warfare in particular and demonstrates her findings by means of a case study. Pointing out the implications of these new developments in warfare not only for the military but also for society and international security in general, Dunn draws attention to the crucial issue of newly emerging threats and risks to the information society.

Dunn was awarded the *Gustav Däniker Award (Förderpreis)*, sponsored by the Society for Security Policy and Military Science (*Verein für Sicherheitspolitik und Wehrwissenschaft, VSWW*), for her master thesis, published here in a slightly modified form.* A jury of experts chose Dunn's thesis for its academic excellence and its ground-breaking findings. At the award presentation, Dunn presented her results to renowned academics, military officers, government staff, and the press.

The editors would like to thank the author, a research assistant at the Center for Security Studies and Conflict Research at the Swiss Federal Institute of Technology (ETH) Zurich, for her con-

* The publication was concluded in October 2001. New developments were not taken into account

tribution to a better understanding of the impacts of the information revolution on the international system and for her pioneering efforts in tackling an as yet barely investigated but highly relevant topic.

Zurich, November 2002

Prof. Dr. Kurt R. Spillmann

Leiter der
Forschungsstelle für Sicherheitspolitik
und Konfliktanalyse

Prof. Dr. Andreas Wenger

Stellvertretender Leiter der
Forschungsstelle für Sicherheitspolitik
und Konfliktanalyse

Abbreviations

AF:	Air Force
AFDD:	Air Force Doctrine Document
ASD PA:	Assistant Secretary of Defense, Public Affairs
AWACS:	Airborne Warning and Control System
C2W:	Command and Control Warfare
C3I:	Command, Control, Communications and Intelligence
C4:	Command, Control, Communications and Computers
C4I:	Command, Control, Communications and Computers and Intelligence
C4ISR:	Command, Control, Computer, Communications, Intelligence, Surveillance, and Reconnaissance
CAOC:	Combined Air Operations Center
CI:	Counter-Information or Counter-Intelligence
CIA:	Central Intelligence Agency
CINCUSAFE:	Commander-In-Chief of US Air Forces in Europe
CJCS:	Chairman of the Joint Chiefs of Staff
CJTF:	Combined Joint Task Force
CNN:	Cable News Network
COTS:	Commercially Off-the-Shelf
DASD PA:	Deputy Assistant Secretary of Defense, Public Affairs
DBA:	Dominant Battlespace Awareness

DBK:	Dominant Battlespace Knowledge
DCI:	Defensive Counter-Information
DIA:	Defense Information Agency
DII:	Defense Information Infrastructure
DIO:	Defensive Information Operations
DoD:	Department of Defense (US)
DV:	Dependent Variable
EMP:	Electro-Magnetic Pulse
EW:	Electronic Warfare
FM:	Field Manual
FRY:	Former Republic of Yugoslavia
FYROM:	Former Yugoslav Republic of Macedonia
GATSGAM:	GPS-Aided Targeting System Guided Air Missile
GIE:	Global Information Environment
GII:	Global Information Infrastructure
GIS:	Geographic Information System
GPS:	Global Positioning System
HERF:	High Energy Radio Frequency
HIC:	High-Intensity Conflict
HQ:	Head Quarters
IA:	Information Assurance
IAC:	Information Age Conflict
IGO:	International Governmental Organizations
IntV:	Intervening Variable
IO:	Information Operations
ISR:	Intelligence, Surveillance and Reconnaissance
IV:	Intervening Variable

IW:	Information Warfare
J-5:	Joint Staff Plans and Policy
JCS:	Joint Chiefs of Staff
JDAM:	Joint Direct Attack Munitions
JP:	Joint Publication
JV:	Joint Vision
KLA:	Kosovo Liberation Army
LIC:	Low Intensity Conflict
MIE:	Military Information Environment
MNC:	Multinational Corporation
MoD:	Ministry of Defense (GB)
MRC:	Major Regional Conflict
NAC:	North Atlantic Council
NATO:	North Atlantic Treaty Organization
NGO:	Non-Governmental Organization
ICT:	Information and Communication Technologies
NII:	National Information Infrastructure
OCI:	Offensive Counter-Information
OIO:	Offensive Information Operations
OOTW:	Operations-Other-Than-War
OPSEC:	Operations Security
PA:	Public Affairs
PAO:	Public Affairs Officer
PGM:	Precision-Guided Munitions
PSYOP:	Psychological Operations
SACEUR:	Supreme Allied Commander Europe
SHAPE:	Supreme Headquarters Allied Powers Europe
SIO:	Special Information Operations

UAV:	Unmanned Aerial Vehicle
US:	United States
USAF:	United States Air Force

List of Tables and Figures

Introduction[*]

> "Information warfare is real. Information operations are being conducted (…) today. While the world has not yet witnessed nor fully comprehended the implications of a global information war, it is now enduring an ongoing information competition with sporadic conflicts in the information domain."
>
> (Edward Waltz, Information Warfare, 1998, 41)

Since these lines were written one conflict has strongly confirmed the relevance of both Information Operations and Information Warfare: Operation "Allied Force", conducted by NATO in Kosovo from 24 March to 10 June 1999, was the world's first conflict taking place largely in the information domain. Even though it was not global, it was nonetheless large-scale enough to be called a precedent for an emerging form and class of future wars: the "*Information Age Conflict*" (IAC).

These IACs take place in an international environment presently transformed by the manifold influences of the *Information Revolution*, an ongoing dynamic development that is driven by the integration of Information and Communication Technologies (ICT) into a multimedia system of communication with global reach, adding increased speed, greater capacity, and enhanced flexibility to the gathering and processing of data, and thus simplifying its transformation into knowledge or wisdom.[1] This materializing environment can best be characterized by the significance assigned to information, knowledge, and ideas as resources in international relations. In military affairs, the Information Revolution leads to

[*] This publication was concluded in October 2001. Newer developments could not be taken into account.

[1] See chapter 2.1 for an in depth exploration of the Information Revolution.

a rising importance of information in the strategic world next to traditional military capabilities and an increased focus on the information domain in combat. It is a principal driver for the current *Revolution in Military Affairs* (RMA) that seeks to transform military affairs by digitizing the battlespace, adopting new doctrine, and developing organizational forms corresponding to the marriage of ICT-systems with those that apply military force.[2] As a consequence, IACs are conducted in accordance to military doctrine papers that describe the waging of defensive and offensive *Information Operations* (IOs). Information Operations are conducted to disrupt or confuse an enemy's ability to collect, process, and disseminate information and at the same time to defend one's own,[3] with the ultimate aim of gaining *Information Superiority* over adversaries.[4] In IACs, at least one party involved should be in possession of high-tech facilities and weaponry that allow for conduct of a comprehensive range of Information Operations as defined in recent doctrine documents – which includes intelligence, surveillance and reconnaissance activities, precision navigation and positioning, electronic warfare, plus physical attacks, directed at the enemy's information infrastructure.[5] Second parties and adversaries however only need a minimum degree of technologization, although, the higher the adversary's technological level the higher his alleged vulnerability to information attacks and the more likely that these are conducted against him. As for the scale of these conflicts, they are not confined to so-called "Strategic Information Warfare"

[2] See chapter II.3.1 for an in depth analysis of the Revolution in Military Affairs.

[3] See mainly Department of the US Air Force, Air Force Doctrine Document 2–5 Information Operations, August 1998 and chapter III.1.

[4] Ibid. "Information Superiority" is describing that degree of dominance in the information domain, which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.

[5] Cf. chapter III.1.

conducted between states, but also include operations waged by all kinds of non-state actors against states and vice versa.

The air campaign conducted under the name "Operation Allied Force" is the first example of a full-fledged IAC. We still have not witnessed a "global" information war, but many current conflicts show various characteristics of conflicts in the information domain. For this thesis, Operation Allied Force is a unique opportunity to analyze features of conflicts in the context of the ongoing Information Revolution. It is well suited for a case study of modern information conflicts because its precedents have a substantial impact on the future of warfare, it is well documented, it is limited in time, and provided a real-world test of newly developed strategic concepts.[6] Because frequency and importance of IACs are likely to increase, analyses of such conflicts seem highly relevant:

- The Information Revolution leads to a growing dependence of developed countries on ICT. This dependency increases the danger that national information infrastructures may become prime targets in conflicts and aggressions of different intensities;[7]
- Aspects of new forms of warfare as outlined in recent US military doctrine papers are being readily adopted by other

[6] Office of the Secretary of Defense, Report to Congress, *Kosovo/ Operation Allied Force After Action Review Report*, 31 January 2000, URL www.defenselink.mil/pubs/kaar02072000.pdf, xxii.

[7] This has led to increasing focus of security politicians on the protection of critical information assets in the last few years (Critical Information Infrastructure Protection (CIIP)). Important publication: President's Commission on Critical Infrastructure Protection. *Critical Foundations. Protecting America's Infrastructures.* Washington D.C., 13 October 1997, online version http://www.ciao.gov/PCCIP/report_index.htm.

states' military planners.[8] This proliferation of ideas shapes perceptions of decision-makers and leads to a growing readiness of states to conduct Information Operations;[9]

- Politically and strategically there seem to be many incentives for state-sponsored information warfare: it is low cost, not location-specific, provides no early warning, inflicts low human life costs, and can be waged in complete anonymity. These factors are good selling points for a democratic populace, which is reluctant to fight wars;[10]
- The proliferation of harmful "information weapons" that are available cheap and easily gives a variety of actors the means to pose substantial asymmetrical threat to today's strongest high-tech forces.[11]

The likelihood that hostilities increasingly shift from the physical to the information domain propels the necessity to gain a better understanding of dynamics and mechanisms of such conflicts. However, the focus of this study is almost completely on the analysis

[8] Examples for *China:* Thomas, Timothy, *Like Adding Wings to the Tiger: Chinese Information War Theory and Practice* (Fort Leavenworth, Foreign Military Studies Office: 2000); for *Russia:* Thomas, Timothy, *Russian Views on Information–based Warfare* (Fort Leavenworth, Foreign Military Studies Office: July 1996); for *India:* Joshi, Akshay, "A Holistic View of the Revolution in Military Affairs (RMA)", *Strategic Analysis,* XXII, 11 (February 1999), online version http://www.idsa-india.org/an-feb9-7.html.

[9] Geiger, Gebhard. *Offensive Informationskriegsführung. Die "Joint Doctrine for Information Operations" der US-Streitkräfte: Sicherheitspolitische Perspektiven.* SWP Studie (Berlin, Stiftung Wissenschaft und Politik: Februar 2002).

[10] Devost, Matthew G., *National Security in the Information Age*, M.A. Thesis (Vermont, The Faculty of the Graduate College: 1995), online version http://www.devost.net/mgd/documents/devostthesis.pdf.

[11] Kolet, Kristin S., "Asymmetric Threats to the United States", *Comparative Strategy*, 20 (2001): 277–292. The word asymmetry is used to describe a broad range of threats and tactics; the gist of the term is the intention to circumvent an opponent's advantage in capabilities by avoiding his strengths and exploiting his weaknesses.

of the offensive side of Information Operations. Defensive aspects, including *Defensive Information Operations*,[12] were not included. Within the broader issue of Information Assurance,[13] the study of Information Operation activities is a contribution towards the better understanding of possible dangers and threats to modern states stemming from hostile activities in the information domain.

Because the systemic context for this kind of conflict has distinctly changed since the beginning of the 90s, the thesis aims at conducting preliminary research that identifies features of the operating environment in which IACs take place. This is done in accordance to the Structural Realist School, which lays emphasis on the importance of identifying the structure of the international system when engaged in theorizing.[14] The thesis is thus principally concerned with identifying those characteristics of IACs that substantially influence their waging and manageability and pose possible problems for decision-makers in particular and international security in general, all in the context of a changing decision-making environment due to the Information Revolution. Basically, it wants to find an answer to the following question:

[12] See Department of the US Air Force, Air Force Doctrine Document 2–5 Information Operations.

[13] In the Swiss understanding, Information Assurance unites the state, the military and the private sector in a continuous fight against a whole variety of incidents, which could have catastrophic impact on the infrastructure of a country. See: Sibilia, Riccardo, *Informationskriegsführung: eine schweizerische Sicht* (Zürich, Institut für militärische Sicherheitstechnik, ETH Zürich: 1997).

[14] As Robert Keohane notes: “Systemic theory is important because we must understand the context of action before we can understand the action itself.” See Keohane, Robert O., “Theory of World Politics: Structural Realism and Beyond”, in: Keohane, Robert O. (ed), *Neorealism and Its Critics* (New York, Columbia University Press: 1986): 173. Page numbering as in Viotti, Paul R. and Mark V. Kauppi, *International Relations Theory. Realism, Pluralism, Globalism, and Beyond,* 3rd Edition (Needham Heights, Prentice Hall: 1999).

> Which are the factors of the operating environment – currently transformed by the Information Revolution – that substantially influence the successful managing and waging of Information Age Conflicts?

The research question implies that the international system is subject to change. In a first step we therefore need to expose how the Information Revolution transforms the international environment, what its (new) characteristics are, and what we can expect of it. For the majority of years, the debate on the impact of the Information Revolution on the international system focused mainly on changes in the nature of warfare, an issue that arose in the United States after the Gulf War in the early 90s.[15] Today, Information Revolution literature can be divided into two broad strands: one that addresses mainly military/strategic implications and the other that explores changes in more political and institutional matters.[16] Most of today's debate is still held in the US, is predominantly policy- and strategy-oriented and dominated by publications from military academies and government consulting think tanks.[17]

The most significant change affecting both politics and military equally is the changing nature and the redistribution of power in the Information Age. Over the last few years, significant theoretical fragments and concepts have been proposed by a variety of scholars to describe Information Revolution induced changes in international relations and security. Though not yet consolidated theories, these fragments comprise crystallizing theorems of the Information Age. It is an aim of this thesis to single out those theorems and use them to develop a framework to devise hypotheses for expected causal phenomena. This is done in part I. It discusses traditional international relations theory and introduces the emerging theorems

[15] E.g. Campen, Alan, *The First Information Warfare* (Fairfax, AFCEA International Press: 1992).

[16] See mainly scholars such as James Rosenau, David Rothkopf, David Alberts/ Daniel Papp, and David Rothkopf.

[17] Such as the RAND Corporation, the National Defense University, or the Strategic Studies Institute of the US Army War College.

of the Information Age. From the five theorems an arrow diagram is deduced that is the basis for the formulation of the hypotheses. The five theorems predominantly cluster around the changing nature of power and its redistribution:

№ 1: Information Superiority is perceived as the key to success in the new operating environment;

№ 2: Asymmetrical credibility becomes the key power resource;

№ 3: Boundaries between states, military-politics, and the military-civilian domain increasingly blur in the Information Age;

№ 4: Networks vs. Hierarchies: Centralized hierarchical organizations lose ground vis-à-vis decentralized flat organizations;

№ 5: Asymmetry vs. Doctrine of Dominance: Small players can impair the traditionally powerful more easily.

The exact extent of these changes is debated: though most scholars agree that the Information Revolution does to some extent change our understanding of power,[18] the majority, mainly realist thinkers, remains cautious about jumping to conclusions about the implications of the development. The resilience of states and the lingering importance of military power in relations between states is their most pungent argument against hasty suppositions: The state keeps its information advantage over all other actors especially in conflicts and other war-like situations, because strategic information is not easily available for everyone and actors other than states mostly

[18] E.g. Rosenau, James, "Global Affairs in an Epochal Transformation", in: Henry, C. Ryan and Edward C. Peartree (eds.) *Information Revolution and International Security* (Washington D.C., Center for Strategic and International Studies Press: 1998): 33–57; or Alberts, David S. and Daniel S. Papp (eds.), *The Information Age: An Anthology of Its Impacts and Consequences* (Washington D.C., National Defense University: 1997) and many more.

lack the ability to collect and edit much significant information.[19] The analysis on hand likewise shows that the outcome of the expected changes is far from being effortlessly comprehended. They rather appear intriguingly complicated, complex, and contradictory. Part II is dedicated to in depth discussion of the debate. It explores characteristics of the Information Revolution, the Internet's role in the process, and the characteristics of an "Information Society". It discusses theoretical fragments and concepts addressing economic, political, and social changes on the one hand and military and strategic implications on the other.

Part III outlines the values and definitions of the model's variables as developed in part I. It starts with the analysis of the most influential US military doctrine papers that influence the way Information Operations are conducted and then moves on to aspects of offensive Information Operations during Operation Allied Force. Data is collected from primary sources; they include journalistic work, NATO press conferences and morning briefings,[20] as well as press briefings from the US Department of Defense.[21] It presents descriptive evidence in considerable detail as the exploration of Information Operations is an important step towards understanding the dynamics and mechanisms of IACs.

Part IV aims to test the model with the values and definitions gained in part III. The analysis of the conjectured relationships is undertaken by "congruence procedure" and "process tracing" that uses causal narrative to explore the chain of events, a process that helps to gain deeper understanding of why relationships occur. Of eight tested hypotheses only one is outright falsified; four on the

[19] Keohane, Robert O. and Joseph S. Nye Jr., "Power and Interdependence in the Information Age", *Foreign Affairs* 77, 5 (September/October 1998): 81–94.

[20] Available from the NATO homepage, URL http://www.nato.int/kosovo/all-frce.htm.

[21] Available from Defenselink, URL http://www.defenselink.mil/briefings/. British Ministry of Defence briefings were not evaluated because they would not have provided any substantially different insight.

other hand show only weak relationships between the Intervening Variable (IV) and the Dependent Variable (DV). In some cases, causal narrative helps to establish whether and how the IV caused variation in the DV. Based on the experience made in part III and IV, the last part revises the underlying assumptions of the five theorems, criticizes the model and offers thoughts on how to improve it for future research.

It is concluded that the most influential factors hampering the successful managing and waging of Information Age Conflicts are:

- asymmetrical threats faced by major conflict parties;
- exogenous factors such as technological, geophysical, environmental, and legal aspects;
- blurring boundaries between military and political domains.

It is further shown that conducting Information Operations successfully is becoming increasingly important in this Information Age of warfare. But the example of Operation Allied Force also shows that the Western Alliance is far from ready to win the multi-facetted information battle as defined by the United States. In fact, the experience indicates how cautiously parties to a conflict must handle control and release of information to the public in order to remain credible in extensive and aggressive media wars, not only to win sympathy for one own side's view but also to sustain public support of democratic electorates, a point in which NATO clearly failed. Moreover, the operation indicates that the refusal of high-tech forces to risk lives will likely fortify the shift of hostilities from the traditional battlefield to civilian opinion and morale at home.

Part I – Model

Development of a Research Framework

Part I – Model

Development of a Research Framework

The emergence of scholarly work concerning the impact of the Information Revolution on aspects of politics and society is a relatively new phenomenon. The difficulty of fitting its major assumptions, namely alterations in the distribution and the nature of power, into conventional international relations theory is one of the most substantial obstacles for the topic's analysis in a social sciences context. Any research framework therefore has to rely heavily on unconventional and not necessarily matured theoretical approaches. Before the assumptions of the most influential Information Revolution scholars are introduced, this part discusses more traditional international relations theory in the context of the topic. It is shown why and how the school of Structural Realism, which stresses the importance of knowing the international system's structure when engaged in theorizing, shapes the research question. In a further step, the emerging theorems of the Information Age are introduced in some detail. From the five theorems a model in the form of an arrow diagram is deduced that provides the basis for the formulation of the hypotheses and their operationalization. Backed by this research framework derived from the theorems hampering factors for the successful managing and waging of IACs can be identified.

1 Theoretical Background

While this thesis is very sympathetic to the idea that the international system is being restructured by the influences of the Information Revolution, it also acknowledges that much more empirically-grounded research is needed before it is possible to convincingly move beyond the anecdotal evidence that is frequently offered in support of this view. The recent and ongoing nature of the development complicates the systematic analysis of the topic and caution is required when interpreting the magnitude of the transformation; difficulties in grasping its true proportions are inevitable because we are in the midst of the process ourselves. On the other hand, numerous theoretical fragments and concepts have been developed over the last few years, which hold emerging theorems of the Information Age. Among the main aims of this thesis is the identification of the most significant of these, which, once consolidated, revised, and tested, may become contributions to a comprehensive approach to a world system subject to the Information Revolution. Such an "Information Age approach" will likely be a suitable mix of existing theoretical concepts, in which especially the role of information and the concept of power in all aspects of international relations and security needs to be reviewed.

Earlier such syntheses have involved combining elements of Realism and Pluralism. Robert Keohane and John Ruggie have indicated why this is desirable and how it might be achieved: They argue that in attempting to construct a comprehensive theory of international relations, one must begin with the Realist emphasis on power and the state and have structural analyses of international politics provide the critical context, in which pluralist insights and actors can be analyzed.[1] One such approach is *Neoliberal Institutionalism*. It encompasses theories that argue that international institutions play an important role in coordinating international cooperation. It adapted the Realist analytical assumption of the rational egoist, unitary state, accepting multiple kinds of state and nonstate actors however; interstate cooperation occurs when states have sig-

[1] Keohane, Robert O., "Theory of World Politics: Structural Realism and Beyond", 153–183; Keohane, Robert O., *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton, Princeton University Press: 1984); Ruggie, John Gerard, "Continuity and Transformation in the World Polity: Toward a Neorealist Synthesis", *World Politics* 35, 2 (January 1983): 261–285.

nificant interests in common. This approach's goal is to discover how and under what conditions institutions influence, and are influenced, by competition and cooperation among states.[2] Neoliberal Institutionalism is useful in explaining the occurrence of cooperation. In the context of IACs, Neoliberal Institutionalism would be a useful approach to explain coalition building in modern warfare.

Related to this approach is *International Regime Theory* that also offers a meeting ground for debate between the various schools of thought in international relations theory. It too focuses on cooperation among actors in a given area of international relations. An international regime is viewed as a set of implicit and explicit principles, norms, rules, and procedures around which actors' expectations converge in a particular issue-area.[3] For some, the US-UN intervention in the Persian Gulf spelt out the possibilities of a "new world order" based on international law, an effective system of collective security, and democracy. Such a system depends on the increasing number of democratic governments and their openness to public opinion, hopes that have been further propelled by the Information Revolution.[4] Regime theory would be very fruitful for explaining possible emerging institutions/regimes due to the conduct of information warfare/ Information Operations in IACs.

Another effort to synthesize elements of Realist and Liberal thought is the *Complex Interdependence Theory***,** an approach that attempts to improve the ability of Realist or neo-Realist analysis to account for change in international regimes. The term 'complex interdependence' was coined by Robert Keohane and Joseph Nye

[2] Keohane, Robert O., "International Institutions: Two Approaches", *International Studies Quarterly,* 32 (December 1988): 379–396. Robert Keohane is the scholar most closely identified with neoliberal institutionalism.

[3] See Krasner, Stephen, *International Regimes* (Ithaca, Cornell University Press: 1983).

[4] Woods, Ngaire, "The Uses of Theory in the Study of International Relations", in: Woods, Ngaire (ed.), *Explaining International Relations since 1945* (Oxford, Oxford University Press: 1996): 16–18.

and refers to the various, complex transnational connections (interdependencies) between states and societies. Interdependence theorists note that such relations, particularly economic ones, are increasing, while the use of military force and power balancing is decreasing (but remains important). Reflecting on these developments, they argue that the decline of military force as a policy tool and the increase in economic and other forms of interdependence should increase the probability of cooperation among states.[5] In IACs this is only true if levels of interdependence are high enough to ensure that the costs of waging information warfare outweighs the perceived political and strategic benefits. Assumptions of interdependence as a permanent constraint are only valid as long as no party actively works toward changing the rules of the game. In addition, interdependence as defined in this theory does nothing to prevent states from waging information warfare against specific corporations and vice versa, nor terrorist groups or asymmetrical actors against states.[6] Despite of these restrictions, the interdependence approach as an underlying idea of world structure remains important for many of the assumptions made in this paper.

All these approaches would allow groundwork research on single components of the overall theme. The necessity of this has already been mentioned. This thesis has different intentions however; by analyzing IACs in an operating environment that is changed by the Information Revolution it pretends that many of the underpinning assumptions have already been empirically confirmed. To overcome part of the problem, this thesis focuses on identifying systemic factors that might influence the conduct of IACs. It is the *Structural Realist* approach within the neo-Realist school that em-

[5] Keohane, R. and J. Nye, *Power and Interdependence: World Politics in Transition,* 2nd edition (Boston, Little Brown Company: 1989). (First edition 1977).

[6] See also Devost, Matthew G, *National Security in the Information Age*, online version, on both Realist and Liberalist theory and Information Warfare.

phasizes the importance of the structure of the international system, seeking to discover various deep-seated constraints on the freedom of actors to choose, and directing attention to fundamental questions of interest and power.[7]

However, some of this approach's weaknesses are those already inherent in Realist theory: it primarily focuses on states as relevant actors, cannot account for important factors such as motivation, and is not precise enough about the concept of power and its relationship to the context of action.[8] Keohane proposes to move beyond it, using a multi-dimensional, multi-level approach, one that draws on the Realist model's strength without sharing its weakness, an approach that encompasses Structural Realism assumptions plus a modified structural research program that gives more attention to "internal-external interactions",[9] deducing actor's behavior from the constraints of the system as modeled in the theory.[10] Even though Keohane still recognizes states as principal actors in world politics he places more emphasis on non-state actors, intergovernmental organizations, and transnational and transgovernmental relations.[11] This thesis tries to follow some of Keohane's suggestions; it acknowledges the state as a principal actor especially in times of conflict,

[7] Structural Realism is a term preferred by Kenneth Waltz and other neo-Realists because in their view it more accurately describes Neorealism's focus on structure as a principal determinant of the behavior of states: Waltz, Kenneth N., *Theory of International Politics* (Reading, Addision-Wesely: 1979).

[8] Ibid.

[9] See also framework developed by Snyder, Richard C., H.W. Bruck, and Burton Sapin, *Foreign Policy Decision Making: An Approach to the Study of International Politics* (New York:, Free Press: 1962). (Originally published in 1954) Despite its innovative nature, Snyder's framework failed to generate more than one major empirical study.

[10] Keohane, *Theory of World Politics: Structural Realism and Beyond*, 173–175.

[11] See Keohane and Nye, *Power and Interdependence: World Politics in Transition*.

but also takes into account the specific surroundings of IACs that give rise to a variety of different and also important actors.

The thesis aims at singling out problems for decision-makers by identifying factors in the emerging operating environment on which successful waging and management of such conflicts depends. For this end, a framework based on emerging theorems of the Information Age drawn from "Information Revolution literature" must be developed. Scholars associated with the view that technology transforms world politics are called *modernization writers.*[12] They describe and explain change in the nature of international relations by focusing on social, political, and economic prerequisites for, and consequences of, technological development. Mostly, traditional modernization writers are concerned with impacts of the industrialization.[13] Even though in the early 70s some scholars stated that telecommunications and other modern gains create a global village, and believed that the territorial state was being outdone by non-territorial actors,[14] "Third Wave" or *Information Revolution literature* is generally associated with writings from the 80s onwards, and has gained much momentum lately, mostly due to the phenomenal rise of the Internet in the 90s.[15] Even if Information Revolution scholars as well as modernists before them correctly point to the fundamental changes now taking place, one of this view's major problems

[12] Viotti and Kauppi, *International Relations Theory: Realism, Pluralism, Globalism, and Beyond*, 211.

[13] Important proponents that explain the impact of modernization on international relations as resulting from the global spread of the industrial revolution are Morse, Edward L., *Modernization and the Transformation of International Relations* (New York, Basic Books: 1976); Kautsky, John H, *The Political Consequences of Modernization* (New York, John Wiley: 1972); and Black, C.E., *The Dynamics of Modernization: A Comparative History* (New York, Harper & Row: 1966).

[14] See for example Brown, Lester R., *World Without Borders: The Interdependence of Nations* (New York, Random House: 1972).

[15] The term "Third Wave" was introduced by Alvin Toffler, in: Toffler, Alvin, *Third Wave* (New York, Bantam Books: 1980).

is exaggerated technological determinism as well as hasty conclusions such as that advances in technology and increases in social and economic transactions will lead to a new world in which states, and their control of force, will cease to be of importance.[16] In the discussion of Information Revolution literature, too extreme positions are excluded.

1.1 Information Revolution Literature: Most Important Proponents

At the core of the anticipated changes is the notion that an ever-widening range of actors now has access to powerful tools for the rapid collection, production, and dissemination of information on a worldwide scale. Control over knowledge, beliefs, and ideas are increasingly regarded as a complement to control over tangible resources such as military forces, raw materials, and economic productive capabilities.[17] The globalization and mass popularization of the Internet provides governments, businesses, NGOs, terrorists, criminals, and other actors with capabilities that were formerly in the hands of only the largest and most powerful entities. Their diverse uses of cyberspace have challenged the power and steering capacity of major states and have significantly increased the turbulence and unpredictability of the international policy environment. In short, we face not only a redistribution of power relationships that has its outcome in a skewed, complex and volatile distribution pattern, but also changes in the nature of power as it was traditionally understood.

[16] See e.g. Angell, Robert, *Peace on the March: Transnational Participation* (New York, Van Nostrand Reinhold Co: 1969).

[17] Rothkopf, David J., "Cyberpolitik: The Changing Nature of Power in the Information Age." *Journal of International Affairs* 51, 2 (Spring 1998): 325–360.

The most prominent proponents of these views are:

- *James Rosenau on the contradictory nature of change:* Rosenau states that developments in the system are contradictory and confusing, and the present epoch seems to derive its order from episodic patterns marked by opposites, with complexity and change being the two defining characteristics. Change is propelled by the dynamics of technology, the emergence of complex issues, the reduced capacity of states to deal effectively with many contemporary problems, and the emergence of "subgroupism" and individuals who are analytically ever more capable and diverse in orientation;[18]
- *Daniel Papp and David Alberts on the redistribution of power:* Papp and Alberts argue that because of ICTs, international actors not restricted by geography (mainly multinational corporations and non-governmental organizations) will increasingly gain the ability to act internationally with little regard to the requests of states. They show how the Information Revolution changes these actors' role and function, reflecting on struggles for power and influence among the different actors that are likely to increase with the progressing revolution;[19]
- *Daniel Papp and David Alberts on diffuse distribution of power:* Struggles for power and influence eventually lead to a redistribution of power. Since the new technologies are absorbed and operationalized by different international actors in different ways and at different speeds, this distinguished pattern naturally leads to different types and rates of change

[18] Rosenau, James, "Global Affairs in an Epochal Transformation", 33–57.

[19] Papp, Daniel S and David S. Alberts, "The Impacts of the Information Age on International Actors and the International System", in: Alberts, David S. and Daniel S. Papp (eds.), *The Information Age: An Anthology of Its Impacts and Consequences* (Washington D.C., National Defense University: 1997): online version, URL http://www.ndu.edu/inss/books/anthology1/ch24.html.

and thus to a more diffuse distribution of power than known before;[20]

- *James Rosenau on the "skill revolution" and the growing complexity of the system:* Rosenau argues that the individual gains considerable influence in the Information Age; it's strengthened position is due to the expansion of its diagnostic capabilities thanks to ICTs, letting citizens become more competent and analytically skillful ("skill revolution"). As a consequence, they demand more influence, leading to a relocation of authority or the decentralization of decision-making. The final result of such a development is the "bifurcation" of global structures in state-centric and multi-centric subsystems in which states are no longer the only key actors;[21]
- *Robert Keohane and Joseph Nye on the changing nature of power:* These two scholars introduce the influential concept of "soft power", the ability to achieve goals through attraction rather than coercion, as challenging the traditional understanding of power and discuss the consequences of this. Central is the notion that "credibility" in connection with the scarcity of attention becomes this age's asymmetrical power resources;[22]
- *David Rothkopf on Cyberpolitik:* Rothkopf offers an approach to the changing nature of power by documenting the change as a transformation from the "Realpolitik" of Metternich to "Cyberpolitik", in which an ever-growing cast of actors have the power to damage or otherwise impact each other's interests. In his view three transitional conflicts affect the three traditional pillars of power: The Private Sector vs. The State Sector (economic); The Doctrine of Dominance

[20] Ibid.

[21] Rosenau, "Global Affairs in an Epochal Transformation".

[22] Keohane and Nye, "Power and Interdependence in the Information Age", 85.

vs. Advantage of Asymmetry (military); Political Institutions vs. Electronic Democracy and Virtual Communities (political).[23]

A whole string of other features are in part due to changing power structures; most notable the blurring of traditional boundaries, in more than one sense and on different levels. For example, there is a *blurring of national boundaries* due to the trans-boundary nature and architecture of global information networks in which information flows more or less freely over political borders that become porous as ideas, capital, people, technology, goods, and services move from one geographic point to another. The blurring of national boundaries has in some ways been theoretically captured by the broad pluralistic thread of thought called *Transnationalism*, of which the modernist writers are a subsection. Transnationalists are interested in interactions and coalitions across state boundaries that involve such diverse nongovernmental actors as multinational corporations and banks, church groups, and terrorist networks.[24] In addition, the blurring of boundaries is also taking place between issues: Again, it is the modernization writers in particular who believe that the distinction between domestic and foreign policy becomes blurred as domestic policy becomes foreign policy and economic and foreign policies become politicized.[25]

[23] Rothkopf, "Cyberpolitik: The Changing Nature of Power in the Information Age".

[24] Viotti and Kauppi, *International Relations Theory: Realism, Pluralism, Globalism, and Beyond*,, 210 ff. The term *transnational* is used both to label the actor, e.g. a transnational actor, or a pattern of behavior, e.g. an international organization that acts *transnationally*, meaning it operates across state borders.

[25] Viotti and Kauppi, *International Relations Theory: Realism, Pluralism, Globalism, and Beyond*, 211.

1.2 Emerging Theorems of the Information Age

The portrayal above has mentioned the majority of aspects of the emerging theorems. Most of them are 'variations' of the idea that the world experiences a change in power structures, a relocation of power, and a change in its nature. To be more concrete, the strongest characteristic of the changing nature of power in the Information Age is the growing importance of *soft power,* the ability to achieve goals through attraction rather than coercion. Five key dimensions cluster around these observations.

Theorem № 1: Key element for operating effectively within the new emerging operating environment is to achieve Information Superiority through the conduct of Information Operations

Today, information has rising importance next to traditional military capabilities. In the evolution of armed forces one of the main goals is to dominate the information spectrum: For full spectrum dominance, it is necessary to gain "*Information Superiority*". Information Superiority in turn is achieved through the conduct of various kinds of "*Information Operations*".[26] The competitive advantage of Information Superiority is derived from the ability to exploit a superior information position that will provide the commander with a near perfect picture of the battlefield so he can make nearly perfect decisions. These military ideas can also be applied to less military matters, especially since Information Operations can be conducted by a variety of actors ranging from states, companies, and criminal organizations over extra-parliamentary activist groups to individuals. If the concept is broadened, not all aspects of Information Operations can be employed by all involved actors; those, which require specialized military hardware, remain the privileges of states with sufficient hard power capabilities.

[26] Department of the Air Force, Air Force Doctrine Document 2–5 Information Operations, August 1998.

Theorem № 2: Asymmetrical Credibility is the Information Age's Key Power Resource

The premise of soft power suggests that the so-called paradox of plenty challenges the easy accumulation of power through information in our information-saturated world and turns credibility, or parallel to Keohane/Nye's earlier concept of asymmetrical interdependence, *asymmetrical credibility,* into the key resource of power in the Information Age.[27] This is true in times of peace as well of conflicts. Even though state officials generally still control a large part of the information flow in crisis situations, this monopoly is being challenged by various factors such as the availability of different information on the Internet. Officials will never lack attention during crises, but very much depends on their credibility: due to the skill revolution the respective populace is likely to exert pressure on decision-makers if their credibility seems questionable.

Theorem № 3: Traditional boundaries become increasingly blurred in the Information Age; between states, between military-politics, and between military-civilian domains

Between States: The Global Information Environment (GIE) is shaped and changed by the Information Revolution. Due to the trans-boundary nature and architecture of global information networks in which information flows more or less freely over political boundaries and in which national information infrastructures (NII) are all inseparable parts of the Global Information Infrastructure (GII) political boundaries become porous.[28]

Between Military – Politics: All military operations take place within the GIE, which is both interactive and omnipresent. It has affected the conduct of military operations in a high degree: audi-

[27] Keohane and Nye, "Power and Interdependence in the Information Age".

[28] See Department of the US Army, *Information Operations, Field Manual No. 100–6, FM 100–6*, Washington DC: 27 August 1996, online version, URL http://www.fas.org/irp/doddir/army/fm100-6/index.html.

ences throughout the world can receive information from conflict parties and instant analysis of events in near-real time and 24-hours a day. The effect is that, at any moment, real-time information can instantaneously influence domestic and international decision makers. This can translate into political pressure on national leaders to make changes in strategic goals, guidance, and objectives that directly impact military missions, policies, and procedures.[29] In the context of coalition warfare, this means that struggles between the political and military exponents of the coalition are inevitable. Even more so because due to the skill revolution, the populace's mood exerts domestic pressure on politicians, which are forced to act in accordance with these pressures at home. Politicians then increasingly try to influence the military components of the coalition, which has a direct influence on Information Operations.

Between Military – Civilian: Other implications of the emergence of an omnipresent GIE are blurring boundaries between military and civilian issues, mainly manifested in the dual-use character of most targets in the information infrastructure, and the dual-use character of new weapons and information tools that allow for Information Operations. The expansion of the battlespace to virtual space and to human perception threatens to result in more civilian involvement. Future warfare scenarios turn combat into something that is no longer an act of last resort; because there is less chance of combat casualties, a much lower cost of engaging in conflict, a blissful anonymity of strikes, it becomes much easier to commit acts of war.

[29] See for example Deutsch, Karl W., "Mass Communications and the Loss of Freedom in National Decision-Making: A Possible Research Approach to Interstate Conflicts", *Journal of Conflict Resolution,* 1, 2 (1957): 200–211.

Theorem № 4: Networks vs. Hierarchies: The Information Revolution demands a shift from centralized and hierarchical organizations and decision-making processes to decentralized and flat organizations such as networked virtual teams

Information networks are a strong defining feature of today's operating environment. The way easily available information flows through these networks changes structures in various issue areas. Traditional authority structures are undermined by the dynamics of change and their own slowness to adapt to the organizational implications of the Information Revolution. In politics, networked virtual teams are more apt to react optimal to a changing environment; the term *Network Power* stands for the ability of actors to combine hard and soft power tools in broad networked coalitions to achieve optimal outcome.[30] The flattening of hierarchical structures is also perceived by military planners: the availability and immediacy of real-time information permits the decentralization or flattening of command structures, taking control functions down to lowest practicable level of command to assure greater combat efficiency within the context of Information Superiority. The likeliness that future conflicts will increasingly be waged by networks as opposed to hierarchies is prompting militaries to reconsider how they are organized.[31] Almost of more importance than the demand

[30] Spillmann, Kurt R., Andreas Wenger, Stephan Libiszewski, and Patrik Schedler, *Informationsgesellschaft und schweizerische Sicherheitspolitik*, Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung, No. 53 (Zürich, Forschungsstelle für Sicherheitspolitik und Konfliktanalyse: 1999).

[31] Arquilla, John and David Ronfeldt, "A New Epoch – and Spectrum – of Conflict", in Arquilla, John and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, RAND: 1997): 1–20.; and Arquilla, John and David F. Ronfeldt, "Cyberwar is Coming!", in Arquilla, John and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, RAND: 1997): 23–60.

that centralized and hierarchical organizations and decision-making processes become decentralized and flat organizations is the perceived consequence of this prospect: flattening hierarchies mean a redistribution of power. One likely outcome is the multiplication of relevant actors.

Theorem № 5: Asymmetry vs. Doctrine of Dominance: Small players can harm mighty foes with the right technology and knowledge

Apart from being perceived as a tremendous opportunity, the Information Revolution has also given rise to new threats and risks (e.g. vulnerability of information networks and other critical infrastructures to terrorist attacks, hackers, and systems failures). The military fears that technology enables an ever-greater number of actors that are linked to the world through the Global Information Environment (GIE) to pursue their interests by attempting to manipulate and control the content and flow of information within the Military Information Environment (MIE), that part of the GIE, which is relevant to the military.[32] Such international asymmetries in the capacities and vulnerabilities of states have the potential to generate new interaction dynamics. Non-state actors as well as small states enter into direct effective conflict with mighty adversaries exerting an advantage of asymmetry by seeking new forms of conflicts such as computer-terrorism.

[32] Department of the Army, Information Operations, Field Manual No. 100–6, 27 August 1996.

2 Developing a Model

These five emerging theorems create a loose framework in which the circumstances that substantially influence the successful managing and waging of IACs can be outlined. They do not exist separately but interact with each other: all of them are caused by the larger set of Information Revolution induced changes but at the same time, some of their aspects additionally enforce aspects within other theorems:

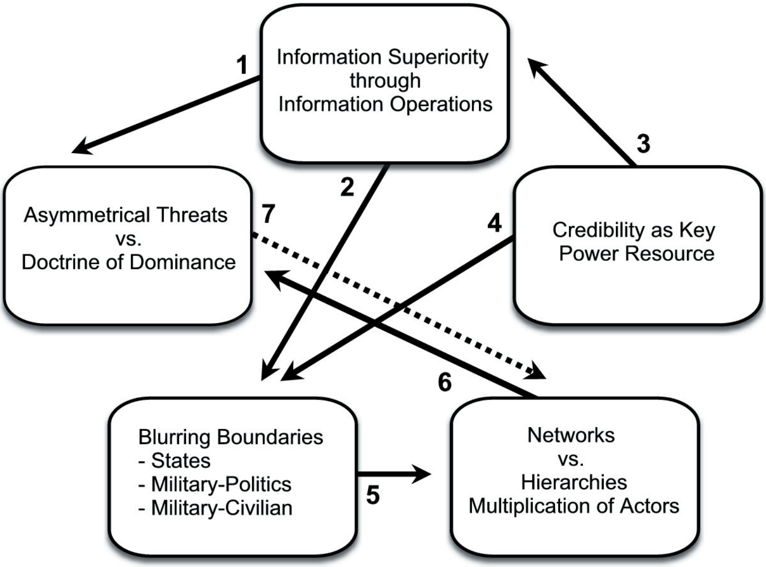

Figure 1: Interaction Between Theorems of the Information Age

Explanation of the relationships labeled with arrows 1 to 7:[33]

1) Asymmetrical threats arise for a large part due to the nature and definition of Information Operations. Some aspects of

[33] As for their ranking in importance, estimating their weight in an argument mainly depends on the specific focus of the particular study. For this thesis that strives to analyze IACs, Theorem № 1 concerned with the conduct of Information Operations is at the center of attention.

IO do not require expensive hardware but can be conducted with tools that are easily available commercially off the shelf (COTS);

2) Information Operations blur boundaries between:
   - States, due to the trans-boundary nature and architecture of global information networks that in some aspects of IO are attacked and/or taken advantage of for attacks;
   - Military – politics, because of the political urgency some of the aspects of IO inflict on the international community, this being mainly those aspects that threaten civilians and which lack a basis in international law;
   - Military – civilian domains, because of the nature of Information Operations; the dual use character infrastructure and weapons, and notions of psychological warfare that ultimately aim at the human mind;[34]
3) Information Superiority and Information Operations need to be credible if to be effective, especially those aspects of IO which have a psychological or deceptive nature;
4) Public demands for intact credibility puts more pressure on political parties, which in turn try to exert more power on military to gain the trust of their populace. This likely leads to blurring boundaries between military and political domains;
5) Blurring boundaries between states empower agile entities such as virtual networks; traditional authority structures are removed and the redistribution of power leads to a multiplication of actors;
6) Networks are asymmetrical threats to hierarchies. More actors constitute an asymmetrical threat to already existing power entities such as states;
7) Asymmetry favors networks and puts hierarchies under pressure.

[34] Cf. chapter IV.7.1 of the thesis on neocortical warfare.

According to Theorem № 1, Information Superiority is the key to winning conflicts in the Information Age. Information Superiority on the other hand is achieved through the conduct of Information Operations. Thus, deduced from Theorem № 1, there is a positive causal relationship between the struggle for Information Superiority through Information Operations and the successful managing and waging of IACs. The basic conjectured relationship between the two phenomena is that *the more ideal Information Operations can be conducted, the greater is the success of waging IACs.* Factors that hamper the conduct of Information Operations are thus also those that substantially influence the successful managing and waging of IACs.

Factors hampering the conduct of Information Operations based on the four remaining theorems can be summarized in a model of interaction between conduct of IO and success in IACs. These systemic factors impede the successful conduct of Information Operations both as a result of the emerging operating environment and of the conduct of Information Operations, as explained in Figure 1:[35]

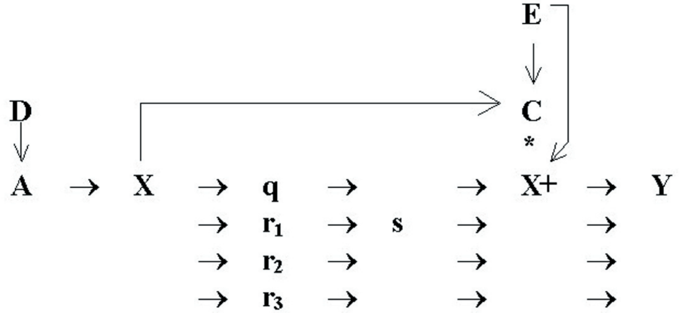

Figure 2: Arrow-Diagram of the Model Explaining Success of Information Age Conflicts

[35] On arrow diagrams plus terminology see Van Evera, Stephen, *Guide to Methods for Students of Political Science* (Ithaca and London, Cornell University Press: 1997): 7–15.

Main Variables (IV, DV):

A: Struggle for Information Superiority (Remote Cause)

X: Conduct of Information Operations (Cause)

X+: Degree of Successful Conduct of Information Operations (Independent Variable IV)

Y: Level of Success in Information Age Conflicts (Dependent Variable DV)

Exegonous Variables:

D: State of the Art of Current Military Doctrine

E: Case-Specific Influencing Factors (Not System Inherent)

Condition Variable:

C: Level of Credibility

Intervening Variables (IntV), System Inherent:

q: Degree of Asymmetrical Threats Faced

r_1: Degree of Blurring Boundaries Between States

r_2: Degree of Blurring Boundaries Between Military-Political Domains

r_3: Degree of Blurring Boundaries Between Military-Civilian Domains

s: Degree of Multiplication of Relevant Actor

Explanation:

- The model's central argument claims that the degree of successful conduct of Information Operations (Variable X+) impacts the level of success in IACs (Variable Y);
- The state of the current (military) doctrine (Variable D) that influences the way Information Operations are conducted and defined in the first place is an important exogenous variable. Change in the doctrine would have a strong influence on the model, since the waging of Information Operations to obtain Information Superiority (Variable A) is dependent on the current state of doctrine and military perception of the world;
- The Intervening Variables (IntVs q, r_1, r_2, r_3, s) that are system inherent and deduced from the identified theorems also are a consequence of the conduct of Information Operations (X) according to Figure 1. These Intervening Variables are those factors, which hamper Information Operations and therefore lessen the success in IACs;
- Subsumed under Variable E are other exogenous variables, which represent case specific influencing factors. These factors are mostly not system inherent. They consist of weather condi-

tions; geophysical dimensions (terrain); infrastructure of a country; technological factors; and the state of the international law and possible existing regimes. These factors are likely to vary considerably from case to case;

- Credibility (Variable C) is seen as the construct's condition variable; this means the values of C govern the size of the impact that the Independent Variable (IV) has on the Dependent Variable (DV). The conduct of Information Operations (X) has also a strong influence on C directly because in the context of IACs the level of credibility is measured by the way these operations are conducted;

One problem that becomes apparent in the model is that direct influences of C on other variables such as r_2 cannot be satisfactorily represented. Another insufficiency is the inability to deal with other cross-influences, mainly the triangular pattern connecting "Blurring Boundaries between States/ Multiplication of Actors/ Asymmetrical Threat" (r1 ⟶ s ⟶q). Even though the results of the analysis might suffer from this deficiency, the relationships s ⟶ q and q ⟶ s will not be made part of the model because the main focus of this thesis is on identifying hampering factors, not on analyzing how they interact.

3 Deducing the Hypotheses and Operationalization

The arrow-diagram suggests a number of possible relationships and hypotheses that help to explain the level of success in IACs:

Main chain of argument:

(D ⟶ A ⟶ X ⟶) X+ ⟶ Y: This relationship states that the current state of military doctrine influences the way Information Superiority is sought by fighting Information Operations (Theorem № 1). A positive relationship is predicted: *The higher the degree of successful conducts of Information Operations, the higher the success in IACs.*

Credibility constructs:

X →C: The conduct of Information Operations has a strong influence on the level of credibility associated with a conflict party because in IACs, credibility will be measured by the conduct of these.

E →C: The argument is that there is a connection between E and C, that *certain case specific factors influence the level of credibility associated with a party.* Each case has different set of values for E and these must be defined separately for each specific operating environment.

C * X+: X+'s influence on Y is magnified by a high value on C and reduced by a low value on C. The relationship is negative. One can predict: *The lesser the level of credibility associated with a party, the lower the degree of satisfactory conduct of Information Operations.*

Information Operations cause Intervening Variables that have a hampering effect:

These relationships have been shown above in Figure 1. The variable X is understood not as a concept that can have different values but as a factor of the system as captured in the five theorems, of more correlational than causal relationship. This unfortunately does not allow for easily testable hypotheses; though this is a flaw in the model, these relationships are embedded in the general theoretical concept that underlies the model and shall in part be elaborated further in the main body of the thesis:

X →q: The conduct of Information Operations by a conflict party within the operating environment changed by the Information Revolution leads to the rise of asymmetrical threats faced by the conflict party. (Theorem № 5 interacting with Theorem № 1)

X →r_1: The conduct of Information Operations by a conflict party within the operating environment changed by the Information Revolution leads to blurring boundaries between states. (Theorem № 3 interacting with Theorem № 1)

$X \longrightarrow r_2$: The conduct of Information Operations by a conflict party within the operating environment changed by the Information Revolution leads to blurring boundaries between the military and the political domain (Theorem № 3 interacting with Theorem № 1)

$X \longrightarrow r_3$: The conduct of Information Operations by a conflict party within the operating environment changed by the Information Revolution leads to blurring boundaries between the military and the civilian domain (Theorem № 3 interacting with Theorem № 1)

Constructs predicting the degree of successful conduct of Information Operations:

Here, the intervening variables are directly linked to the degree of successful conduct of Information Operations. The hypotheses are such in form that the variables can be assigned possible values and evidence that would falsify the hypotheses can be identified. All relationships are negative:

$E \longrightarrow X+$: *External factors like weather, terrain, and technological failure directly hamper Information Operations.* This direct connection between case specific influencing factors and the degree of satisfactory conduct of Information Operations is more likely than the relationship $E \longrightarrow C$.

$q \longrightarrow X+$: *The higher the degree of asymmetrical challenge faced by a conflict party, the lower the level of successful conduct of Information Operations by this conflict party.*

$r_1 \longrightarrow s \longrightarrow X+$: The degree of blurring boundaries between states leads to a multiplication of actors: *The higher the degree of blurring boundaries between states, the greater the degree of multiplication of relevant actors.* The more influential and relevant actors a conflict party has to deal with or *the more non-traditional actors have the ability to intervene against the wishes of a party to a conflict, the lower the level of successful conduct of Information Operations by this conflict party.*

r_2 →X+: *The higher the degree of blurring boundaries between military and political domains faced by a conflict party, the lower the level of successful conduct of Information Operations by this conflict party.*

r_3 → X+: *The higher the degree of blurring boundaries between military and civilian domains faced by a party to a conflict, the lower the level of successful conduct of Information Operations by this conflict party.*

Casting a shadow over the proposed approach to IACs is the fact that this analysis rests on one single case.[36] Even though different aspects of Information Operations provide some interesting evidence for different aspects of the model, valid conclusion in qualitative research generally requires more cases than explanatory variables.[37] Plus, we have to rely on theorems that lack consolidated theoretical backing. So, even if fairly reliable measurements can be provided, the findings cannot be generalized to other cases.

The thesis hopes to improve these circumstances by systematic comparisons of predicted and observed values. This shall be accomplished through the use of tables for each hypothesis comparing the value of the IV, the predicted value for the DV (based on the value of the IV) and the actually observed value of the DV ("congruence procedure"). The following table lists the evidence for falsification of the eight testable hypotheses: the "falsified if" column presents possible values of the Independent Variable (IV) and those of the Dependent (DV) that show that a connection between the two variables is not likely:

[36] A case is "a phenomenon for which one observes a single value for each variable in a hypothesis". See Mitchell, Ronald and Thomas Bernauer, *Empirical Research on International Environmental Policy: Qualitative Case Studies*, Studien zur Politikwissenschaft Nr. 301 (Zürich, Institut für Politikwissenschaft der Universität Zürich: 1997): 9.

[37] Ibid., 14.

Hypothesis	Falsified if				
1) The higher the degree of successful conduct of InfOps, the higher the success in IACs (X+ ⟶ Y)	IV	0 not successful	1 some successful	2 successful	3 highly successful
	DV	2 / 3 reasonable / high success	3 high success	0 / 1 low / some success	0 / 1 low/ some success
2) The lower the level of credibility associated with a conflict party, the lower the degree of satisfactory conduct of InfOs by this conflict party (C ⟶ X+)	IV	0 low credibility	1 medium	2 good	3 high
	DV	2 / 3 successful/ highly successful	3 highly successful	0 / 1 not / some successful	0 / 1 not / some successful
3) The more external factors are able to influence InfOs, the lower the level of successful conduct of InfOs (E ⟶ X+)	IV	0 low	1 some	2 reasonable	3 high
	DV	0 / 1 not / some successful	2 / 3 successful/ highly successful	3 highly successful	3 highly successful
4) The higher the degree of asymmetrical challenge faced by a conflict party, the lower the level of successful conduct of InfOps by this conflict party (q ⟶ X+)	IV	0 low	1 some	2 reasonable	3 high
	DV	0 / 1 not / some successful	2 / 3 successful/ highly successful	3 highly successful	3 highly successful
5) The higher the degree of blurring boundaries between states, the greater the degree of multiplication of relevant actors (r_1 ⟶ s)	IV	0 low	1 some	2 reasonable	3 high
	DV	2 / 3 reasonable/ high	3 high	0 / 1 low/ some	0 / 1 low/ some
6) The more non-traditional actors have the ability to intervene against the wishes of a conflict party, the lower the level of successful conduct of InfOps by this conflict party (s ⟶ X+)	IV	0 low	1 some	2 reasonable	3 high
	DV	0 / 1 not / some successful	2 / 3 successful/ highly successful	3 highly successful	3 highly successful
7) The more political parties influence military parties due to domestic pressure, the lower the level of successful conduct of InfOps by this conflict party (r_2 ⟶ X+)	IV	0 low	1 some	2 reasonable	3 high
	DV	0 / 1 not / some successful	2 / 3 successful/ highly successful	3 highly successful	3 highly successful
8) The higher the degree of blurring boundaries between military and civilian domains caused by a conflict party, the lower the level of successful conduct of InfOps by this conflict party (r_3 ⟶ X+)	IV	0 low	1 some	2 reasonable	3 high
	DV	0 / 1 not / some successful	2 / 3 successful/ highly successful	3 highly successful	3 highly successful

Table 1: Circumstances for Falsification of the Hypotheses

If co-variation is found and evidence suggests a real causal relationship and not false co-variation caused by other variables, then attention is given to providing a causal narrative of why and how the IV caused variation in the DV ("process tracing"). In examining the causal pathways that link an IV and DV it is possible to evaluate the significance of this relationship as well as gain more insight into why this is the case, a fact that will enhance the understanding of the dynamics of IACs.[38]

Necessarily, this thesis has to rely on causal qualitative analysis that captures the values of variables in words and analyzes these data through other techniques than statistical algorithms. To suffice principles of empirical research, qualitative methodology should evaluate causal relationships not by isolating them through large number of cases and statistical procedures, but by holding specific exogenous (control) variables constant through careful case selection that seeks to approximate experimental conditions.[39] This cannot be applied to this single case. Also, because this is only a one-case study, the findings will only be applicable to other cases in a very limited way. However, the same model could be utilized for other cases with the specific characteristics attributed to IACs.

Next, observable proxies (indicators) must be named. This should be done so that the construct's validity is optimized, meaning the data must relate to the theoretical construct as accurately as possible.[40] Of the thirteen conjectured relationships the smallest part can be tested in ways that suffice performance criteria for case study research. This is mainly due to the considerably ambitious outline of the thesis. Still, by means of descriptive analysis where necessary, the author hopes to gain insight into workings of IACs. The following tables lists the model's variables and names their possible values as well as observable proxies, or specifies further definitions that need to be made:

[38] Ibid., 20–24.

[39] Ibid., 5.

[40] Ibid., 19. Problems could be overcome by defining a variety of indicators for each variable, thereby resembling the values of the conceptual variables of interest more accurately and reliably.

	Variable's Role	Variable Name/ Definition	Possible Values	Indicator(s)/ Definitions
1.	Causing Variable	X: Conduct of Information Operations	—	Definition drawn from current doctrine papers; different aspects of IO are identified and each of them can be treated as separate case in interaction with the Intervening Variables
2.	Independent Variable (IV)	X+: Degree of Successful Conduct of Information Operations	0 = not successful 1 = some success 2 = successful 3 = highly successful	Values can be assigned to this variable by comparison of Information Operations aspects as defined for variable X, their ideal form compared with the actual form as observed in the case study
3.	Dependent Variable (DV)	Y: Level of Success in Information Age Conflicts	0 = low success 1 = some success 2 = reasonable success 3 = high success	Degree of how the political and military outcome of a conflict differs from the one desired. This is gained from direct comparison of (publicly) stated objectives and actually achieved ones
4.	Remote Cause	A: Struggle for Information Superiority	—	Definition drawn from current doctrine papers
5.	Condition Variable	C: Level of Credibility	0 = low credibility 1 = some credibility 2 = satisfact. credibility 3 = high credibility	Conjectured truth and honesty of public statements of the conflict parties concerning certain incidents. Depends largely on information available to judge it
6.	Exogenous Factors	D: State of the Art of Current Military Doctrine	—	Analysis of current doctrine papers
7.		E: Case Specific Influencing Factors	Influence Exerted: 0 = low 1 = some 2 = reasonable 3 = high	Analysis of case (Operation Allied Force) and definition of these case specific factors
8.	Intervening Variables (IntV)	q: Degree of Asymmetrical Threats Faced	0 = low 1 = some 2 = reasonable 3 = high	Occurrences that cannot be mastered by traditional military force and capabilities
9.		r_1: Degree of Blurring Boundaries between States	0 = low 1 = some 2 = reasonable 3 = high	• Traffic across boundaries • Penetration of boundaries
10.		r_2: Degree of Blurring Boundaries between Military-Politics	0 = low 1 = some 2 = reasonable 3 = high	• Political influence on military • Amount of force exerted by political bodies on military bodies
11.		r_3: Degree of Blurring Boundaries between Military-Civilian	0 = low 1 = some 2 = reasonable 3 = high	Amount of civilian space invaded by military operations, according to law of war and international law
12.		s: Degree of Multiplication of Relevant Actors	0 = low 1 = some 2 = reasonable 3 = high	Amount of newly involved actors that are relevant

Table 2: The Model's Variables, their Values, and Operationalization

In the following part, the Information Revolution's impact on both political and military affairs is delved into to broaden the understanding of the anticipated changes in the international system. After, part III and IV meticulously test the model and its hypotheses on the case of Operation Allied Force in Kosovo to identify those factors in the emerging operating environment that substantially influence the successful managing and waging of IACs.

Part II – Theory

Concepts to Explain a Changing International System

Part II – Theory

Concepts to Explain a Changing International System

"Information Revolution" is a term currently used by many different parties for many different facets of an elusive phenomenon, leaving the researcher with a confusing diversity of usually poorly defined concepts. Some tout the Information Revolution as a technological leap forward in which all aspects of life will be transformed. Advocates of this view argue that the deepening and extension of current developments in ICTs are set to reshape the economic basis of modern society, thereby also transforming commerce, politics, social relations, and conflicts.[1] More skeptical observers point to the limited economic and social impact of information technologies and argue that the process of change is more evolutionary than revolutionary. These observers point to the superficial impact of ICT in enhancing productivity or transforming industrial economies; they also warn against adopting a technological deterministic approach to the changing nature of society, politics, and conflicts.[2]

Generally, it is too early to resolve this debate: Some of the anticipated changes seem apparent; others still have to come fully into the open. While economic and military changes are well under way, transformations in the political system are more sluggish and lagging behind, as structures in politics tend to be resistant to fast changes, meeting the opposition of a well established elite or found-

[1] Toffler, Alvin and Heidi Toffler, *War and Anti-War* (New York, Warner Books: 1993).

[2] Cf. Kitchin, Rob, *Cyberspace: The World in the Wires* (Chichester, Wiley and Sons: 1998); or Keohane and Nye, "Power and Interdependence in the Information Age".

er on solid institutions.[3] In addition, many observe that complexity and change are the two defining characteristics of the Information Age, since the present epoch is marked by persistent opposites and derives its order from episodic patterns with very contradictory outcomes,[4] and try to describe the process by which the world appears to be simultaneously linking up and breaking apart by neologisms like "fragmegration" (fragmentation/ integration) or "glocalization" (globalization/ localization).[5]

Nevertheless, this part seeks to discuss those changes in the international system, which seems to have a lasting effect on the operating environment. It's primary objective is to discuss scholarly work that provides snapshots of various features of an international system subject to the Information Revolution. This part is divided into three chapters: Since many of the underlying assumptions of this paper build upon an understanding of the Information Revolution, the first chapter undertakes to provide a definition of this term and to discuss a number of open questions and related concepts. The second explores the shifting of existing power structures, identified as the common denominator of change. It looks at definitions of power as well as ways to measure it, deals with the nature of power in the Information Age, and finally looks at the ongoing

[3] The political world unlike the business and military world is not driven by internal or external competition, and is thus not equally eager for technological enhancement to extend its global reach: Ronfeldt, David and John Arquilla, "What if There is a Revolution in Diplomatic Affairs?", *United States Institute of Peace*, Released 25 February 1999, online version, URL http://www.usip.org/oc/vd/vdr/ronarqlSA99.html.

[4] Rosenau, James N., *Turbulence in World Politics: A Theory of Change and Continuity* (Princeton, Princeton University Press: 1990), and various articles by the same author; Center for Strategic and International Studies, *The Information Revolution and International Security*: *Robert F. McMormich Tribune Foundation Report* (Washington D.C., Center for Strategic and International Studies: 1996).

[5] Rosenau, "Global Affairs in an Epochal Transformation", 33–37.

redistribution of power in today's world. The third chapter focuses on changes in military affairs, looking closely at the current Revolution in Military Affairs and the popular concept of "Information Warfare".

1 The Background of Change: A Phenomenon Dubbed Information Revolution

This chapter is as fairly comprehensive introduction to the overall theme of the "Information Revolution". It explores the meaning of the term, touching upon the technologies that seem to drive the revolution forward, and offers a technologically focused definition of the term. One of the most fascinating aspects of the Information Revolution, discussed in the second subsection, is the Internet in all its manifold facets. The concept of an emerging "Information Society" is also examined. After considering objections raised by the concept's most virulent critics, a definition is proposed for the concept.

1.1 Characteristics of an Evolutionary Trend

"Information Revolution" is a broadly accepted term used to describe the phenomena of change observable in today's world.[6] Even though lingering doubts about its accuracy remain, its utilization has been more or less acknowledged by the scientific community. Although more precise expressions would be far more appropriate, their usual clumsiness and ungainliness disqualifies them, leaving little choice for the use of words to depict the phenomena of change. This situation confronts scholars with the need for critical assessment of meaning and appropriateness of the term "Informa-

[6] R. Solomon states that he heard the term first used by Walt Wriston, author of "The Twilight of Sovereignty", in 1977, in: Solomon, Richard H, "The Information Revolution and International Conflict Management", USIP Peaceworks, Keynote Address from the Virtual Diplomacy Conference, June 1997.

tion Revolution" as well as careful evaluation of its use: this chapter tries to explore objections as well as approvals vis-à-vis the term and attempts to provide a satisfactory definition in a social science context. It does so in three steps, separately looking at the terms information and revolution, before pulling them together.

Information: Information is seen by many as the defining feature of the modern world, being so important as to become the symbol for the age we live in. Our present time has been coined the "Information Age"[7], the present society the "Information Society", and it even looks as if information might become the very essence and manifestation of competition, conflict, and warfare in this century. Still, the use of the term has many critics: there is no uniform concept of information and its relationship with pure data and connection to knowledge is a scientific field of its own.[8] The term itself is imprecise, having a variety of different meanings for different academic disciplines: for the communication engineer information is often nothing more than organized set of data[9], for social-scientists it must have at least minimal semantic content or meaning.[10] Various characteristics make information very hard to seize or quantify and pose difficult problems for empirical research into Information Revolution matters:

- Information is abstract: it is an intangible asset and can take the form of an entity (e.g. description, measurement) or a process (e.g. encryption process, relationship);
- Information has multiple, often even simultaneous uses and intentional users;
- Information is inexhaustible and limitless, but its value is temporal: only fresh information has value for the majority of actors;

[7] This term has been introduced by the futurists Alvin and Heidi Toffler in the book "The Third Wave", in 1980.

[8] See Waltz, Edward, *Information Warfare. Principles and Operations* (Boston, Artech House: 1998): 49–81, for a good introduction of the role of Information Science in warfare.

- Information's relationship to utility is complex and non-linear, a function of potential data, content of information, and the impact of knowledge. This functional relationship from data to knowledge is complex and unique to each application of ICT.[11]

Often, the term is seen as the first level of abstraction in the "cognitive hierarchy", which is based on data. The classic schematic of the so-called "cognitive hierarchy pyramid" is data – information – knowledge – wisdom.[12] In a political/sociological context, which focuses on human interaction, information by itself has no value: it is but a raw material that gains its worth only if processed in specific ways, getting meaning and a certain quality attached to it. The possibility of its transformation into *knowledge*, which is explained and understood information, or even *wisdom*, the effective application of this knowledge, makes it such an immensely precious resource. Strictly speaking, critics thus rightly claim that it is not information that is this age's defining feature, but knowledge.

Revolution: A revolution is usually understood as a sudden, radical, or complete change.[13] Common sense makes it feel as if indeed, changes and developments all around us are rapid enough

[9] Shannon and Weaver's information theory: Information is a quantity measured in bits and defined in terms of the probabilities of occurrence of symbol. (Main work: Shannon, Claude and Warren Weaver, *The Mathematical Theory of Communications* (Urbana: 1949)).

[10] Cf. Webster, Frank, "What Information Society?", in: Alberts and Papp, *The Information Age Anthology*; online version, URL http://www.ndu.edu/inss/books/anthology1/ch04.html; or Webster, Frank, *Theories of the Information Society* (London, Routledge: 1995); or Roszak, Theodore, *The Cult of Information: The Folklore of Computers and the True Art of Thinking* (Cambridge, Lutterworth Press: 1986).

[11] Waltz, Edward, *Information Warfare*, 49–50.

[12] Cf. Arquilla, John and David Ronfeldt, "Information, Power, and Grand Strategy: In Athena's Camp – Section 1", in: Arquilla and Ronfeldt (eds.), *In Athena's Camp*, 146, 448; or Waltz, Edward, *Information Warfare*, 1, 49–56. The cognitive hierarchy is often pictured as a pyramid.

[13] Definition as given by Merriam-Webster's Collegiate Online Dictionary online version, URL http://www.britannica.com/.

to be called sudden, radical, or fundamental. A closer look reveals transformations less sudden, violent and fast, however, it being a more gradual process with neither clear beginning nor foreseeable end, making the application of the term "revolution" in its constricted sense somewhat questionable. To speak of an "evolution" would seem much more appropriate: it could give more substance to the gradual adjustment and the non-linearity of the development. Nevertheless, in the context of scientific-technical transformation the term revolution has been used less strictly:[14] definitions also include concepts that can be applied to our case, for example understood as a "fundamental change in the way of thinking about or visualizing something: a change of theorems" or more suitable even as a "changeover in use or preference especially in technology".[15]

Information Revolution: It is common knowledge that information or knowledge as crucial resources are not unique just to our time; they have always been vital to humankind. It is also commonly understood that throughout history advances in scientific-technical fields have always played major roles in changing human affairs; there have been other information and communication revolutions during the last one hundred and fifty years, all significantly shaping history, human activities, and their institutions.[16] In this sense, what gives the current Information Revolution its defining characteristics and specialties? Why does information/knowledge seem to have become so central to our times?

[14] For example the "Agricultural Revolution", "The Industrial Revolution", or "The Long Revolution" that took place from 1800–1945. cf. Waldrop, Mitchell M., "Is There an Information Revolution?", in: Henry and Peartree, *Information Revolution and International Security*, 1–9.

[15] Definition as given by Merriam-Webster's Collegiate Online Dictionary online version, URL http://www.britannica.com/.

[16] Papp, Daniel S, David S. Alberts, and Alissa Tuyahov, "Historical Impacts of Information Technologies: An Overview", in: Alberts and Papp, *The Information Age Anthology*, online version, URL http://www.ndu.edu/inss/books/anthology1/ch02a.html. The authors speak of two passed revolutions, the first involving telegraph, telephone and radio, the second television and early generation computers.

These questions are best answered by pointing out the increased speed, greater capacity, and enhanced flexibility with which data can be gathered, processed, and transmitted today. This significantly enhances humankind's ability to communicate, to utilize information, and to overcome obstacles earlier presented to communication by distance, time, and location. The technologies that make this possible are generally called *(New) Information and Communication Technologies (ICT)*.[17]

Especially the marriage of computers and telecommunications, integration of these technologies into a multimedia system of communication that has global reach, and their worldwide inexpensive availability brings about a fundamental transformation in the way one communicates and thus interacts. A secondary impact of the Revolution is heightened interest in, and exploding demand of, these technologies, resulting from, but also leading to, factors such as falling costs, increased availability, greater utility, and ease of use of these tools. This has lead to an immense proliferation of ICT, occurring unevenly but steadily throughout organizations, societies, and between international actors. A return to the ways of before is all but impossible: societies in developed countries already heavily rely on these technologies, not only for storage of information, but also for processing, with the aim to let these technologies perform more and more intelligent tasks.

For a concluding definition of what the "Information Revolution" is it seems most satisfying to consider its evolutionary, gradual process; the importance of not just information but rather

[17] Eight of the most important technologies of the current scientific-technical revolution are: Advanced computing, networking, and semiconductors; cellular/wireless technology; digital transmission/ compression; fiber optics; improved human-computer interaction; and satellite technology. Cf. Alberts, David S., Daniel S. Papp, and W. Thomas Kemp III, "The Technologies of the Information Revolution", in: Alberts and Papp, *The Information Age Anthology*, online version, URL http://www.ndu.edu/inss/books/anthology1/ch03.html.

knowledge; the wide-ranging spread of ICT; and the way information can be handled today. This generates a fairly technologically focused definition – which has vices, because the revolution is also very much about changing human factors – but nevertheless suits the ends of this thesis in an acceptable way:

> *Definition of the* "*Information Revolution*": The Information Revolution is an ongoing dynamic development that adds increased speed, greater capacity, and enhanced flexibility to the gathering, procession, and transmission of data into knowledge, hence significantly enhancing humankind's ability to communicate. Falling costs, increased availability, greater utility, and ease of use have lead to an immense proliferation of Information and Communication Technologies, the tools of the Information Revolution, making society in developed countries thoroughly dependent on them.

1.2 The Internet as Heart, Pulse and Bloodstream of the Revolution

The global decentralized communication network of computer networks is the pulse, the bloodstream, and the essence of the Information Revolution, vibrantly radiating the "suggestive power of virtual technologies".[18] It is the most popular and most amazing manifestation of ICT with its unprecedented boom, phenomenal growth rate, and the massive political, social, cultural, and economic changes stimulated by it. The Internet is a very young phenomenon measured by its ascent into commercial and public awareness in the early 90s,[19] surely one of the reasons why Internet Studies are still a new and fairly untouched field in social sciences.

[18] Term used by Virilio, Paul, "Speed and Information: Cyberspace Alarm!", *Ctheory*, 18 March 1995.

[19] According to the Merriam-Webster's Collegiate Online Dictionary, the word first appeared in 1987.

The Internet's story of success is dazzling: not only has it substantially transformed the way business is performed and the ways people interact, it has also created something one might call "*Cybercult*", by giving rise to new socio-cultural patterns such as hacker-communities, new forms of art, stipulating the imagination of designers, writers, the movie industry, overall, has come to be an essential part of many lives and source for inspiration. It creates a new dimension, a detached place that has come to be called "*Cyberspace*"[20] or "*Infosphere*".[21] These two concepts differ somewhat in their emphasis and meaning, but basically they both stand for the fusion of all communication networks, databases, and sources of information into a huge, tangled, and diverse blanket of electronic interchange; this global fusion of networks creates a "network ecosystem", a place that is no part of the normal, physical world: it is "virtual", or in other words:

> Cyberspace is a bioelectronic environment that is literally universal, it exists everywhere there are telephone wires, coaxial cables, fiber-optic lines or electromagnetic waves. This environment is inhabited by knowledge, existing in electronic form.[22]

How this newly emerging "place" affects the individual or the sociological structure as a whole cannot be given much room in this paper. Here, the question is mainly how it is transforming the environment, the settings, and the rules for the operating environment of IACs.

[20] The term was created by W. Gibson in his cyberpunk novel "Neuromancer" (1984). It was first used referring to the Internet in 1991, cf. http://keithlynch.net/timeline.html. Often when it is understood as the space computer networks create, it is called "Barlovian Cyberspace", after John Perry Barlow.

[21] Term mainly used by Vlahos, Michael, "Entering the Infosphere", *Journal of International Affairs*, 2 (Spring 1998): 497–525.

[22] Arquilla and Ronfeldt, "Cyberwar is Coming!", 41.

For one thing the Internet has a strong inclination towards the free flow of information.[23] The hacker ethics "information wants to be free" or "all information should be free"[24] are too extreme and unlikely to ever become reality. At the same time however, the Internet has already set new standards for all actors in the public sphere and presses governments and other organizations into providing more and more information online to everyone, adding transparency to many political processes.[25] This "open source" availability has increasingly given researchers, policy professionals, and interested individuals the possibility to take advantage of the Internet as a vast "library" of valuable information. The easy accessibility of information for anyone at any time is one of the cornerstones of change to the structure of the international system.

An additionally transforming factor is that information does not only flow more freely but also a lot faster in global networks; the availability of real-time information in conflicts poses a challenge to decision makers and essentially changes the work of official organizations with the media in crisis situations. The Internet is also substantially changing business transactions and financial exchange; it grows into a global marketplace for commercial and financial exchange transactions, a key economic forum for shopping, advertising, booking, and paying for services.

[23] It has been build by the military to overcome obstacles, to deliver data from one end of a network to the other, even if one or more nodes are destroyed.

[24] This popular cyber-maxim or hacker's ethic was verbalized by Steven Levy in his 1984 book: *Hackers: Heroes of the Computer Revolution* and promoted by Stewart Brand in his 1987 book *The Media Lab*. Other interesting projects for the free availability of information include the Global Internet Liberty Campaign online version, URL http://www.gilc.org/; or the Online Magna Charta "Charta of Freedom for Information and Communication" online version, URL http://sem.lipsia.de/charta/.

[25] See for example OSCE Code of Conduct on Politico-Military Aspects of Security, Budapest 3 December 1994, Chapter VII, Article 22. "Each state will (…) provide for transparency and public access to information related to the armed forces".

Many Information Age theorists and politicians claim that the Internet has democratizing effects.[26] These thoughts have also triggered a debate over "teledemocracy" and the Internet's support of increased civic participation in the democratic process.[27] Scholars usually maintain that the Internet may suppress as well as promote democracy, depending on many determining factors: future development, attractiveness, accessibility, availability, regulation of ICT, the unhindered flow of information and, very important, human behavior.[28] Three main arguments for the proliferation of global democracy can be identified; for every positive statement there is at least one negative one, showing clearly how the Internet can both extend and/or impede democracy's reach, depending on many external factors:

[26] See for example Loader, Brian D., "The Governance of Cyberspace: Politics, Technology, and Global Restructuring", in: Loader, Brian D., *The Governance of Cyberspace* (London and New York: Routledge: 1997): 1–19; Thornton, Alinta, *Does Internet Create Democracy?*, Master Thesis, University of Technology (Sydney: October 1996), Online version, URL http://www.wr.com.au/democracy/index.html; Dutton, William H. (ed.), *Society on the Line: Information Politics in the Digital Age* (Oxford, Oxford University Press: 1999): mainly 174–201.

[27] Schwartz, Edward, *NetActivism: How Citizens Use the Internet* (Sebastopol, Songline Studios: 1996). (See also "Das Internet als Alternative", Beilage Medien und Informatik, Neue Zürcher Zeitung, 15 September 2000, Nr. 215, on the use of the Internet in the 2000 American Presidential Elections) On further experiments in teledemocracy, see http://www.teledemocracy.org/.

[28] Shapiro, Andrew L, "Think Again: The Internet", *Foreign Policy* (Summer 1999): 14–27; and The Benton Foundation, "Telecommunications and Democracy", in: Alberts and Papp, *The Information Age Anthology*, online version, URL http://www.ndu.edu/inss/books/anthology1/ch14.html

Argument	Pro	Contra
It empowers individuals and traditionally suppressed speakers	It allows everyone to spread their views and opinions cheaply; therefore, it grants considerable political benefits to the individual	• Attention is an increasingly scare resource: making oneself heard is the problem, not the ability to publish • The already wealthy and powerful usually gain most attention: they have the means to attract traffic to their sites through advertisements or special campaigns • Restrictive governments may still practice censorship the "old-fashioned" way: with force
It encourages citizens around the world to participate in public dialogue	• Its decentralized structure helps individuals to bypass obstacles • Its nonproprietary nature suggests openness and public purpose • Information flows freely and to everyone who seeks it	• Computer codes and programs are bendable → governments or corporations desiring to filter and restrict access to certain information can do so easily • Normal Internet user might not be aware of such filtering action → certain information might not be there even for those who actively seek it • Internet is no means against political disinterest
It enhances cross-cultural understanding and empathy	• Dialogue with people from all over the world is possible • It creates the sense of a "global village" and a virtual community	• Internet allows individuals to filter and personalize information → they might rather use information to reinforce existing political beliefs than to learn different views • Virtual gated communities can be built where there is no interaction with people who are different from ourselves[29] • Existing prejudices will not be washed away by the Internet

Table 3: Pro and Contra Arguments for a Democratizing Effect of the Internet

All too euphoric prophets of the Internet's many virtues tend to forget that it is entirely shaped by human beings, by itself no more than a vessel, a means to distribute content. The Internet will never have the ability to change human basic psychology and thus, the human factor remains the most challenging, uncertain, and most important part of the equation.

[29] In social psychology this is called "selective avoidance".

1.3 Implications for the Individual and Society

Even though analyses of international relations and security often tend to exclude sociological issues, the Information Revolution's twin concept on the societal level, the "Information Society", deserves special attention since many noteworthy changes having effect on the operating environment of IACs happen on the individual or group level. For example, the individual gains more influence in the process of the revolution, a fact that has a significant impact on the overall structure of the international system. Like the Information Revolution the "Information Society"-idea is a debated concept. For a start, there are at least three primary views on how technology and society interact:

- Technology causes change in society, with society having a minimal influence on technology;
- Society and its values drive technology in certain directions. Technology is therefore subsidiary to society and its values;
- The relationship between technology and society is intricate and complex. Technologies generate shifts in human thinking and social organization and vice versa. Either can influence the other to move in different directions.[30]

Even though the first and the second view have some appeal in certain circumstances, the third best displays the full range of complexity that is a feature of the Information Revolution. The Internet itself is a proof for the evolutionary interdependence of technology and society; technical innovations are a consequence of society's demand, as is the development of countless tools to facilitate life on the Net, and new forms of interactions emerge among Internet-users what again creates new demand and technological innovation.

[30] Porter, Alan L (ed.), *A Guidebook for Technology Assessment and Impact Analysis* (New York, North-Holland: 1980); and Papp, Daniel S and David Alberts, "Preface: Technology and Change in Human Affairs", in: Alberts and Papp, *The Information Age Anthology*, online version, URL http://www.ndu.edu/inss/books/anthology1/preface.html.

On the other hand, that does not necessarily mean that we are witnessing the emergence of an "Information Society" that is markedly different from previously existing societies. Some scholars, even though admitting that information has taken on a special significance in the modern era, insist that the form and function of information is subordinate to long established principles and practices, that the central feature of the present is its continuity with the past.[31] Frank Webster for example warns from leaping to hasty

Definitions of Information Society	Major Proponents	Main Arguments
Technological	• Alvin Toffler • Christopher Evans • James Martin	• Breakthroughs in information processing, storage and transmission as well as falling costs have led to the application of ICT in all corners of society • Convergence of telecommunications and computing leads to networking and thus growing connection of all parts of society
Economic	• Fritz Machlup • Peter Drucker • Marc Uri Porat	• Shift from an economy of goods to a knowledge economy • Knowledge and organization are the prime creators of wealth
Occupational	• Daniel Bell • Marc Uri Porat	• More and more people employed in third sector (white collar workers) • Decline of industrial labor
Spatial	• John Goddard • Anthony Giddens • Manuel Castells	• Information Networks that connect locations have dramatic effects on the organization of time and space • Integration of national and regional economies • "time/space compression"
Cultural	• Jean Baudrillard • Thoedore Roszak	• Increase of information in social circulation • Intrusion of information into everything, growth of institutions dedicated to spread of information • We live in a media-saturated environment

Table 4: Five Major Thematic Definitions of the Information Society[32]

[31] See Webster, "What Information Society?", and Witol, Gregory, "International Relations in a Digital World", in: Campen, Alan D. and Douglas H. Dearth (ed.), *Cyberwar 2.0: Myths, Mysteries and Reality*, online book, available at www.infowar.com, 2000, for more details.

[32] Webster, Frank, "What Information Society?", and more comprehensive Webster, *Theories of the Information Society*.

conclusions about an Information Society stimulated by the Information Revolution. He criticizes underdeveloped definitions of the concept and the vagueness of the operational criteria and methodology practically all Information-Society-theorists are guilty of. Definitions of the Information Society usually emphasize one of five characteristics of change. Table 4 lists distinctions between technological, economic, occupational, spatial, and cultural analytical definitions of the Information Society and their different emphasis on exactly what marks the new.

By comparing these five analytical dimensions Frank Webster comes to the conclusion that there are immense difficulties in "measuring" the Information Society. He most of all stresses that information by itself has no significance or value, and that it is crucial to take into consideration the meaning and quality of information, not just its quantity. He accepts that as a heuristic device the term has value in exploring features of the contemporary world but is too inexact to be acceptable as a definitive term.

His findings are thus similar to what has been noted in chapter I.1: even though lingering doubts over the accuracy of the term remain, the force of the habit and its general acceptance seem reason enough to further employ it in order to depict a society that is subjected to the Information Revolution. A definition has to take into account the critique brought forward by Webster, as well as considering that the Information Society envelops only certain parts of the populace, though growing with the ongoing dynamic process of the Information Revolution.

> *Definition of the* "*Information Society*": The information society is that part of society that experiences an Information Revolution. It is a society increasingly dependent on ICT and in which the regular utilization of ICT is the standard. It relies already largely on ICT for work, for economic transactions, every-day life, their well-being, for comfort, and personal interaction.

In the future, further digitalization of the media, proliferation of more sophisticated, increasingly cheaper hardware, the shrinking of devices, and other consumer-friendly innovations will bring on an increased "informatization" of life in the industrialized world and thus more and more people will become part of the Information Society.

More often than not the emergence of the Information Society is celebrated enthusiastically. But such a society is also likely to face certain dangers, challenges, and problems: apart from vulnerabilities that spring from the growing dependency on ICT, the dangers connected with so called information warfare and new kinds of terrorism that aim at the information infrastructure, the Information Society is also challenged by problems stemming from the proliferation of ICT itself, some of which have a certain importance for the case study. One of these problems is "information overload": the ability to have almost unlimited amount of information often impairs the ability to understand it; the important cannot be distinguished from the unimportant and too large amounts of information simply cannot be absorbed. The explosion of information might even lead to a devaluation of the content it carries, to a "collapse of meaning".[33] Two basic types of information overload can be distinguished: too much information that matters for a human being to grasp; or "information entropy", which is very poorly organized information, so that it cannot be used.[34]

A second problem concerns the quality of information, more precisely the considerable difficulty of distinguishing between false and valuable information. "Bad" or even damaging information

[33] Shenk, D., *Data Smog: Surviving the Information Age* (San Francisco, Harper: 1997): 35–50. Shenk even asserts that information overload leads to health problems, like increased heart and blood pressure, because the glut of information is so confusing and the inability to manage it leads to frustration!

[34] Jordan, Tim, *Cyberpower. The Culture and Politics of Cyberspace and the Internet* (London, Barnes and Noble: 1999):117–127.

flows just as fast and uncontrolled as does the good and it flourishes mostly were knowledge and likewise judgment is sparse. Outright manipulation of information or propaganda is not a new phenomenon or specific to the Information Revolution, but the speed with which information is circulated today and its broad distribution add a delicate dimension to the problem.[35]

Some virulent critics of ICT propose a list of other hazards that are less discernible and tangible and sometimes even outright belittled. Among those dangers lists "loss of orientation"[36] or the likely disturbance in the perception of what reality is or means. Modern war fighting capacities already pose certain aspects of this problem to soldiers of high-tech forces. The more of our senses can be attached to or simulated by computers the more likely certain nightmarish cyberspace scenarios of disturbance of reality actually become.

2 Redistribution and Changing Nature of Power

This chapter tries to explore the changing nature and new meaning of power in the Information Age. This is achieved by looking at definitions of a number of influential "power theorists", each offering a different approach to the subject. Three different methods on how to empirically observe power are introduced, though without being further applied. A second chapter focuses on the changing nature of power, identifying ICTs as today's ultimate and most important power resources. The increasing importance of "soft power", the ability to achieve goals through attraction rather than coercion, is examined after that. The chapter concludes with ideas on the redistribution of power.

[35] Rothkopf, David J., "The Disinformation Age", *Foreign Policy*, 114 (Spring 1999): 83–96 looks at misinformation in economic matters.

[36] Paul Virilio is among the most violent critics of technology and stresses these problems in all his publications.

2.1 Definitions and Measurement of Power

Power in the abstract is an elusive concept, especially if it wants to be applied to social or political science matters. Table 5 lists a sample of the most important power concepts and theories in the context of the paper. They include power as the possession of individuals, as the constituent of social order, power as domination, and the concept of asymmetrical interdependence as the main source of power in a changing international system:

Power Theorist	Main work	Concept of Power
Max Weber	Wirtschaft und Gesellschaft	• Power as the possession of individuals • It is intentional; it is the capacity to produce desired outcomes • It needs resistance to manifest itself. It is a negative phenomenon: it forces actions that are against the will of someone
Barry Barnes	• The Nature of Power • The Elements of Social Theory	• Power as the constituent of social order: the result of interactions between knowledgeable individuals • Power is capacity for action created by collectively held knowledge • Structures that constitute a society are the result of the knowledge individuals have of those structures and of the consequences actions will likely have • Knowledge and power are essentially the same
Michel Foucault	Les mots et les choses. Une archéologie des sciences humaines	• Power as domination, strategies that situate subjects as dominated or dominator • Power cannot be defined completely but only as an analytics or methodology for studying it, which then allows the analysis of different strategies of power • It is constituted in tactics that insinuate everyday life and create an overall strategy, but for which there is no overall guiding will, either individual or organizational • It is multiple and productive, not merely a battle or repressive
Nye/Keohane	Power and Interdependence	• Asymmetrical interdependence is the main source of power • Power as control over outcomes and resources • Two dimensions of interdependence: sensitivity and vulnerability. Manipulation of this interdependence can be an instrument of power • Bargaining processes translate power resources into power over outcomes

Table 5: Theories and Concepts of Power[37]

[37] Jordan, *Cyberpower. The Culture and Politics of Cyberspace and the Internet*, 9–19.

Even for the Realist, for which power is the core concept, there is no clear consensus on how to understand power: Some hold it to be the sum of military, economic, technological, diplomatic, and other capabilities at the disposal of the state. Others see power not as an absolute value determined for each state, but as capabilities relative to the capabilities of others. These two approaches assume a static view of power; Power as a dynamic concept focuses on the interactions between states, mainly their willingness to use their capabilities as well as the perception of other states of this willingness.[38] Consistent with these three different perceptions, scholars who focus on power in the international system have proposed three different approaches on how to measure power in order to use it as an analytical concept: to view power either as a resource, as a relationship, or as a structure:[39]

- Realist theories often rely on the *power as a resource* approach. Power is measured in terms of certain capabilities, which are a function of control over specific types of resources, as for example land, population, energy, etc. In recent years, technological capabilities have become increasingly accepted as important power resources;[40]
- In the *power as a relationship* approach, power is measured in terms of interactions between pairs of social actors. It can

[38] Viotti and Kauppi, *International Relations Theory: Realism*, *Pluralism*, *Globalism*, *and Beyond*, 64–65.

[39] Hart, J.A., "Three Approaches to the Measurement of Power in International Relations", *International Organization*, 30, 2 (Spring 1976): 289–305.

[40] A.F.K. Organski, for example, has argued that gross national product, or national income, is the best index of national capabilities. (Organski, A.F.K., *World Politics*, 2nd edition (New York, Alfred A. Knopf: 1968) J. David Singer and his associates emphasize military, industrial, and demographic capacities. (Singer, David J, Stuart Bremer and John Stuckey, "Capability Distribution, Uncertainty, and Major Power War, 1820–1965", in: Russett, Bruce (ed.), *Peace*, *War*, *and Numbers* (Beverly Hills, Sage Publications: 1972): 21–27).

result from either coercion or persuasion. The difficulty with this approach is that measurement requires knowing both A and B's preferences, before and after the interaction;

- The *structural power approach* takes into consideration that international actors seem to be thinking more about the larger set of norms, rules and procedures that govern the world political and economic systems now that the Cold War is over. They are thus more interested in exercising structural power, a power, which is less visible, since the possessor of power, which is relative in the relationship of partners, is able to change the range of choices open to others without apparent use of pressure.[41]

The structural power approach, this will be shown later, is describing this age's mechanisms for exercising power best. Basically, mechanisms have been shifting from relational power to structural power because of certain new characteristics power seems to take on in the Information Age. This is shown in the next chapter.

2.2 The Nature of Power in the Information Age

Power in politics is often divided into three subsections: economic, military, and political power. All three are the pillars on which the ability of nation states to achieve their goals rests. Economic power is derived from the resources within a state's boarders and the aptitude to trade them, military power from ready availability of people and material, and political power is drawn from the potency of leaders and institutions, the people's support as well as the endorsement from other nation states.[42] The traditional Realist political science view in a basic form is that military power dominates other forms, and that states with the most military power therefore dominate world affairs. This interpretation of the Realist school was critically

[41] Hart and Kim, "Power in the Information Age".

[42] Rothkopf, "Cyberpolitik: The Changing Nature of Power in the Information Age", 325–326.

confronted as early as 1977, mainly as a reaction to observations about a changing economic world.[43] Since then, the resources that produce power capabilities have become even more complex; today, the three "pillars of power" are being shaken by the growing influence of ICT on international relations.

Control over knowledge, beliefs, and ideas are increasingly regarded as a complement to control over tangible resources such as military forces, raw materials, and economic productive capability. Often, one hears that "information is power". In a political science view this is the case because information reduces uncertainty and can result in an asymmetrical advantage over others with less information at hands. ICTs, which help to accumulate information that can be turned into knowledge, therefore are today's ultimate and most important power resource. Economic instruments too have gained growing importance for exercising power; this mainly empowers multinational corporations and other business entities; they cannot compare with military force in their coercive and deterrent effects however.[44] The most influential and most cited article on the topic is Keohane and Nye's "Power and Interdependence in the Information Age".[45] Practically every other scholar writing on related subjects has taken up their description of the growing importance of *soft power* in all aspects of international relations:

> Soft power is the ability to achieve goals through attraction rather than coercion. It works by convincing others to follow or getting them to agree to norms and institutions that produce the desired behavior. Soft

[43] Keohane and Nye, *Power and Interdependence: World Politics in Transition*; Nye, Joseph S. Jr. and William A. Owens, "America's Information Edge", *Foreign Affairs* (March/April 1996): 22; Bell, Daniel, "Thinking Ahead", *Harvard Business Review*, 26 (May/June 1979): 26.

[44] Nye, Joseph S. Jr., "U.S. Security Policy: Challenges for the 21st Century", *USIA Electronic Journal*, 3, 3 (July 1998).

[45] Keohane and Nye, "Power and Interdependence in the Information Age", 85.

> power (…) depends largely on the persuasiveness of the free information that an actors seeks to transmit.[46]

The importance of soft power in both behavioral and resource power springs from the changed international system after the Cold War. As previously noted, international actors nowadays seek to exercise forms of structural power, exercised without apparent use of pressure to alter the range of choices open to the others. For this, the notion of soft power tools is crucial.

The importance of soft power also has other implications for the nature of power: Of particular interest is the so-called paradox of plenty, then "a plenitude of information leads to a poverty of attention".[47] It is thus that all information providers struggle for *attention*, which consequently becomes one of this age's scarcest resources; the scale of this struggle depends on the attributes of the prevailing market. It makes little sense to measure power as a resource by just counting numbers or penetration of ICT, since "information power" flows to those who secure attention, not to those with the highest numbers in technological assets, equipment, or hardware. Attention is further closely related to *credibility:* In an almost totally transparent world, those who can best edit and credibly validate information get the most attention because their information also appears the most valuable. Parallel to Keohane/Nye's earlier concept of asymmetrical interdependence, *asymmetrical credibility* is the new emerging key resource of power in the Information Age.[48]

[46] Ibid.

[47] Ibid., 88–93.

[48] Nye, Joseph S. Jr., *Bound To Lead: The Changing Nature of American Power* (New York, Basic Books: 1990).

2.3 The Redistribution of Power

Most scholars agree to some extent that the Information Revolution leads to a shift in power structures. They disagree however on the degree and the exact nature of this change. While some say that the notion of state sovereignty is rapidly eroding in the world of the 21st century, others, mainly Realist thinkers, cautiously question the necessity of redefining customary notions of national security and players in the international power game. Their strongest objection is that the most pungent of all forms of power remains the military pillar and therefore changes are not as thorough as Liberal thinkers like to predict. It is still the state that has the information advantage most of the time: strategic information is not widely available and actors other than states mostly lack the abilities and resources to collect and edit specific information. Also, information must flow in a political space that is already occupied and exist in the context of existing structures and by itself has no power to substantially change them.[49]

Nevertheless, arguments in both camps usually run that the main locus of power resources has shifted from military, to economic, and now to informational resources as noted in the previous chapter. Transfer of authority is going in diverse directions through "fragmegrative" dynamics,[50] creation of wealth today happens through ideas, knowledge, and opportunity. Power increasingly flows to centers of innovations and technological know-how and on the individual level to a new kind of technological elite, those specialists who control or master ICT through extraordinary skills or ideas.

Two central conflicts that reveal the nature of the ongoing redistribution of power are discussed in some more detail below: first the idea that with the emergence of a global electronic marketplace

[49] Keohane and Nye, *Power and Interdependence: World Politics in Transition*.

[50] Rosenau, "Global Affairs in an Epochal Transformation", 37.

comes the inevitable collapse of the state's economic pillar of power as companies increasingly become global citizens and economic boundaries no longer correspond to political ones,[51] second, the notion that the Information Revolution empowers new forms of international actors, such as NGOs and activists, thus challenging the state's status as the major player in the international system.

2.3.1 Growing Economic Interdependence and Virtual States

Because economically fostered interconnections between states as well as the move towards the service sector by most developed countries seems to have such a big effect on the current conduct of international relations, the changing economic substructure becomes exceedingly important for considerations of change in the operating environment. In contrast to most of the political and some military changes, the economic revolution has started a lot earlier and is well underway. Three key points can be distinguished:

- The future of the economy belongs to *intangible assets*: knowledge and thus the flow of information is already considered to be the most valuable resource in this world;
- The economy is *dependent on networks*: ICT have substantially changed business transactions and financial exchange: they already take part largely in a "virtual" environment that is also becoming a key economic forum for shopping, advertising, booking and paying for services;
- ICT intensify *economic interdependence between states:* the phenomenon, which is often called "globalization", is not brought on by ICT alone, but is strongly helped and furthered by them.

Economic interdependence is usually one of the strongest arguments to prove that something in the international system is changing. Of importance is also the notion that the state's loss of control

[51] Rothkopf, "Cyberpolitik: The Changing Nature of Power in the Information Age", 331–356.

over economic transactions and new creation of wealth is resulting in redistribution of power. The importance of knowledge and information as a resource for wealth has lead to the idea that the future might belong to "virtual states" with little military power and natural resources, hardly any agriculture and manufacturing, but smartly skilled in using managerial, financial, and creative tools to use assets in foreign countries.[52]

Interstate violence is likely to decline, mainly because the Information Revolution knits countries closely together, but also because traditional hard power military conquest in such an environment seems incongruous; armies can only seize real estate which does not confer knowledge or capital and is basically worthless for the virtual state.[53] As for inner-state conflicts arguments run that countries will exist for a long time at different states of industrial or virtual maturity and that among some of the lesser developed states conflicts will still occur, but will be increasingly eliminated as they move up the "virtualization" ladder.[54]

Most remarkable about this idea is that the ultimate competition among these entities will be the competition for information resources: developed nations struggle no longer for political dominance but for their share of world output. These states do not need and will not desire additional territory, because well educated labor, capital, and information triumph over the old factor land.[55] However, this view clearly fails to address new threats that arise from increased dependencies on ICT and increased vulnerabilities that can be exploited by other actors. Means of "Information Warfare" constitute an excellent tool in any level of conflict, very much so also between "virtual states". New conflict dimensions of a trade

[52] Rosecrance, Richard, *The Rise of the Virtual State. Wealth and Power in the Coming Century* (New York, Basic Books: 1999): 4.

[53] Ibid., 15–18.

[54] Ibid., 57–82.

[55] Ibid.

and economics nature, concerning for example intellectual property issues, will become more and more important in the future.

2.3.2 Multiplication of Influential International Actors

Whether the Information Revolution is challenging the state's function and status as a prime actor is one of the most excessively discussed topics among Information Revolution scholars. Those taking up extreme positions announce that "global villages" and non-territorial actors will make the nation state altogether obsolete.[56] Even though such radical conversions are implausible, the state's primacy as the central actor in international affairs is indeed being challenged by ICT: it shows difficulties in keeping up its role as a provider for security and economic well being for its population, two of the state's main duties. For example, states fail to provide substantial security against the threats of information warfare and "cyber-terrorism", and since economic activity is increasingly being conducted beyond the confines of individual states, their ability to ensure and control it is being further reduced. Because of ICT, international actors not restricted by geography, such as multinational corporations (MNCs) and some non-governmental organizations (NGOs), increasingly gain the ability to act internationally with little regard to the requests of states.[57] Claims for transparency of political process push governments and state-like organizations into providing easily accessible information, leading to the loss of the traditional information monopoly of states and their institutions.

[56] See so called modernist or "prophetic" writings, Drucker, Peter F., *The New Realities: In Government and Politics, in Economics and Business, in Society and World View* (New York, Harper Collings Publisher, 1989); and Toffler publications.

[57] Papp and Alberts, "The Impacts of the Information Age on International Actors and the International System"; Nichiporuk, Brian and Carl H. Builder, "Societal Implications", in: Arquilla and Ronfeldt, *In Athena's Camp*, 295–314.

But this does not mean that the state is in any imminent danger of disappearing: Governments all around the world are already reacting to the Information Revolution and try to redefine their role in a changing international system. The emergence of "E-government" ideas is just one of the visible outcomes of states' efforts to embrace new ideas and adjust their functions.[58] Other endeavors are the assessment of the ways ICT can help mediate the communication processes that are essential to conflict management and resolution, the development of "virtual diplomacy" abilities,[59] and of course efforts to create means to protect vital national information infrastructures. Also notable are attempts to build "global public policy networks", alliances of government agencies, international organizations, corporations, and elements of civil society that join together to achieve what they cannot accomplish alone.[60]

The Information Revolution not only affects the role and position of states but also position and influence of other actors in international affairs. These are mainly international governmental organizations (IGOs), multinational corporations (MNCs), and non-governmental organization (NGOs), as well as considerable influence on the role of the individual. The strengthened position of the individual can be explained by the expansion of the individual's diagnostic capabilities thanks to the advance of ICT, letting citizens become more competent and analytically skillful. This development has been labeled "*skill revolution*".[61] Table 6 shows how the Information Revolution changes these actor's role and function and lists the results of these changes on the status of the specific actor.

[58] See for example: The Economist, "A Survey of Government and the Internet: The Next Revolution", The Economist, 24 June 2000.

[59] Virtual diplomacy are social, economic and political interactions that are mediated through electronic means rather than face-to-face communication.

[60] Cf. Reinicke, Wolfgang. H., "The Other World Wide Web: Global Public Policy Networks" *Foreign Policy*, 117 (Winter 1999–2000): 44–56.

[61] Rosenau, "Global Affairs in an Epochal Transformation", 42–45.

Because the redistribution of power occurs unevenly on different levels, different speeds and times, it will most likely have its outcome in a skewed, complex, and volatile distribution pattern.[62]

Actors	Changes Induced by the Information Revolution	Result
States	• The Information Revolution significantly affects states' ability to provide for the security of its population against the threat of information warfare • Economic activity is increasingly being conducted beyond the confines of individual states → this affects their ability to provide for economic well being of their population	• Loses primacy of central actor in international affairs • Other international actors gain considerable influence • State needs to redefine itself
International Governmental Organizations (IGOs)	By transcending state boundaries IGOs can undertake tasks that states on their own can not accomplish successfully	Possibly migration of more responsibility from states to IGOs
Multinational Corporations (MNCs)	• Already largest users of ICT; remain central in the usage and development of them • Trend toward "glocalization" of business accelerates • Increasing ability to act internationally beyond confines of states	Enhancement of the role MNCs play in international affairs
Non-Governmental Organizations (NGOs)	• Networks allow to reach scattered members • Proliferation of NGOs because of low costs of ICT • Possibility of entirely "virtual organizations"	NGOs become increasingly active, better coordinated and more influential
Individuals	• Citizens become more competent and analytically skillful • Skill revolution empowers individuals to have more direct impact on governments	Individuals exert more direct force on governments through (domestic) pressure
Redistribution of Power Relationships (skewed, complex, and volatile distribution pattern)		

Table 6: Impact of ICT on the Pattern of International Actors

It has been noted before that complexity seems to be one of the defining characteristics of the Information Age. At the center of this growing complexity are the empowerment of the individual and the resulting relocation of authority. The "skill revolution" is

[62] Papp and Alberts, "The Impacts of the Information Age on International Actors and the International System"; Solomon, "The Information Revolution and International Conflict Management"; Wriston, Walt, Bits, "Bytes and Diplomacy", USIP Peaceworks, Keynote Address from the Virtual Diplomacy Conference, June 1997.

the principal driver: as it lets citizens become more competent and analytically skillful, they demand more influence, which can lead to a relocation of authority or the decentralization of decision-making. A considerable list of contradictory phenomena further adds to complexity: The Information Revolution empowers individuals as well as elites; it breaks down hierarchies and creates new power structures; it has a fragmentizing as well as an integrating effect; it amplifies the capacity to analyze but reduces reaction times; it offers better information but also more questions about authenticity and security.[63] The final result of such a development might well be a "bifurcation" of global structures in state-centric and multi-centric subsystems in which states are no longer the only key actors.[64] This new world power structure is still in its founding, inviting speculation on how the end product will look like.

3 The Information Revolution's Impact on Military Affairs

This chapter investigates the Information Revolution's effects on military affairs, how the military reacts to these changes, and what the consequences are for the waging of IACs. It is divided into two chapters. The first subsection takes a look at the current Revolution in Military Affairs that takes place against the background of a larger historical watershed involving the end of the Cold War and the advent of the Information Age. It is characterized by rising importance of information in the strategic world next to traditional physically based military capabilities and the advent of a number of new strategic concepts, such as "Information Superiority" as key to winning wars. The Information Revolution seems to create abundant new opportunities for those who master it, but at the same time, it creates new security threats and vulnerabilities for

[63] Rothkopf, "Cyberpolitik: The Changing Nature of Power in the Information Age", 327–328.

[64] Rosenau, "Global Affairs in an Epochal Transformation", 41–51.

those heavily dependent on ICT. Activities in the information environment against adversaries are usually subsumed under the term "Information Warfare", the next subsection's focus.

3.1 Revolution in Military Affairs: New Strategic Environment, New Strategic Concepts

In the sphere of defense, an American-lead revolution in military affairs dominates the debate on how the Information Revolution changes military affairs. It refers to the strategic, operational, and tactical consequences of the marriage of systems that collect, process, and communicate information with those that apply military force, seeking to transform armed forces and war fighting by digitizing the battlespace and adopting new doctrine and organizational forms. It is driven by three primary factors: rapid technological advance; the end of the Cold War; and a decline in defense budgets.[65] Beginnings of the current RMA can be traced back to the late 1970s, when the development of precision-guided munitions (PGM) and off-board sensors marked the beginning of the fusion of high-tech systems with conventional weapons.[66] In the early 1980s, Soviet officials started speaking of a "military-technical revolution"; the concepts they developed were adopted by the Americans and exploited for their own debate that took off in the early 90s.[67]

[65] Tilford, Earl H. Jr., *The Revolution in Military Affairs: Prospects and Cautions*, Strategic Studies Institute (Carlisle Barracks, Strategic Studies Institute: 1995): 2.

[66] Libicki, Martin, *Illuminating Tomorrow's War*, Mc Nair Paper 61 (Washington, D.C., National Defense University: 1999), online version, chapter 1, URL http://www.ndu.edu/inss/macnair/mcnair61/itech01.html.

[67] The debate was led by Marshal Nikolai Ogarkov. Of major importance is his seminal paper published in 1982. Cf. Cohen, Eliot, "A Revolution in Military Affairs", *Foreign Affairs*, 75, 2 (March/April 1996): 39; David, Norman C., "An Information-Based Revolution in Military Affairs", in: Arquilla and Ronfeldt, *In Athena's Camp*, 84–85; Cooper, Jeffrey R., "Another View of the Revolution in Military Affairs", in: Arquilla and Ronfeldt, *In Athena's Camp*, 123 ff. and many others.

It was the Gulf War that first popularized a high-tech, low-casualty, sterile form of warfare; the current RMA is an attempt to make the most of the strategic possibilities that were revealed. American experts believe that it will reinforce established tendencies towards military capabilities far superior to that of any other country or even of any group of countries, according to what has been called "America's Information Edge".[68] They hold that speed, knowledge, and precision will minimize casualties and lead to the rapid resolution of wars, thus minimizing the problems associated with the challenges to the political utility of force, reducing risks far enough to maintain public support for military operations.[69] The central resources of conflicts is shifting from the physical weapon to the abstract information processes and contents, moving the object of warfare from the tangible realm to the abstract.[70]

A revolution in military affairs can be understood as a fundamental change, or discontinuity, in the way military strategy and operations are planned and conducted. It can be driven by technological innovation, operational innovations, societal changes, or a combination of these factors.[71] All the passed RMAs have developed in similar ways:[72] Emerging and enabling new technologies are adapted for military purposes and integrated into existing

[68] Nye and Owens, "America's Information Edge", 20–54.

[69] Metz, Steven, *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare* (Carlisle Barracks, Strategic Studies Institute: April 2000), online version, URL http://carlisle-www.army.mil/usassi/ssipubs/pubs2000/conflict/conflict.htm (electronic pdf-version without page numbering).

[70] Waltz, Edward, *Information Operations*, 10.

[71] Cooper, "Another View of the Revolution in Military Affairs", 117–123.

[72] The current RMA is merely the latest in a series of such movements. On earlier RMAs see for example Krepinevich, Andrew F., "Cavalry to Computers – The Patterns of Military Revolutions", *The National Interest*, 33 (Fall 1994): 30–42 or Van Creveld, Martin, *Technology and War, From 2000 BC to the Present* (New York, Free Press: 1989).

structures in the first phase; military doctrine and organizational changes are made to suit the new capabilities in the second; leading in a third and final stage to the emergence of notably different ways of looking at military operations and the conduct of war.[73] Presently, development seems to have advanced to a stage somewhere between the first and the second phase.

Currently, the RMA is an umbrella concept that encompasses a variety of issues without a clear definition, a clear indication that it is far from over. The most important of those issues, taking up key positions in the debate, are Information Superiority, the System of Systems, new forms of conflicts, and network centric warfare. The following chapter gives a short introduction to the concept of "*Information Superiority*". The second section discusses *Cyberwar and Netwar*, both new forms of warfare. It concludes by showing how the Information Revolution is forcing the military to reconsider its organizational structure.

3.1.1 Information Superiority as Key to Winning Wars

The future of warfare is sometimes characterized by high speed and adaptability plus agility, both features brought on by accurate and timely information.[74] Some even argue that as a result of the development of ICT, warfare will cease to be a force-on-force experience, but will increasingly be characterized by hide-and-seek,

[73] Dearth, Douglas, "Imperatives of Information Operations and Information Warfare", in: Campen and Dearth, *Cyberwar 2.0: Myths*, *Mysteries and Reality*.

[74] See van Creveld, Martin, *The Transformation of War. The Most Radical Reinterpretation of Armed Conflict Since Clausewitz* (New York, Free Press: 1991), for an analyses on twentieth century influences of technology and the limits of technology in future physical and ideological low intensity conflicts; Scales, Robert H Jr., *Future Warfare* (Carlisle Barracks, Strategic Studies Institute: 1999); Metz, *Armed Conflict in the 21st Century*.

with the seekers having the edge.[75] The Information Revolution is seen to change combat in three essential ways:[76]

- In the war fighting terminology, the expression "*Battlespace*" replaced the traditional term "*Battlefield*" to communicate the impression of the battleground encompassing more than just the traditional physical theater, but also the information spectrum, including virtual ("cyberspace") dimensions;
- It changes the nature of combatants in the battlespace: civilians play an increasingly important role for the running of operations;[77]
- It leads to the loss of privacy and remoteness of armed forces in combat: television has captured the initiative in defining the context in which events take place, how they are proceeding, and how the military is performing.[78]

The Gulf War implied that the ability to "see" the battlespace is the key to victory in this new emerging environment. The main goal of the RMA as the future evolution of armed forces is thus to *dominate the information spectrum*: For full spectrum dominance, which is the effective application of military power by information-based planning and execution of military operations, it is necessary to gain "*Information Superiority*".[79] Information superior-

[75] Libicki, Martin, *The Mesh and the Net. Speculations on Armed Conflict in an Age of Free Silicon*, McNair Paper 28 (Washington D.C., National Defense University: 1994.

[76] Alberts, David S., John J. Garstka and Frederick P. Stein, *Network Centric Warfare*, 2nd Edition (Washington, D.C., National Defense University: September 1999): 60.

[77] There is an ongoing debate about how the Defense Department should organize itself to support the emerging high-tech field of Information Operations; certain portions of the IO field have been opened to civilian contractors.

[78] Anthony Zinni, quoted by U.S. Institute of Peace Watch – June 1997, online version, URL http://www.usip.org/pubs/PW/697/media.html.

[79] Chairman of the Joint Chiefs of Staff, US Armed Forces, Joint Vision 2010 (Washington, D.C., U.S. Department of Defense: 1996). (JV 2010).

ity in turn is achieved through "dominant battlespace awareness" (DBA), which is the understanding of the current situation based on both sensor observations and human sources and "dominant battlespace knowledge" (DBK), the understanding of the meaning of the current situation, gained from analysis.[80] Information superiority should be understood as a component of an overall strategy for application of military power; it is the enabling capability for the four military operating concepts defined in the US Joint Vision (JV) 2010 and 2020: dominant maneuver, precision engagement, full dimensional protection, and focused logistics.[81] Figure 3 summarizes this hierarchy:

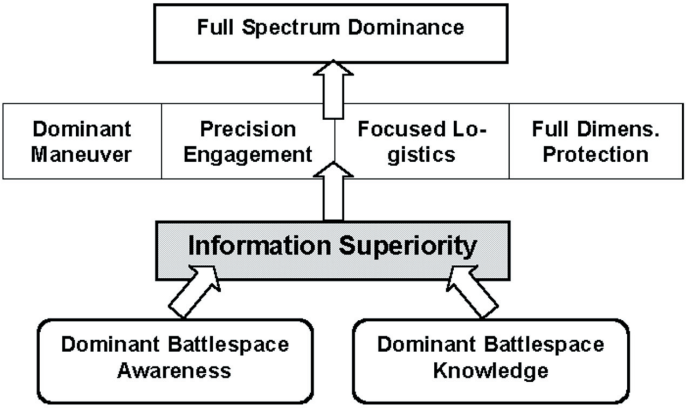

Figure 3: Information Superiority as a Component of an Overall Strategy for Application of Military Power

[80] For the principles of Information Superiority and methods of creating and delivering the "uninterrupted flow of information" see Waltz, Edward, *Information Operations*, 107–133.

[81] JV 2010; US Armed Forces, Chairman of the Joint Chiefs of Staff, US Armed Forces, Joint Vision 2020 (Washington, D.C., U.S. Department of Defense: 2000).

Information superiority is “the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same”[82] or, in other words, the “superiority in the generation, manipulation and use of information sufficient to assure its possessor’s military dominance.’[83] Another slightly different concept that helps to gain domination of the information spectrum is called “*Battlespace Illumination*”:[84] It depicts the military’s goal to create a near-perfect, seamless link between information collected on the battlefield, the decision maker using it, and the action taken to implement the decisions. Through better technology and these new concepts, the military hopes to see through some of the ominous “fog of war”, Clausewitz’s famous phrase for the chaotic uncertainty of battle.

Information superiority or battlespace illumination is meant to provide the commander with a near perfect picture of the battlefield so he can make nearly perfect decisions. This means he has to have access to the total of the available brand new information, any time and anywhere. To enable this, the military wants to implement a “System of Systems”[85], a highly capable network for information exchange and related services that also holds the bulk of battle space knowledge.[86] The parts of the System are linked by what has

[82] This is the standard terminology from the Joint Chiefs of Staff, Joint Publication 3–13, Joint Doctrine for Information Operations, 9 October 1998.

[83] Libicki, Martin, *Information Dominance*, Strategic Forum No. 132 (Washington D.C., National Defense University: November 1997).

[84] Libicki, *Illuminating Tomorrow’s War*.

[85] Current definition provided by Admiral Owens, William A, “The Emerging System of Systems”, *Naval Institute Proceedings 121*, 5 (May 1995): 35–39; or Mahnken, Thomas G, “War in the Information Age”, *Joint Force Quarterly*, 10 (Winter 1995/1996).

[86] Metz, Steven, “Lessons from the Military Experience: The U.S. Military and the IR: The Pitfalls of Uneven Adaptation”, in: Copeland, Thomas E. (ed.), *The Information Revolution and National Security* (Carlisle, Strategic Studies Institute: August 2000): 56–61.

been called a “Global Grid” or “the Grid”, the means by which each part of the system is linked and can be accessed.[87]

Information superiority is not only a central key aspect of the new doctrine but also very important for political considerations: Because information is flexible, divisible and intangible, the capabilities of dominant situational awareness can easily be shared with allies. The possessor of the “information edge” hence offers an “Information Umbrella” for its less powerful allies, similar to extended nuclear deterrence, sharing matters of interest with other nations.[88] Such a relationship already became apparent in the Kosovo conflict, where the US’ provided the bulk of information to the other NATO members.

3.1.2 New Forms of Conflict: Network Centric Warfare, Cyberwar, and Netwar

It seems as if the Information Revolution put hierarchical forms under attack and favored and strengthened network forms of organization. Furthermore, it is likely that conflicts will increasingly be waged by networks as opposed to hierarchies. This is prompting militaries to reconsider how they are organized.[89] In the “frontless” battlespace of tomorrow, the soldier’s task is to provide the command and control function in real-time. He is equipped with advanced weapons and a combat helmet for telecommunications, which serves as the “cyber soldier’s” interface: all contact with the communication systems takes place inside it.[90] The System of Systems, or another kind of powerful network construct, assures that the information gets to and fro as needed.

[87] Libicki, *Illuminating Tomorrow’s War*.

[88] Nye and Owens, “America’s Information Edge”, 27.

[89] Arquilla and Ronfeldt, “A New Epoch – and Spectrum – of Conflict”, 6.

[90] Waller, Douglas, “Onward Cyber Soldiers”, *Time Magazine*, 21 August 1995, 38–44.

The availability and immediacy of real-time information permits the decentralization or flattening of command structures, taking control functions down to lowest practicable level of command to assure greater combat efficiency: Individual units, for example equipped like the "cyber soldier", are permitted to "Self-synchronize" in the classical "Observe-Orient-Decide-Act" loop (OODA).[91] This idea of flat hierarchies, which is opposed to the traditional "platform centric" warfare idea, is called "Network centric warfare".[92]

Other theorems use similar terminology, but account for more than just organizational changes. The most famous are Arquilla and Ronfeldt's concepts of Cyberwar and Netwar, in their own words being "comprehensive approaches to conflict based on the centrality of information [combining] organizational, doctrinal, strategic, tactical and technological innovations for both offense and defense."[93] One of their credos is that networks can defeat institutions, and that it takes networks to counter networks: conflicts will increasingly be waged by networks as opposed to hierarchies and likely be won by them.[94] The two concepts revolve around information and communications matters, are forms of war about "knowledge" and are mainly network-based.

- *Cyberwar*: Cyberwar is a set of new operational techniques and a new mode of warfare. It is used in most intense level of conflicts to target opponents' military and control. It is thus a new form of Command and Control Warfare (C2W), de-

[91] The term OODA cycle has been coined by Boyd, John, *A Discourse on Winning and Losing* (Maxwell, Air University: August 1987).

[92] Cebrowski, Arthur K. and John J. Garstka, "Network-Centric Warfare: Its Origin and Future", *Proceedings of the Naval Institute*, 124, 1 (January 1998); Libicki, Martin, "The Small and the Many", in: Arquilla and Ronfeldt, *In Athena's Camp*, 191–216.

[93] Arquilla, "A New Epoch – and Spectrum – of Conflict", 6.

[94] Arquilla, "Cyberwar is Coming!", 23–60.

pendent less on geographic terrain than on the nature of the electronic cyberspace.[95]

- *Netwar*: Netwar has been used to describe the emergence of diffuse, often trans-national, distributed forms of warfare, in which the players are largely hidden to avoid conventional attack, using the general populace to hide within.[96] Both modes do not necessarily depend on ICT and do not only occur in cyberspace or the infosphere, but they are facilitated by it.

Cyberwar	Netwar
Comprehensive information-oriented approach to battle: Refers to conducting and preparing military operations according to information-related principles	Comprehensive information-oriented approach to social conflict: Refers to information-related conflict at a grand level between nations or societies
Term for conflicts at the military end of the spectrum: • High-intensity conflicts (HICs) • Major regional conflicts (MRCs)	Term for conflicts at the societal end of the spectrum: • Low-intensity conflict (LIC) • Operations-other-than-war (OOTW) • Other, mostly non-military modes of conflict and crime
Features formal military forces pitted against each other	Involves non-state, paramilitary, irregular forces
Aims at disrupting or destroying the information and communications systems on which the adversary relies in order to "know" itself: • Focus on military communications network • May involve diverse technologies and techniques, as described in the Information Warfare chapter • Can also be called Command and Control Warfare	Aims at disrupting, damaging or modifying what target population knows or thinks: • Focus on public or elite opinion or both • May involve public diplomacy, propaganda, psychological campaigns, political/cultural subversion, interference with local media, infiltration of computer systems

Table 7: Comparison of the Concepts Cyberwar and Netwar

[95] Ibid., 30–31.

[96] Ibid., 28–30 and Arquilla, John and David F. Ronfeldt, *The Advent of Netwar* (Santa Monica, RAND: 1996); and Arquilla, John, David Ronfeldt and Michele Zanini, *Networks*, *Netwar and the Information Age* (Santa Monica, RAND: 1996).

The two forms of conflict are basically independent, but can also be overlapping: they might be mounted at the same time, leading to a very difficult situation for conflict managers. These ideas have been taken very seriously by the military community and have had also a substantive influence on doctrine.

3.2 Number One Security Paradox: "Information Warfare"

The RMA appears to further enhance the already unique military power of the United States: The development of the US military's system of systems along with precision strike, dominant maneuver, and focused logistics are indeed likely to have the capacity to triumph over any *traditional* military opponent. Massive investments of the United States DoD in advanced technology further broaden the gap between the US and her allies as well as foes.[97] Nonetheless, there is a lot of concern that the Information Revolution and the proliferation of technologies in the globalized marketplace may be counterproductive to US military security, constituting the number one security paradox in the Information Age: the increasing value of information and the availability of electronic means to manage its ever growing volume have not only made information an invaluable weapon of warfare but a lucrative target too. Advantages in use and dissemination of ICT also connote an over-proportional vulnerability, which lets experts fear that the United States might suffer from its very strength; those who are likely to fail against the American war machine might instead plan to bring the US to its knees by striking at home.[98]

[97] Johnson, Stuart E. and Martin C. Libicki, *Introduction to Dominant Battle-Space Knowledge: The Winning Edge* (Washington, D.C., National Defense University: 1995).

[98] Berkowitz, Bruce D., "Warfare in the Information Age", in: Arquilla and Ronfeldt, *In Athena's Camp*, 175–190.

The twofold debate on “Information Warfare” (IW) was triggered by the benefits of the “information differential” provided by C4I component systems employed in the Gulf War on the one hand[99] and experiences with the threat of data intrusion as perpetrated by hacker attacks during the conflict on the other.[100] Conferences since 1993 created an open environment for the discussion of the topic. During the same period, the US DoD Defense Science Board issued two separate studies[101] and recommended significant investments in organization of IW responsibilities, protection of the Defense Information Infrastructure (DII), and IW research and development. In the last couple of years, technological advances as well as governmental and international actions have changed the world of information security even further.

As a consequence, the subject of information warfare has been extensively discussed and analyzed, both within and outside the information technology and defense communities; so many different activities have been put under that label that it is now tricky to understand exactly what it means, more so because of the inconsistent and still advancing terminology. For experts dealing with security policy aspects of the issue, the understanding of information warfare should encompass more than just information and data security and should be limited to actions taken by actors with specific political and strategic goals, to exclude “playful” hacker-attacks or industrial espionage.

[99] Campen, Alan, *The First Information Warfare*. The Tofflers’ *War and Anti-War* heightened the awareness and study of implications of information warfare at a popular level.

[100] Devost, *National Security in the Information Age*, 10.

[101] Defense Science Board, *Report of the Defense Science Board Task Force on Information Architecture for the Battlefield* (Washington, D.C., Office of Secretary of Defense: October 1994); and Defense Science Board, *Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)* (Washington, D.C., Office of Secretary of Defense: November 1996).

One of the main threats perceived by security practitioners is that most of the means of offence, exceptions are only weapons for the physical destruction of information systems, are widely available, inexpensive, and fairly easy to use. They are available commercially off-the-shelf (COTS) and virtually everyone with computer and skills can become a potentially harmful cracker or "cyber-terrorist". Plus, these tools get more sophisticated and easier to acquire day after day. "Information Weapons" or "Information Warfare Tools" basically include all the means to exploit, distort, disrupt and destruct information resources, ranging from a simple hacker tool to futuristic devices called "Weapons of Mass *Disruption*" that could destroy the entire infrastructure of modern societies.

The term "Information Weapon" has never received an exact definition and seems lately to have disappeared from the IW debate. What makes these tools hard to define in a military sense is the fact that the majority of information technologies are of dual or non-military application, militarization only occurring when civil and military technologies converge and when civil technologies are borrowed or taken over by the military sector.[102] The actors participating in information warfare activities are manifold, can be states, companies, criminal organizations, extra-parliamentary activist groups and very important, individuals. Attacks can be launched from anywhere in the world, and discovering their origin, if they are detected in time at all, remains a major difficulty. Security officials fear the anonymity of the threat, consequent difficulties of

[102] Krutskikh, Andrei, "Information Challenges to Security", *International Affairs*, 45, 2 (1999): 30. Military technologies for IW are not discussed further. Important is that their development is driven by commercial development rather than classified military research and development. For technologies see Waltz, Edward, *Information Operations*, 38 and 357 ff.

relying on a counterstrategy based on retaliation, and the enemy's ability to act independently of geographical distance.[103]

It remains an open question whether state-sponsored IW exists or will exists in the future, whether a group of state-sponsored terrorists or individual crackers could damage the information infrastructure of another nation so as to cause a major strategic disruption. The DoD certainly thinks so, but as it is often the case with extensively debated issues, some defense analysts and information security experts doubt the actual size of the information warfare threat as it is presented by the media and in some official reports. Break-ins are definitely real, do harm or cause serious damage, but are far form representing an "Electronic Pearl Harbor".[104] Strategic information warfare on a state level still remains simply theory. Even if the technology existed, its use would raise a mass of legal and ethical issues. But until proven ineffective, states and nonstate actors which have the capacity to attempt it probably will, doing so because it appears potentially effective and less risky than other forms of armed conflict.

[103] Hundley, Richard O. and Robert H. Anderson, "Emerging Challenge: Security and Safety in Cyberspace", in: Arquilla and Ronfeldt, *In Athena's Camp*, 231–252; Waltz, Edward, *Information Operations*, 29–30; Molander, R.C., A.S. Riddle, and P.A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, RAND: 1996).

[104] Winn Schwartau has used this term first time in 1991 in a Congress hearing, as he states in Schwartau, Winn, *Information Warfare. Chaos on the Electronic Superhighway* (New York, Thunder's Mouth Press: 1994): 43; an interesting article on the hype surrounding the issue: Isenberg, David, "An Electronic Pearl Harbor? Not Likely", in: Copeland, *The Information Revolution and National Security*, 92–102.

Part III – Data Collection

Operation Allied Force, 25 March–10 June 1999

Part III – Data Collection

Operation Allied Force, 25 March–10 June 1999

As was established in part I, the five emerging theorems provide a framework in which the circumstances that substantially influence the successful managing and waging of IACs can be outlined. This part aims to identify definitions and values of the various variables; the actual analysis is undertaken in the subsequent part.[1] The first subchapter strives to resolve the relationship D → A → X, discussing military doctrine concerned with the conduct of Information Operations and some scholarly work. It aims at coming up with valid definitions for the struggle for Information Superiority (A) as well as the conduct of Information Operations (X) dependent on the current doctrine (D). It further explores actual aspects of these Information Operations as experienced during Operation Allied Force, going into considerable details to specify X as well as X+: Information Operations are not only described but also in part assessed. This description is also used to assign values to the other variables in the four remaining chapters: the exogenous variables subsumed under E, assigning reasonably strong impact of these on the overall conduct of Information Operations; the level of credibility C throughout the operation for which a "credibility curve" is drawn; the five intervening variables and each one's degree of influence; and finally, the value for the independent variable Y, the level of success in this Information Age Conflict, which is also shown to have been fairly low.

[1] For more details and explanations concerning the model, operationalization and questions of methodology, refer to part I.

1 Current Military Doctrinal Perception of Information's Role in Warfare

The state of the current military doctrine (Variable D) is essential in the analysis of IACs because it considerably influences the way Information Operations are conducted. Estimates for D, struggle for Information Superiority (A), and their influence on the conduct of Information Operations (X) are given by analysis of recent unclassified military doctrine papers, preceded by the discussion of non-military writings to introduce the issue. Three concepts in the emerging doctrine structure are focused on: Information warfare, central to the earlier doctrine papers; Information Superiority; and Information Operations, both by definition key aspects of IACs. In four key documents, in chronological order of their publication, these concepts are first examined and then compared in order to gain accurate understanding of their current nature.[2]

1.1 Scholarly Approaches to Information Warfare

It was mentioned above that a focused understanding of IW should be limited to actions taken by actors with specific political and strategic goals; this leaves a number of approaches and definitions outside the DoD that deserve mentioning. In general, scholarly approaches to IW do not vary considerably; the main distinction be-

[2] Due to unavailability, the following papers are missing from the analysis: Joint Chiefs of Staff (JCS), *Memorandum of Policy on Information Warfare*, MOP 30; Department of Defense (DoD), *Directive 3600.1* which is classified "Top Secret"; Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.01A, *Joint Information Operations Policy* (not available); and further study of JV 2010, which is not specific enough. Doctrine papers addressing sub-concepts of Information Operations – electronic warfare, psychological operations, and public affairs operations – are not discussed in detail; some of their aspects are mentioned below (analysis of IOs during Operation Allied Force).

tween them is different emphases and preferences in classifying IW according to the source, the form, and the tactical objectives.[3]

Sub-concepts of Information Warfare	Subtypes	Form and Nature of Attack
Command and Control Warfare (C2W)	• Anti-head • Anti-neck	• Attack on systems • Military strategy that implements IW on the battlefield and integrates physical destruction • Objective: "decapitate" the enemy's command structure from its body of command forces
Intelligence-based Warfare (IBW)	• Offensive IBW • Defensive IBW	• Attack by systems • Direct application of intelligence into operations (targeting, battle damage assessment)
Electronic Warfare (EW)	• Anti-radar • Anti-communications • Cryptography	• Radio-electronic and cryptographic • War in the realm of communications • Attempts to degrade the physical basis for transferring information
Psychological Warfare	• Anti-will • Anti-troop • Anti commander • "Kulturkampf"	• Use of information against the human mind • Aim is to induce or reinforce foreign attitudes and behavior favorable to the overall national security interests of attacking state
Hacker warfare	• Physical attack • Syntactic attack • Semantic attack • Offensive/defensive	• Attacks on civilian targets (military ones fall under C2W) • Intent of attack ranges from total paralysis to intermittent shutdown, data errors, theft of information, false message traffic, etc.
Economic Information Warfare	• Information Blockade • Information Imperialism	• Cutting of access to data could cripple economy • Variant of economic blockade • "Trade is war"
Cyberwar	Info terrorism • Semantic attack • Simula-warfare • Gibson-warfare	• Least tractable because most fictitious • "Grab bag of futuristic scenarios"

Table 8: Martin Libicki's Seven Sub-Concepts of Information Warfare

Martin Libicki's "What is Information Warfare?" is one of the earlier substantial proposals of how to understand IW.[4] He holds that information warfare as a single and separate technique of wag-

[3] The defensive side of the matter, even though of equal importance, is omitted here because the analysis focuses on offensive operations exclusively.

[4] Libicki, Martin, *What is Information Warfare?* (Washington, D.C., National Defense University: 1995), online version, URL http://www.ndu.edu/inss/actpubs/act003/a003.html.

ing war does not exist, but that seven sub-concepts should be distinguished instead; each type requires its own rules of engagement, based on its methods, objectives, and technologies.

Winn Schwartau's distinction of three classes of information warfare includes attacks at the personal level aimed at private individuals.[5] He uses the term information warfare to refer almost exclusively to attacks on computer networks applying a consumer-oriented data-security perspective; only Class 3 Warfare is what defense practitioners usually talk about. This is one of the broader definitions of information warfare, which does not fit exactly into our context, but should still be mentioned because Schwartau's approach had a great impact on the public's perception of IW issues:

Class	Aimed at	Objective
Class 1: Personal Information Warfare	Individual's electronic privacy: • Digital records • Digital files • Other portions of a person's electronic essence	• Theft (credit card numbers, etc.) • Damaging a person's public image • Blackmail
Class 2: Corporate Information Warfare	Companies	• Industrial espionage • Acquisition and use of valuable information • Damaging of reputation • Denial of service
Class 3: Global Information Warfare	• Industries • Political spheres of influence • Global economic forces • Entire countries	• Turning information against its owners • Denying an enemy use of technology and information

Table 9: Winn Schwartau's Class Distinction of Information Warfare

Very substantial is Edward Waltz's contribution, which distinguishes three levels or layers of functions on both the attack and the target sides in his comprehensive approach to IW. The ultimate objective of the attacker is to influence the target at the perceptual

[5] Schwartau, *Information Warfare*, 258–312.

level by actions that may occur at all levels of the cognitive hierarchy: The highest-level target is thus the human mind, the ultimate objective to influence its perceptions.[6]

Levels or Layers of Functions	Aim of the Attack	Abstract Components	Desired Outcome of the Attack
1 Perceptual or Psychological Level	Knowledge	• Objectives • Plans • Perceptions • Beliefs • Decisions	• Cognitive: • Indecision • Delay of decision • Biasing specific decision
2 Information Structure Level	Information	• Data structures • Processes • Protocols • Data content	Functional: • Influence of effectiveness and performance of information functions
3 Physical System Level	Data	• Computers • Storage • Networks • Electrical Power	Technical: Affect technical performance and capacity

Table 10: Operational Model for Information Attacks by Edward Waltz

Similar to Waltz's approach but less abstract is the way of classifying IW according to the source, the form, and the tactical objectives of the attack. The Center for Strategic Studies in Washington defines four categories of attacks (classification by form). They originate either from outside or from within the targeted system, and can further be categorized by their goals or tactical objectives. They can be aimed at exploitation, deception, disruption and/or destruction of information systems:[7]

[6] Waltz, Edward, *Information Operations*, 148–152.

[7] Center for Strategic and International Studies (CSIS), "Cybercrime, Cyberterrorism, Cyberwarfare", 9–11.

Category or Form	**Type and Aim of the Attack**
Data attacks	Inserting data into a system to make it malfunction
Software attacks	Penetrating systems with software, causing failure or making them perform functions different from those intended
Hacking or cracking	Seizing control of an information system to disrupt, deny use, steal resources or data, etc.
Physical attacks	Bombing, assaulting and destroying information systems with "traditional" measures such as bombs.
Goals/ Tactical objectives	
Exploitation – Deception – Disruption – Destruction of information systems	

Table 11: Center for Strategic Studies' Categories of Information Attacks

The next approach distinguishes attacks by their objectives. This is the least abstract. The author also offers the category's equivalent in electronic air combat and information warfare, a nice way to illustrate some of the methods of IW:[8]

Four categories	**Equivalent in electronic combat**	**Equivalent in Information Warfare**
Denial of Information: concealment and camouflage, or stealth	Stealth fighter	Use of encryption
Deception and Mimicry: insertion of intentionally misleading information	Defensive jamming equipment which emits signals of erroneous position measurement	Various techniques for masking the identity of a penetrating party into a system
Disruption and Destruction: insertion of information which produces a dysfunction inside the opponent's system	• High power noise jamming blinding opposing radars • Disrupting of radio communications • HPM / EMP weapons	• Denial of Service attack • "Ping to death" • EMP bomb
Subversion: insertion of information which triggers a self destructive process in the opponent's target system	Use of deceptive signals which trigger premature initiation of weapon fuses	• Logic bombs • Viruses • Other destructive programs which use system resources to damage the system itself

Table 12: C. Kopp's Classification Scheme of Information Warfare

[8] Kopp, Carlo, "Information Warfare: A Fundamental Theorem of Infowar", *Systems - Enterprise Computing Monthly* (February 2000): 46–55.

Next to the principal sources for information warfare policy, strategy and operations,[9] official doctrine papers offer insight on the state of the current RMA and its central concepts; these doctrine papers are discussed in the following chapters.

1.2 United States Air Force: Cornerstones of Information Warfare

In 1995, the United States Air Force (USAF) fashioned one of the earliest official military documents on information warfare, called "Cornerstones of Information Warfare".[10] Its goal is to provide the Air Force with a "sound foundation" on how to adjust its own doctrine in order to adapt to information warfare issues, thus bridging the gap between literature that mainly focuses on technical developments in the information technology domain and the need to reveal how these developments impact doctrine. To achieve this, it strives to establish definitions of arising issues, drawing on institutional experience made, and existing doctrinal concepts. By means of these definitions, the document establishes the first "Information Warfare" taxonomy.

At the very beginning, the authors stress the fundamental difference between *information age warfare* and *Information Warfare*; while the first is understood as the use of ICT as tools in combat, which is not further explored, the second is treating information, consisting of data and instructions, as a separate sphere that is technology independent, it so being both a powerful weapon as well as a

[9] Principal sources: US National Defense University's Strategic Forum; Journal of Infrastructure Warfare, which prepares high-level analyzes and publishes articles on infrastructure warfare and conflict activities worldwide; and the US Defense Science Board, RAND Corporation. (Waltz, Edward, *Information Operations*, 40).

[10] Department of the United States Air Force, *Cornerstones of Information Warfare*, circa 1995, online version, URL http://www.af.mil/lib/corner.html.

lucrative target. Their subsequent definition of information warfare is the following:

> [Information warfare is] Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.[11]

Information warfare is thus either an *attack* against information functions[12] or an action to *protect* those, an implicit distinction between defensive and offensive IW. Rather than differentiating between these two, the paper stresses an indirect and a direct way to influence the adversary's information functions:

- *Indirect IW* affects information by creating phenomena, which the adversary will perceive, interpret, and act upon;
- *Direct IW* affects information through altering its components without relying on the adversary's powers of perception or interpretation.[13]

The concept of Information Operations is introduced, but it is defined as a separate and rather insignificant subset of information warfare, in contrast to the following doctrine documents. The authors see it as a means to enhance total force effectiveness by exploiting information, dealing with information as both its resource and its product. In "Cornerstones of Information Warfare", Information Operations are defined as "any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces", thus being the slightly enhanced and directed version of information functions.[14] The next figure reproduces one image presented in the publication showing the early understanding of information warfare structure:

[11] Ibid.

[12] Definition of information function: any activity involving the acquisition, transmission, storage, or transformation of information, Department of the United States Air Force, Cornerstones of IW.

[13] Department of the United States Air Force, Cornerstones of IW.

[14] Ibid.

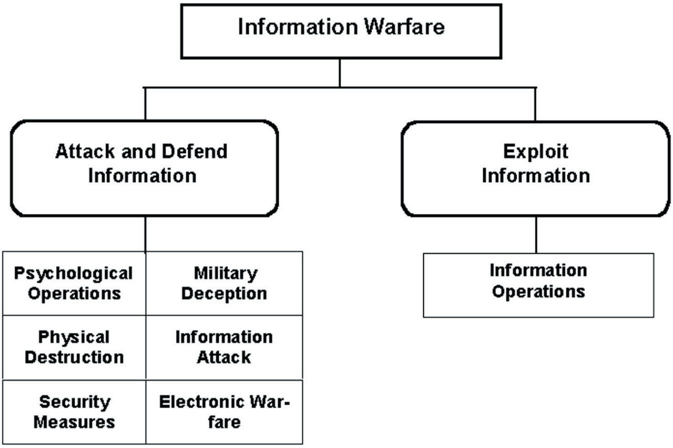

Figure 4: Cornerstone of Information Warfare Diagram of Information Warfare Structure

Neither Information Superiority, nor dominant battlespace knowledge, or other terms with similar meaning are mentioned. Also notable are the secondary nature of defensive concepts and the total lack of emphasis on national security threats and vulnerabilities. It is likely that the explosive growth of the Internet in the second half of the 90s and increasing dependency of all segments of society on ICT added to growing fears of incidents and the perception of vulnerability of later years.

1.3 Field Manual № 100–6: Information Operations

This publication is considerably more thorough in addressing the new emerging concepts than “Cornerstones of Information Warfare”. Its main focus is Information Operations (IO). The extensive publication stands out through detailed and pointed exploration of changes in the strategic settings. It introduces the idea of different “environments”; it maintains that the military faces an expanding information domain termed the *Global Information Environment (GIE)*, of which the *Military Information Environment (MIE)* is part, along with geostrategic and technological environments, the Global Information Infrastructure (GII), The National Information Infrastructure (NII), and the Defense Information Infrastructures (DII). Actors in both environments are diverse and include political leaders, the media, industries, International Organizations, and more. Within the whole GIE, the concept of information dominance is identified as the key element for operating effectively.[15]

Unlike "Cornerstones of Information Warfare", FM 100–6 presents significant thoughts on threats to Information Systems and the Information Infrastructure, exploring its sources, identifying aggressors, and different levels of hostility. A number of challenges for commanders and national leaders are described, such as information security, public opinion, morale, and legal considerations. Information dominance is seen as a response to these challenges.[16]

In FM 100–6, information warfare is basically replaced by the concept of Information Operations, a general trend that started in 1996 and has been adopted by a considerable number of documents. It is an attempt to broaden the general understanding of information warfare by accentuating that information issues permeate the full range of military operations from peace to war, beyond the traditional context of warfare. In their simplest form Information Operations, are seen as activities that gain information and knowledge and improve friendly execution of operations while denying an adversary similar capabilities. Three components of Information Operations to gain and maintain information dominance are distinguished:

[15] Department of the US Army, FM 100–6, chapter 1 on the Geostrategic and Technological Environments, online version, URL http://www.fas.org/irp/doddir/army/fm100-6/ch1.htm.

[16] Ibid.

- *Command and Control Warfare (C2W)*; seen as "the integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions";[17]
- Civil Affairs Operations (CA): CA activities establish, maintain, influence, or exploit relations among military forces, civil authorities, and the civilian populace to facilitate military operations. Conditions differ across the spectrum of conflict;18
- Public Affairs Operations (PA): PA activities are used to monitor public perceptions and to develop and disseminate clear and objective messages about military operations.19

These three concepts are closely interrelated: CA and PA provide liaison and connectivity with essential actors and influences and interact with specific C2W elements.[20] The following figure captures the relationship as conceived by the Army:

[17] Department of the US Army, FM 100–6, Glossary, online version, URL http://www.fas.org/irp/doddir/army/fm100-6/glossary.htm, cited after Joint Chiefs of Staff, Joint Publication 1–02, DOD Dictionary of Military and Associated Terms, as amended through 1 September 2000, online version, URL http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf. C2W applies across the operational continuum and all levels of conflict.

[18] Department of the US Army, FM 100–6, chapter 2, online version, URL http://www.fas.org/irp/doddir/army/fm100-6/ch2.htm.

[19] Ibid.

[20] Ibid., chapter 3, online version, URL http://www.fas.org/irp/doddir/army/fm100-6/ch3.htm.

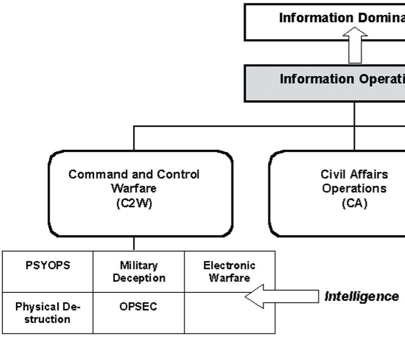

Figure 5: Information Operations Constructs as Perceived by the Army

The Field-Manual 100–6 introduces interesting ideas about a changing operating environment, which poses new challenges to commanders and their staffs. Among the discussed doctrine papers it stands out as the most different and also the most confusing, which is mainly due to its length and the understanding of the components of Information Operations.

1.4 Air Force Doctrine Document 2–5: Information Operations

Air Force Doctrine Document (AFDD) 2–5 is noticeably more focused on the topic than FM 100–6. Three years after the milestone "Cornerstones of Information Warfare", the USAF has fully adopted the new concepts in its doctrine. The execution of Information Operations in air, space, and also in "cyberspace" are seen to constitute the means by which to provide Information Superiority, and are defined as actions taken to gain, exploit, defend or attack information and information systems. Similar to the understanding in FM 100–6, they apply across the whole range of military operations, from peace to all-out conflict.[21] Information Operations com-

[21] Department of the US Air Force, Air Force Doctrine Document 2–5 (AFDD 2–5) Chapter 1, online version, URL http://www.doctrine.af.mil/Library/Doctrine/afdd2-5.pdf, 1–3.

prise two distinct but interrelated pillars: *Information-in-warfare* which includes activities to "gain" and "exploit" information and *Information Warfare* which covers "attack" and "defend" aspects. The latter is the documents prime focus.

Information Warfare: It is defined as "Information Operations conducted to defend one's own information and information systems or attacking and affecting an adversary's information and information systems."[22] It therefore generally includes and subsumes previous Air Force definitions for command and control warfare. Information warfare responsibilities are implemented through *counterinformation* (CI), a function that establishes Information Superiority by neutralizing influencing adversary information activities to varying degrees. CI has an offensive (OCI) and a defensive (DCI) division:[23]

- *Offensive Counterinformation (OCI)* includes actions taken to control the information environment. It is designed to limit, degrade, disrupt, and destroy adversary information capabilities through such actions as PSYOP, electronic warfare, military deception, physical attack, and information attacks;[24]
- *Defensive Counterinformation (DCI)* includes actions that protect information, information systems, and Information Operations from any potential adversary. It includes operations security (OPSEC), counterintelligence, information assurance, and counter-psychological operations.[25]

Information-in-warfare on the other hand defines operation-supporting functions that include intelligence, precision navigation and positioning, surveillance and reconnaissance, weather services, and others activities that contribute to the overall Information Superior-

[22] Ibid.

[23] Ibid., 9; compare to definition of Command and Control Warfare as provided by FM 100–6, Footnote 17.

[24] Ibid., 1–15.

[25] Ibid., 15–19.

ity effectiveness.[26] Figure 6 shows the Air Force Information Superiority construct as proposed in the AFDD 2–5:

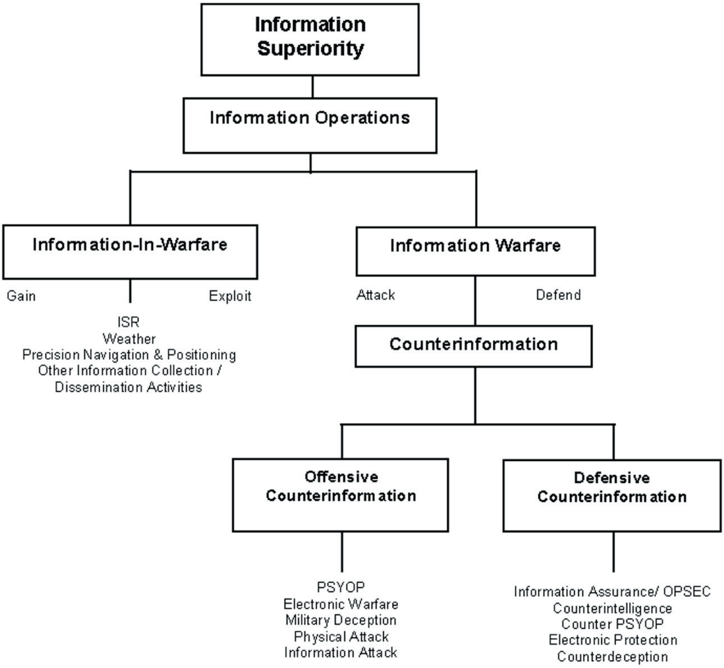

Figure 6: United States Air Force Information Superiority Construct II

AFDD 2–5 does not address the changing strategic environment or any impact of the Information Revolution in depth. It briefly comments on Information Age threats however, to the military and the United States in general. These threats fall into four categories: compromise, deception/corruption, denial/loss, and physical destruction. Each of those poses an inherent risk to both standalone and networked weapon and support systems that rely on information systems, mainly due to an increasing dependence of the military upon commercial systems: in peacetime, over 95 percent of DoD communications and a significant amount of open-source intelligence is carried by commercial means over relatively unprotected public switch networks and are largely outside the direct control or influence of the military.[27]

1.5 Joint Publication 3–13: Joint Doctrine for Information Operations

The newest of the discussed publications draws on all the three older ones, there are many similarities and parallels to FM 100–6 and the AFDD 2–5. However, JP 3–13 has a much narrower focus on IO than the others. Its main emphasis is on organization, the strategic, operational, and tactical planning aspects of IO, and training through exercises, modeling, and simulation as a key ingredient to successful IO.

The threats faced today are seen as more ambiguous and regionally focused than during the Cold War period, leading to a wide variety of factors that challenge stability in the areas of responsibility. To ensure effective operations in this new security environment, commanders must achieve and sustain *Information Superiority.* To accomplish this, they must integrate offensive and defensive aspects of Information Operations:

- *Offensive Information Operations (OIO):* involve the integrated use of supporting capabilities and activities that are: OPSEC, military deception, PSYOP, Electronic Warfare, physical attack/destruction, and Special Information Operations (SIO);[28]
- *Defensive Information Operations (DIO):* are conducted and assisted through information assurance (IA), OPSEC, physical security, counderdeception, counterpropaganda, counter-

[26] Ibid., 21–25.

[27] Ibid., 4–7.

[28] Ibid., chapter 2, 1–7.

intelligence (CI), electronic warfare, and Special Information Operations (SIO).[29]

Apart from offensive and defensive aspects, successful conduct of Information Operations also requires the integration of intelligence and other information related activities, as well as activities to include friendly (allied) decision-making processes into one's own.[30] IOs are conducted through the integration of the sub concepts of OIO and DIO and IO-related activities that consist of public affairs (PA) and civil affairs (CA) actions:

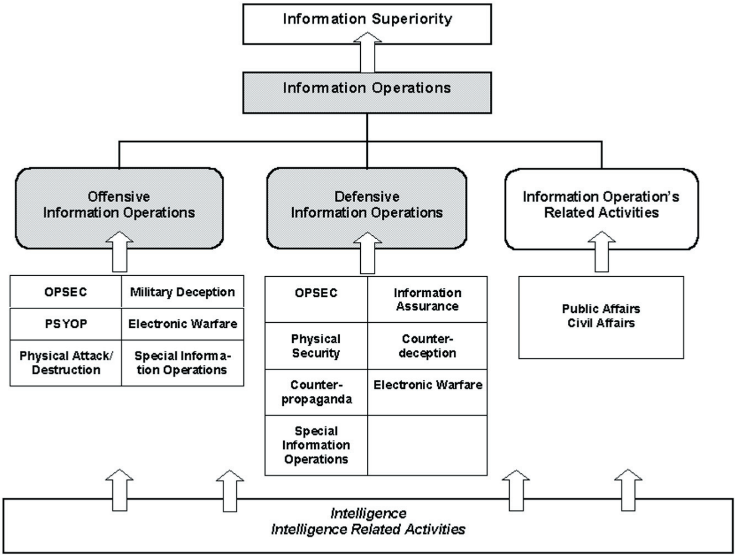
Information Superiority
Information Operations
Offensive Information Operations
Defensive Information Operations
Information Operation's Related Activities
OPSEC
Military Deception
PSYOP
Electronic Warfare
Physical Attack/ Destruction
Special Informa-tion Operations
OPSEC
Information Assurance
Physical Security
Counter-deception
Counter-propaganda
Electronic Warfare
Special Information Operations
Public Affairs
Civil Affairs
Intelligence
Intelligence Related Activities

Figure 7: Joint Publication 3–13 Information Operations Construct

Information Operations as defined in JP 3–13 are applied across all phases of an operation, the whole range of military operations and at the strategic, operational and tactical level of war; they involve

[29] Ibid., chapter 3, 1–14.

[30] Joint Chiefs of Staff, JP 3–13, 1–2.

actions taken to affect the adversary's information and information systems while defending one's own information and information systems, taking advantage of the world's growing sophistication, connectivity and reliance on Information Technology. The commander is told to apply the term "adversary" broadly to include a wide range of organizations, groups or decision makers. The concept of information warfare is even further downgraded and hardly discussed at all. In a short paragraph it is described as something that can be waged in crisis or conflict within and beyond the traditional military battlefield, conducted to shape the battlespace and prepare the way for future operations.[31] IO may be conducted across the range of military operations, hopefully having their greatest impact on adversary decision maker in peacetime and the initial states of a crisis. The primary goal is therefore to maintain peace, defuse crisis, and deter conflict. If deterrence fails however, all IO capabilities might be applied to meet the stated objectives.[32]

JP 3–13 is very specialized and adds little new to what has already been covered in FM 100–6 and AFDD 2–5. It stresses the need to merge traditionally separate capabilities and activities for the new era of conflicts. Special attention is given to the uncertain and complex legal issues surrounding the conduct of Information Operations: JP 3–13 stresses the importance of understanding legal limitations in different domains, such as domestic and international criminal and civil laws and international treaties and agreements.[33] These legal limitations will be of further interest in the upcoming chapters.

[31] Ibid., Chapter I, 4.

[32] Ibid., Chapter II, 7.

[33] Ibid., Chapter I, 1–3, 11–20.

1.6 Comparison of Key Concepts across the Doctrine Spectrum

Comparison of the concepts of information warfare, Information Superiority, and Information Operations is not only difficult because definitions vary considerably but also because even the most basic terminology is chaotic and inconsistent; this disorder in the doctrine is a clear indication that the current RMA is far from over. Furthermore, a new taxonomy has been established in the DoD since December 1996, in which Information Operations has replaced the principal concept of information warfare:[34] Even though information warfare is defined in similar terms today, it is either classified (along with information-in-war) as a subset of "Information Operations", supporting the ultimate objective of Information Superiority as in AFDD 2–5 or treated just as a special form of Information Operations as in JP 3–13. Table 13 roughly compares the concepts gained from the four doctrine papers.

The trend seems to limit information warfare to offensive military measures in the states of crisis or war. Early publications saw information warfare as a form of warfare at the strategic/security political level for the entire time scale of peace-crisis-war, Command and Control Warfare (C2W) as the military function at the operative level, and Information Operations at the tactical level. What is new is that Information Operations are understood as actions taken at every level of war. It is an elegant solution to drop the word "war" in dealing with information activities, not only because it stresses or implies the nonviolent nature that such undertaking should and could have, but also because Information Operations include such a wide range of actors outside the military realm. This paper proposes to take up this new taxonomy, but to expand the concept even further to include actions taken by military as well as political parties, thus taking the definition offered by military papers a step further.

[34] DoD directive S3600.1 "Information Operations" replaces directive TS3600.1 "Information Warfare". DoDD 3600.1 is classified "top secret".

	Cornerstones of Information Warfare	Field Manual No. 100–6	Air Force Doctrine Document 2–5	Joint Doctrine for IO, JP 3–13
Information Warfare	"Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions."(p 3) Consists of direct IW and indirect IW (p 5)	"Actions taken to achieve Information Superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks." (chapter 2)	"IW is Information Operations conducted to defend the Air Force's own information and information systems or conducted to attack and affect an adversary's information and information systems – Consists of Counterinformation (CI) and its two subsets, offensive CI and defensive CI." (p 2–3)	"IW is Information Operations conducted during time of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries (…) within and beyond the traditional military battlespace." (I–1,4)
Information Operations	"Any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces."(p 9)	"Continuous military operations within the Military Information Environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; IO include interacting with the Global Information Environment and exploiting or denying and adversary's information and decision capabilities." (chapter 2)	"Comprise those actions taken to gain, exploit, defend, or attack information and information systems and include both information-in-warfare and Information Warfare and are conducted throughout all phases of an operation and across the range of military operations." (p 2)	"IO involve actions taken to affect adversary information and information systems while defending one's own information and information systems, across all phases of an operation, throughout the range of military operations, and at every level of war." (p I–1,9) "IO-related activities include, but are not limited to, public affairs (PA) and civil affairs (CA) activities. There are two major subdivisions within IO: offensive IO and defensive IO." (I–9–10)
Information Superiority	(not defined!)	(Information Dominance): "The degree of Information Superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations short of war, while denying those capabilities to the adversary." (chapter 1) Is achieved through C2W, CA, PA	"Degree of dominance that allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition" → State of relative advantage, not a capability	"The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." (I–10)
Conclusion	• IO is a subset of IW • IO concept is underdeveloped and subsidiary • Concept of Information Superiority is still missing	• Offers a broader approach to IO than others, which are more narrowly focused on the impact of information during actual conflict • Information Warfare has already become a secondary concept • Information Superiority a key element to effective operations	• Early IW definition (Cornerstone) has been taken as definition of IO and expanded • Information Superiority is one of the six Air Force core competencies	• IW concept totally subsidiary • IO takes place of IW completely • To ensure effective operations commanders must achieve and sustain Information Superiority

Table 13: Information Activity Concepts from Four Different Doctrine Documents

1.7 Variables A and X: Two Definitions

The state of the current military doctrine (Variable D) was explored in the previous chapters. Drawing on this examination, definition shall be proposed for Variable A, the struggle for Information Superiority, and Variable X, the conduct of Information Operations. For this analysis, the Air Force's Information Superiority construct outlined in Doctrine Document 2–5 offers the most fruitful approach to information-based activities in the military sphere.

> *Definition of Information Superiority*: Information Superiority is a state of relative advantage describing that degree of dominance in the information domain, which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition from adversaries. Information Superiority is achieved through the conduct of Information Operations.
>
> *Definition of Information Operations*: Information Operations are defensive and offensive operations, conducted to disrupt or confuse an enemy's ability to collect, process, and disseminate information. They can be conducted by a variety of actors ranging from states, companies, and criminal organizations over extra-parliamentary activist groups to individuals. Information Operations comprise two distinct but interrelated pillars: Information-In-Warfare which includes activities to "gain" and "exploit" information and Information Warfare which covers "attack" and "defend" aspects.[35]

[35] This is a definition proposed by the author, gained from various doctrine papers. See mainly: Department of the US Air Force, AFDD 2–5.

2 Struggle for Air and Information Superiority: Aspects of Information Operations

As mentioned before, Operation Allied Force in Kosovo represents the first and currently sole exemplar for what this paper proposes the term "Information Age Conflict". To explore its Information Operations is therefore an important step towards understanding the mechanisms of this new form of warfare. In doing so, this chapter's structure reflects the Air Force's understanding of Information Operations in large parts; defensive aspects, even though very important for all definitions of Information Operations, remained minor in this conflict.[36]

An important difference to AFDD 2–5 further is the embrace of old Command and Control Warfare (C2W) ideas during Operation Allied Force; they gained new impetus in Kosovo even though they had merged with the new doctrine and had been taken up by new terminology.[37] The following picture shows the Air Force Information Operation's construct, redefined for the specific case of Operation Allied Force.

This chapter is divided into three parts: the first chapter focuses on the gain and exploit dimension of Information Operations (information-in-warfare) in three chapters; the second focuses on the information warfare dimension, likewise in three subchapters. Since the defensive aspects remained of minimal importance during the conflict, only the attack branch of counterinformation is considered. The third chapter draws a conclusion concerning the conduct of Information Operations in these IACs, assigning a concrete value to the Variable X+.

[36] This might be partly due to the relatively low-tech adversary faced and partly due to classification of relevant material: whatsoever, neither secondary nor primary sources mention any such.

[37] See for example Department of the US Army, FM 100–6, definition of C2W; and Department of the US Air Force, AFDD 2–5, definition of Offensive Information Operations.

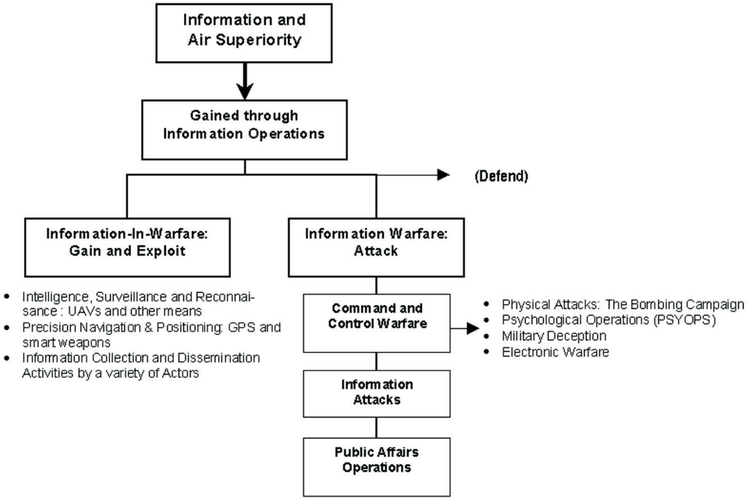
Information and Air Superiority
Gained through Information Operations
(Defend)
Information-In-Warfare: Gain and Exploit
Information Warfare: Attack
• Intelligence, Surveillance and Reconnaisance : UAVs and other means
• Precision Navigation & Positioning: GPS and smart weapons
• Information Collection and Dissemination Activities by a variety of Actors
Command and Control Warfare
• Physical Attacks: The Bombing Campaign
• Psychological Operations (PSYOPS)
• Military Deception
• Electronic Warfare
Information Attacks
Public Affairs Operations

Figure 8: Information Operations Construct, Kosovo Specific

2.1 Information-In-Warfare: The Gain and Exploit Dimension

Information-in-Warfare enhances and supports Information Operations by providing the means for (dominant) battlespace awareness and Information Superiority. The gain and exploit aspects of Information Operations are both aided and thwarted by the Revolution in Military Affairs and new technologies at large: the gathering of information in an environment increasingly marked by the rapid flow of information and the explosive expansion in the opportunities for access and manipulation of operationally relevant information by the wide array of individuals, organizations, and systems found in the GIE poses both new opportunities and challenges for IOs.[38]

Many gain and exploit facets are purely military domains and require expensive hardware, unavailable for other actors: military assets to collect and disseminate information used in Kosovo include the Airborne Warning and Control System (AWACS), Joint

[38] Department of the US Army, FM 100–6, chapter 2.

Surveillance Target Attack Radar System (JSTARS), unmanned aerial vehicles (UAV), airborne reconnaissance platforms, weather platforms, and of course space systems such as satellites.[39] Other assets, mainly the Internet, aid the newly emerging actors to exercise their influence easily and cheaply while the traditional conflict parties have no advantage in this global network.

This chapter looks at three dimensions of Information-in-Warfare: the first is concerned with intelligence, surveillance, and reconnaissance (ISR) and focuses mainly on the use of Unmanned Aerial Vehicles (UAVs), and on how advances in information technology changes the way relevant information is gathered; the second focuses on precision navigation, positioning capabilities, and so-called smart weapons, with special emphasis on what this development in warfare means for the conduct of such operations; and the third introduces aspects of information collection and dissemination activities conducted by a variety of actors, mainly focusing on the impact of the Internet on this part of warfare.[40]

[39] Department of the US Air Force, AFDD 2–5, 21–24; Eash, Joseph J III., "Harnessing Technology for Coalition Warfare", *NATO Review* (Summer/Autumn 2000): 32–34.

[40] Department of the US Air Force, AFDD 2–5, 2. Further gain and exploit aspects of Information Operations are put forth in the Department of the US Air Force, Air Force Doctrine Documents 2–5.1, Electronic Warfare Operations, and Department of the US Air Force, Air Force Doctrine Documents 2–5.2, Intelligence, Surveillance, and Reconnaissance.

2.1.1 Remote Controlled Intelligence, Surveillance and Reconnaissance

Effective Information Operations depend on ensuring that the right person has the right information at the right time. Intelligence, Surveillance and Reconnaissance (ISR) provide this relevant information and are thus assigned a crucial role:

- *Intelligence* seeks to obtain a superior understanding of the strengths and weakness of an adversary. It is conducted incessantly. It is either "the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas"[41] or "information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding".[42]
- *Surveillance and reconnaissance* provide real-time or near-real-time information for tailored, mission-focused situations. Both might be conducted by the same collection platform or team, but they are differentiated the following: "surveillance is continuous collection of information from the air, space, and earth's surface; reconnaissance is conducted to gain information on localized and specific targets within a constrained time frame".[43]

The extensive databases in which collected information is stored gained dubious fame in Kosovo, when outdated information was made responsible for the bombing and destruction of the Chinese embassy on May 7. The CIA took full responsibility for incorrect identification of the target and the DIA accepted at least partial liability for maintaining the database that failed to show that the

[41] Joint Chiefs of Staff, Joint Pub 1–02. The importance of open source information gathering has risen considerably in the Information Age, cf. Stewart, John F., "Intelligence Strategy for the 21st Century", *Military Review* (September–October 1995): 75–81.

[42] Joint Chiefs of Staff, Joint Pub 1–02.

[43] Department of the US Air Force, AFDD 2–5, 23.

Chinese Embassy had moved three years earlier.[44] Even though some insist that the bombing was not a mistake but full intention after it was discovered that the embassy was being used to transmit Yugoslav army communications,[45] this incident shows how the danger earlier identified as "Information overload" can effect military operations; in a background briefing given on May 10, DoD intelligence officials stated that even the database for cities the size of Belgrade were overwhelming challenges to maintain currently and accurately.

The incident also offers some insight on how intelligence was used to identify targets: in the briefings after the incident, officials explained in length the efforts to identify targets by their functions and to evaluate whether or not they were legitimate for a given purpose, mentioning a multi-stage check, both within the intelligence committee and the DoD, to confirm the location.[46] Obviously, none of the fail-safes in this multi-step process worked in the specific case of the Chinese embassy. In the aftermath of the embassy incident, the (mainly American) intelligence process and the accuracy of the collected information was questioned whenever NATO had to admit collateral damage; especially probing were the questions after two incidents, when NATO bombed a prison it declared to be

[44] The agency sacked a leading CIA official on 9 April 2000 that was responsible for identifying the target in the first place. Six additional employees received written or oral admonishment (cf. Myers, Steven Lee, "C.I.A. Fires Officer Blamed in Bombing of China Embassy", *New York Times*, 9 April 2000).

[45] Jane's News Brief, 19 October 1999. A journalist also suggested that there "was in fact secret collaboration between China and Belgrade, that China was giving intelligence on the conflict to Belgrade and that Serbia had moved equipment and people into the Chinese embassy making at least one part of that embassy a legitimate target", cf. Press Conference given by NATO Spokesman, Jamie Shea and SHAPE Spokesman, Major General Walter Jertz, 9 May 1999, updated 9 May 1999, NATO HQ.

[46] DoD Background Briefing, Monday, May 10, 1999 – 4:42 p.m. Subject: Chinese Embassy Strike. Presenter: Senior Intelligence Officials.

unused which it was clearly not[47] and after it bombed an area which had previously been taken over by the KLA, which should have been well known.[48]

Nonetheless, in comparison to Desert Storm in 1991 when complaints about intelligence revealed that eleven satellite imagery dissemination systems maintained by the various military services could not communicate with each other, information collection in Kosovo was said to show considerable improvement. As Major General Wald from the J–5 joint staff plan and policy said in a DoD briefing:

> It's night and day from the Gulf War (…) our intelligence is in a magnitude of number bigger (…), better from the standpoint of real time information to both the cockpit as well as on the ground.[49]

Advances in information technology greatly improved the way relevant information was gathered and disseminated: fusion of information from a variety of sources as well as the development in sensors, processors, and communicators provided detailed information, which connectivity allowed to be broadcasted instantaneously.[50] Once targets were located, the information could rapidly be passed to the Allied planes: a wideband dissemination system transmitted imagery of emerging targets, thus significantly shortening the time between finding the target and hitting it.[51] The ca-

[47] Press Conference given by NATO Spokesman, Jamie Shea and SHAPE Spokesman, Major General Walter Jertz, 22 May 1999, updated 22 May 1999, NATO HQ, Brussels.

[48] Press Conference given by NATO Spokesman, Jamie Shea and SHAPE Spokesman, Major General Walter Jertz, 23 May 1999, updated 23 May 1999, NATO HQ, Brussels.

[49] Major General Wald's lengthy explanation of the improved intelligence situation, DoD News Briefing, Friday, April 9, 1999 – 3:00 p.m. Presenter: Mr. Kenneth H. Bacon, ASD PA (Also participating in this briefing was Major General Chuck Wald, J–5).

[50] Department of the US Army, FM 100–6, chapter 2.

[51] Eash, "Harnessing Technology for Coalition Warfare", 33.

pability to directly "modem" target information into the cockpit of aircrafts was also used to program the precision-guided bombs in the wing of specific aircraft.[52]

The operation also employed Unmanned Aerial Vehicles (UAVs) to an unprecedented degree in order to conduct essential reconnaissance operations.[53] In this "zero-death" conflict, these remote-controlled machines carrying video cameras and other sensing devices could provide surveillance information without the risk of losing aircrew. The so-called "Predators" kept almost constant surveillance on enemy forces operating in open country, were used to observe refugees, and to assess battle damage, by sending back real time pictures or infrared.[54] These new intelligence-gathering platforms were also used to help shorten the cycle between the detection of a target and the dropping of bombs: a system was set up to link airplanes with the data from the UAVs, to get imagery into the cockpit fairly real time. General Jumper, Commander-In-Chief of the US Air Forces in Europe, described this process in one of the DoD briefings:

> The U–2 can snap a picture from very high altitude, beam it back in what we call reach-back to the States where it is very quickly analyzed and (…) getting the right targeting data very quickly back into the CAOC [Combined Air Operations Center] in Vicenza to pass on to people in

[52] Major General Wald in DoD News Briefing, Wednesday, May 5, 1999 – 2: 00 p.m. Presenter: Captain Mike Doubleday, DASD PA. Also Participating: Maj. Gen. Chuck Wald, J–5 and Brig. Gen. Leroy Barnidge Jr., 509th Bomber Wing.

[53] Joint Chiefs of Staff, *Joint Statement on the Kosovo After Action Review* (initial assessment), presented by Secretary of Defense William S. Cohen and Gen. Henry H. Shelton, Chairman of the Joint Chiefs of Staff, before the Senate Armed Services Committee, 14 October 1999, online version, URL http://www.defenselink.mil/news/Oct1999/b10141999_bt478-99.html.

[54] DoD News Briefing, Friday, 26 March 1999 – 5:20 p.m. Presenter: Mr. Kenneth H. Bacon, ASD PA, online version; Eash, "Harnessing Technology for Coalition Warfare", 33.

> the cockpit. That can be further refined by use of the Predator UAV, which we find to be very useful in doing the sort of precise location, and with latest iterations of software we are able to derive now from Predator imagery very precise location coordinates.[55]

It soon became clear, however, that despite of these new high-tech machines, the ability to search and gain information in the face of bad weather posed a serious problem to the Alliance. Not only were they unable to peer through the layer of clouds, they were also "weathered out" in the beginning of Operation Allied Force, because the Predator was vulnerable to icing, which made flying in cold early spring weather impossible.[56] Even though the UAVs should also have provided imagery for tracking of refugees, by the end of April it had to be admitted that their performance in this domain was insufficient. As a result, NATO promised to intensify air operations not only "for strike purposes but also things like reconnaissance, being able to see what is happening to the internally displaced persons inside Kosovo."[57]

All the high-tech machinery also was not able to overcome the fooling tactics of the Serbs and prevent the Allied planes from hitting tank "dummies". Plus, the slow and low flying aircraft proved particularly vulnerable to anti-aircraft fire: losses totaled fifteen UAVs, most of which are believed to have been shot down by the Serbs, which most likely knew how valuable these reconnaissance and intelligence gathering platforms were for the Alliance. This

[55] DoD News Briefing, Friday, 14 May 1999 – 2:00 p.m. Presenter: Mr. Kenneth H. Bacon, ASD PA. Also participating in the briefing were Gen. John P. Jumper, CINCUSAFE and Major General Chuck Wald, J–5.

[56] DoD News Briefing, Monday, 29 March 1999 – 4:17 p.m. Presenter: Mr. Kenneth H. Bacon, ASD PA.

[57] Jamie Shea at the Press Conference given by NATO Spokesman, Jamie Shea and Colonel Konrad Freytag, SHAPE, 25 April 1999, updated 25 April 1999, Washington.

loss seems considerable, but UAVs are designed deliberately at acceptable cost to be dispensable, because there is no other ISR option available that promises equally low risk of pilots lives.[58]

2.1.2 Precision Navigation and Positioning: Smarter Weapons, Less Collateral Damage

Precision navigation and positioning have enhanced both weapons and delivery platforms to target and hit with greater accuracy. A GPS-Aided Targeting System (GATSGAM) on board of the airplanes helps to constantly update weapons such as the new Joint Direct Attack Munition (JDAM) as to where they are in space:[59] When these bombs depart the airplane they have updated knowledge of where they are supposed to go on the planet's surface, using GPS information in flight to guide them to that point.[60] Apart from precision-guided munitions that are directed at geo-located coordinates, modern aircraft sensors, targeting systems, space support, integrated intelligence, and precision navigation equipment allow fairly accurate delivery of unguided ordnance, also called gravity or "dumb" bombs. Major General Wald explains in one meeting how laser-guided bombs that cannot be guided through the clouds could instead be dropped ballistically:

> There's a computer-controlled system in the aircraft that has GPS – Global Positioning Satellite – inputs as well as internal navigation system input that tells you when you're at the exact right place to drop

[58] Joint Chiefs of Staff, *Joint Statement on the Kosovo After Action Review*.

[59] The new Joint Direct Attack Munition (JDAM) employed by the Americans were rendered into "smart bombs" (that were in short supply) by adding a global positioning satellite guidance system onto a basic gravity bomb, with comparatively low cost ($18,000 each), turning them into what was called "precision-guided, all-weather munitions" that can be programmed in flight.

[60] DoD News Briefing, Wednesday, 5 May 1999 – 2:00 p.m. Presenter: Captain Mike Doubleday, DASD PA. Also Participating: Maj. Gen. Chuck Wald, J–5 and Brig. Gen. Leroy Barnidge Jr., 509th Bomber Wing.

> the bomb. With that type of delivery, the bombs are very, very accurate. We're talking instead of several feet of accuracy, probably in the category of maybe 10 meters or 15 meters.[61]

To morally and legally justify the intensive air war that expanded to highly delicate areas such as cities, almost 100% precision in the delivery of bombs had to be assured; only through the development in precision strike capabilities could the Alliance assure halfway credibly that they were going only after militarily significant targets, wanted to keep collateral damage at a minimum, and were taking all possible measures to avoid civilian casualties.

The avoidance of civilian casualties and collateral damage through precision strike munitions also meant considerably higher expenses; these were publicly questioned when it came to measuring success in getting at the Serb forces in the field: the Yugoslav army, experts at camouflage, deception, and the use of decoys, thoroughly fooled the Alliance. The question put forward by a reporter "are you using million-dollar munitions to hit 10'000–dollar targets and does this make military sense,"[62] accurately voiced the problem, even more so as it became clear at the end of the campaign that hardly any of the Serbs' armor in the field had been destroyed.[63]

Again, the weather was a serious problem. Generally, NATO is claimed to have had the capability to operate even through solid cloud cover,[64] and the most important reason why there were restrictions imposed on the operations in bad weather was the commitment to only strike military and military-related targets. Many of the weapons in use required laser guidance, which could not

[61] DoD News Briefing, Tuesday, 18 May 1999 – 2:10 p.m. Presenter: Mr. Kenneth H. Bacon, ASD PA. Also Participating: Major General Chuck Wald, J–5.

[62] Press Conference by Jamie Shea and General Wesley Clark, 27 April 1999, updated 27 April 1999, NATO HQ, Brussels.

[63] Bendrath, Ralf, "Bombiger Erfolg oder peinliche Lügen?", *telepolis,* 30 August 2001.

[64] Joint Chiefs of Staff, *Joint Statement on the Kosovo After Action Review*.

penetrate through very thick cloud cover, or even required visual recognition of the targets.[65]

Another problem met was the over-proportional attention collateral damage incidents received, even though the percentage of the precision weapons that did not hit their targets or went astray remained comparatively low.[66] The more the "surgical precision" of weapons was praised, the heavier mistakes weighed. Not only does technology have the tendency to appear faultless, the "zero-death" expectations raised for pilots as well as for innocent civilians on the ground evoked by this high-tech war also were substantial, even though military officials stressed repeatedly that there was no doubt that at some stage during the operation some weapons might miss,[67] not only because pilots were in a difficult situation flying in fear of a dangerous air defense system, and flying through tricky weather but also, as they said, because "not every single piece of mechanical equipment operates 100%, 100% of the time".[68]

When collateral damage and mistakes began to occur more often, the considerable height on which the planes flew, 15'000 feet, was questioned frequently; military briefers usually stressed that the height did not matter at all for precision-guided munitions, but admitted that for the ballistic dropping using a GPS system, the altitude from which the drop occurred would affect the accuracy of the bomb "somewhat".[69] In any case, the 15'000 feet ceiling

[65] Press Conference given by NATO Spokesman, Jamie Shea and SHAPE Spokesman, Major General Walter Jertz (no date) updated 10 May 1999, NATO HQ, Brussels.

[66] Around 99.9 %, according to Wald, DoD News Briefing, Tuesday, 4 May 1999 – 2:00 p.m. Presenter: Mr. Kenneth H. Bacon, ASD PA. Also participating is Major General Chuck Wald, J–5.

[67] Wilby at the Press Conference by NATO Spokesman, Jamie Shea and Air Commodore David Wilby, SHAPE, 26 March 1999, updated 26 March 1999, NATO HQ.

[68] DoD News Briefing, Saturday, May 8, 1999, 11:05 a.m. Presenter: Mr. Kenneth H. Bacon, ASD PA. Also participating is Major General Chuck Wald, J–5.

[69] Wald at the DoD News Briefing, Friday, 14 May 1999.

was an irrevocable political constraint and even though there were statements that this limit has been broken several times despite the air defense danger, it was an awkward contrast to the claim that all possible measures were taken to avoid civilian casualties, seriously undermining the Alliance's credibility.[70]

2.1.3 Information Collection and Dissemination: Free Flow of Information Alters Warfare

A thoroughly new development in IACs as opposed to the total wars in the 20th century is that all possible channels with the other side remain open throughout the campaign: phone-calls, faxes, E-mails, they continue to cross boundaries.[71] In Kosovo, the interlinked networked world created the circumstance of relative transparency that made it easier for both sides to anticipate each other's next move and also personalized and documented the conflict in a unique way.

The military was aware of the impact of instantaneous broadcast, the global availability of the same data and information to all the conflict parties, and effects on strategic direction and the range of military operations. The Alliance saw in Milosevic an "opponent with a very comprehensive intelligence-gathering organization".[72] They stressed more than once that too much information given at the briefings would jeopardize troop's safety and endanger projects and operations, especially because they believed that the Serbs monitored TV very closely and used that information to make various defensive calculations.[73] Some of the problems with getting at

[70] Ignatieff, Michael, *Virtual War. Kosovo and Beyond* (London, Chatto and Windus: 2000): 105; also see Jumper at the DoD News Briefing, Friday, 14 May 1999.

[71] Ignatieff, *Virtual War*, 138–139.

[72] Wilby at the Press Conference by NATO Spokesman, Jamie Shea and Air Commodore David Wilby, SHAPE, Transcript 5 April, updated 5 April 1999, NATO HQ.

[73] DoD News Briefing, Monday, 29 March 1999 – 4:17 p.m. Presenter: Mr. Kenneth H. Bacon, ASD PA.

the Serbian troops on the ground were explained with Milosevic's ability to guess when and where hits would be made:

> It is a very cunning enemy out there, they know when we take off, because the numbers of reporters and people that are sitting outside the various air bases, they can calculate how long we're going to be before we enter the area and they make sure that during those times they go very much into their hideaway positions.[74]

The Alliance was also aware of the fact that the Yugoslav army had a network of "ham radio" operators who monitored communications among aircraft. Because the lack of interoperable secure communications among the nations forced them to rely on non-secure methods of transmission,[75] they had to assume that some of the aviators' conversations could be heard, which likely gave advance warning of some targets.[76] The Alliance wanted to side step the problem by using code words that were changed at least daily, but this measure only proved partially successful.[77]

Next to these impacts on military operations, Kosovo saw the rise of one very important issue: the use of the Internet in conflicts. It is the first armed conflict in which all sides, including a variety of actors not directly involved, had an active presence on the Internet, and the first conflict where there was extensive use of the Internet for the exchange and publication of conflict-relevant information, some of which could only be found online.[78] This paper addresses

[74] Wibly at the Press Conference by NATO Spokesman, Jamie Shea and Air Commodore David Wilby, SHAPE, Transcript 6 April, updated 6 April 1999, NATO HQ.

[75] Joint Chiefs of Staff, *Joint Statement on the Kosovo After Action Review*.

[76] Bacon at the DoD News Briefing, Monday, 17 May 1999.

[77] DoD News Briefing, Saturday, 1 May 1999 – 12:00 noon. Presenter: Mr. Kenneth H. Bacon, ASD PA (Also participating in this briefing was Major General Chuck F. Wald, J–5).

[78] "There is information about this war that you will only find online": John Pike, director of the Space Policy Project at the Federation of American Scientists cited in Lynch, April, "Kosovo Being Called First Internet War", *San Francisco Chronicle*, 15 April 1999.

the matter in two separate chapters: the upcoming "Information Warfare" chapter deals with aggressive and harmful aspects; this one looks at the "peaceful" use of the network to spread information. First-hand accounts of events as they were being witnessed from individuals inside Yugoslavia posted to the Internet, mostly stories of fear and devastation, might not directly have had impact on the waging or the outcome of the war, but the Web helped to personalize human beings in Yugoslavia in some ways, even if, as previously noted, the Internet does not necessarily help to overcome prejudices as the likeliness of "selective avoidance", a social psychology concept, even increases during conflicts.[79]

Organizations and individuals throughout the world used the Internet to publish information on the conflict. Governments and government-related organizations tended to upload material that supported their official policies. NATO used the Internet as primary distribution channel for material such as spy satellite imagery that showed targets before and after they were hit, cockpit videos, transcripts of press conferences and morning briefings, as well as slides presented there. In some more clearly politically motivated cases, it was also used to request support for political activities: the London based Kosova Task Force for example relied on the Internet to coordinate its actions: to mobilize support it distributed action plans to Muslims and supporters of Kosovo.[80] Serbs used E-mail distribution lists to reach tens of thousands of users, mostly in the USA. These E-mails that were for the most part sent to American new organizations called for an end to the bombing, some of them using heated

[79] Goodman, Ellen, "Kosovo – our first Internet War", *Reporternews.Com*, 9 April 1999, online version, URL www.reporternews.com/1999/opinion/good0409.html.

[80] Denning, Dorothy E, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", presented at Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking Workshop, 10 December 1999, online version, URL http://www.nautilus.org/info-policy/workshop/papers/denning.html, 11.

anti-NATO rhetoric, others containing moving stories describing life under the bombs.[81] Some Newsgroups were flooded with thousands of postings on Kosovo each day. Most of the contributions just aimed at fighting a war of words, abusing the other side. Others however contained interesting information and rumors, or they questioned the reliability of NATO's press briefings, pointing to inconsistencies in its story. On one military string of E-mails, plane spotters noted the take-off times of aircraft from British bases, information that might have been useful for the Serb military.[82]

It is indeed likely that both sides' intelligence services monitored the digital traffic. In anticipation of Serbian censorship measures, Western private parties set up anonymous remailers, so that individuals that feared government reprisals could post their messages to discussion forums without being identified. However, censorship or attempts to change outgoing E-mail messages did, if at all, occur sporadically:[83] it appears likely that this kind of information flow across battle lines appeared too valuable to be stopped. NATO deliberately did not bomb Internet service providers or shut down the satellite links bringing the Internet to Yugoslavia, because "full and open access to the Internet can only help the Serbian people know the ugly truth about the atrocities and crimes against humanity being perpetrated in Kosovo".[84] Serbs thought that it would evoke sympathy and make the Western public more doubtful of their leader's actions, eventually undermining public support, while NATO thought that communication of the Serbian people with democratic voices in the West would weaken their morale and in turn their support of the regime.

[81] Ibid., 5–8.

[82] Taylor, Ros, "UK: Partisans Wage Virtual War", *The Guardian*, 22 April 1999.

[83] Dennis Longley, professor at the Information Security Research Center at the Australia Queensland University of Technology, cited in Denning, "Activism, Hacktivism, and Cyberterrorism", 6–7.

[84] James P. Rubin, spokesman for the US State Department cited in Ibid., 1.

While the first assumption was partly right, the second was not: hopes that communication of the Serbian people with democratic voices in the West would undermine their support of the regime remained fruitless; even though Serbs had access to Western new reports through the Internet, satellite and cable television, many simply did not believe what they saw and heard from Western media: they considered coverage on Western television stations such as CNN and Sky News to be as biased as the on the Yugoslav stations.[85]

In this conflict in which public opinion was the main target of political rhetoric, the Internet became a valuable tool for more and especially different information. As the NATO briefings began to evoke an escalating sense of frustration and irritation among journalists – the Alliance's aggressive information policy also included the feeding of false and speculative stories[86] – they looked for other ways to get to relevant information. Transcripts of press briefings show that journalists actively used the Internet as an alternative source of information parallel to the official information provided.[87] This aspect is important for credibility-struggles: in the extensive media war, it was not enough to justify actions, trying to show that right was on the Alliance's side and stressing that the military action was effective: alternative sources of information seriously

[85] An article in US News quotes Ann Pincus of the US Information Agency saying, "the vast majority of war coverage [from Western sources] that is getting into Serbia is not believed", see Satchell, Michael, "Captain Dragan's Serbian Cybercops. How Milosevic Took the Internet Battlefield", *U.S. News*, 10 May 1999; see also Denning, "Activism, Hacktivism, and Cyberterrorism", 4.

[86] Goff, Peter (ed.), *The Kosovo News and Propaganda War* (Vienna, the International Press Institute: 1999).

[87] For example Jake Lynch (Skynews) during the Press Conference by NATO Spokesman, Jamie Shea and SHAPE Spokesman, Major General Walter Jertz on 14 May 1999, NATO HQ, Brussels: "Just before I came in colleagues in London picked up reports on an internet site which has proven reliable on previous incidents to a certain extent, according to which 20 refugee tractors were destroyed in this attack (…)".

challenged the Alliance's credibility more than once, causing danger of not only losing the propaganda battle against the enemy but also at the home front.

2.2 Information Warfare against Serbia: Physical Attacks Predominate

During Operation Allied Force, both sides used information warfare aspects to harm the enemy. Much of this involved traditional use of propaganda and the media, but there were also extensive efforts to intercept the other side's communications, jam or deceive sensors, and conduct other forms of electronic warfare.[88] The most important pillar proved to be the physical attack and destruction dimension. Defensive aspects, equally important next to the attack dimension of information warfare activities, remained of minor importance in the campaign.

Due to the muddle in the taxonomy, clear cataloging of information warfare activities is tricky. In slight variation from the Air Force Information Superiority construct, the first chapter follows the official NATO rhetoric that emphasized offensive Command and Control Warfare ideas. Information attacks make up the second chapter, in which much emphasize is laid on the aggressive use of the Internet. The last chapter considers public affairs operations that do not range in the AFDD structure but are essential in both the FM 100–6 and the JP 3–13 idea of Information Operations and fit well into the definition of IO proposed in chapter III.1.7.

[88] Cordesman, Anthony H., *Defending America. Redefining the Conceptual Borders of Homeland Defense. Critical Infrastructure Protection and Information Warfare*, Rough Draft for Comment (Washington D.C., Center for Strategic and International Studies: July 19, 2000): 45. Newer Version, Final Draft for Comment, December 8, 2000, available online, URL http://www.csis.org/homeland/reports/dacriticalipiw.pdf.

2.2.1 Striking at the Command and Control Ability

Offensive Command and Control Warfare (C2W) is anti-head or anti-neck warfare to “decapitate” the enemy’s command structure from its body of command forces.[89] This concept is not new, but efforts to coordinate C2W aspects in a joint, high-tech environment have only been undertaken recently. The five pillars of C2W are:

- *Physical Destruction*; the application of combat power to destroy or neutralize enemy forces and installations;
- *Psychological Operations (PSYOP*); inducing or reinforcing foreign attitudes and behavior favorable to the friendly force;
- *Military Deception*; actions to mislead adversary military decision makers as to get foes to take specific actions/ inactions that contribute to the accomplishment of the friendly mission;
- *Electronic Warfare (EW);* actions involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or attack the adversary;
- *Operations Security (OPSEC)*; measures that eliminate or reduce the vulnerabilities of friendly actions to adversary exploitation.[90]

Even though NATO’s justification for being involved in the conflict and its military objectives were altered several times during Operation Allied Force, at the core remained the intention to weaken the Yugoslav military and security forces in order to impair their ability to wage combat operations. At the very first Allied Force press briefings in Brussels, General Clark said:

> We are going to systematically and progressively attack, disrupt, degrade, devastate and ultimately destroy these forces and their facilities and

[89] Libicki, *What is Information Warfare*.

[90] Department of the US Army, FM 100–6, chapter 1 and 3.

> support, unless President Milosevic complies with the demands of the international community.[91]

This implicitly is a declaration to apply Command and Control Warfare (C2W) since it seeks to weaken the adversary's ability to direct the disposition and employment of forces. FM 100–6 at one stage states that the complexity and range of today's MIE increases the difficulty of achieving a comprehensive disruption of an adversary's C2 capabilities through any singly attack or application of combat power: that makes the integration of the five pillars of C2W essential.[92] Accordingly, aspects of the four offensive aspects of C2W can be distinguished in Kosovo, with strong emphasis on the physical destruction pillar. The four following chapters explore those aspects. The principal problem with the Serbian C2-infrastructure proved to be its dual-use character: the dual-use nature of targets created rightful questions concerning the Alliance's selection of targets, particularly since the Alliance kept insisting they were only targeting militarily significant targets while taking all possible measures to avoid civilian damage.

2.2.1.1 Physical Destruction: Dual Use Character of C2 Targets

Physical attacks were directed against the Serbian air defense system, command and control facilities and infrastructure, as well as against forces in the field. The attacks against the C2 aimed at degrading the infrastructure and facilities permanently or for a period of time, employing the latest generation of air-delivered munitions. The most prominent C2 targets included the following:

[91] Press Conference by Secretary General, Dr. Javier Solana and SACEUR, Gen. Wesley Clark, Transcript 25 March 1999, updated 25 April (sic) 1999, NATO HQ – 15.00 Hours.

[92] Department of the US Army, FM 100–6, chapter 2.

- *The destruction of the Yugoslav and Serbian interior ministries in Belgrade on April 3*;[93]
- *The headquarters of the Serbian Socialist Party and Milosevic's private residence on April 21*: General Marani reports that in support of NATO's effort to disrupt the regime and degrade the FRY propaganda apparatus, Allied forces struck directly at President Milosevic's primary communications and stresses that these targets formed an integral part of the strategic communications network;[94]
- *The Serbian state television building on April 23*: selection of this controversial target was justified by declaring that the building not only orchestrated much of the regime's propaganda program but also housed a large multi-purpose communications satellite antenna dish that was an integral part of the FRY's command, control and communications network;[95]
- *On April 30 the VJ headquarters and Defense Ministry*;[96] "because they are the brain that guides the operations in Kosovo";[97]
- *Power transmission facilities at Obrenovac and elsewhere on May 2*: These strikes took out the five main electric yards that distributed power to the Serb armed forces, "the power which supplies his airfields, his headquarters, his communication

[93] Press Conference by NATO Spokesman, Jamie Shea and Air Commodore David Wilby, SHAPE, Transcript 3 April, updated 3 April 1999, NATO HQ.

[94] General Marani at the Press Conference given by Jamie Shea, General Giuseppe Marani and Commander Fabrizio Maltinti, 21 April 1999, updated 21 April 1999, NATO HQ.

[95] Konrad Freytag at the Press Conference by NATO Spokesman, Jamie Shea and Colonel Konrad Freytag, SHAPE, 23 April 1999, updated 23 April 1999, Washington.

[96] Press Conference by Dr. Jamie Shea and Brigadier General Giuseppe Marani, 30 April 1999, updated 30 April 1999, NATO HQ.

[97] Morning Briefing by Mr Jamie Shea, 30 April 1999, updated 30 April 1999, NATO HQ.

systems, his command-and-control network and no power means no runway lights, no computers, no secure communications." They were done by using "graphite bombs" causing the transformer yards to short out rather than disabling the generators themselves;[98]

- *Start of serious bombing of Yugoslav electricity grid on May 23*:[99] heavier munitions took the grid out completely. NATO stressed that by cutting off electricity they forced the Yugoslav army to divert large amounts of fuel to very fuel inefficient generators, "another way of choking off their military's ability to move and to support itself".[100]

The Serbian command and control infrastructure had a thorough dual-use character: General Clark reported that there were more than 100 radio relay sites around the country, that most of the commercial systems served the military, and that the military systems likewise could be put to use for the commercial system. Obviously, everything was interconnected and no distinction between military and commercial could be made easily.[101]

The dual-use nature of targets such as bridges, television stations and electrical transformers created numerous questions concerning the Alliance's intentions. Various times, briefers had to admit, often not candidly, that their strikes had an effect on the civilian population; the most effective C2-strikes were often also the most problematic in the light of civilian suffering. One of the turning points in the campaign were the "clean strikes" against the transformer yards with graphite bombs, taking out electricity in major cities for

[98] Shea at the Morning Briefing by Jamie Shea, NATO Spokesman, 3 May 1999, updated 3 May 1999, NATO HQ.

[99] Morning Briefing by Jamie Shea, 23 May 1999, updated 23 May 1999, NATO HQ.

[100] Major General Jertz at the Press Conference by Mr Jamie Shea, NATO Spokesman and Major General Walter Jertz, SHAPE, 28 May 1999, updated 28 May 1999, NATO HQ, Brussels.

[101] NATO Press Conference, 27 April 1999.

between eight and twenty-four hours. NATO wanted to show that it was able to "disrupt and degrade at will the power that drives the military machine", without harming the civilian population,[102] always stressing that before targeting, great pain had been taken to make sure that facilities such as hospitals would have sufficient uninterrupted power to continue life-sustaining and other essential equipment.[103] The heavier munitions against the grid from May 23 onwards however created a rather problematic credibility problem, more so because NATO stubbornly maintained that the war was not against the Serbian people, even though the air raids caused a breakdown of the water supply in Belgrade and elsewhere.[104] It is likely that these sadly successful strikes sent a very powerful message to the civilian population and helped to drive Milosevic to the negotiation table.

2.2.1.2 Psychological Operations: Leaflets and "Commando Solo"

Defensive Psychological Operations (PSYOP) are based on the projection of truth with credible messages. They are basically designed to convey selected information and indicators to foreign leaders and foreign populations to influence their emotions, motives, objective reasoning, and ultimately their behavior, to get the "human factor" to favor friendly objectives.

Examples of such operations include promises, threats of force or retaliation, and conditions of surrender.[105] PSYOP can both in-

[102] DoD Morning Briefing, 3 May 1999.

[103] Konrad Freytag at the Press Conference by NATO Spokesman, Jamie Shea and Colonel Konrad Freytag, SHAPE, 23 April 1999, updated 23 April 1999, Washington.

[104] Press Conference by Mr Peter Daniel and Major General Walter Jertz, Mr Isa Zymberi, in Brussels and Mr Fatmir Gashi in Kukes, updated 24 May 1999, NATO HQ, Brussels.

[105] Department of the US Air Force, AFDD 2–5, 11; Joint Chiefs of Staff, JP 3–53, Doctrine for Joint Psychological Operation, July 1996, I–1; and Joint Chiefs of Staff, Joint Publication 1–02, DoD Dictionary of Military and Associated Terms.

volve traditional means like tactical leaflets and loudspeakers, but also carefully coordinated words and deeds to send clear and persuasive messages to selected international actors. Increasing interest of military planners in PSYOP derives from the fact that as a result of the explosion of ICT, nation states are less and less able to control the flow of information across their borders, which makes the subtle manipulation of available information, by selectively denying some information about one's capabilities and intentions, or the introduction of new information into a foe's decision-making process, supposedly easier. The growing likeliness of low-intensity conflicts in urban settings, with daily contact to local residents, further facilitates these operations.[106]

In Kosovo, PSYOP operations were no great success. The two main activities consisted of dropping leaflets and broadcasting Western information: By the end of May, the Alliance had dropped over 50 million leaflets, most of them dumped off aircrafts and then letting the wind carry them away. Several different types of leaflets were released, both in English and in Serbo-Croatian.[107] One of them featured the picture of an Apache helicopter saying: "We are coming to get you" and "Don't wait for me!",[108] others warned Serbian troops "Remain in Kosovo and face certain death", or explained NATO's actions to the Serbs: "Hundreds of thousands of refugees are fleeing Milosevic's pogrom. Do not allow misguided patriotism to bind you to his atrocities."[109] Major General Wald

[106] Williamson, Charles A., "Psychological Operations in the Information Age", in: Campen and Dearth, *Cyberwar 2.0: Myths, Mysteries and Reality*.

[107] DoD News Briefing, Friday, 28 May 1999 – 1:35 p.m. Presenter: Mr. Kenneth H. Bacon, ASD PA. Also participating in this briefing are Lieutenant General Mike McDuffie, J–4 and Major General Chuck Wald, J–5.

[108] Morning Briefing by Jamie Shea, 22 May 1999, updated 22 May 1999, NATO HQ. Some of them were publicly shown at the DoD Press briefing at May 28; cf. Jertz, Walter, *Krieg der Worte, Macht der Bilder. Manipulation oder Wahrheit im Kosovo-Konflikt?* (Bonn, Bernhard & Graefe: 2001): 92.

[109] Satchell, "Captain Dragan's Serbian Cybercops"; Jertz, ibid.

called these leaflets “factual propaganda”,[110] that seemed to be having an effect from the standpoint of letting Serbian forces know that there was another side to the story.[111] However, there was never any indication that any of these had had an effect on the moral of the Serb forces. An official Yugoslav Army spokesman later called the leaflets “clumsily, almost amateurishly written, lacking the basic knowledge of the people’s spirit”, as well as featuring poor Serbian wording and syntax.[112]

The other major PSYOP operation was the employment of “Commando Solo” planes, flying radio stations transmitting one-hour programs four times daily. They broadcasted NATO briefings, some of the news reports from independent journalists via Radio Free Europe and Voice of America, for both television and radio, interspersed with European pop music.[113] The efforts were unable to affect the FRY state media: “Commando Solo” was hampered by the air defense threat in the area, when it tried to broadcast directly to the Yugoslav troops, being an easy target as a slow moving platform. Fear of anti-aircraft also let it fly far away from Belgrade, its signals being far too weak to affect TV coverage at all.[114] The conclusion: Attempts to influence Serbian emotions and motives with credible messages failed. Milosevic kept the Information Superiority over his own people at all times.

2.2.1.3 Military Deception: Effective Hide and Seek

Military deception is the primary means to influence the adversary commander’s decision through distortion, concealment, and/or falsification of friendly intentions. The goal of deception is to mislead adversaries, causing them to act in accordance with the originator’s objectives cause.[115]

[110] DoD News Briefing, Thursday, 27 May 1999.

[111] DoD News Briefing, Friday, 28 May 1999.

[112] Arkin, William M., “NATO’s Info Strategy Bombs”, *Special to Washington Post*, 26 April 1999.

In Kosovo, an absolute low-tech deception tactic aimed at the Alliance was painfully effective: The Serbs cover and conceal tactics as well as the effective use of decoys led to the dropping of million-dollar weapons on dummies such as fake bridges and sham tanks.[116] At official NATO briefings numbers of destroyed tanks and armored vehicles were distributed regularly, however, when the Serbian forces retreated in mid-June in their tanks it became obvious that these reports had been greatly exaggerated.[117]

On the Allied side, the twenty-four Apache helicopters, designed for combat support in a ground invasion, that were deployed to Albania together with the 5'000–man Task Force Hawk in early April, most probably served to give Serbian military the impression that ground troops were imminent. It is not certain whether this deceit was planned or not. Even though president Clinton had ruled out the ground options in the run up to the congressional elections in 1998, the Task Force Hawk in Albania, combined with the increasing public discussion of the possibility of and planning for the use of ground forces, is likely to have given the impression that NATO would further step up its campaign at all costs.[118]

Other military deception efforts are kept classified, but some reports claim that NATO was able to penetrate some Serbian air defense systems in order to manipulate and alter data to protect some of NATO's attacking aircraft.[119] It is uncertain how much of the false target information actually appeared on Serbia radars and data read

[113] DoD News Briefing, Friday, 28 May 1999.

[114] Satchell, "Captain Dragan's Serbian Cybercops".

[115] Department of the US Army, FM 100–6, chapter 3.

[116] Ignatieff, *Virtual War*, 105.

[117] Goff, *The Kosovo News and Propaganda War*, 46.

[118] Joint Chiefs of Staff, *Joint Statement on the Kosovo After Action Review*. The numerous political and military challenges the use of the Apache's faced, culminating in the only deaths the Alliance had to mourn when two pilots crashed in a training mission on May 5, will not be given more room here.

[119] Cordesman, *Defending America*, 47.

outs. The primacy method of attack seems to have been the use of false radar images supported by false communications and emissions designed to deceive Serbian electronic intelligence.[120]

2.2.1.4 Electronic Warfare: Up Against the Serbian Air Defense

Electronic Warfare (EW) is any military action involving the use of electromagnetic and directed energy to manipulate the electromagnetic spectrum or to attack an adversary, employing both offensive electronic attack and defensive electronic protection.[121]

Electronic Warfare operations in Kosovo are not very transparent and belong to the classified secrets of modern warfare. It is likely that they were mainly directed at the threatening Serbian air defense, supporting Command and Control attacks through jamming. Electronic intelligence and electronic warfare aircraft were employed in numbers roughly equivalent to those anticipated for a major theater war, but the Serbian air defense capabilities remained a threat throughout the entire campaign:[122] Because these systems often turned off their radar, they prevented NATO radar-seeking missiles and electronic jamming equipment from fixing on them.[123] The system was well connected and well integrated with fiber-optic cables, the Yugoslav air defense forces well trained, and the equipment, though not state-of-the-art, in good shape. Shorter-range Serbian antiaircraft artillery and man-portable air defense systems were numerous, and their locations were difficult to predict.[124] While electronic warfare planes succeeded to suppress air defenses, they could not destroy them: their continued existence led commanders and politician to define altitudes for operation beyond

[120] Aviation Week and Space Technology, 1 November 1999, 33–36.

[121] Schleher, Curtis D., *Electronic Warfare in the Information Age* (Boston, Artech House: 1999): 1– 8.

[122] Joint Chiefs of Staff, *Joint Statement on the Kosovo After Action Review*.

[123] Eash, "Harnessing Technology for Coalition Warfare", 34.

[124] DoD News Briefing, Tuesday, March 25, 1999 – 1:45 p.m. Presenter: Mr. Kenneth H. Bacon, ASD PA.

the range of most of the Serbian anti-aircraft systems.[125] The 15'000 feet's ceiling was questioned repeatedly in connection with collateral damage that seemed to prove that war from such a height was not precise enough.

The (physical) attack against TV stations led to questions concerning the use of electronic warfare and jamming against such targets, mainly because these stations seemed to be able to re-transmit within a few hours. SACEUR replied, that the Alliance was not jamming the transmitters.[126] Major General Jertz later provided an explanation for this statement when he described the efforts that would be necessary to jam transmitters:

> If you really want to jam and do nothing but jamming, you need a continuous effect and to reach continuous effect you need a lot of aircraft for a special amount of time and you would not be able to reach the same amount which we did by using the weapon.[127]

Although NATO forces struggled against the Serbian air defense systems, the FRY forces had minimal success downing manned aircraft. The fear that use of the system would trigger immediate counterattack limited the effectiveness of the air defense, even leading to the occasional firing of missiles without ground-launch guidance signals rather than to expose the air defense systems.[128]

2.2.2 Information Attacks and Cyberwarfare

Information attacks in their military sense refer to activities taken to manipulate or destroy an adversary's information or information system without necessarily visibly changing the physical entity within which it resides. It can thus be seen as a direct attack against

[125] Eash, "Harnessing Technology for Coalition Warfare", 34.

[126] NATO Press Conference, 27 April 1999.

[127] Press Conference by Dr. Jamie Shea and Major General Walter Jertz, 3 May 1999, updated 3 May 1999, NATO HQ.

[128] Joint Chiefs of Staff, *Joint Statement on the Kosovo After Action Review*.

the "observation" and "orientation" component of the OODA-Loop because the adversary's ability to rely on "observations" is affected.[129] Because of the proliferation of influential actors however, information attacks in a less military sense can be understood as activities conducted for the exploitation, disruption, or destruction of data by a variety of actors apart from state or the state's organizations.

The Kosovo conflict has readily been dubbed the world's first "Internet-" or "Cyber-War" by the press and even some high officials:[130] the actual meaning of these terms in a security-related context is often left unconsidered as they are used as basic "catchwords". However, it has already been shown that in this armed there was extensive use of the Internet for the exchange and publication of conflict-relevant information. Apart from these defensive actions involving the Internet, there were also incidents offensive in nature.

One example is the so-called "news and propaganda war", a battle for the hearts and minds of the civilian population, which turned cyberspace into some kind of "ethereal war zone" in which a "soft war" was waged through the use of electronic images and words.[131] Some US and British officials claim that the government controlled all four Internet access providers in Yugoslavia and only kept them open for the purpose of spreading disinformation and propaganda.[132] A US News article maintains that more than 1'000 volunteers in Belgrade, mainly students, worked intensively to debate in chat rooms, translated articles into English, updated web

[129] Department of the US Air Force, AFDD 2–5, 15.

[130] Deputy Secretary of Defense John Hamre boasted at a symposium on information assurance in mid-April 1999 that this was "the first cyber war we're fighting": "Hamre: Balkans Fighting Called 'First Cyber War'", PR Newswire, 19 April 1999, online version, URL http://www.infowar.com/mil_c4i/99/mil_c4i_042399a_j.shtml.

[131] Dunn, Ashley, "Crisis in Yugoslavia – Battle Spilling Over Onto the Internet", Los Angeles Times, 3 April 1999.

[132] Denning, "Activism, Hacktivism, and Cyberterrorism", 2.

sites, and networked with anti-NATO groups around the world.[133] Whatever true, the Internet became a new global propaganda tool for both sides during the campaign in Kosovo. Even though many articles wildly hypothesize and speculate on "war in cyberspace", circulating grotesque stories of what they considered to be part of a raging "Internet War", some aspects of the Internet- or Cyberwar are likely to have occurred and to be of lasting importance for the future of conflicts.

Apart from the propaganda war, one pattern that seems of significance is the offensive online activity called "hacktivism". "Hacktivism" stands for the merger of hacking and activism, covering operations that use hacking techniques for political-activist reasons, mostly directed against a target's Internet site with the intent to disrupt normal operations but not causing serious damage.[134] In hacktivism, the Internet is mainly used to draw attention to a cause, helped by the news media that report readily and regularly on such incidents. This was also the case with attacks on various Internet servers during the Kosovo conflict. Disruption of the NATO server began on March 27: the attacks included so called "Ping"-bombardment to cause denial of service, E-mail spamming attacks as well as viruses. Jamie Shea said on that matter:

> It seems that we have been dealing with some hackers in Belgrade who have hacked into our Website and caused line saturation of the server by using bombardment strategy. At the same time, our E-mail system has also been saturated by one individual who is currently sending us 2,000

[133] Satchell, "Captain Dragan's Serbian Cybercops".

[134] Bendrath, Ralf, "Der Kosovo-Krieg im Cyberspace. Cracker, Infowar und Medienkrieg“, *telepolis*, 19 July 1999. The next step and final category in the escalation ladder would be "Cyberterrorism", the convergence of cyberspace and terrorism, intended to cause grave harm. There have not been acts of cyberterrorism ever so far.

> E-mails a day. And we are dealing with macro viruses from Yugoslavia into our E-mail system.[135]

After the bombing of the Chinese embassy in Belgrade, Chinese hackers joined the online war, targeting US government sites including the White House site, which was unavailable for three days.[136] These kinds of denial of service attacks are directed only against an organization's public face and relatively harmless, even though they are considered to be an embarrassment for organizations like NATO, especially during a war in which one part tries to convince through the display of its high-tech force.

A step further up the aggression ladder are those actions which not merely deny information but also destruct by replacing content: The Serbian hacker group CHC for example substituted two US government sites for anti- NATO sites at the beginning of April, calling NATO the "National American Terrorist Organization". On the other side, "Dutchthreat", a Dutch hacker group, broke into Yugoslavian Web servers, replacing an anti NATO site with a pro-NATO "Help-Kosovo" page. Several Russian hacker groups also participated in targeting and changing NATO websites.[137] A Serbian newspaper even claimed that a member of the hacker group "Black Hand" broke into a Navy computer and deleted all data. DoD officials never commented on the incident, nevertheless, Navy servers did remain temporarily unavailable at the end of March.[138] The Hacker News Network later announced that around 14 military or

[135] Press Conference by NATO Spokesman, Jamie Shea and Air Commodore David Wilby, SHAPE, Transcript 31 March 1999, updated 31 March 1999, NATO HQ.

[136] Brewin, Bob, "Cyberattacks Against NATO Traced to China", *Federal Computer Week*, 2 September 1999.

[137] Archive of Hacked Website: Digital R3sist4nc3 online version, URL http://freespeech.org/resistance, see also Bendrath, "Der Kosovo-Krieg im Cyberspace".

[138] Bendrath, "Der Kosovo-Krieg im Cyberspace".

other governmental website were hacked in connection with Operation Allied Force.[139]

There remains the question whether any of these attacks were state-sponsored and so fall under the definition of strategic information warfare. A report from the Center for Strategic and International Studies (CSIS) on homeland defense makes it sound that way when it says: "Serbia launched a computer attack on the NATO web page – perhaps the first attack of its kind."[140] Other sources maintain that it is rather doubtful that the Yugoslav government orchestrated these attacks.[141] Successful attacks against internal Allied military command and control networks are unlikely anyway because they run over separate channels not directly accessible over public networks, with high security measures as well as operating systems and software that is not commercially available and therefore cannot be exploited for "bugs".[142] Other reports claim that NATO was able to penetrate some Serbian air defense systems in order to manipulate and alter data to protect NATO's attacking aircraft.[143] It is uncertain how much of the false target information actually appeared on Serbia radars and data read outs if at all. The primary method of attack seems to have been the use of false radar images supported by false communications and emissions designed to deceive Serbian electronic intelligence.[144]

There is also rather substantive evidence against the rumors that during Operation Allied Force, the United States launched the first

[139] Available through http://www.hackernews.com/archive/crackarch.html.

[140] Cordesman, *Defending America*, 45.

[141] An after action review of the Serbian attacks on DoD web sites and computer systems asserts that it is not clear if any of these were sponsored by the Serbian government; cf. Wolfe, Frank, "Pentagon Analyzing Serb Attacks on DoD Web Sites", www.infowar.com, 22 June 1999.

[142] Bendrath, "Der Kosovo-Krieg im Cyberspace".

[143] Cordesman, *Defending America*, 47; Hoffmann, Lisa, "U.S. Opened Cyber-War During Kosovo Fight", *Washington Times*, 24 October 1999, C1.

[144] *Aviation Week and Space Technology*, 1 November 1999, 33–36.

offensive "Cyberwar" in history. The numerous publications and press releases on this topic as well as military rhetoric before and even during the conflict raised expectations that this new warfare tool would be employed in conflict. The rumors reached their first height at the end of May, when a Newsweek article reported on the launch of computer attacks on Yugoslav systems by the United States. According to the article, defense analysts said, the US computer hackers burrowed into Serb government E-mail systems to read Belgrade's mind day by day, while some infiltrated their way into the internet systems of banks around the world in search of accounts held by Milosevic and other Serbian leaders.[145] Later in the year, the Washington Times took the story up again and wrote that details remained still classified, but top US military officials had now confirmed that during NATO's air, the United States launched a computer attack on Yugoslav systems in the first such broad use of offensive cyber-warfare during a conflict and had thus "triggered a superweapon that catapulted the country into a military era that could forever alter the ways of war and the march of history."[146]

There are at least two strong points that can be held against most of these claims: Cyber warfare against a relatively low-tech enemy cannot be expected to be overly effective. Right at the beginning of Operation Allied Force, an article set down that according to military experts, NATO's information warfare efforts were likely to be targeted more at radar transmissions than at Web-connected computers, mainly because Yugoslavia had little in the way of an Internet infrastructure, and its military wasn't likely to be using the

[145] Vistica, Gregory L., "Cyberwar and Sabotage", *Newsweek*, 31 May 1999, 22.

[146] Hoffmann, "U.S. Opened Cyber-War During Kosovo Fight"; see also Burns, Robert, "Computer Warfare Used in Yugoslavia", AP, 7 October 1999, online version, URL http://www.infowar.com/mil_c4i/99/mil_c4i_100999b_j.shtml.

Web to communicate.[147] The second point that weighs even stronger is that because Cyberwar ideas are still in their infancy, the US found that there existed neither a clear basis in law for computer-attacks nor any for retaliation against possible Serbian attacks. Other reports state that while the US Air Force planned such cyber-attacks in depth, they were blocked by the US intelligence community that felt that they would do more to corrupt the quality of intelligence collection than damage Serbs operations.[148] The uncertainty surrounding international law, especially because effects of information attacks are still totally unpredictable, evoked fear that their use might make American military commanders liable to war crimes charges.[149] These and other legal constraints for the use of "cyber-weapons" are further explored in chapter IV.2 on the international law affecting Information Operations.

2.2.3 Public Affairs Operations and the Primacy of Sound-Bites

Today, military operations are conducted under the full glare of public scrutiny. IACs are as much fought on the airwaves as on the real battlefield, for public support and credibility. The military is aware that 24-hour media reporting and instant, real-time analysis of events forms public debate and shapes public opinion, indirectly impacting political, strategic, and operational planning as well as decision-making, and might ultimately decide about mission success or failure. ICT and the expansion of international media alliances are expected to affect the conduct of military operations "in

[147] Seminerio, Maria, "Infowar Part of NATO arsenal?", *ZDNet*, 25 March 1999, online version, URL http://www.zdnet.com/zdnn/stories/news/0,4586,2231976,00.html.

[148] Cordesman, *Defending America*, v and 47.

[149] Metz, Steven, "The Next Twist of the RMA", *Parameters*, XXX, 3 (Autumn 2000): 40–53.

a degree equal to that of emerging weapons technologies."[150] The evolution of the global information environment has intensified the demand and competition for information: the pressure to fill more channels of communication has created competition to uncover and report more unique, more captivating stories that ensure interest of the audience.[151] The military faces a similar challenge: it is expected to provide information which is varied enough to meet the demand for a 24-hour media cycle, has to ensure that info is both timely and accurate, and has to be as truthful as possible without endangering life during military operations.[152] A large part of Public Affairs Operations has as strong "gain and exploit" dimension and could be considered as supporting the Information-In-Warfare dimension of Information Operations. Often however, public affairs operations are also conducted to support offensive information warfare activities, in order to help defeat adversary efforts to diminish national will, degrade morale, and turn world opinion against friendly operations.[153] The aggressive news and propaganda war that was waged during Operation Allied Force is the focal point of this chapter.

Milosevic could certainly not defeat NATO in battle: his only chance of success was in breaking Allied solidarity, and that could only come about if Belgrade won the media war. NATO was rightly aware of the fact that it was absolutely crucial to appear unified, strong, and absolutely set if it wanted to hold together an Alliance consisting of nineteen independent states and their populace. Several Alliance members were able to draw on their experience during the Gulf War and Operation Desert Fox (Iraq, 1998) in preparing for the media operation. Some of the key lessons learned were that

[150] United Air Force, AF DD 2–54, Public Affairs Operations, 25 October 1999, 4; see also Department of the US Army, FM 100–6, chapter 3.

[151] Department of the US Air Force, AF DD 2–54, 4–5.

[152] Eyal, Jonathan, "The Media and the Military: Continuing the Dialogue after Kosovo", *RUSI Journal*, 145, 2 (April 2000): 37.

[153] Department of the US Air Force, AF DD 2–54, 8.

one had to deliver clear, simple and effective message, to identify and understand target audiences as well as the real needs of the media, and to integrate media operations firmly into the military campaign.[154]

The end product of these efforts was altered and adapted several times. Basically, NATO applied a strong Anglo-American model of communication policy, inspired by techniques of political marketing which are focused on television audiences and go back at least 40 years, drawing on US experience with media strategy during conflicts.[155] The usual structure of the briefings every afternoon consisted of Jamie Shea, NATO spokesman, giving an update on political development and alternating generals from the UK, Italy, and Germany that reported on military aspects. After slides and cockpit videos, journalists were encouraged to ask questions. These briefings were broadcasted live by CNN, EURONEWS, and other TV stations, entirely at the beginning of the air raids, later only CNN continued. When after the convoy disaster on April 14 critical voices concerning the public affairs operations became louder, more staff, resources, and professional support was added to the information apparatus of the Alliance in Brussels, in order to better coordinate daily briefings from London, Brussels, and Washington. A Media Strategy Group was established to assist Solana and Shea in the definition of the messages and the daily events, as well as the Media Operation Center, a vast operative cell with a twofold aim: to harmonize the information circulated by the capitals and select, out of the media and the political debate of each country, the news that could be useful to the key messages.[156]

[154] Eyal, "The Media and the Military", 37.

[155] Pounder, Gary, "Opportunity Lost: Public Affairs, Information Operations, and the Air War against Serbia", *Aerospace Power Journal*, XIV, 2 (Summer 2000): 56–77; Brivio, Enrico, "Soundbites and Irony: NATO Information is Made in London", in: Goff*, The Kosovo News and Propaganda War*, 514–515.

[156] Brivio, "Soundbites and Irony", 517.

The Alliance was dedicated to occupy the news channels, because every void could be filled with information that was not necessarily welcome. Jamie Shea is quoted as having said, “The one thing we did well in the Kosovo crisis was to occupy the media space. We created a situation which nobody in the world who was a regular TV watcher could escape the NATO message.”[157] Indeed, there was a MoD briefing from London late in the morning, then followed the NATO 3pm briefing, and closely afterwards the Pentagon, State Department, and the White House briefings were held. From April 29 onwards, in addition to the traditional afternoon NATO briefings, journalists received a communiqué with an update on the military operation at 9.30 am, and at 10.30 am there was an off-camera morning briefing with Jamie Shea.[158]

The NATO briefings evoked an escalating sense of frustration and irritation among journalists that came to experience them as mere platforms to disseminate sound bites, effective sentences to be quoted by TV news and newspapers headlines, and blunt NATO propaganda aimed at consolidating the Alliance. The whole strategy aimed at emphasizing the success of the military operation, the political unity of the Allies, and their commitment to the humanitarian aspect, stretched credibility to the braking point: mainly criticized were the growing simplification of the messages and the didactic repetition of certain key messages.[159] The DoD briefings were less rhetorical and by some journalists considered to be more

[157] Shea, Jamie, *The Kosovo Crisis and the Media: Reflections of a NATO Spokesman*, speech before the Atlantic Council of the United Kingdom, Reform Club, London, 15 July 1999, cited in Pounder, “Opportunity Lost”, 12.

[158] Pounder, “Opportunity Lost”, 12.

[159] For example see Hammond, Philip, “A War of Words and Pictures”, *The Independent*, 6 April 1999.

informative.[160] These and other points will be taken up again in the chapter tracking the manageability of IACs, including not only the intensification of news and propaganda war but also problems with credibility and a strained relationship with the media, harmful insofar as in every future conflict, the media will examine official information from an initial standpoint of disbelief.

2.3 Value for Variable X+

Even though new strategic concepts were hardly mentioned publicly, the primacy of Information Operations is an undeclared reality: the previous analysis has shown that the struggle for Information Superiority, top priority of the new military concepts, was ongoing at various levels during Operation Allied Force. In that light, Kosovo qualifies as a stage for future wars in terms of weapons targeted at the information infrastructure to affect the decision processes of both government leaders and the general civilian population. The overall emphasis was laid on Command and Control Warfare, and of its five pillars, physical destruction of the infrastructure was predominant.

The previous analysis allows for an assessment of the level of successful conduct of Information Operations (X+). The next table lists every aspect separately, assigning the values 0 for not successful, 1 for somewhat successful, 2 for successful, or 3 for highly successful to each. Numbers in brackets are an estimation that might be inaccurate due to the degree of unavailable and classified information in this domain. Each of the two sub-branches of IO was assigned a value derived from the average of values. The

[160] Mark Laity, BBC at the Morning Briefing of Jamie Shea, NATO Spokesman, 6 May 1999, updated 6 May 1999, NATO HQ: "(…) the Pentagon briefings which are, to be blunt, far more useful to us than the NATO briefings (…) So I would like to reiterate that not just from our point of view, but from your point of view, you would be better off if you were giving us more of what the Pentagon is giving us."

overall level of success is likewise the arithmetical mean of the nine different aspects.[161]

Information Operations				Level of Successful Conduct	
Information-In-Warfare Gain & Exploit			Intelligence, Surveillance, Reconnaissance (ISR)	1	(1.666)
			Precision Navigation and Positioning	2	
			Collection and Dissemination Activities	2	
Information Warfare	Attack	C2W	Physical Attack	2	(1.166)
			PSYOP	0	
			Military Deception	(1)	
			Electronic Warfare	(2)	
			Information Attack (Cyberwar)	(1)	
			Public Affairs Operations (aggressive)	1	
				1.333	

Table 14: Level of Successful Conduct of Information Operations (Variable X+)

Explanation:

- *Intelligence, Surveillance, Reconnaissance (ISR):* This aspect of IO was conducted somehow successfully (1). Reasons for the relatively modest level of success are difficulties with intelligence databases, the weather that "weathered out" planes and made it difficult to pear through clouds, and the Serbian air defense that was successful at shooting down numerous reconnaissance aircraft;

[161] By calculating a simple arithmetic mean, this is also done in later occasions, it is assumed that all the different aspects have the same amount of impact. This clearly is an oversimplification of matters, but nevertheless allows an estimation of the level of successful conduct of Information Operations.

- *Precision Navigation and Positioning:* This aspect of IO was conducted successfully (2). Problems arose from technological failures, a shortage of "smart bombs", the weather, and pressure that arose when "collateral damage" became more frequent;
- *Collection and Dissemination Activities:* This aspect of IO was conducted successfully (2). In this domain where a number of different actors were involved, the Alliance handled the dissemination part particularly well by using the Internet as a means to publish conflict relevant information;
- *Physical Attack and Destruction:* This aspect of IO is considered to have been in large parts conducted successfully (2). Even though one can argue that the effects were rather ambiguous not only due to the dual use character of many targets, but also because the Serb forces in the field remained largely unscarred, this main emphasis of the campaign was conducted more or less as expected;
- *Psychological Operations:* This aspect of IO was conducted not at all successfully (0). The actions taken, dropping of leaflets and broadcasting from planes, did not bring about any desired outcome;
- *Military Deception:* This aspect of IO was conducted somehow successfully (1). Many aspects remain classified. Possible Allied deceptions include the penetration of Serbian air defense systems in order to feed it false target information. Serbian deception (low-tech) proved more successful than the possible Allied one;
- *Electronic Warfare:* This aspect of IO was conducted successfully (2). Many aspects remain classified. The jamming of the Serbian air defense and the fear of the FRY forces that use of their systems would trigger counterattack limited the effectiveness of the air defense. NATO was not successful however in jamming Serbian media outlets;
- *Information Attack (Cyberwar):* This aspect of IO was conducted somehow successfully (1). Aspects of Cyberwarfare belong to the highly secretive aspects of military operations and it is uncertain

whether any such attacks were undertaken, especially because of numerous constraints such as legal, ethical, and political considerations. This makes judgment on the level of success difficult. It is assumed that some aspects were conducted with success. In this domain, especially asymmetrical actors were successful (Hacktivism);

- *Public Affairs Operations (aggressive):* This aspect of IO was conducted only somehow successfully (1). Even though the various briefings were organized in detail and the end product of these efforts altered several times, they evoked an escalating sense of frustration among journalists, because it was felt that NATO information was too much blunt propaganda and not enough truth.

The three values for Information-In-Warfare (1.666), information warfare aspects (1.166) and the total level of successful waging of Information Operations (1.333) lead to the following conclusion: The gain and exploit dimension was handled better than the attack dimension. The model would explain this fact by less influence exerted from the intervening and the condition variables. Many gain and exploit aspects rest solely in military hands and depend largely on the military technology available, with system influence having a minor impact. The relationships IntVs →X+ that are explored later verify this assumption.

The value 1.333 for the overall level of success says that IO were conducted some more than a little successfully, but not even close to successful. In the relationship X+ →Y, a low level of success in IOs also predicts a low level of success in this Information Age Conflict. This is supported by the Lessons Learned of the Department of Defense that states that even though the importance of information warfare capabilities was recognized fully during Operation Allied Force, "the conduct of an integrated Information Operations campaign was delayed by the lack of both advance planning and strategic guidance defining key objectives."[162]

[162] Joint Chiefs of Staff, *Joint Statement on the Kosovo After Action Review*.

3 Influencing Factors in Kosovo

Variable E is an exogenous variable symbolizing case specific influencing factors that are not directly system inherent and likely to vary considerably from case to case. Imaginable classification features are weather conditions; geophysical conditions (terrain);

Case Specific Influencing Factor	**(Negative) Influence Exerted During Operation Allied Force**	**Strength of Influence**
Weather Condition	Thick layer of clouds • hampered the collection of data; • hampered the actual bombing operations: weapons in use usually required either laser guidance that could not penetrate through very thick cloud cover or even visual recognition of the targets; • led to lacking ability to cope with the extensive "cover and concealment" tactics of the Serbian militia; • "weathered out" planes vulnerable to icing in the beginning of Operation Allied Force.	3 high
Geophysics/ Terrain	Difficult terrain • to conduct any sort of campaign (heavy vegetation, rugged terrain, mountains, poor mapping, unmarked structures, wires);[163] • helped FRY forces to camouflage their positions (forests, deserted villages, rugged terrain, mountainous areas); • in connection with bad weather dangerous for pilots (mountains).	1 some
Technology: Infrastructure/ Weapons	Information Infrastructure: • Large parts of FRY and its military not very dependent on ICT or the Internet → cyber attacks make little sense State of the art weapon technology: • Human failure factor remains high; • "smart" bombs often not smart enough.[164]	2 reasonable
International Law/ Regime	International Law • clauses protecting civilians mainly hamper Cyberwarfare activities.	2 reasonable
		2

Table 15: Case Specific Influencing Factors (Variable E)

[163] Press Conference given by Mr. Jamie Shea and Major General Walter Jertz, 5 May 1999, updated 5 May 1999, NATO HQ.

[164] "NATO's Weapons. Are They Too Clever by Half? High Technology Against Serbia Has Yet to Prove Itself a Winner", *The Economist*, 1 May 1999, 28–29.

state specific critical infrastructure; technological factors such as modern weapon technology and its functioning in use; as well as constraining international legal conditions and regimes. In Kosovo, the analysis of Information Operations in the previous chapter discloses the following case specific influencing factors:

Case specific influencing factors exerted a reasonably strong influence (2) on the overall conduct of Information Operations.

4 Level of Credibility throughout Operation Allied Force

The value of C can be obtained by tracking the credibility for the whole Operation Allied Force, and by assigning each day/ incident one of the values 0–1–2–3 standing for low credibility to high credibility. The resulting "credibility curve" is a way to illustrate the course of the estimated level of credibility during the campaign. Unfortunately, credibility is hard to measure satisfactorily: here it is understood as the "conjectured truth and honesty of public statements of the conflict parties concerning certain incidents." The ability to form an opinion about it largely depends on information available and is also highly dependent on personal subjectivity and mindset. A further substantial difficulty is that credibility assigned might also vary considerably with elapsed time, when more and different things about certain incidents are discovered that might change the surmised rate of credibility.[165] The following curve is an attempt to judge the level of credibility in retrospect and from a momentary base of knowledge:[166]

[165] For example, according to a report in the "Forensic Science International" Finnish forensic experts found no evidence that Serb security forces massacred ethnic Albanian civilians in the Kosovo village of Racak in January 1999. This incident served many politicians as a reason to go to war against Serbia.

[166] March 2001.

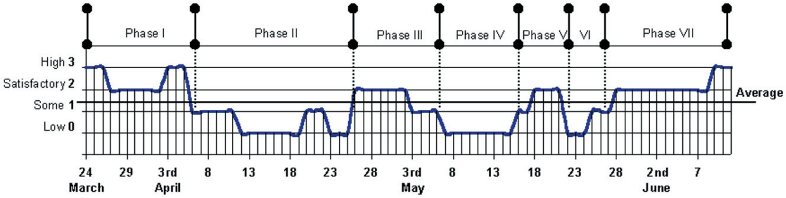

Figure 9: Level of Credibility Curve for Operation Allied Force

Explanation:

- *Phase I (24 March–6 April)*: Initially, the level of credibility was high (value 3). After 27 March, when a US F–117 stealth fighter went down near Belgrade, evasive answers concerning the lengthy and covert operation to rescue the pilot let credibility fall slightly (value 2). It stayed at this at least satisfactory level, even after three US soldiers were captured near the Macedonia-FRY border and shown, bruised, on Serb TV, on 1 April. Two days later, NATO missiles hit central Belgrade for the first time, destroying Yugoslav and Serbian interior ministries, a strong signal of the Alliance's willingness to go through with the campaign, also credibly communicated (value 3);
- *Phase II (6 April–26 April)*: A first severe decline in the level occurred between 6 April and 26: 6 April marked the first serious civilian deaths and started a long series of unintended "collateral damage", when air strikes hit a residential area in Aleksinac, killing five. Official reactions gave a poor impression (value 1). On 12 April, NATO hit a passenger train south of Belgrade, killing at least 30 and even though NATO apologized, investigational inconsistencies and confusing severely damaged credibility even in the aftermath of the incident, even more so, when only three days later, NATO hit a Kosovar civilian convoy, and 64 dead were reported (value 0). Credibility stayed low and only recovered towards 21 April and 22, when NATO missiles hit headquarters of Milosevic's Serbian Socialist Party and his private

residence and strong political signals from the NATO summit in Washington (temporary rise towards 1). The next drawback occurred on 23 April, when NATO destroyed the Serbian state television building, killing at least 10 employees. This was read as a sign of growing frustration about Milosevic's media tactics and generated a lot of uproar all around the world. Again, official statements projected very low credibility (value 0);

- *Phase III (26 April–7 May)*: Credibility was restored somehow over the period at the end of April, when NATO hit VJ headquarters and the Defense Ministry and Reverend Jackson secured the release of the three captured US servicemen following a lengthy meeting with Milosevic on 1 May (back to value 2). In the aftermath of the 2 May incident when NATO hit power transmission facility at Obrenovac, cutting of power in most FRY cities, voices demanding justification concerning the civilian involvement were awkwardly rebuffed by officials (value 1);
- *Phase IV (7 May–16 May)*: The severest setback occurred during the crisis during and after the bombing of the Chinese embassy that lasted until 13 May, further carried on by the killing of about 87 Kosovars in Korisa by NATO bombing. Official statements were lastingly giving the impression of low credibility (value 0);
- *Phase V (16 May–22 May)*: The level lifted slightly on 16 May when a Kosovar refugee reported that Kosovars had been forced to serve as human shields in Korisa (value 1);
- *Phase VI (22 May– 27 May)*: The level plunged again severely on 22 May, when NATO bombs hit and destroyed army barracks at Kosare, being unaware it was captured by KLA a month earlier (value 0). Then NATO began its bombing campaign of the Yugoslav electricity grid, being very effective and forcing major disruption of power and water supplies on the 23. Credibility was low despite the great effect of the strikes because rightful questions concerning the civilian suffering were countered with blunt statements (value 1);

- *Phase VII (27 May–11 June):* Towards the end of the campaign, the level of credibility rose again to its previous height at the end of March, mainly supported by no more "collateral damage" that had to be explained and the diplomatic effort's shifting away attention from the bombing campaign at large (value 2, then 3).

The average value of this curve is below 1.5 (1.33), meaning the overall credibility was fairly low during the whole campaign.

5 Intervening Variables

The following table lists the values for the intervening variables, including a short explanation:

Variable	Explanation	Value
q: Degree of asymmetrical threats faced	• Efficient and very low-tech Serbian deception tactics • Hacking attacks against the public face of the Alliance (hacktivism and probably more harmful attacks) • Very aggressive battle for "hearts and mind" of the engaged parties' population at home: media and propaganda war • Serbian use of cellular phones to warn of NATO take-offs (see below chapter IV,3)	2 reasonable
r_1: Degree of blurring boundaries between states	• Communication flows over national boundaries never stopped during conflict (phone-calls, faxes, E-mails, other uses of the Internet) • Governments have little ability to control information flow over their boundaries: PSYOP and manipulation of information a growing threat • No way to control the use of ones National Information Infrastructure for possibly harmful attacks: servers might be use for illegal activity	2 reasonable
r_2: Degree of blurring boundaries between military-politics	• Political constraints on military considerable: politicians tried to "micromanage" the campaign (due to public pressure) • Ground forces never any real option • Planning and targeting done with constant tension between political and military parties • Legal and moral evaluation of targets was built into their computerized selection • Very strict pilot's rule: pilot's only allowed to fire on visual recognition of a target	3 high
r_3: Degree of blurring boundaries between military-civilian	• Dual use character of targets (electricity grid) • Dual use character of targets in the information infrastructure (cyberwarfare) • Dual use character of many information warfare tools • PSYOP aims largely at the human mind	3 high
s: Degree of multiplication of relevant actor	• Military keeps a lot of the advantage in conflicts, over resources and information (information monopoly still largely rests with the military) • The Internet challenges this information monopoly, but is too diverse too have a major impact • Home based democratic population has a great amount of power over governments that go to war	1 some

Table 16: Values of Intervening Variables (Variables q, r_1, r_2, r_3, s)

The degrees of blurring boundaries between military-politics and between military-civilian domains appear to have been high, both the degree of asymmetrical threats faced and the degree of blurring boundaries between states reasonable, while the multiplication of relevant actors was not particularly strong.

6 Level of Success of Operation Allied Force

The level of success in a conflict can be judged by the degree of how the actual political and military outcome of a conflict differs from the one desired. At the beginning of April, NATO defined five core objectives, both political and military, for the resolution of the Kosovo crisis, which were both endorsed and reiterated at the meeting of NATO foreign ministers, and repeatedly thereafter. These five points became the conditions to Milosevic that would stop the bombing:

- A verifiable end to all Serb military actions and the immediate end of violence and repression;
- The withdrawal of all Milosevic's military police and paramilitary forces;
- The stationing in Kosovo of an international military force;
- The unconditional and safe return of refugees and internally displaced persons and unhindered access for the humanitarian relief organizations;
- The credible assurance of a willingness to work towards a political framework based on the Rambouillet Agreement.[167]

Previous to the declaration of the official five points there was a variation of different objectives stated at various press briefings. Generally, four dimensions can be distinguished: humanitarian aspects regarding the flood of refugees; geopolitical ones concerning the credibility and continuity of NATO as a security institution in

[167] Cited from Press Conference by Jamie Shea and Brigadier General Giuseppe Marani, 14 April 1999, updated 14 April 1999, NATO HQ, Brussels.

Europe; a security-political dimension mainly concerned with deterring spread of the conflict and ensuring lasting stability in the region; and finally purely short-term military aspects to obtain the above. The humanitarian aspect provided the foremost reason for justifying the military intervention. Among the most important of these statements at the beginning of the campaign range:

- *NATO Secretary General Solana's* explanation on the eve of the air strikes that these were undertaken "to prevent more human suffering and more repression and violence against the civilian population of Kosovo (…) and to prevent instability spreading in the region."[168] This covers the humanitarian and the security-political dimensions;
- *US President Clinton's* address to the nation on March 24, differentiating between three main goals of the campaign, being to demonstrate the seriousness of NATO's opposition to Belgrade's aggression in the Balkans; deter Milosevic from continuing and escalating his attacks on helpless civilians and create conditions to reverse his ethnic cleansing; and damage Serbia's capacity to wage war against Kosovo in the future or spread the war to neighbors by diminishing or degrading its ability to wage military operations.[169] The first point is mainly a geopolitical aspect, the second both a security-political and a military motivated dimension, the third purely military;
- A *DoD News Briefing* on March 24 asserting that the military objective of the action was "to deter further action against the Kosovars and to diminish the ability of the Yugoslav army

[168] Press Statement by Dr. Javier Solana, Secretary General of NATO, 23 March 1999; Two days later his wording was slightly different when he said that NATO was determined to continue the campaign until their objectives "to halt the violence and to stop further humanitarian catastrophe" would be achieved.

[169] President Clinton, Address to the Nation, Washington DC, 24 March 1999.

to continue those attacks if necessary" and that these actions were designed to "reduce the ability of the Serbian military forces to continue their offensive operations against the people of Kosovo."[170] This covers humanitarian reasons followed by military ways of achieving these as well as a long-term security-political dimension;

- *General Clark's* specification of the military mission on March 25, saying that it was "to attack Yugoslav military and security forces and associated facilities with sufficient effect to degrade its capacity to continue repression of the civilian population and to deter its further military actions against his own people."[171] This covers mainly the military dimension with emphasis on the humanitarian necessity of such actions;
- *British Secretary of State George Robertson* at a MoD press briefing on March 25, maintaining that the military objective of these operations was "to avert an impending humanitarian catastrophe by disrupting the violent attacks currently being carried out by the Yugoslav security forces against the Kosovar Albanians and to limit their ability to conduct such repression in the future."[172] In that sense, humanitarian, military, and a long time security-political objective was stated.

The level of success of Operation Allied Force is measured by comparison of how the actual political and military outcomes differ from the ones desired. The official five-point plan is clearly insufficient to provide the framework for this, lacking more than one important dimension evident from the above collection of statements. For example, the necessity to prove NATO's strength, unity,

[170] DoD News Briefing, Wednesday, 24 March 1999 – 5:15 p.m. Presenter: Secretary of Defense William S. Cohen and CJCS General Shelton.

[171] NATO Press Conference, Transcript 25 March 1999.

[172] UK MoD Briefing by Mr. George Robertson, Secretary of State for Defence, and General Sir Charles Guthrie, Chief of the Defence Staff, 25 March 1999.

and determination in a changed political landscape should not be underestimated; that this was indeed very important becomes apparent from NATO's press briefings in which much emphasis was laid on proving this point.[173] Destabilization of Milosevic's regime is also considered a clandestine objective with both rhetoric and action pointing in that direction. Analysis suggests seven core objectives, in different categories, summarized in the following table along with the surmised level of success in achieving each:

Outcome Desired	**Level of Success in Achieving Outcome**
Disruption, degradation, devastation and ultimately destruction of the Serb forces and their facilities and support → short-term military with some long-term security-political intentions	1 some success
Weakening Serb forces in Kosovo to end Serb military actions as well as violence and repression → short-term military objective with long-term humanitarian and security-political intentions	0 low success
Stopping the humanitarian catastrophe in the Balkans → short-term humanitarian objective	1 some success
Hinder spread of conflict to neighboring countries → short-term security-political intention	2 reasonable success
Prove Alliance unity, strength, and determination → geopolitical objective	2 reasonable success
To break Milosevic's power in Yugoslavia → long-term military and security-political intention	2 reasonable success
Ensuring (lasting) stability in the region → long-term security-political intention	1 some success
	1.28 **some success +**

Table 17: Level of Success in this Information Age Conflict (Variable Y)

[173] See also Joint Chiefs of Staff, *Joint Statement on the Kosovo After Action Review*: "Milosevic's conduct leading up to Operation Allied Force directly challenged the credibility of NATO (…). The Federal Republic of Yugoslavia and the Republic of Serbia signed agreements in October 1998 that were (…) monitored by NATO. In the period leading up to March 1999, the FRY increasingly and flagrantly violated these agreements. Had NATO not eventually responded to these violations and other acts of the FRY, its own credibility, as well as the credibility of U.S. security commitments throughout the world, would have been called into question."

Explanation:

- The disruption, degradation, devastation and ultimately destruction of the Serb forces and their facilities and support through mainly Command and Control Warfare was only somewhat effective. Even though the bombing campaign destroyed much of the Serbian infrastructure, aspired "decapitation" of the enemy's command structure from its body of command forces either did not take place or then did not show the desired effects;
- The attempts to weaken Serb forces in Kosovo to end Serb military actions as well as violence and repression were hardly effective at all. Destruction of the forces in the field proved to be difficult because of the bad weather and very effective Serb deception tactics;
- The bombing did not succeed in stopping the humanitarian catastrophe or human suffering in the Balkans, might even have elevated the flood of refugees into neighboring countries as refugee numbers suggest,[174] and the handling of the situation shows numerous deficiencies;[175]
- The operation did prove quite successful in hindering the spread of the violence to unstable neighboring countries such as Macedonia, Albania, and Montenegro (at the time!);
- NATO managed to uphold the outward impression of unity among the Alliance's members; closer scrutiny though makes a lot of ruptures evident. Still, Milosevic did not succeed in his

[174] See OSCE, *Kosovo/Kosova As Seen, As Told. An Analysis of the Human Rights Findings of the OSCE Kosovo Verification Mission, Part I*, October 1998 to June 1999, Chapter 14, online version, URL http://www.osce.org/kosovo/reports/hr/part1/index.htm. NATO claimed that this was Serbian propaganda.

[175] Joint Chiefs of Staff, *Joint Statement on the Kosovo After Action Review*: "Shortage of linguists and civil affairs personnel was acute (…). Engineering assets, capable of emergency repair of roads and bridges in very austere environments, were also in short supply, as were detailed maps of the relevant areas."

goal to break the Alliance apart, which managed fairly well to propel the image despite numerous odds;

- The air campaign did not immediately break Milosevic's power in Yugoslavia. Evidence suggests that it even strengthened his position temporarily. Further, the Belgrade Agreement is a far cry from what was sought in Rambouillet;
- Stabilizing armed forces (KFOR under Operation Joint Guardian) that moved in after the bombing campaign help to provide brittle but nonetheless so far sufficient stability in the region.

The overall level of success of this first Information Age Conflict was fairly low. An average of the seven aspects suggests the value of 1.28, standing for some success. This seems an accurate value even though to assume that all of the aspects had the same impact on the overall level of success is certainly too much simplification.

Evidence suggests that a covert "Information Warfare" plan, referred to as "Elephant Blanket", also was basically a failure: Not only did it have to be revised almost immediately to become the American-only "Day 54 plan" because there developed serious problems with the former plan due to the inferior security clearance of the entire corps of European officers that did not have access to it,[176] but also were the political constraints on the coalition of such magnitude that most of the plan's efforts were hardly implemented; moreover, Milosevic himself was far more efficient in the game of Information Operations than the Alliance, dominating Western media with his messages at almost all times.[177]

[176] Arkin, William and Robert Windrew, "The Other Kosovo War: Baby Steps – and Missteps – for Information Warfare", Special to MSNBC, 29 August 2001.

[177] Ibid. There are even hints that Belgrade's own covert psychological warfare had an impact on NATO.

Part IV – Analysis

Identifying Factors that Influence Information Age Conflicts

Part IV – Analysis

Identifying Factors that Influence Information Age Conflicts

The previous chapter succeeded in assigning concrete values and definitions to each of the model's variables. This chapter undertakes analysis of eight conjectured relationships by ways of

- *"congruence procedure"*: Each relationship is visualized by way of a table listing the respective intervening variable, the dependent variable's predicted value, and the actual observed value, as well as a control field whether the 0-Hypothesis, stating that there is no relationship between the respective intervening and dependent variable, can be rejected or not. Its rejection is seen as presumed evidence that there is some kind of relationship between the respective independent and the dependent value;[1]
- *"process tracing"* with which the proof that a given stimulus caused a given response might be found in the sequence and structure of events but also in the testimony of certain actors explaining why they acted as they did. By means of thorough process tracing even a single case can offer a reasonably strong test of a model, attributable to confirmation of the validity of the theory through its ability to explain at least one case.[2]

Difficulties arise from the general problem of presenting enough evidence for some aspects, mainly hypothesis 2.1 and 2.2 of the credibility construct, predicting relationships between the conduct of Information Operations and external influencing factors on cred-

[1] Van Evera, *Guide to Methods for Students of Political Science*, 61–63.

[2] Ibid., 65–66.

ibility. Only some of this can be resolved by ways of causal tracking, a matter that is considered little grave however, since these two relationships are of minor importance for the model. Slightly more problematic is the deficiency to explore origins of the intervening variables in more detail, which have been shown to stem partially from the conduct of Information Operations themselves. This clearly constitutes a weakness of this analysis.

Of the eight tested hypotheses only one is outright falsified ($r_1 \rightarrow$ s); four on the other hand show only weak relationships between IV and DV (E→X+; q→X+; r_2→X+; r_3→X+). In those cases, causal narrative helps to establish how the IV caused variation in the DV.

1 Asymmetric Credibility

C has been described as the construct's condition variable that has influence on the intervening variables through its impact on X+, since X+'s influence on Y is magnified by a high value on C and reduced by a low value on C. To find evidence of such conditioning influence of credibility on Information Operations seems highly unlikely after the previous chapters. Instead, an easy causal relationship is tested; one can predict that the lesser the level of credibility associated with a party, the lower the degree of satisfactory conduct of Information Operations (C → X+):

	Intervening Variable's Value	Dependent Variable (X+) Predicted	Dependent Variable (X+) Observed	0-Hypothesis Rejected? (Yes/No)
C	≈ 1.33 (some credibility +)	1 or 2 (some successful or successful)	1.333 (some successful +)	Yes

The above shows that the observed value for X+ is in the range of the predicted; therefore, the 0-hypothesis can be rejected. This is indication that there is some kind of relationship between the level of credibility and the level of successful conduct of Information Operations.

1.1 The Credibility-Problem: Untrustworthy Public Information Policy and Failure to Conduct Satisfactory Public Affairs Operations

As was established in theorem № 2, in today's information-saturated world, attention is an increasingly scarce resource and among actors struggling to accumulate information power, (asymmetrical) credibility or the reputation for providing correct information is crucial. The struggle for a high level of credibility therefore becomes an essential part of any political or military operation, aggravated by the skill revolution that lets the populace exert pressure on decision-makers if their credibility seems questionable. This not only might result in loss of control over the situation, but also significantly reduce the overall success of operations. In the special context of IACs, Information Operations need to be credible to be effective, especially those aspects that have a psychological or deceptive nature within the counterinformation domain; lacking credibility can therefore be expected to lessen the overall success in such conflicts through hampering of Information Operations.

In Kosovo, control and release of military information to the public was handled unsatisfactorily in the above context: likely underestimating the credibility-problem, both the United States and NATO were poorly prepared to win the extensive and aggressive media war, the competition for press attention, credibility, and ultimately sympathy for one side's view.[3] It became clear relatively fast that in the emerging environment it was not sufficient to rationalize actions, trying to show that right was on the Alliance's side and stressing that the military action was effective when numerous incidents put trustworthiness at stake. During the whole campaign there was a serious problem concerning the ability to match rhetoric with will, action, and capabilities, in this sense putting NATO's

[3] Pounder, "Opportunity Lost".

credibility as a whole at risk.[4] Among general impressions that undermine credibility are the following:

- NATO's justification for being involved in the conflict and its military objectives were regularly altered – at first the war was designed to get Milosevic to sign Rambouillet accord, then the reason was to avert, then to halt, humanitarian disaster. Even later, the objective was to allow refugees to return to their homes;
- Again and again, officials had predicted a quick victory and it was believed that several days of bombing would force Milosevic to negotiate. After a month of war, the target list was expanded. This seemed to communicate NATO's frustration at not being able to achieve its political objectives within the target list it had been pursuing;[5]
- There was every effort made to question the credibility of any development that did not serve NATO's purpose. However, hardly any mistakes, even absolutely obvious ones, were admitted on the Alliance's side;
- It seemed NATO was either exaggerating wildly in demonizing Milosevic to justify bombings because real motives would not stand public opinion, or else, analogies were appropriate, in which case surely stronger measures, this being mainly effective ground troops, should have been taken to rid the world of this threat.[6]

Two examples of how lacking credibility hampered trustworthy public affairs' operations are the convoy attack near the village of Djakovica on April 14, and the bombing of the Chinese embassy on May 7. To begin with, it took the Alliance five days to respond to the convoy incident, and three days to the bombing of the Chinese

[4] Kay, Sean, "After Kosovo: NATO's Credibility Dilemma", *Security Dialogue*, 31, 1 (March 2000): 73.

[5] Arkin, "NATO's Info Strategy Bombs"; Kay, "After Kosovo: NATO's Credibility Dilemma", 75.

[6] Goff*, The Kosovo News and Propaganda War*, 16.

embassy, almost an eternity in an era of instant, news coverage and 24-hour news cycles – raising suspicion that they had something to hide.[7] The Djakovica incident especially led to a chain of awkward NATO statements: immediately after, the German defense minister Rudolf Sharping accused the Serbs of the attack. On the next day, NATO admitted one of its planes had dropped one bomb on a civilian vehicle by mistake but continued to imply that the Serbs were in some way culpable.[8] They insisted for days that only in this one case they had hit a civilian target. On April 19 however, they changed the official story and admitted that it had hit two convoys using about 12 planes dropping a total of nine bombs. On April 15, a recording of one of the pilots allegedly responsible for bombing the first convoy was publicly played. Two days later, NATO admitted after a lot of probing questions that the recording had no connection with the bombing of the convoys and had just been "an example".[9]

Especially the NATO briefings evoked an escalating sense of frustration and irritation, not only among journalists. The public affairs strategy was clearly aimed at emphasizing the success of the military operation, the political unity of the Allies, and their commitment to the humanitarian aspect, if necessary by "spinning" unfavorable information. The Alliance's aggressive information policy also included the dishing up of rumor, occasional wild exaggerations as well as the feeding of false and speculative stories.[10] Civilian casualties and the bombing of dual-use targets was

[7] Pounder, "Opportunity Lost", 17.

[8] Press Conference by Jamie Shea and Brigadier General Giuseppe Marani, 15 April 1999, updated 15 April 1999, NATO HQ, Brussels.

[9] At the Press Conference by Jamie Shea and Brigadier General Giuseppe Marani, 18 April 1999, updated 18 April 1999, NATO HQ, Brussels. General Marani: "I brought you that tape to try to clarify what was the process of the pilot, how the pilot was acting and what he was saying and looking at. There are many pilots flying over Kosovo doing every day that type of action on different targets, that one was an example."

[10] Examples see Classen, Elvi, "Medienrealität im Kosovo-Krieg", *telepolis*, 30 October 1999, Goff, *The Kosovo News and Propaganda War*, 14–15.

generally downplayed, and repeatedly the sentence "we are not at war with the Yugoslav people" used as an awkward excuse. It had been recognized that the killing of civilians was the issue with the greatest potential to erode unity of military alliance, so investigating questions on aspects of civilian casualties or other critical comments were countered either with rhetorical formulas, dealt with evasively, or just simply ignored; each new civilian tragedy was offset by repeated Serb atrocity stories and pictures of the plight of refugees. Madeleine Albright conceded on April 20 in front of Congress that the Alliance's information warfare strategy was failing and that "the battle for hearts and minds has been hopelessly ineffective".[11] Only a few days after, NATO bombed Serbian state television (RTS), killing 16 foreign journalists and leaving an uneasy feeling about the use of force against media outlets, for many a sign that if there was need to bomb the enemy's TV stations, then one had definitely failed in the public-information campaign.[12]

An internal NATO report leaked to the Spanish daily "El Mundo" on 31 May further strengthened the belief that the NATO briefings were designed to manipulate the news rather than accurately present developments: this report said something like "NATO headquarters does not have the mechanisms, resources or experience necessary to conduct an information campaign in wartime"[13] and that public opinion should be prepared for a long period of air raids, made ready for more intensive air raids aimed not solely at military targets, and twisted towards accepting a land invasion.[14] Some reporters and columnists who covered the war stated that the media manipulation got so transparent that they did not believe anything Jamie Shea or Ken Bacon had to say.[15]

[11] Arkin, "NATO's Info Strategy Bombs".

[12] Colonel Ivy cited in Pounder, "Opportunity Lost", 17.

[13] Morning Briefing by Jamie Shea, 31 May 1999, updated 31 May 1999, NATO HQ.

[14] Goff*, The Kosovo News and Propaganda War*, 18.

[15] Pounder, "Opportunity Lost", 13.

The Internet also had a role to play in the struggle for credibility: thanks to the Internet, Kosovo was no Gulf War where the only information available was what the US military chose to let CNN show the world. One of the Internet's effects on Kosovo was a sort of "net" surrounding the conflict, informing it and keeping other media in check, being a vessel for diverse news sources and even eyewitness reports. Thanks to the Internet, journalists had the possibility to turn elsewhere for different information when they found many aspects of NATO's propaganda campaign disappointingly one-dimensional. Even though the trustworthiness of the sources was not always granted, many of these online-reports further undermined the Alliance's credibility and thus challenged the public-information campaign.

1.2 Discussion of Hypothesis C → X+

The level of credibility associated with a party has its strongest impact on the aspect of public affairs operations within the Information Operations family. Interestingly, all doctrine papers on public affairs strongly emphasize that messages communicated must be truthful to ensure that credibility is not undermined,[16] even stating that they should provide objective reporting, without intent to propagandize.[17] Nevertheless, many aspects of NATO's propaganda campaign, in contrast to the Serbian's measured by different "truth-standards", was disappointingly one-dimensional, its statements too triumphant when hailing the Alliance and too demonizing when mentioning the Serbs. The competition for press attention, credibility and sympathy for one side's view was a crucial part of the Operation Allied Force against the Serbian propaganda machine. Missing NATO trustworthiness seriously threatened to undermine fickle public support, which was absolutely necessary to keep the war going.

[16] Department of the US Army, FM 100–6, chapter 3.

[17] Joint Chiefs of Staff, Joint Publication 3–53, Doctrine for Joint Psychological Operations, 10 July 1996, 1–5.

Apart from the strain on public affairs operations, low credibility also lessened the effects of other aspects of Information operations, mainly psychological operations: the efforts made in this domain, mostly dropping of tons of leaflets, were seen as ludicrous; programs and messages broadcasted did not have much effect partly due to lacking credibility. Apart from these aspects of IO that have a psychological or deceptive nature, it also becomes apparent that lacking credibility has a direct and maybe conditioning impact on the level of success in IACs (C → Y) because it changes the way such a success is measured, a relationship that is not part of the current model. In this sense, low credibility due to the lacking ability to match rhetoric with action especially in areas concerned with value-driven military engagement inflicts lasting damage on conflict parties and challenges their status in the international system.

2 Technology, Terrain, Weather, International Law

Predicted is a direct connection between case specific influencing factors like weather, terrain, and for example technological failures and the degree of satisfactory conduct of Information Operations, because such factors directly hamper these.

	Intervening Variable's Value	**Dependent Variable (X+) Predicted**	**Dependent Variable (X+) Observed**	**0-Hypothesis Rejected? (Yes/No)**
E	2 (some influence)	0 or 1 (not successful or some successful)	1.333 (some successful +)	(**Yes**) but X+ observed slightly too high

The values suggest that there is some kind of relationship between E, the influence exerted by the case specific exogenous factors, and X+, the degree of successful conduct of Information Operations. However, the relatively high value associated with E let expect a slightly lower level of success than actually observed. On the other hand, the observed value is not high enough to allow acceptance of the 0 – hypothesis. This relationship therefore needs closer examination by ways of causal narrative to see whether and how the IV caused variation in the DV.

2.1 Case Specific Exogenous Variables Affect All Dimensions of IO

For the correlation E → X+, the comparison of values did not establish enough clearly that there is a causal relation between case specific exogenous factors and the conduct of successful Information Operations. Yet, in chapter III.3, considerable evidence of such a relationship has already been presented:

Influencing Factor	Negative Influence	Aspect of IOs Affected/ Hampered
Thick Layer of Clouds (Weather Condition)	Weather hampered the collection of data	⇒ Intelligence, Surveillance, Reconnaissance
	Weather hampered the actual bombing operations	⇒ Precision Navigation and Positioning ⇒ Physical Attack
	Weather lead to lacking ability to cope with "cover and concealment" tactics	⇒ Physical Attack
	Planes "weathered out"	⇒ Intelligence, Surveillance, Reconnaissance ⇒ Precision Navigation and Positioning ⇒ Physical Attack ⇒ PSYOP ⇒ Electronic Warfare
Difficult Terrain (Geophysics/ Terrain)	Heavy vegetation, terrain, mountains, poor mapping, unmarked structures, wires, etc.	⇒ Intelligence, Surveillance, Reconnaissance ⇒ Precision Navigation and Positioning ⇒ Physical Attack ⇒ PSYOP ⇒ Electronic Warfare
	Terrain helped FRY forces to camouflage their positions	⇒ Precision Navigation and Positioning ⇒ Physical Attack
Weapon Technology/ Information Infrastructure (Technological Factors)	No large dependency on ICT	⇒ Military Deception ⇒ Information Attack
	"Smart" bombs often not smart enough	⇒ Physical Attacks
	Lack of clear policies and international agreement on key IT issues[18]	⇒ All aspects (coordination)
	Human failure factor remains high	⇒ Physical Attacks
	IO- concepts remain underdeveloped	⇒ All aspects
International Law	Clauses protecting civilians	⇒ Information Attack

Table 18: How Case Specific Influencing Factors Hamper the Conduct of Information Operations

Interesting for future IACs is mainly the connection of Cyberwar and international law: Cyberwar ideas are still in their infancy. The example of Kosovo has shown clearly that the world's major military power is far from willing to launch such attacks: during Operation Allied Force, the US demonstrated that is was not ready for either defensive of offensive cyberwarfare, mainly because officials were worried about the legal implications of launching the world's first "Cyberwar" of which they found was no clear basis in law.[19] The same principles of the traditional law of armed conflict applied to bombs and missiles must also apply to a military cyber attack: such assaults aimed at civilian targets like financial systems, power and water facilities, could constitute a war crime. In the case of attacks involving foreign governments and major foreign movements or terrorists and extremist, it is not clear what laws apply, what constitutes an attack of war, and what kind of counterattack or offensive operation is justified.

A 50-page booklet with guidelines for waging Cyberwar, named "Assessment of International Legal Issues in Information Operations", issued in May 1999 by the Pentagon's general counsel office, foremost warns commanders to be cautious of targeting institutions that are essentially civilian.[20] There are also many more ambiguous legal parameters involved, such as the fact that the role of third nations or "neutrals" in preventing the use of their cyber facilities and information systems is not clear. In fact, even Allies participating in the NATO operations had no basis for deciding what actions they could take to limit the use of relatively unsophis-

[18] Verton, Daniel, "Report Sheds Light on NATO's High-Tech Problems in Kosovo", *Federal Computer Week*, 9 February 2000.

[19] Reuters, "U.S. Military Grapples With Cyber Warfare Rules", Washington: 8 November 1999, online version, URL http://www.infowar.com/mil_c4i/99/mil_c4i_110899b_j.shtml.

[20] Department of Defense, Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (Washington, D.C., Department of Defense: May 1999); and Joint Chiefs of Staff, Joint Pub 3–13, I–12.

ticated technology like cell phones, extensively used by Serb forces to pass on valuable information.[21]

Another constraint for the use of "cyber-weapons" was the fear of giving away a alleged strategic advantage: Cyberwar experts Arquilla and Libicki believe that the Pentagon actually did hack into Serbian computers to spy, but refrained from causing chaos principally for strategic reasons: widespread use of these new weapons and tools probably would accelerated and focus foreign military research on them and threaten to deprive the US of its information warfare edge in a field in which foes could catch up quickly and cheaply, an argument similar to the one in connection with nuclear weapons in the 50s.[22]

Even though military lawyers' were assigned a considerable role in the legal and moral assessment of targets during Operation Allied Force,[23] for some time to come, IACs are likely to set fundamental new precedents for approaches to Information Operations, the laws of war, and international law. This has a great impeding effect on Information Operations because especially the United States are wary of their vulnerabilities and fears not only of retaliation, but also of a new arms race that not necessarily must resolve to their advantage.

[21] Graham, Bradley, "Cyberwarfare: It's Still a Pandora's Box", *International Herald Tribune*, 9 November 1999, 1 and 10, Di Censo, David J., "IW Cyberlaw: The Legal Issues of Information Warfare", *Aerospace Power Journal*, XIII, 2 (Summer 1999): 85–102.

[22] Borger, Julian, "Pentagon Kept the Lid on Cyberwar in Kosovo", *The Guardian*, 9 November 1999; Minkwitz, Olivier and Georg Schöfbänker, "Neue Herausforderung für die Rüstungskontrolle", *telepolis*, 31 May 2000.

[23] DoD News Briefing, Thursday, May 13, 1999 – 3:00 p.m. Presenter: Mr. Kenneth H. Bacon, ASD PA. Also Participating: Major General Chuck Wald, J–5; Ignatieff, *Virtual War*, 100 ff.

2.2 Discussion of Hypothesis E → X+

The exogenous factors had a hampering impact on basically all the aspects of IO. Bad weather surely had a very strong effect on the actual bombing campaign and all the other aspects of air war; the American After Action Review Report for Kosovo points up that adverse weather affected target acquisition and identification, increased risk to aircrews, and complicated collateral damage concerns. Cloud cover was greater than 50% more than 70% of the time, the weather conditions allowed unimpeded air strikes on only 24 of 78 days.[24] Technological factors were mainly impeding due to shortcomings in weapon technologies that also subsume failures. Last, there has been evidence presented that the state of the international law and emerging regimes curtail the willingness of democratic nation states to launch serious cyberattacks against adversaries, both because of legal implications as well as a great policy concern in the United States about being the "first mover" and losing a strategic advantage.[25]

Even though the comparison of values for the correlation E →X+ did not establish enough clearly that there is a causal relation between case specific exogenous factors and the conduct of successful Information Operations, by means of process tracing this chapter presented reasonably good evidence of such a relationship.

[24] Office of the Secretary of Defense, *Report to Congress, Kosovo/Operation Allied Force After Action Review Report*, 60.

[25] Cf. Kreml, Stefan, "Interview with John Arquilla: Be Prepared: Cyberwar is Coming – Or Maybe Not", *telepolis*, 13 March 2001.

3 Asymmetrical Challenge

The relationship q →X+ claims that the higher the degree of asymmetrical challenge faced by a conflict party the lower the level of successful conduct of Information Operations by this conflict party:

	Intervening Variable's Value	Dependent Variable (X+) predicted	Dependent Variable (X+) observed	0- Hypothesis Rejected? (Yes/No)
q	2 (reasonable)	0 or 1 (not successful or some successful)	1.333 (some successful +)	(**Yes**) but X+ observed slightly too high

Again, there seems to be some kind of relationship between asymmetrical threats and successful waging of Information Operations. However, as was the case with variable E, the relatively high value associated with q let expect a somewhat lower level of success than the observed. Yet again, it is not high enough to lead to acceptance of the No-relationship assumption. This too will have to be further differentiated by means of causal tracking.

3.1 Asymmetry vs. Doctrine of Dominance: Serbian Information Operations Challenge NATO's Information Superiority

Theorem № 5 established that in the information age, small players increasingly have the ability to harm powerful foes with the right technology and knowledge. Aggressors are left with two options: they can pursue indirect or camouflaged aggression, or they can attempt to deter or counter asymmetrically.[26] For example, there is no need of military power if private entities can effectively penetrate the adversary's decision-making cycle by using new media and tools.

As with the relationship discussed in the previous chapter, the comparison of values for q and X+ was not entirely satisfactory. This chapter tries to show that there was substantial hampering

[26] Metz, *Armed Conflict in the 21st Century*.

influence of asymmetrical threats on the successful waging of Information Operations during Operation Allied Force. In this paper, asymmetrical threats are understood as occurrences that cannot be mastered by traditional military force and capabilities.

During the campaign, there never was a direct clash of massed military forces and Milosevic knew he was unable to challenge superior Allied military capabilities directly. Therefore, he chose to fight chiefly through indirect, asynchronous, and asymmetrical means: use of terror tactics against Kosovar civilians; attempts to exploit the alleged aversion of the Alliance to civilian casualties and collateral damage; attempts to break the Alliance's unity; the curbing of a destabilizing humanitarian crisis; and the conduct of disinformation and propaganda campaigns.[27] Especially Serbia's clever use of its own information warfare arsenal enabled it to seriously challenge NATO's strategy and determination. Moreover, through such asymmetrical means, Serbia achieved Information Superiority over the most powerful and technologically superior alliance ever: in an Information Operation's campaign of their own, Serbia aimed to influence internal and external perceptions of the NATO bombing by using means of both defensive and offensive IO, including the use of the Internet. To achieve information assurance the Milosevic regime used (counter-) propaganda and the control over domestic media and large parts of the international press corps inside Yugoslavia, and further, media control and propaganda were used to conduct psychological operations against world public opinion.[28] Though unsuccessful in outright fracturing the Alliance, this IO campaign nonetheless managed to widen rifts between NATO Allies as well as between the Alliance and Russia, and undermined

[27] Joint Chiefs of Staff, *Joint Statement on the Kosovo After Action Review*.

[28] Larsen, Wayne A., *Serbian Information Operations During Operations Allied Force*, A Research Report Submitted to the Faculty of Air Command And Staff College Air University (Alabama, Maxwell Air Force Base: April 2000): 23 ff. Through its EUSat communications link, the Serbian Radio and Television Service RTS was able to reach all of Europe and was even rebroadcast in the US on CSPAN.

public support for the bombing. In the end, NATO never achieved information dominance. As the press became an asymmetrical asset for the enemy, NATO was forced to continually react to its collateral damage problem even though Milosevic forces killed thousands of people. Despite technological supremacy, a broad spectrum of IO capabilities, as well as a partly established Information Operations' doctrine, the Alliance clearly lost the information war. Reasons for this failure are likely misperception of the length and seriousness of the campaign that resulted in absent planning for such an operation[29] as well as shortcomings in the general IO doctrine.[30]

Another asymmetrical tool used was the cellular phone: NATO experts suspect that Serbians regularly observed NATO air bases and facilities, and would phone home to warn of NATO take-offs and probable attacks.[31] NATO struck constantly at military relay stations, but only damaged three out of about 20 telephone nodes and none of the three network control stations that supported Serbian cell phones; this left most communications and Internet access intact.[32] Hampering the actual bombing campaign likewise was the alleged ability of Serbian air defense personnel to template large parts of US and NATO air operations based on observations made during the Gulf War and in Bosnia; the Serb military let armored

[29] Joint Chiefs of Staff, *Joint Statement on the Kosovo After Action Review*: "The conduct of an integrated Information Operations campaign was delayed by the lack of both advance planning and strategic guidance defining key objectives." Office of the Secretary of Defense, *Kosovo After Action Report*, 21: "The second option was known as the Limited Air Response and was designed to be a short notice, limited air response to a serious, but limited incident in Kosovo (…) The Limited Air Response was eventually integrated into Phase 1 of the air campaign."

[30] Pounder, "Opportunity Lost".

[31] Graham, "Cyberwarfare"; Thomas, Timothy L., "Kosovo and the Current Myth of Information Superiority", *Parameters (*Spring 2000): 13–29. Cited after online version, URL http://www.carlisle-www.army.mil/usawc/Parameters/00spring/thomas.htm.

[32] Cordesman, *Defending America*, 46; *Aviation Week and Space Technology*, 8 November 1999, 81–82.

vehicles to be picked as targets for reconnaissance flights or satellite imagery and then they would move the actual targets; afterwards, the Serbs used decoys to create a variety of false targets such as old tractors they put in the target's place with a telephone pole attached to make it look like a tank.[33]

Another measure against the high-tech force that was effective for a period of time was the only sporadic use of the Serbian air defense assets: to prevent its air defense assets from being neutralized, the Serbian armed forces turned their assets on only as needed. This did not only result in NATO using its most strained assets (JSTARTS and AWACS) to conduct additional searches for air defense, it also forced aircraft to fly above 15'000 feet, making hitting targets difficult and increasing the risk to pilots of collateral damage.[34] This tactic hampered all the aspects of IO in which aircraft was involved, thus ISR, physical attack, PSYOP, and EW.

3.2 Discussion of Hypothesis q→ X+

The chief asymmetrical threat faced was the effective employment of Serbian information warfare tools against the Alliance that won the media war and Information Superiority. Other aspects of asymmetrical threats are the use of ICTs such as cell phones and the Internet in the information battle, and low-tech deception tactics that were very effective. In addition, Cyberwar dimension might have been hampered by fears of retaliation or loss of strategic advantage and fear of asymmetric threats increasing in this domain.

Even though the comparison of values for the correlation q →X+ did not establish enough clearly that there is a causal rela-

[33] Thomas, "Kosovo and the Current Myth of Information Superiority"; Office of the Secretary of Defense, *Kosovo After Action Report*, 62.

[34] Interview with Admiral James Ellis, Commander-in-Chief of NATO's Allied Forces Southern Europe, in: Thomas, "Kosovo and the Current Myth of Information Superiority"; and Grossman, Elaine, "U.S. Commander in Kosovo Sees Low-Tech Threats to High-Tech Warfare", *Inside the Pentagon*, 9 September 1999, 1.

tion between asymmetrical threats and the conduct of successful Information Operations, by means of process tracing this chapter presented reasonably good evidence of such a relationship.

4 Blurring State Boundaries and Multiplication of Actors

The relationship $r_1 \rightarrow s$ stands for the assertion that the degree of blurring boundaries between states leads to a multiplication of actors. Put differently we can predict that the higher the degree of blurring boundaries between states, the greater the degree of multiplication of relevant actors:

	Intervening Variable's Value	**Dependent Variable Predicted**	**Dependent Variable observed**	**0- Hypothesis Rejected? (Yes/No)**
r_1	2 (reasonable)	2 or 3 (reasonable or high)	1 some	**No**

From the above comparison of values, there is no evidence of imminent connection between the phenomena. From Table 1 further follows that the hypothesis is falsified if the DV shows 1 for IV = 2. The 0-hypothesis therefore cannot be rejected.

4.1 "War-at-a-Distance" and the Virtualization of War

It was established in Theorem № 3 that traditional boundaries become increasingly blurred in the Information Age in three different areas: between states, military-politics, and military-civilians. The model does not predict a direct hampering effect of the blurring boundaries between states on successful waging of Information Operations, but rather a connection to the multiplication of actors. The relationship predicting that the degree of blurring boundaries between states effects the degree of multiplication of relevant actors was rejected. This chapter then does not whish to accomplish this either, but wants to explore the blurring boundaries and their implications for wars in the information age more generally. Its focus is a phenomenon called the "virtualization of war".

The war in Kosovo in many aspects was a virtual war. It was automated and remote controlled, a "war-at-a-distance". It left a strange sense of remoteness and virtuality, because it was fought from a distance, without physical contact. This was ineffective in many ways: For one thing, it totally bypassed any sense of territory and traditional boundaries. It took place almost entirely in the air, with hardly any Allied armed personnel on the ground, no real state of siege, and practically no blockade. Soldiers only set foot on the territory once the war was over.[35] It propelled the notion of war as a purely technological event, taking place behind radar and computer screens, with no casualties; as indeed there was no Allied life lost in battle, but it also did not mobilize great parts of societies, not seeming quite real even to those who fought it.[36] And every afternoon, NATO showed video footage taken from the cockpits, strangely reducing the destruction to a horrid video arcade game and seduced to marvel at the technological aptitude of the mainly US forces.

The effects of such a war also appear more virtual than actual: the substantial air power applied was not able to change the Serbian regime; it only barely damaged its capacity to do future harm at the time. Relying exclusively on war-at-a-distance also uncovered other limits: planes are effective against fixed strategic targets like petroleum storages, bridges, and command bunkers. Against mobile targets and forces, its limitations became more obvious: NATO's initial claims that it did destroy much of the Serbian armor in the field have been greatly revised since. More important, it became clear that air power alone cannot protect civilians at risk, that it cannot stop ethnic cleansing from a remote 15'000 thousand feet.

[35] Armitage, John, "CTheory Interview with Paul Virilio: The Kosovo War Took Place in Orbital Space", Paul Virilio in Conversation with John Armitage, translated by Patrice Riemens, *CTheory, Theory, Technology and Culture*, 23, 3, 18 October 2000.

[36] Ignatieff, *Virtual War*, 191.

Political constraints meant air power, translating into low risks and low gains, as opposed to ground troops, meaning higher risks but also likely higher gains. Since virtual wars appear to be almost risk-free and casualty-averse, democratic electorates may be more willing to fight, even more so if the cause is justified in the language of human rights and even democracy itself. Virtual war is the form of future wars, because it is linked to precision weaponry and precise targeting, creating the expectation, which military, public and politicians alike come to share, that war can be clean and mistake free, and thus in a sense legal and even moral.[37]

There are a number of obvious perils stemming from the over-technologization of conflicts. The bombing of the Chinese embassy has shown that high-tech is no help in the failure of human beings to understand a political or military situation; being able to see targets and knowing which, when, and whether to hit them is not the same. Today, the enormous volumes of information can only be mastered by total dependence and trust in technical aids to help organize and manage it. This reliance on computers has generally eroded manual skills to analyze and understand certain occurrences, or to distinguish between good and false information.[38] Even more, the stream of electronic input can overwhelm the human dimension of decision-making. Worse still, false information can easily become an integral part of data-pools, as was allegedly the case with the Chinese Embassy, and hardly ever be detected until a serious error occurs.

Too much information has the potential to lead to sensory overload. Admiral James Ellis stated in an interview that “information saturation is additive to the ‘fog of war’ (…) uncontrolled, it will control you and your staffs and lengthen your decision-cycle times”, including video teleconferencing in this statement that consumed

[37] Virilio, Paul, *Information und Apokalypse. Die Strategie der Täuschung* (München, Hanser: 2000): 182–185.

[38] Thomas, Timothy L., “Infosphere Threats”, *Military Review*, LXXXIX, 5 (September/October 1999): 46–51.

key staff and leadership working hours at high rates in Kosovo.[39] Sensory overload also bears other dangers; a journalist once noted “high tech forces are prisoners of a technology so speedy and complex that it forces the fallible humans who run it into snap decisions that can run into disaster.”[40] The danger of this “perception-reaction chain” becomes apparent if we consider that triggered response-actions in virtual wars are based on observations of electronic images, with usually no possible way to check the reliability of these in time. Whether these images are real or artificially inserted by an enemy, both will equally influence emotions, motives, or the objective reasoning of individuals that base their decisions on this input.[41]

Even though there is no direct relationship between the blurring of geographical boundaries and the waging of IACs in the model, the virtualization of war is likely to have a general impact on both successful waging of future conflict and dangers arising from the dependency on machines. This possible relationship should be considered in a revised version of the model, even more so since the relationship between blurring boundaries and the multiplication of actors is not verifiable.

[39] Admiral James Ellis cited in Thomas, “Kosovo and the Current Myth of Information Superiority”.

[40] Quoted in Thomas, “Infosphere Threats”.

[41] Ibid.

5 Multiplication of Influential Actors

The more influential and relevant actors a conflict party has to deal with and the more these non-traditional actors have the ability to intervene against the wishes of the party the lower the level of successful conduct of Information Operations by this conflict party:

	Intervening Variable's Value	Dependent Variable (X+) Predicted	Dependent Variable (X+) Observed	0- Hypothesis Rejected? (Yes/No)
s	1 (some)	1 or 2 (some successful or successful)	1.333 (some successful +)	**Yes**

The above table shows that the observed value for X+ is within the range of the predicted; there is some kind of relationship between s and X+ and the 0-hypothesis can be rejected.

5.1 New Dimensions in Warfare Resulting from the Internet

Theorem № 4 predicts a redistribution of power among actors on the international stage that destabilizes traditional structures of authority, empowering small entities as well as individuals, with a multiplication of relevant actors and a growing complexity of the operating environment. The comparison of values above suggests that there was a connection between the multiplication of actors and the low level of successful Information Operations. The degree of multiplication of actors is generally low: in conflicts, much of the traditional information monopoly still rests with the major conflict parties. The Internet challenges this information monopoly in some ways, but is too diverse too have a major impact, as will be shown below. Also, due to the skill revolution, home-based democratic population has a great amount of power over governments that go to war. The most fruitful approach in exploring the multiplication of actors and successful waging of Information Operations is to focus on how the new media and global communications change the operating environment by accelerating and expanding collective awareness of events, issues, and concerns.

Debates over the role of media in war and conflicts remains similar for both the traditional and the new media, but the real-time factor adds a decisive new dimension: it is commonly understood that new communication technologies and the expansion of international media alliances have greatly affected the conduct of military operations in a variety of ways.[42] Transparency, mainly global availability of the same data and information to all the conflict parties, has a direct impact on the course of conflicts themselves since adversaries might learn of their foes actions or strategies and react to it.[43] Examples of this have already been shown: Serbian affiliates used mobile phones and other technological equipment to warn forces in the field when NATO planes were starting. It was also made apparent that global transparency turns the media into a tool for deciding an increasingly important battle: that for the hearts and minds of the citizens at home.

The Kosovo conflict has also lead to the emergence of another new topic: the use of the Internet during conflicts. While some voices seem convinced that the use of the Internet made a real difference and thoroughly changes the way wars and conflicts are being fought[44] others deconstruct the notion of an "Internet War" by saying that the media hyped the Web's role in Kosovo and that the actual impact of these activities in Cyberspace remain insignificant for outcome and course of conflicts.[45] This debate will not be resolved in this paper. So far, effects and impacts are far from clear and straightforward. Generally, two categories of usage could be

[42] See Department of the US Army, FM 100–6.

[43] Gowing, Nik, "Information in Echtzeit. Folgen für die internationale Konfliktlösung", *Internationale Politik*, 54, 2–3 (Februar/März 1999): 81–86.

[44] Goodman, "Kosovo – Our First Internet War".

[45] Katz, Jon, "The Browser: The Myth of The Internet War", Brill's Content, June 1999, online version, URL www.brillscontent.com/columns/browser_0699.html; Bendrath, "Kosovo im Cyberspace".

distinguished: the "peaceful" online collection and dissemination of information that is considered to enhances democracy, and the aggressive use of the Internet, in some of its facets called Cyberwar, to potentially harm the adversary. Both aspects mainly have an influence on collection and dissemination of information and on public affairs operations:

Collection and Dissemination Activities	Information Attacks Dimension
As a platform for the publication of all kinds of information. It allows everyone – states, companies, organizations, activist groups, individuals, etc. – to spread their views and opinions cheaply, leading to a proliferation of alternative voices;	For harmful information activities (attacks) that might damage through misinformation or sabotage of information: this includes the use of the Internet as a propaganda tool and so-called hacktivism;
As a means to gather "open source" information during all phases of a conflict: this possibility is open to the military as well as civilians as long as channels of communication stay open and phone lines remain working;	For cyberterrorism, which is information-oriented computer-based terrorism, or information warfare activities (Cyberwar) that might be state-conducted with specific political and strategic goals (strategic information warfare);

Table 19: Two Aspects of the Internet's Use in Conflicts

It is definitely wrong to say that "there isn't a single thing on the Internet that has truly affected this war",[46] but it is true that even though the free flow of information across boundaries does change some facets of conflict, it really did not have any direct impact on its waging or its outcome, especially since it did not evoke any major shifts in public opinion or policy: even though the Internet adds a new dimension to the propaganda war, television remains its prime media. Mostly it is provocative, kaleidoscopic TV images that dominate coverage and dictates the public's position.[47] Although the Internet has become an additional propaganda tool, television, mainly CNN, still reaches a far vaster international audience and features far more impressive images than the Internet, which is simply too diverse, too fragmented to achieve the same. It is very unlikely that

[46] Jon Katz, editor of the "brills content" in Lynch, "Kosovo Being Called First Internet War".

[47] Goff, *The Kosovo News and Propaganda War*, 19.

critical masses of people all attend to the same source simultaneously, and therefore few websites or online news sources have the audience to influence public opinion.

5.2 Discussion of Hypothesis s → X+

The relationship between the multiplication of actors and the conduct of Information Operations is not easily provable. Generally, the multiplication of actors seems to be lower than expected. However, the Internet and other new media challenge the established information monopoly of traditional actors and therefore also have an influence on some aspects of Information Operations because they empower a variety of new actors to exert some influence even during conflicts. The volume of Kosovo-related information and comment that was and still is available on the Internet was astounding and many people used it to fill information gaps. It was the first time that civilian populations involved in the war were able to speak to each other directly, via E-mail. The proliferation of alternative voices online is most likely having an incremental effect and a gradual influence on the way we interact in conflicts. By ways of the skill revolution, democratic electorate mainly gains influence over their respective political leaders; this had some effect on the physical attack dimension due to domestic pressure.

6 Blurring of Boundaries between Military and Politics

If the higher the degree of blurring boundaries between military and political domains faced by a conflict party the lower the level of successful conduct of Information Operations by this conflict party, then we can assume that the more political parties influence military parties due to domestic pressure the less successful the outcome.

	Intervening Variable's Value	Dependent Variable (X+) Predicted	Dependent Variable (X+) Observed	0-Hypothesis Rejected? (Yes/No)
r_2	3 (high)	0 or 1 (not successful or some successful)	1.333 (some successful +)	**(Yes)** but X+ observed is too high

As for both E and q, there seems to be some kind of relationship between the blurring of boundaries between military and political domains and successful waging of Information Operations, but the observed variable for X+ is too high for the very high value in r_2. Even though 1.333 is not enough to falsify the hypothesis, the relationship seems questionable. The 0-hypothesis can be partially rejected but further analysis of this relationship is necessary.

6.1 Public Awareness and Pressure Leads to Decisions Made with Daily Opinion Polls

The blurring of boundaries between military and political responsibilities in the context of coalition warfare makes struggles between the two factions inevitable. News and propaganda wars are fought for the heart and minds of the public: because large parts of IACs are fought on camera and are directed primarily at the opponent's will to fight, decision-makers are aware that success is very much dependent on public acceptance and begin to make their decisions with the aid of daily opinion polls.[48]

[48] This relationship only focuses on the negative impacts of such a blurring and on how they influence the conduct of IOs. Positive impacts such as more control of political bodies over military ones are not considered.

As for both the constructs comparing external factors and asymmetrical threats to the conduct of Information Operations, there seemed to be some kind of relationship shown by comparison of the variables r_2 and X+, but the observed level of success in IO was too high for the high degree of blurring between the domains. This chapter tries to resolve this uncertainty by process tracking.

A solution to overcome the reluctance of modern democracies to go to war seems to be the promise of "zero-death" conflicts. As noted above, high-tech conflicts that are promoted to be risk-free and casualty-averse seem to guarantee support of democratic electorates, at least as long as such an illusion can be maintained. This is even more so since their promise of precision weaponry and precise targeting satisfies citizens' sensitiveness to moral issues: in a war that can hit precisely, the high technological level of an attack is its moral and legal legitimacy. As the Revolution in Military Affairs increases the precision of targeting, it allows for more or less credible claims that everything possible is done to minimize collateral damage or unintended consequences of weapons' use.

During Allied Force these promises were furthered even by use of an automated planning tool that calculated the effect of more than one type of munitions on a given target, including legal and moral evaluation of targets into the computerized operation.[49] Kosovo was a contest that was so debated that NATO could only preserve its sense of moral advantage by observing especially strict rules of engagement assisted by linguistic maneuvers: language at the briefings was sanitized and dehumanized.[50] Words in public affairs operations were carefully selected to propel the image of clean, technical warfare: "Collateral damage", to generically unite casualties and civilian damage, is one of these terms. Along with "war" words such as "enemy" have practically disappeared from public state-

[49] Eash, "Harnessing Technology for Coalition Warfare", 33.

[50] Campbell, Alastair, "Communications Lessons for NATO, the Military and Media", *RUSI Journal*, 144, 4 (August 1999): 32; Ignatieff, *Virtual War*, 161–162.

ments, “dead” is mentioned seldom. Among the most used terms were “refugees”, “targets”, “operations”, and “success”.[51]

Decision-making guided by opinion polls necessarily leads to a change of relationship between armed forces and political leadership. The high likeliness that politicians have a strong bearing on military micromanagement ends the clear separation between political and military decision-making and is a price of coalition warfare.[52] One sharp example is the lengthy and slow target selection process that was highly politicized and generally considered to have prolonged the campaign; every morning, commanders and experts at various bases in different countries put together target folder over SIPERNET, the US military’s secure digitalized network, which were evaluated legally and morally by military lawyers that judged targets in terms of the Geneva Convention and the laws of war, before they were discussed with NATO force leaders politically. To speed up this very meticulous process of choosing and validating targets, all operations using American assets were managed not through the NATO chain of command but through EUCOM, with clearance from the Joint Chiefs of Staff in Washington.[53]

NATO adapted its military operations and target sets as the campaign proceeded, modifying types and locations of targets. After the decision at the NATO Summit in Washington on April 23, to further intensify the air campaign by expanding the target set to include military-industrial infrastructure and media targets, NATO reserved approval for selected categories of targets – for example,

[51] Bivio, “Soundbites and Irony”, 516. The adoption of a technical-military language, with acronyms and euphemisms to sanitize and dehumanize the horrors of war, goes back to the times of Secretary of Defense Robert McNamara during the Vietnam War and has become more refined since.

[52] Bendrath, Ralf, “Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges”, in: Bittner, Peter and Jens Woinowski (ed.), *Mensch – Informatisierung – Gesellschaft* (Münster, Lit Verlag: 1999): 141–161.

[53] Ignatieff, *Virtual War*, 99–101.

targets in downtown Belgrade, in Montenegro, or targets likely to involve high collateral damage – for higher political authorities.[54] This mechanism was necessary to ensure that member nations were fully cognizant of particularly sensitive military operations, which not only helped in satisfying political bodies but also to sustain the unity of the Alliance.[55] Operational actions were taken from NATO political authorities, these being the North Atlantic Council (NAC) and the NATO Secretary General who made the final decisions in consultation with the nations.[56] It was these political bodies that decided to start the campaign with mild sets of air strikes, allegedly against all air war principles, causing considerable critique from military professionals that saw this clearly limiting its effectiveness.[57] Political constraints that demanded that pilots fly above a certain height to minimize casualties degraded the effectiveness of information systems, thus greatly influencing the physical attack and other air war dimension of the operation.[58]

Another hotly debated issue that at times threatened to break up the Alliance and that considerably dampened the success of the overall operation was the reluctance to deploy ground troops, a direct consequence of war-averted democratic electorates and contrary to what most military experts assumed required. After

[54] Press Conference by NATO Spokesman, Jamie Shea and Colonel Konrad Freytag, GEAF, SHAPE, 24 April 1999, updated 24 April 1999, corrected version, Washington.

[55] Office of the Secretary of Defense, *Kosovo After Action Report*, xxi.

[56] Press Conference NATO, Transcript 25 March 1999; General Clark: "I would just tell you that from a military perspective, we are prepared to continue the strikes. But I want to note that of course we're taking actions from NATO political authorities, from the NATO Secretary General, so he'll make the final decision in consultation with the nations (…) I want to make it clear that we military leaders will not make that decision".

[57] Drozdiak, William and Dana Priest, "NATO's Computerized Campaign: A War With 'No Loss of Aircraft'", International Herald Tribune, 18 May 1999, 7.

[58] Thomas, "Kosovo and the Current Myth of Information Superiority".

General Wesley Clark, Supreme Allied Commander Europe, and burdened with the task of managing the difficult relations between NAC and the military bodies, had been rather frank in expressing his view that there was no winning the battle without ground troops, he was kept away from press briefings on orders of the Pentagon.[59] President Clinton had denied the military part of NATO this option as early as 1998 in the run up to the congressional elections, committing America to intervention only if impunity could be guaranteed. For other NATO Allies a ground war was also a political impossibility. Clark was forced to translate the political wishes of NATO governments into an unconventional air war, violating many basic principles of air power that more than once threatened to break up the solidity of the Alliance.[60]

6.2 Discussion of Hypothesis r_2 →X+

Since the Kosovo campaign was conducted entirely from the air without a ground component, it confirmed the notion that technological superiority hides a crucial weakness: a refusal to risk lives. In this coalition warfare, the strong political influence on military micromanagement ended the clear separation between political and military decision-making and resulted into an unconventional air war that had to implement the political wishes of NATO governments. These political constraints that demanded that pilots fly above 15’000 feet to nullify casualties, hampered all air war aspects of the Information Operations by degrading the effectiveness of information systems. Even though the comparison of values for the correlation r_2 → X+ did not establish enough clearly that there is a causal relation between the blurring between military/political

[59] Ignatieff, *Virtual War*, 93. He also publicly admitted on April 27 that a month of bombing had not stopped the Serbs from reinforcing their troops in Kosovo, contrary to the official NATO message.

[60] Drozdiak, “NATO’s Computerized Campaign”.

boundaries and the conduct of successful Information Operations, by means of process tracing this chapter presented reasonably good evidence of such a relationship.

7 Blurring of Boundaries between Battlefield and Civilian Realm

The higher the degree of blurring boundaries between military and civilian domains caused by a conflict party the lower the level of successful conduct of Information Operations:

	Intervening Variable's Value	**Dependent Variable (X+) Predicted**	**Dependent Variable (X+) Observed**	**0-Hypothesis Rejected? (Yes/No)**
r_3	3 (high)	0 or 1 (not successful or some successful)	1.333 (some successful +)	(**Yes**) but X+ observed is too high

The findings for r_3 are similar to the ones r_2. The high value of r_3 and the observed value for the dependent do not correspond optimally. Though not enough to accept the 0-hypothesis, the relationship remains questionable until proven further.

7.1 Neocortical Warfare and the Targeting of the Human Mind

The conclusions from the comparison of the value of r_3 with X+ were similar to the ones of r_2 with X+: the values do not correspond optimally. However, the thorough dual-use character of most targets in the information infrastructure, and the dual use character of new weapons and information tools that allow for Information Operations are a clear indication for such blurring boundaries between military and civilian issues.

Inherent in ideas of Information Operations is an extension of the battlefield to encompass the human mind as the ultimate target.[61] Targets may exist in physical space, in cyberspace, or be the human perception, with the objective of influencing this perception to affect decisions and resulting activities. In the new notion of "Neocortical" warfare military power uses language, images, and information to assault the mind, hurt morale, and change the will.[62] But not only decision-makers, policymakers, and military commanders are the targets of these assaults, today, even entire populations might be subject to such attacks: This "militarization" of the public turns the public into a tool for warfare, especially overtly seen in the definitions of psychological operations that define the entire populace as their targets. The idea of "Soft power" as understood by Keohane and Nye or the concept of "Noopolitik" developed by Arquilla and Ronfeldt,[63] both information forces that aim at spreading values worldwide, are in their core such forms of domination and occupation of everyone's mind with the aid of influencing messages and images. Battles for the hearts and minds crystallize in aggressive news and propaganda wars: to be successful on the battlefield loses in importance vis-à-vis efforts to manipulate its media representation.

Precision guided munitions might well reverse some of the 20th century trend towards great civilian casualties, but Information Operations that are directed at society at large, rather than against its fielded forces, necessarily blur the distinction between civilian and military objectives.[64] The "dual use" of many assets and technologies makes distinction even harder. In Kosovo, the most important targets were dual use targets, as for example power

[61] Top level attacked in Information Operations is the perception or the knowledge of an adversary with the objective to influence decisions and behaviors. (Waltz, Edward, *Information Operations*, 151).

[62] Szafranski, Richard, "Neocortical Warfare? The Acme of Skill", in: Arquilla and Ronfeldt, *In Athena's Camp*, 395–416.

[63] Cf. Arquilla, John and David Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy* (Santa Monica, RAND: 1999).

[64] Ignatieff, *Virtual War*, 170.

stations: they powered military computers as well as water pumping stations and hospitals. Striking them meant bringing war to the people, aiming not only at their morale but also endangering lives. It is also noteworthy that even those information technologies that are of maximum relevance to military operations have escaped from military control and have been taken up by the civilian sector in part or whole. An example is the GPS system, open to civilian use that was used by NATO, the Serbs, and KLA units equally. As a result, the distinction between civilian and military information system is increasingly blurred – a pattern that is likely to be equally true in future conflicts.[65]

Future wars that take place in even less physical space will bring even less physical destruction, and fewer casualties – but civilians are likely to suffer differently: In future cyberwars, who will be able to distinguish between what is a military and what is a civilian target? They will bring direct distress as a result of the cyber-targeting of civilian installations, which can as deadly as bombs. The Cyberwar scenarios turn war into something that is no longer an act of last resort; because there is less chance of combat casualties, a much lower cost of engaging in conflict, a blissful anonymity of strikes, it becomes much easier to commit acts of war.[66] It also blurs the boundaries of war and peace; it begins in peacetime to investigate faults and security failures, and declaration of war is basically the first serious attack.[67]

[65] Cordesman, *Defending America*, 46.

[66] Hoffmann, Lisa, "Computers Change Rules of War, Civilians Still Get Hurt", *The Washington Times*, 24 October 1999, C8.

[67] Cf. Arquilla, John, "A Fact-Based Fiction Cyberwar Scenario: The Great Cyberwar of 2002", *Wired* (February 1998): 122–138.

7.2 Discussion of Hypothesis r_3 → X+

Both dual use issues as well as targets in a Cyberwar pose an array of unresolved and uncertain legal issues that already have been touched upon in one of the previous chapters. In itself those issues only partly impede the conduct of Information Operations. This chapter did not succeed in establishing a strong connection between r_3 and X+, but rather between the conduct of Information Operations (X) and r_3. As hampering effects the dual use characters of mainly Cyberwar targets in connection with legal consideration as well as some restraints concerning actual targeting should be considered. Even though the phenomena of amalgamation between what is military and what is civilian seems not overtly impeding for military operations, it should be a signal to politicians that have a strong responsibility to protect their populace from too much involvement in conflicts, because if states lose their ability to protect, they also lose part of their legitimacy.

8 Information Operations Decisive in Information Age Conflicts

The last of the relationships is concerned with testing the relationship stating that there is a connection between the conduct of Information Operations and the level of success in IACs, by claiming that the higher the degree of successful conduct of Information Operations the higher the success in IACs:

	Independent Variable's Value	Dependent Variable (Y) Predicted	Dependent Variable (Y) Observed	0- Hypothesis Rejected? (Yes/No)
X+	1.33 (some success +)	1 or 2 (some successful or successful)	1.28 (some success)	**Yes**

The values indeed suggest that the surmised connection is valid: the 0-hypothesis can be rejected. There is thus some indirect proof that if intervening factors hamper Information Operations then they lessen the success of IACs. Further evidence of this statement can be found sufficiently in chapter III.2.

9 Conclusion: Which Influencing Factors Hamper Information Age Conflicts and How Strongly

The descriptive evidence offered in chapters IV, 1 to 8 can be summarized in order to demonstrate how *strongly* each of the influencing factors impacted the conduct of Information Operations. In the table below, value (0) stands for no influence, (1) for some influence, (2) for strong influence of the variables on the respective aspect of IOs as adapted to the case of Kosovo.[68] The sum of each column is an estimated value for how strongly a factor was able to affect the whole array of IOs, the sum of each row a number for how strongly each single aspect of IO was influenced.

Results suggest that the intervening variable *q (asymmetrical threats)* and the *technological factors* (part of the exogenous factors subsumed under *E*) most strongly influenced the successful conduct of Information Operations in Kosovo. Next in line is the influence exerted by the weather, followed closely by effects of political parties on military parties. The influence of blurring boundaries between military-civilian domains is very low, in accordance to the findings of chapter III.5 Both the credibility's (*C*) and the multiplication of actors' (*s*) impacts are lower than expected.

[68] This is not to be confused with part III, which served only to assign values to the intervening variables and did not strive to prove any connection between the phenomena. These findings are an estimate based on the descriptive evidence of part IV, 1–8, being a good basis for discussion even though not based on "hard" facts.

			Influencing Factors										
			Condition Variable	Intervening Variables					Exogenous Variables, Case specific				
Information Operations			C: Level of Credibility	q: Asymmetrical Threats	s: Multiplication of actors	Blurring of Boundaries between			Weather	Terrain	Technolog. Factors*	International Law / Regimes	
						~~r_1: states~~	r_2: military – politics	r_3: military-civilian					
Information-In-Warfare ***Gain & Exploit***		Intelligence, Surveillance, Reconnaissance (ISR)	0	2 (asymmetrically used air defense)	0		0	0	2 (thick layer of clouds)	1 (vegetation, mountains, etc.)	1 (technological inadequacy)	0	*6*
		Precision Navigation and Positioning	0	0	0		2 (collateral damage)	0	2 (thick layer of clouds)	1 (vegetation, mountains, etc.)	1 (technological inadequacy)	0	*6*
		Collection and dissemination activities	0	0	2 (more, different, information)		0	0	0	0	0	0	*2*
Information Warfare ***Attack***	C2W	PSYOP	2 (lacking truthfulness of messages)	1 (air defense)	0		0	0	1 (planes hampered)	1 (vegetation, mountains, etc.)	2 (broadcasting problems)	1 (restriction on measures)	*8*
		Electronic Warfare	1 (programs broadcasted)	1 (air defense)	0		0	0	1 (planes hampered)	1 (vegetation, mountains, etc.)	1 (not enough planes)	0	*5*
		Military Deception	0	1 (fear of retaliation)	0		0	0	0	0	1 (little infrastructure)	0	*2*
		Physical Attack	0	2 (air defense)	2 (domestic populace/ pressure)		2 (collateral damage)	1 (dual-use)	2 (thick layer of clouds)	2 (help to camouflage)	2 (technological failure)	2 (restraints on targets)	*15*
		Information Attack (Cyberwar)	0	2 (fear of retaliation)	0		2 (law, etc.)	2 (dual-use)	0	0	2 (no ability Cyberwar)	2 (fear to commit war crimes)	*10*
		Public Affairs Operations	2 (low trustworthiness)	2 (Serbs have info superiority)	1 (more information sources)		1 (language)	0	0	0	0	0	*6*
			5	11	5		7	3	8	6	10	5	

Table 20: How Strongly Influencing Factors Hamper the Conduct of Information Operations

The following tables lists the influencing factors in order of their influence exerted:

Influencing Factor	Influence Exerted
q: Asymmetrical Threats	11
E: Technological Factors	10
E: Weather	8
r_2: Blurring between Military/Politics	7
E: Terrain	6
C: Credibility s: Multiplication of Actors E: International Law/ Regime	5
r_3: Blurring between Military/Civilian	3

Table 21: Hampering Factors in Decreasing Order of their Influence on Information Age Conflicts

In addition, Table 20 indicates which aspects of Information Operations were the most affected: the value of the physical attacks dimension clearly stands out. It must be noted however that this result was likely biased by the focus on this aspect of IOs in the campaign, leading also to a focus in analysis due to the amount of information available. Information attacks/Cyberwar ideas also seem to have been hampered considerably according to the summary, while collection and dissemination and military deception have hardly been influenced.

The following tables lists the aspects of Information Operations in order of being influenced:

Aspects of Information Operations	Influenced
Physical Attack	15
Information Attack/ Cyberwar	10
PSYOP	8
• Intelligence, Surveillance, Reconnaissance • Precision Navigation and Positioning • Public Affairs Operations	6
Electronic Warfare	5
• Collection and Dissemination • Military Deception	2

Table 22: Aspects of Information Operations in Decreasing Order of Being Influenced

Omitted from the summary of influencing factors above is the state of the current military doctrine, which emerges as a critical exogenous variable in this analysis as it directly influences the way Information Operations are defined and conducted. Operation Allied Force provided the first real-world test of concepts that see the conduct of Information Operations to obtain Information Superiority over adversaries as increasingly important in this Information Age of warfare: the experience reveals an obvious weakness in translating many of the theoretical concepts into action. The After Action Review of the Office of the Secretary of Defense states that

> the importance of such capabilities was recognized fully during Operation Allied Force, but the conduct of an integrated Information Operations campaign was delayed by the lack of both advance planning and strategic guidance defining key objectives.[69]

These shortcomings help to explain the relatively low success of the operation. It is not the task of this thesis to speculate on implications of this for US or other nations defense strategy. Results presented in the Kosovo After Action Review highlight a broad range of issues and problems – from the demands of alliance and coalition warfare to employment of military forces to the functioning C4ISR systems.[70] Even though or precisely because it revealed faults in the doctrine, the United States can view the war in Kosovo as a test site for experimentation with untried ideas, as it will likely encourage the further development of the Pentagon’s Revolution in Military Affairs.

[69] Cf. Office of the Secretary of Defense, *Kosovo After Action Review*.

[70] Ibid.

Part V – Review

Criticizing the Model

Part V

Review: Criticizing the Model

Before looking at the broader implications of these findings for international security, we need to complete the research cycle. This short chapter aims to relate the findings of the preceding chapters back to the broader theoretical questions that motivated the research, drawing conclusions for revising the underlying assumptions and the model. The first chapter confronts the five theorems of the Information Age by criticizing and reassessing them. The second criticizes the arrow diagram and includes thoughts on reliability and validity of the model. A revised version that might produce better results in future research is suggested.

1 Reassessing the Five Theorems

The analysis of Information Age Conflicts was based on five theorems of the Information Age, which were derived from fragments and concepts of so-called Information Revolution literature. The case study allows us to reconsider these assumptions. Each theorem is evaluated in the light of whether it was confirmed or refuted by the analysis.

Theorem № 1: Information Superiority as key to success in the new operating environment

Theorem № 1 was the fruitful fundamental assumption for the analysis of IACs. Both the analysis of doctrinal papers and supportive evidence in the case study have shown that the competitive advantage over an adversary is crucial in this Information Age of warfare. Successful conduct of Information Operations thus (at least partly) defines the degree of successful outcome of conflicts. In this analysis, a military focus was predominant, but it became obvious nonetheless that many aspects of Information Operations can be conducted by a variety of other actors.

(confirmed)

Theorem № 2: Asymmetrical credibility as key power resource

Even though theorem № 2 is one of the most popular credos of the Information Age, the case study did not clearly reveal its importance and influence. Moreover, it seems that a whole range of diverse power tools is important today, still mainly dominated by traditional hard power military resources, which many Information Revolution scholars like to pronounce as becoming obsolete. It becomes obvious once more that the whole discussion about the redistribution and the changing nature of power is based on much speculation; in this domain, which nonetheless is still believed to lie at the heart of changes brought on by the Information Revolution, the need for basic empirical research is clearly evident.

(partly refuted)

Theorem № 3: Traditional boundaries blur in the Information Age

- *Between States*: The blurring of boundaries between states is an issue related to the redistribution of power; likewise, though common sense feeling points in that direction, there is little solid proof of such a development. It is also a concept that is hard to capture; findings are very dependent on the understanding of the issue and its operationalization. Still, it serves fairly well as part of a theorem that tries to denote the free flow of information traffic over geographical boundaries and the importance of virtual space;

(no statement possible)

- *Between Military – Politics*: The blurring of boundaries between military and politics is also challenging to capture, however, there was evidence presented that the skill revolution and domestic pressure end the clear separation between military and political domains. Though the analysis only focused on negative aspects of such an amalgamation, there certainly are many positive aspects that could be considered. Again, more basic research on power redistribution in connection with the skill revolution would certainly be appreciated;

  (partly confirmed)

- *Between Military – Civilian*: The expansion of the battlefield to the human perception and to „virtual space" threatens to result in more civilian involvement in conflicts. More so due to the dual use character of most targets in the information infrastructure and the dual use character of new weapons and information tools that allow for Information Operations. These facts definitely pose a considerable problem for decision-makers. Of the three parts of Theorem № 3, this one is the most evident and most confirmed, even though its direct hampering effect on IACs could not be established.

  (confirmed)

Theorem № 4: Networks vs. Hierarchies: From centralized hierarchical to decentralized flat organizations

Like theorem № 2, № 4 also is a popular belief in Information Revolution literature, also with little empirical backing, though information networks are a key feature of today's operating environment. The model tries to integrate it via a variable standing for the multiplication of actors, which is, admittedly, somehow far fetched. A revised model should try to integrate the idea of networks as gaining power over hierarchies more directly, even more so because it is an increasingly important notion in military perception. More ground research on this could be done by way of social network analysis or similar approaches.

(no statement possible)

Theorem № 5: Asymmetry vs. Doctrine of Dominance: Small players harm the powerful easily

This theorem was strongly confirmed in the case study; it is also a fashionable argument in US military publications to underscore perceived vulnerability. It is true that such emerging international asymmetries in the capacities and vulnerabilities of states have the potential to generate new interaction dynamics, but it should be considered more than just a good argument for the necessity of further arming and military expenditure; rather it should give inducement to think over structures of organizations and develop new approaches to security.

(strongly confirmed)

In conclusion, the analysis calls into question the very essence of the Information Revolution theorems: While information superiority can be held up as being decisive in today's strategic environment, partly due to the changing nature of power, particular statements about the redistribution of power might have to be reconsidered. This threatens basically all the theorems, above all number 2, 3, and 4. A word of caution however: This does not mean that they and this whole analysis do necessarily become obsolete. It rather seems that this is a result of the skewed, complex, and volatile distribution pattern that was predicted in chapter II.2.3, partly because we are in a transition period, but more likely because the outcome of change will truly be contradictory and a lot less explicit than scholars like to envisage.

2 Revising the Model

What does this mean for the model? Realistically, it must be upheld that it stands on shaky legs and does only partly hold up to scrutiny. But since it is a first effort and food for thought in an area that has seen little research it is certainly not a loss of time to go back and try to advance it by eradicating internal mistakes. Four aspects of the model's validity/reliability that should be as high as possible to assure good quality research are considered.[1]

- The *Construct Validity*, or the accuracy with which the collected data captures the model's concepts/variables is only half good. Parts of the operationalization are problematic due to the abstract nature of the phenomena analyzed. Subsequently, data collected in part 3 not always captures the variables optimally. However, process tracing and causal narrative provided additional in-depth analysis that helps to overcome part of the problem and helped to gain better results.
- The *Internal Validity* was too low. Internal validity means that the variation observed in the independent variable correlates with observed variation in the dependent variable in a way that no other variable provides a more plausible explanation of variation. It has been refrained from identifying alternative explanations or rival hypotheses, which would have been the most effective defense against charges that the outcome observed in the case was caused by variables other than those claimed.[2] Insufficiencies of a study based solely on one case very high. This lessens the overall internal validity considerably.
- The *External validity* was also low. It was repeatedly stated that the external validity of this model is very low because it

[1] Mitchell and Bernauer, *Empirical Research on International Environmental Policy: Qualitative Case Studies*.

[2] Ibid., 23.

only passes a single-case-study test. Any model that passes a single-case-study test may require rare antecedent conditions,[3] which remain easily hidden in such an investigation. More case studies in given time would lift the external validity however. Through thorough process tracing some of this deficiency was repaired already because it confirmed the validity of the theory through its ability to explain at least one case.

- The *Reliability*, or the possibility that other researches can replicate the research techniques and arrive at the same results, is fairly good. Basically all research steps are laid open in this analysis. It is believed that other researchers using the same material would arrive at similar results.

Generally, these results are not very satisfactory. Especially internal and external validity of the model are too low; more case studies with a similar model could help to overcome some of these deficiencies. Another problem, which can hardly be solved without completely changing the approach, is the problem with operationalizing "soft" and very complex concepts such as credibility.

Apart from that, the model proved fairly well suited to explain factors that hamper the conduct of IACs. However, some faults were exposed in the model; to optimize it, the following changes could be undertaken:

- A direct relationship between the blurring of geographical boundaries and the waging of IACs should be included in the model ($r_1 \rightarrow X+/Y$), because the virtualization of war is likely to have a general impact on the successful waging of future conflicts and also heightens dangers from the dependency on high-tech machinery;

[3] Van Evera, *Guide to Methods for Students of Political Science*, 10–11: "Antecedent conditions are phenomena whose presence activates or magnifies the action of a causal law or hypothesis." They are also called preconditions, enabling conditions, auxiliary assumptions.

- The blurring of boundaries between the military and the civilian domains only partly impedes the conduct of Information Operations; the study did not succeed in establishing any real connection between r_3 and X+, but rather between the conduct of Information Operations (X) and r_3. These relationships should be thought over and maybe omitted. The issue remains of importance for decision-makers however;
- The claims that the conduct of Information Operations has a strong influence on the level of credibility associated with a conflict party (X → C) were not further followed. However, it seems adequate to keep up this statement for future research. It is difficult on the other hand to find evidence for the direct connection between E and C, stating that certain case specific factors influence the level of credibility associated with a party. Rather, E has an indirect influence on C by hampering Information Operations and thus challenging the image projected by rhetoric;
- There was no evidence for a conditioning effect of C. It also became apparent that the level of credibility might have more of a direct impact on the level of success in IACs (C → Y) than on the conduct of IO because it changes the way success is assessed. In this sense, low credibility due to failure to match rhetoric with action, especially in areas concerned with value-driven military engagement, inflicts lasting damage on conflict parties;
- The relationship between the conduct and ideas of Information Operations and the intervening variables has, apart from evidence presented for the relationship $X \rightarrow r_3$ and some for $X \rightarrow r_1$, not been analyzed. This is clearly a weakness of this study and it remains uncertain whether these relationships should be kept up in a revised model.

The following figure shows a revised arrow diagram that would be suggested for further research.

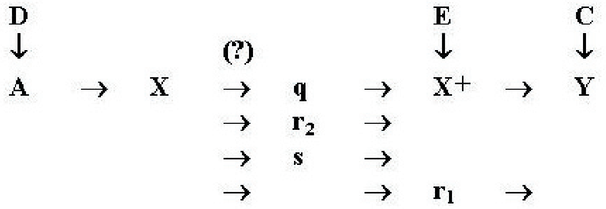

Figure 10: Model and Arrow Diagram Revised

As has been noted repeatedly, there is also a great need for more basic research on the underlying assumptions of this construct.

Conclusion

Most experts agree today that the Information Revolution is having an essential impact on the international system. The Information Revolution is a dynamic and continuing progress driven by information and communication technologies that enable humankind to gather, process, and transmit data with higher speed, larger capacity, and greater flexibility. Societies in developed countries thoroughly depend on them for their well-being, every-day life, work, economic transactions, comfort, entertainment, and many personal interactions. Even though there is no consensus on how precisely this influence manifests itself, arguments mainly run that the Information Revolution turns the world into an environment in which information, knowledge, and ideas become supreme resources in economics, politics, and military operations alike. At the heart of the matter lays the debate about changing nature and possible redistribution of power.

Some scholars claim that power in the global information society depends less on hard factors such as territory, military power, and natural resources but rather on soft power factors such as information, technology, and institutional flexibility. Consequently, opposing powers are less inclined to battle out their differences in the physical arena. Rather, they focus their activities on the "virtual" arena of information: The central strategic principle of today is to gain comparative advantage over adversaries in the information domain. At the same time, the transnational architecture of global information networks has reduced the significance of territorial borders. The cross-border movement of goods, services, ideas, and capital has noticeably increased, resulting in a substantial intensification in transnational cultural and political exchanges and in the emergence of many institutions, actors, and structures that also transcend state borders. But the overall development is not that clear-cut and plainly intelligible: The distribution of power has become increasingly volatile and complex, as traditional political and cultural boundaries are beginning to disintegrate. The diffusion of territorial, societal, and economic space is not only taking place in a global and transnational outward movement but also in the opposite inward direction, as it empowers local communities and actors to act independently. Hence, the movement is not only globalizing but also localizing, not only fragmentizing but also integrating in nature. All the above facts basically mean that we have reached a point where the traditional domestic-international framework no longer holds and most of the traditional theoretical approaches therefore no longer suffice to explain matters of the 21st century.

The thesis aimed to pinpoint systemic factors in this newly emerging operating environment that substantially influence the successful managing and waging of Information Age Conflicts (IACs). IACs take place in an international environment currently altered by the diverse effects of the Information Revolution and are conducted with the ultimate aim to gain Information Superiority over adversaries. In order to identify the factors, a model was developed based on five theorems, which were drawn from Information Revolution literature. The five theorems take into account that the Information Revolution is restructuring the international system in an unprecedented way and they have a special focus on the redistribution and the changing nature of power. The theorems address new military doctrine that sees the successful conduct of so-called Information Operations as the crucial feature of warfare in the Information Age; further look at the importance of credibility for political success in the long run; deal with the fact of blurring boundaries between states, military-politics, and the military-civilian domain; focus on the statement that networks wage wars today and appear to outmatch centralized hierarchical forms of organization; and finally strongly emphasize that small players can outmaneuver huge opponents by using asymmetrical forms of warfare. Mainly six factors were predicted to influence the successful conduct of IACs. In the case of Operation Allied Force, the hampering effects of three of them were relatively strong, two had only medium impact, and for one, there was no evidence found to support the causal relationship. Apart from these factors, current inadequacies in doctrine and organization as well as apparent flaws in translating theoretical concepts into action further account for observed shortcomings during NATO's operation in Kosovo.

The strongest hampering influence was observed for the *degree of asymmetrical challenge faced* by the Western alliance. In Kosovo, the chief asymmetrical threat was the effective employment of Serbian Information Operations, which won Milosevic the advantage of Information Superiority most of the time. Further remarkable asymmetrical aspects were the use of cell phones to warn of incoming NATO planes and the effective use of the Internet in the information battle. These kind of asymmetrical forms of warfare remove conflict activities to a sub- or supranational sphere where there are harder for governments to control. The tools of the military can assist only marginally in countering the challenges of asymmetrical strategies and tactics because they are at present ill-suited for doing so: Their focus is still on the traditionally restricted battlespace, the defined box in which conflicts take place, or on the actions of known and visible enemies. Even the newest doctrine, which was the focus of this study, is prey to such inadequacies when it comes to countering asymmetry. And even America, ahead of all others in reacting to the imperatives of the Information Revolution, has not yet reorganized its troops around the strategic doctrine, which the Revolution in Military Affairs (RMA) seems to make possible. This makes apparent the need to reshape the whole politico-military system in order to deal with the most probable threats of asymmetrical strategies. In this new environment, it has become clearer than ever that technology alone guarantees no victory. The importance of organizational change and institutional reform grows during periods of technological innovation, since new technologies merely create possibilities; whether they are exploited depends on the ability of essentially conservative institutions to embrace them.

A second important set of factors that hamper the conduct of IACs are *case specific external factors* like bad weather, an unfavorable terrain, and technological failure, which impact basically all aspects of Information Operations. Remarkable is the curtailing influence that aspects of international law had on the willingness of the US to launch serious cyber attacks against adversaries. However, the rules of international law and the law of war can only insufficiently guarantee the non-utilization of possible "cyber weapons": Most technical possibilities of offensive Information Operations are not regulated by existing agreements, since many aspects do not fall under the traditional understanding of violence or are not regulated due to inadequate legal terminology. As long as this condition of partial non-regulation lasts, international law is at best a voluntary guideline for the selection of offensive, defensive, or retaliatory action in information battles but never an obstacle for political resolution or military willingness to engage in "Cyberwar" activities.

Still considerably strong was the influence of *blurring boundaries between military and political domain* on the conduct of IACs. In this coalition warfare, strong political influence on military micromanagement, partly due to the skill revolution, resulted in an unconventional air war. These political constraints hampered all air war aspects by degrading the effectiveness of Information Operations. It further revealed a weakness of war waging democracies: The refusal to risk lives. The struggle between politicians and military over influence, which politicians are likely to win more often than not, will likely boost the use of asymmetrical means to drive a wedge between allied conflict parties. In this, the focus of hostilities is shifting from the enemy's fielded forces to the civilian opinion at home, which sustains the will to fight, or might even result in direct attacks against mostly civilian (information) infrastructure to directly influence politicians.

The influence of *credibility* on the conduct of Information Operations was lower than expected. Lacking credibility mostly affected those aspects of IOs that have a psychological or deceptive nature, including public affairs operations. But credibility also plays an important part in other aspects of IACs: The competition for press attention and sympathy for one side's view was a crucial part of Operation Allied Force and lacking trustworthiness threatened to undermine public support in the Allied countries, which was necessary to keep the war going. Even though the influence of credibility was not overtly great, in future wars that have a strong propaganda war component, Western conflict parties certainly need to be very careful how they handle control and release of information to the public in order to win extensive and aggressive media wars. Furthermore, low credibility due to lacking ability to match rhetoric with action, especially in areas concerned with value-driven military engagement, inflicts lasting damage on conflict parties and challenges their status in the international system.

The relationship between the *multiplication of actors* and the conduct of Information Operations remains unclear. The diffusion of power to new contenders seems lower than generally predicted and there is not much evidence that the forces driving global change are substantially undermining the state and its political agency, at least not in times of conflict. However, the Internet and other new media challenge the established information monopoly of traditional actors and therefore also have an influence on some aspects of Information Operations because they empower a variety of new actors to exert some influence during conflicts. The proliferation of alternative voices online is having an incremental effect and a gradual influence on the way one interacts in conflicts. There was also no success in establishing a clear connection between the degree of *blurring boundaries between military and civilian domains* and the successful conduct of Information Operations. Yet, the dual use character of Cyberwar targets as well as restraints on actual targeting in connection with legal considerations should be considered as partly hampering effects.

If we take a critical look at the underlying assumptions of the model, we get ambiguous results. On the one hand, the analysis shows clearly that the preoccupation of the military with the impact of the Information Revolution on military affairs indeed has an immense impact on the way warfare is conducted today and will be conducted in the future. On the other hand, the analysis cannot sufficiently show enough proof for many other Information Revolution concepts; and, what's more, they appear insufficient in their current state to model real world circumstances. This does not mean that there is no change in the nature of power and consequently adjustment in the way power is understood; this principal statement is considered valid until proven otherwise. But our understanding of the consequences of these changes for international relations and security remains limited at best. Statements about the redistribution of power must further be seen in much more relative terms than generally suggested, especially because the outcome of change is truly contradictory and a lot less explicit than some scholars like to envisage. The complexity and volatility of the development severely challenges current attempts to capture it in comprehensible forms. Since there remains much ambiguity about what kind of world the current global transformations will ultimately create it would be wrong or at least too early to dismiss the Information Revolution just as a change in the "exogenous variables" that impact in some unspecific way people's political preferences but which as a whole have no great impact on the nature of world politics.

The doctrinal development observable today and the precedents of the world's first Information Age Conflict allow us to draw a number of conclusions that go beyond the identification of hampering factors in the operating environment. Investigation of emerging Information Operations doctrine is not only relevant from a strategic or operative viewpoint but also in a broader security policy perspective. Emerging doctrine goes far beyond being a mere guideline for technology supported military operations; it openly considers the use of non-military and asymmetrical alternatives in international conflicts. The candid announcement to focus activities in conflicts on Information Operations and furthermore to exploit IOs as a tool for international politics detached from military battlefield operations – e.g. to conduct computer espionage and -sabotage as well as "truth projection" over electronic mass media at all times – makes the worldwide proliferating effect of these ideas ever the more likely. In this, the emerging doctrine represents a fundamental challenge for both arms control and international law, which need to address the fundamental questions of control of IO tools and the adjustment of international law to cover the new doctrinal ideas and intentions.

Information Operations concepts at hand further consider the targeting of civil targets on the physical, the psychological, and the cyber level. Adding this to the general trend towards asymmetric strategies, we are likely heading towards warfare in which battlefields envelop entire societies, the distinction between civilian and military disappears, and military objectives shift from annihilating tidy enemy lines to eroding popular support for the war within the enemy's society. In IACs, military power uses language, images, and information to assault the mind, hurt morale, and change the will: Information Operations generally expand the battlefield to encompass the human minds of the world's population. Herein, they blur boundaries between civilian and military objectives and systems, and also between war and peace since many aspects of IOs are conducted ceaselessly. Even though IACs are often pictured as less violent and bloody than former wars, the trend towards more civilian involvement is not encouraging. Suddenly, frontlines are "everywhere". Through this change in room and space of future acts of war there are new challenges concerning the protection of society. The development towards willful integration of civil infrastructure and stronger shift towards deception of whole societies is truly alarming. There is an essential need to protect civilians from too much involvement in these conflicts, or else they become central targets of these new forms of warfare through the targeting of civilian installations or worse, the targeting of the human mind.

Information Operation concepts focus security policy on the vulnerability of civil infrastructures and thus ultimately raise an array of questions about nature, scale, and ultimately management of future international conflicts. Foremost, the necessity to protect society against asymmetrical threats has become *the* central security policy concern today, and not only after 11 September. Changes in the international environment have turned the traditional foundations of security upside down: For one thing, the object of security is no longer simply the territorial integrity of the state. Modern information technologies have brought about new vulnerabilities and risks for developed societies, as the Information Revolution has dramatically increased the dependence of developed countries on national and transnational information infrastructures. Key critical infrastructures – power, communications, information, transportation, and other systems on which the economy, national security, and quality of life depend – are reliant on information systems for their smooth, reliable, and continuous operations. Fears that terrorists or enemy states might target these critical infrastructures have been around for a while. Compared to more traditional security threats, which were usually categorized in the dimensions actor, intention, and capabilities, modern threats, which include but do not only consist of all aspects of Information Operations, cannot longer be labeled that easily. There is no clearly identifiable actor who could become a possible enemy; cyber attackers can be teenagers, rogue nations, terrorists or disgruntled insiders, even private companies or political activists. This implies that it is very hard to get verifiable information on the hostile intentions of the possible attacker, even if he can be identified without doubt. And it remains unclear whether the possible enemy has the capability to wage a large-scale cyber attack, because traditional means of intelligence do not help very much in this field.

In this radically changed strategic context of security policy the call for capable protection of these critical infrastructures becomes an interesting question. Clearly, the state is not the only international actor that provides public services such as security, welfare, education, and law. But the scale of the threat and the complexity of the task at hand call for a leading role of the state, even though the developments of the past decade appear to undermine the state and its political agency. Evidently, the state has to adapt its functions to the conditions of a rapidly changing international environment. Herein, the dispute about the adequate protection of critical information infrastructures is closely linked to the discourse about the role of the state in a changed world. A reduction of risks will not only require increased multilateral cooperation but also intensified collaboration with non-state actors – most notably those in the private sector who own information systems. In order to understand and skillfully adapt to these changes, states need to develop new conceptual repertoires and develop adequate strategic tool kits that will better equip them to meet the challenges posed by the new threat picture, the speed with which the world is evolving, and the extreme global complexity that is emerging.

Bibliography

Alberts, David S. and Daniel S. Papp (eds.), *The Information Age: An Anthology of Its Impacts and Consequences* (Washington D.C., National Defense University: 1997).

Alberts, David S., Daniel S. Papp, and W. Thomas Kemp III, "The Technologies of the Information Revolution", in: Alberts, David S. and Daniel S. Papp (eds.), *The Information Age: An Anthology of Its Impacts and Consequences* (Washington D.C., National Defense University: 1997).

Alberts, David S., John J. Garstka and Frederick P. Stein, *Network Centric Warfare*, 2nd Edition (Washington, D.C., National Defense University: 1999).

Angell, Robert, *Peace on the March: Transnational Participation* (New York: Van Nostrand Reinhold Co: 1969).

Arkin, William and Robert Windrew, "The Other Kosovo War: Baby Steps – and Missteps – for Information Warfare", Special to MSNBC, 29 August 2001.

Arkin, William M., "NATO's Info Strategy Bombs", *Special to Washington Post*, 26 April 1999.

Armitage, John, "CTheory Interview with Paul Virilio: The Kosovo War Took Place in Orbital Space", Paul Virilio in Conversation with John Armitage, translated by Patrice Riemens, *CTheory,* 23, 3, 18 October 2000.

Arquilla, John and David F. Ronfeldt, "Cyberwar is Coming!", in: Arquilla, John and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, RAND: 1997): 23–60.

Arquilla, John and David F. Ronfeldt, *The Advent of Netwar* (Santa Monica, RAND: 1996).

Arquilla, John and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, RAND: 1997).

Arquilla, John and David Ronfeldt, "A New Epoch – and Spectrum – of Conflict", in: Arquilla, John and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, RAND: 1997): 1–20.

Arquilla, John and David Ronfeldt, "Information, Power, and Grand Strategy: In Athena's Camp – Section 1", in: Arquilla, John and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, RAND: 1997): 141–171.

Arquilla, John and David Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy* (Santa Monica, RAND: 1999).

Arquilla, John, "A Fact-Based Fiction Cyberwar Scenario: The Great Cyberwar of 2002", *Wired* (February 1998): 122–138.

Arquilla, John, David Ronfeldt and Michele Zanini, *Networks, Netwar And The Information Age* (Santa Monica, RAND: 1996).

Baumard, Philippe, "Knowledge Warfare", in: Campen, Alan D., Douglas Dearth, and Thomas Goodden (eds.), *Cyberwar: Security, Strategy and Conflict in the Information Age* (Fairfax, AFCEA International Press: 1996): 147–160.

Becher, Klaus, "Changing Information Requirements in Foreign-Policy Institutions", European Information Network on International Relations and Area Studies 8th Annual Conference, Barcelona, 2–3 October 1998, online version available, URL http://www.cidob.org/einiras/presentations/becher.htm.

Bell, Daniel, "Thinking Ahead", *Harvard Business Review*, 26 (May/June 1979).

Bendrath, Ralf, "Bombiger Erfolg oder Peinliche Lügen?", *telepolis*, 30 August 2001.

Bendrath, Ralf, "Der Kosovo-Krieg im Cyberspace. Cracker, Infowar und Medienkrieg", *telepolis*, 19 July 1999.

Bendrath, Ralf, "Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges", in: Bittner, Peter and Jens Woinowski (eds.), *Mensch – Informatisierung – Gesellschaft* (Münster: Lit Verlag, 1999): 141–161.

Berkowitz, Bruce D., "Warfare in the Information Age", in: Arquilla, John and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, RAND: 1997): 175 –190.

Berkowitz, S. D., *An Introduction to Structural Analysis: The Network Approach to Social Research* (Toronto, Butterworths: 1982).

Black, C.E., *The Dynamics of Modernization: A Study of Comparative History* (New York, Harper & Row: 1966).

Borger, Julian, "Pentagon Kept the Lid on Cyberwar in Kosovo", *The Guardian*, 9 November 1999.

Boyd, John, *A Discourse on Winning and Losing* (Maxwell, Air University: 1987).

Brewin, Bob, "Cyberattacks Against NATO Traced to China", *Federal Computer Week*, 2 September 1999.

Brivio, Enrico, "Soundbites and Irony: NATO Information is Made in London", in: Goff, Peter (ed.), *The Kosovo News and Propaganda War* (Vienna, The International Press Institute: 1999): 514–527.

Brown, Lester R., *World Without Borders: The Interdependence of Nations* (New York, Random House: 1972).

Burns, Robert, "Computer Warfare Used in Yugoslavia", AP, 7 October 1999.

Campbell, Alastair, "Communications Lessons for NATO, the Military and Media", *RUSI Journal*,144, 4 (August 1999): 31–36.

Campen, Alan D. and Douglas H. Dearth (eds.*), Cyberwar 2.0: Myths, Mysteries and Reality* (Fairfax, AFCEA International Press: 1998).

Campen, Alan D., Douglas Dearth, and Thomas Goodden (eds.), *Cyberwar: Security, Strategy and Conflict in the Information Age* (Fairfax, AFCEA International Press: 1996).

Campen, Alan, *The First Information Warfare* (Fairfax, AFCEA International Press: 1992).

Castells, Manuel, *The Information Age: Economy, Society and Culture* (Malden, Blackwell: 1997).

Cebrowski, Arthur K. and John J. Garstka, "Network-Centric Warfare: Its Origin and Future", *Proceedings of the Naval Institute*, 124, 1 (January 1998).

Center for Strategic and International Studies (CSIS), *Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo*, CSIS Task Force Report (Washington D.C., Center for Strategic and International Studies: 1998).

Center for Strategic and International Studies, *The Information Revolution and International Security*: *Robert F. McMormich Tribune Foundation Report* (Washington D.C., Center for Strategic and International Studies: 1996).

Classen, Elvi, "Medienrealität im Kosovo-Krieg", *telepolis*, 30 October 1999.

Cohen, Eliot, “A Revolution in Military Affairs”, *Foreign Affairs*, 75, 2 (March/April 1996): 37–54.

Cooper, Jeffrey R., “Another View of the Revolution in Military Affairs”, in: Arquilla, John and David Ronfeldt (eds.), *In Athena’s Camp: Preparing for Conflict in the Information Age* (Santa Monica, RAND: 1997): 99–140.

Copeland, Thomas E. (ed.), *The Information Revolution and National Security* (Carlisle Barracks, Strategic Studies Institute: August 2000).

Cordesman, Anthony H*, Defending America. Redefining the Conceptual Borders of Homeland Defense. Critical Infrastructure Protection and Information Warfar*e, Rough Draft for Comment (Washington D.C., Center for Strategic and International Studies: 19 July 2000).

David, Norman C., “An Information-Based Revolution in Military Affairs”, in: Arquilla, John and David Ronfeldt (eds.), *In Athena’s Camp: Preparing for Conflict in the Information Age* (Santa Monica, RAND: 1997): 79–98.

Dearth, Douglas, “Imperatives of Information Operations and Information Warfare”, in: Campen, Alan D. and Douglas H. Dearth (eds*.), Cyberwar 2.0: Myths, Mysteries and Reality* (Fairfax, AFCEA International Press: 1998).

Defense Science Board, *Report of the Defense Science Board Task Force on Information Architecture for the Battlefield* (Washington, D.C., Office of Secretary of Defense: October 1994).

Defense Science Board, *Report of the Defense Science Board Task Force on Information Warfare-Defense* (Washington, D.C., Office of Secretary of Defense: November 1996).

Denning, Dorothy E, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy”, presented at Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking Workshop, 10 December 1999, available online, URL http://www.nautilus.org/info-policy/workshop/papers/denning.html.

Department of Defense, Office of General Counsel*, An Assessment of International Legal Issues in Information Operations* (Washington, D.C., Department of Defense: May 1999).

Department of the Army, *Information Operations, Field Manual No. 100–6, FM 100–6* (Washington D.C., Department of the Army: 27 August 1996).

Department of the United States Air Force, *Air Force Doctrine Document 2–5, Information Operations* (Washington DC, Department of the United States Air Force: August 1998).

Department of the United States Air Force, *Cornerstones of Information Warfare* (Washington D.C., Department of the United States Air Force: circa 1995).

Deutsch, Karl W., "Mass Communications and the Loss of Freedom in National Decision-Making: A Possible Research Approach to Interstate Conflicts", *Journal of Conflict Resolution*, 1, 2 (1957): 200–211.

Devost, Matthew G, *National Security in the Information Age*, M.A. Thesis (Vermont, The Faculty of the Graduate College: 1995), URL http://www.devost.net/mgd/documents/devostthesis.pdf.

Di Censo, David J., "IW Cyberlaw: The Legal Issues of Information Warfare", *Aerospace Power Journal*, 13, 2 (Summer 1999): 85–102.

Drozdiak, William and Dana Priest, "NATO's Computerized Campaign: A War With 'No Loss of Aircraft'", *International Herald Tribune*, 18 May 1999.

Drucker, Peter F., *The New Realities: In Government and Politics, in Economics and Business, in Society and World View* (New York, Harper Collins Publishers: 1989).

Dunn, Ashley, "Crisis in Yugoslavia – Battle Spilling Over Onto the Internet", *Los Angeles Times*, 3 April 1999.

Dutton, William H. (ed.), *Society on the Line: Information Politics in the Digital Age* (Oxford, Oxford University Press: 1999).

Eash, Joseph J III., "Harnessing Technology for Coalition Warfare", *NATO Review* (Summer/Autumn 2000): 32–34.

Eyal, Jonathan, "The Media and the Military: Continuing the Dialogue after Kosovo", *RUSI Journal*, 145, 2 (April 2000): 37–43.

Geiger, Gebhard. *Offensive Informationskriegsführung. Die "Joint Doctrine for Information Operations" der US-Streitkräfte: Sicherheitspolitische Perspektiven.* SWP Studie (Berlin, Stiftung Wissenschaft und Politik: Februar 2002).

Goff, Peter (ed.), *The Kosovo News and Propaganda War* (Vienna, The International Press Institute: 1999).

Goodman, Ellen, "Kosovo – Our First Internet War", Reporternews.Com, 9 April 1999, URL www.reporternews.com/1999/opinion/good0409.html.

Gowing, Nik, "Information in Echtzeit. Folgen für die internationale Konfliktlösung", *Internationale Politik*, 54, 2–3 (Februar/März 1999): 81–86.

Graham, Bradley, "Cyberwarfare: It's Still a Pandora's Box", *International Herald Tribune*, 9 November 1999.

Grossman, Elaine, "U.S. Commander in Kosovo Sees Low-Tech Threats to High-Tech Warfare", *Inside the Pentagon*, 9 September 1999.

Hammond, Philip, "A War of Words and Pictures", *The Independent*, 6 April 1999.

Hart, J.A., "Three Approaches to the Measurement of Power in International Relations", *International Organization*, 30, 2 (Spring 1976): 289–305.

Hart, Jeffrey, and Sangbae A. Kim, "Power in the Information Age", in: Ciprut, Jose V. (ed.), *Of Fears and Foes: International Relations in an Evolving Global Political Economy* (Westport CT: Praeger, 2000), online version, URL http://www.vii.org/papers/ciprut2.htm.

Henry, C. Ryan and Edward C. Peartree (eds.), *Information Revolution and International Security* (Washington, Center for Strategic and International Studies Press: 1998).

Hoffmann, Lisa, "Computers Change Rules of War, Civilians Still Get Hurt", *Washington Times*, 24 October 1999.

Hoffmann, Lisa, "U.S. Opened Cyber-War During Kosovo Fight", *Washington Times*, 24 October 1999.

Hundley, Richard O. and Robert H. Anderson, "Emerging Challenge: Security and Safety in Cyberspace", in: Arquilla, John and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, RAND: 1997): 231–252.

Ignatieff, Michael, *Virtual War. Kosovo and Beyond* (London, Chatto and Windus: 2000).

Isenberg, David, "An Electronic Pearl Harbor? Not Likely", in: Copeland, Thomas E. (ed.), *The Information Revolution and National Security* (Carlisle Barracks: US Army War College, Strategic Studies Institute: August 2000): 92–102.

Jertz, Walter, *Krieg der Worte, Macht der Bilder. Manipulation oder Wahrheit im Kosovo-Konflikt?* (Bonn, Bernard & Graefe: 2001).

Johnson, Stuart E. and Martin C. Libicki, *Introduction to Dominant Battle-Space Knowledge: The Winning Edge* (Washington D.C., National Defense University: 1995).

Joint Chiefs of Staff, *Joint Publication 1–02, DOD Dictionary of Military and Associated Terms*, as Amended through 1 September 2000.

Joint Chiefs of Staff, *Joint Publication 3–13, Joint Doctrine for Information Operations* (Washinton D.C., 9 October 1998).

Joint Chiefs of Staff, *Joint Publication 3–53, Doctrine for Joint Psychological Operations* (Washington D.C., 10 July 1996).

Joint Chiefs of Staff, *Joint Statement on the Kosovo After Action Review* (initial assessment), presented by Secretary of Defense William S. Cohen and Gen. Henry H. Shelton, Chairman of the Joint Chiefs of Staff, before the Senate Armed Services Committee, 14 October 1999.

Jordan, Tim, *Cyberpower. The Culture and Politics of Cyberspace and the Internet* (London, Barnes and Noble: 1999).

Joshi, Akshay, "A Holistic View of the Revolution in Military Affairs (RMA)", *Strategic Analysis*, 22, 11 (February 1999).

Katz, Jon, "The Browser: The Myth of The Internet War", Brill's Content, June 1999, online version, URL www.brillscontent.com/columns/browser_0699.html.

Kautsky, John H, *The Political Consequences of Modernization* (New York, John Wiley: 1972).

Kay, Sean, "After Kosovo: NATO's Credibility Dilemma", *Security Dialogue*, 31, 1 (March 2000): 71–84.

Keohane, R. and J. Nye, *Power and Interdependence: World Politics in Transition*, 2nd edition (Boston, Little Brown and Company: 1989).

Keohane, Robert O, "International Institutions: Two Approaches", *International Studies Quarterly*, 32 (December 1988): 379–396.

Keohane, Robert O, "Theory of World Politics: Structural Realism and Beyond", in Keohane, Robert O. (ed), *Neorealism and Its Critics* (New York, Columbia University Press: 1986): 158–203.

Keohane, Robert O, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton, Princeton University Press: 1984).

Keohane, Robert O. and Joseph S. Nye Jr., "Power and Interdependence in the Information Age", *Foreign Affairs* 77, 5 (September/October 1998): 81–94.

Kitchin, Rob, *Cyberspace: The World in the Wires* (Chichester, Wiley and Sons: 1998).

Kolet, Kristin. S. "Asymmetric Threats to the United States", *Comparative Strategy*, 20 (2001): 277–292.

Kopp, Carlo, "Information Warfare: A Fundamental Theorem of Infowar", *Systems – Enterprise Computing Monthly* (February 2000): 46–55.

Krasner, Stephen, *International Regimes* (Ithaca, Cornell University Press: 1983).

Kreml, Stefan, "Interview with John Arquilla: Be Prepared: Cyberwar is Coming – Or Maybe Not", *telepolis*, 13 March 2001.

Krepinevich, Andrew F., "Cavalry to Computers – The Patterns of Military Revolutions", *The National Interest*, 33 (Fall 1994): 30–42.

Krutskikh, Andrei, "Information Challenges to Security", *International Affairs*, 45, 2 (1999): 29–37

Larsen, Wayne A., *Serbian Information Operations During Operations Allied Force*, a Research Report Submitted to the Faculty of Air Command And Staff College Air University (Alabama, Maxwell Air Force Base: April 2000).

Libicki, Martin, "The Small and the Many", in: Arquilla, John and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, RAND: 1997): 191–216.

Libicki, Martin, *Illuminating Tomorrow's War*, Mc Nair Paper 61 (Washington, D.C., National Defense University: 1999).

Libicki, Martin, *Information Dominance*, Strategic Forum No. 132 (Washington, D.C., National Defense University: November 1997).

Libicki, Martin, *The Mesh and the Net. Speculations on Armed Conflict in an Age of Free Silicon*, McNair Paper 28 (Washington D.C., National Defense University: 1994).

Libicki, Martin, *What is Information Warfare?* (Washington D.C., National Defense University: 1995).

Loader, Brian D., “The Governance of Cyberspace: Politics, Technology, and Global Restructuring”, in: Loader, Brian D., *The Governance of Cyberspace* (London and New York, Routledge: 1997): 1–19.

Loader, Brian D., *The Governance of Cyberspace* (London and New York: Routledge: 1997).

Lonsdale, David J., “Information Power: Strategy, Geopolitics, and the Fifth Dimension”, *The Journal of Strategic Studies*, 22, 2/3 (June/September 1999).

Lynch, April, “Kosovo Being Called First Internet War”, San Francisco Chronicle, 15 April 1999.

Lyon, David, “Cyberspace Sociality. Controversies over Computer-Mediated Relationships”, in: Loader, Brian D., *The Governance of Cyberspace* (London and New York: Routledge: 1997): 23–37.

Mahnken, Thomas G, “War in the Information Age”, *Joint Force Quarterly*, 10 (Winter 1995/1996).

Metz, Steven, “Lessons from the Military Experience: The U.S. Military and the IR: The Pitfalls of Uneven Adaptation”, in: Copeland, Thomas E. (ed.), *The Information Revolution and National Security* (Carlisle Barracks, Strategic Studies Institute: August 2000).

Metz, Steven, “The Next Twist of the RMA”, *Parameters,* XXX, 3 (Autumn 2000): 40–53.

Metz, Steven, *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare* (Carlisle Barracks, Strategic Studies Institute: April 2000).

Minkwitz, Olivier and Georg Schöfbänker, “Neue Herausforderung für die Rüstungskontrolle”, *telepolis*, 31 May 2000.

Mitchell, Ronald and Thomas Bernauer, *Empirical Research on International Environmental Policy: Qualitative Case Studies*, Studien zur Politikwissenschaft Nr. 301 (Zürich, Institut für Politikwissenschaft Zürich: 1997).

Molander, R.C., A.S. Riddle, and P.A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, RAND: 1996).

Morse, Edward. L, *Modernization and the Transformation of International Relations* (New York, Basic Books: 1976).

Nance, Scott, “Networks, Robots Key to Future War*”, Defense Week,* 3 July 2000.

Nichiporuk, Brian and Carl H. Builder, "Societal Implications", in: Arquilla, John and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, RAND: 1997): 295–314.

Nye, Joseph S. Jr. and William A. Owens, "America's Information Edge", *Foreign Affairs* (March/April 1996): 20– 36.

Nye, Joseph S. Jr., "U.S. Security Policy: Challenges for the 21st Century", *USIA Electronic Journal*, 3, 3 (July 1998).

Nye, Joseph S. Jr., *Bound To Lead: The Changing Nature of American Power* (New York, Basic Books: 1990).

Office of the Secretary of Defense, *Report to Congress, Kosovo/Operation Allied Force After Action Review Report*, 31 January 2000.

Organski, A.F.K., *World Politics*, 2nd Edition (New York, Alfred A. Knopf: 1968).

Owens, William A., "The Emerging System of Systems", *Naval Institute Proceedings* 121, 5 (May 1995): 35–39.

Papp, Daniel S and David Alberts, "Preface: Technology and Change in Human Affairs", in: Alberts, David S., Daniel S. Papp (eds.), *The Information Age: An Anthology of Its Impacts and Consequences* (Washington D.C., National Defense University: 1997).

Papp, Daniel S and David S. Alberts, "The Impacts of the Information Age on International Actors and the International System", in: Alberts, David S. and Daniel S. Papp (eds.), *The Information Age: An Anthology of Its Impacts and Consequences* (Washington D.C., National Defense University: 1997).

Papp, Daniel S and David S. Alberts, "The Impacts of the Information Age on International Actors and the International System", in: Alberts, David S. and Daniel S. Papp (eds.), *The Information Age: An Anthology of Its Impacts and Consequences* (Washington D.C., National Defense University: 1997).

Papp, Daniel S, David S. Alberts, and Alissa Tuyahov, "Historical Impacts of Information Technologies: An Overview", in: Alberts, David S. and Daniel S. Papp (eds.), *The Information Age: An Anthology of Its Impacts and Consequences* (Washington D.C., National Defense University: 1997).

Porter, Alan L (ed.), *A Guidebook for Technology Assessment and Impact Analysis* (New York, North-Holland: 1980).

Pounder, Gary, “Opportunity Lost: Public Affairs, Information Operations, and the Air War against Serbia”, *Aerospace Power Journal*, XIV, 2 (Summer 2000): 56–77.

PR Newswire, “Hamre: Balkans Fighting Called ‚First Cyber War‘“, *PR Newswire*, 19 April 1999.

Reinicke, Wolfgang. H., “The Other World Wide Web: Global Public Policy Networks”. *Foreign Policy*, 117 (Winter 1999–2000): 44–56.

Reuters, “U.S. Military Grapples With Cyber Warfare Rules”, 8 November 1999.

Robinson, James, “Technology, Change, and the International Order”, in: Alberts, David S., Daniel S. Papp (eds.), *The Information Age: An Anthology of Its Impacts and Consequences* (Washington D.C., National Defense University: 1997).

Ronfeldt, David and John Arquilla, “What if There is a Revolution in Diplomatic Affairs?”, United States Institute of Peace, Released 25 February 1999, available online, URL http://www.usip.org/oc/vd/vdr/ronarqlSA99.html.

Rosecrance, Richard, *The Rise of the Virtual State. Wealth and Power in the Coming Century* (New York, Basic Books: 1999).

Rosenau, James (ed.), *Linkage Politics: Essays on the Convergence of National and International Systems* (New York, The Free Press: 1969).

Rosenau, James N., “Introduction: Political Science in a Shrinking World”, in: Rosenau, James (ed.), *Linkage Politics: Essays on the Convergence of National and International Systems* (New York, The Free Press: 1969): 1–17.

Rosenau, James N., *Turbulence in World Politics: A Theory of Change and Continuity* (Princeton, Princeton University Press: 1990).

Rosenau, James, “Global Affairs in an Epochal Transformation”, in: Henry, C. Ryan and Edward C. Peartree (eds.) *Information Revolution and International Security* (Washington D.C., Center for Strategic and International Studies Press: 1998): 33 –57.

Roszak, Theodore, *The Cult of Information: The Folklore of Computers and the True Art of Thinking* (Cambridge, Lutterworth Press: 1986).

Rothkopf, David J, “Cyberpolitik: The Changing Nature of Power in the Information Age.” *Journal of International Affairs* 51, 2 (Spring 1998): 325–360.

Rothkopf, David J., “The Disinformation Age”, *Foreign Policy*, 114 (Spring 1999): 83–96.

Ruggie, John Gerard, “Continuity and Transformation in the World Polity: Toward a Neorealist Synthesis”, *World Politics* 35, 2 (January 1983): 261–85.

Satchell, Michael, “Captain Dragan’s Serbian Cybercops. How Milosevic Took the Internet Battlefield”, *U.S. News*, 10 May 1999.

Scales, Robert H Jr., *Future Warfare* (Carlisle Barracks, Strategic Studies Institute: 1999).

Schleher, Curtis D., *Electronic Warfare in the Information Age* (Boston, Artech House: 1999).

Schwartau, Winn, *Information Warfare. Chaos on the Electronic Superhighway* (New York, Thunder‘s Mouth Press: 1994).

Schwartz, Edward, *NetActivism: How Citizens Use the Internet* (Sebastopol**,** Songline Studios: 1996).

Seminerio, Maria, “Infowar Part of NATO Arsenal?”, ZDNet, 25 March 1999.

Shapiro, Andrew L, “Think Again: The Internet”, *Foreign Policy* (Summer 1999): 14–27.

Shenk, D., *Data Smog: Surviving the Information Age* (San Francisco, Harper: 1997).

Sibilia, Riccardo, *Informationskriegsführung: eine schweizerische Sicht* (Zürich, Institut für militärische Sicherheitstechnik, ETH Zürich: 1997).

Singer, David J, Stuart Bremer and John Stuckey, “Capability Distribution, Uncertainty, and Major Power War, 1820–1965”, in: Russett, Bruce (ed.), *Peace, War, and Numbers* (Beverly Hills, Sage Publications: 1972): 21–27.

Snyder, Richard C., H.W. Bruck, and Burton Sapin, *Foreign Policy Decision Making: An Approach to the Study of International Politics* (New York, Free Press: 1962).

Solomon, Richard H, “The Information Revolution and International Conflict Management”, USIP Peaceworks, Keynote Address from the Virtual Diplomacy Conference, June 1997.

Spillmann, Kurt R., Andreas Wenger, Stephan Libiszewski, and Patrik Schedler, *Informationsgesellschaft und schweizerische Sicherheitspolitik*, Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung, No. 53

(Zürich, Forschungsstelle für Sicherheitspolitik und Konfliktanalyse: 1999).

Stewart, John F., "Intelligence Strategy for the 21st Century", *Military Review (*September/October 1995): 75–81.

Szafranski, Richard, "Neocortical Warfare? The Acme of Skill", in: Arquilla, John and David Ronfeldt (eds.), In: *Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, RAND: 1997): 395–416.

Taylor, Ros, "UK: Partisans Wage Virtual War", *The Guardian*, 22 April 1999.

The Benton Foundation, "Telecommunications and Democracy", in: Alberts, David S. and Daniel S. Papp (eds.), *The Information Age: An Anthology of Its Impacts and Consequences* (Washington D.C., National Defense University: 1997).

The Economist, "A Survey of Government and the Internet: The Next Revolution", *The Economist*, 24 June 2000.

The Economist, "NATO's Weapons. Are They Too Clever by Half? High Technology Against Serbia Has Yet to Prove Itself a Winner", *The Economist*, 1 May 1999.

Thomas, Timothy L., "Infosphere Threats", *Military Review*, LXXXIX, 5 (September/ October 1999): 46–51.

Thomas, Timothy L., "Kosovo and the Current Myth of Information Superiority", *Parameters* (Spring 2000): 13–29.

Thomas, Timothy, *Like Adding Wings to the Tiger: Chinese Information War Theory and Practice* (Fort Leavenworth, Foreign Military Studies Office: 2000).

Thomas, Timothy, *Russian Views on Information-Based Warfare* (Fort Leavenworth, Foreign Military Studies Office: 1996).

Thornton, Alinta, *Does Internet Create Democracy?*, Master Thesis, University of Technology (Sydney: October 1996), Online version, URL http: //www.wr.com.au/democracy/index.html.

Tilford, Earl H. Jr., *The Revolution in Military Affairs: Prospects and Cautions* (Carlisle Barracks, Strategic Studies Institute: 1995).

Toffler, Alvin and Heidi Toffler, *War and Anti-War* (New York, Warner Books: 1993).

Toffler, Alvin, *Third Wave* (New York, Bantam Books: 1980).

Chairman of the Joint Chiefs of Staff, *US Armed Forces, Joint Vision 2010* (Washington, D.C., U.S. Department of Defense: 1996).

Chairman of the Joint Chiefs of Staff, *US Armed Forces, Joint Vision 2020* (Washington, D.C., U.S. Department of Defense: 2000.)

Van Creveld, Martin, *Technology and War: From 2000 BC to the Present* (New York, Free Press: 1989).

Van Creveld, Martin, *The Transformation of War. The Most Radical Reinterpretation of Armed Conflict Since Clausewitz* (New York, Free Press: 1991).

Van Evera, Stephen, *Guide to Methods for Students of Political Science* (Ithaca and London, Cornell University Press: 1997).

Verton, Daniel, "Intelligence, Logistics Placed under Microscope", *Federal Computer Week*, 2 September 2000.

Verton, Daniel, "Report Sheds Light on NATO's High-Tech Problems in Kosovo", *Federal Computer Week*, 9 February 2000.

Viotti, Paul R. and Mark V. Kauppi, *International Relations Theory. Realism, Pluralism, Globalism, and Beyond,* 3rd Edition (Needham Heights, Prentice Hall: 1999).

Virilio, Paul, "Speed and Information: Cyberspace Alarm!", *Ctheory*, 18 March 1995

Virilio, Paul, *Information und Apokalypse. Die Strategie der Täuschung* (München, Hanser: 2000).

Vlahos, Michael, "Entering the Infosphere", *Journal of International Affairs*, 2 (Spring 1998): 497–525.

Waldrop, Mitchell M., "Is There an Information Revolution?", in: Henry, C. Ryan and Edward C. Peartree (eds.), *Information Revolution and International Security* (Washington, Center for Strategic and International Studies Press: 1998): 1–9.

Waller, Douglas, "Onward Cyber Soldiers", *Time Magazine*, 21 August 1995.

Waltz, Edward, *Information Warfare. Principles and Operations* (Boston, Artech House: 1998).

Waltz, Kenneth N., *Theory of International Politics* (Reading, Addision-Wesely: 1979).

Wasserman, S. and K. Faust, *Social Network Analysis: Methods and Applications* (Cambridge, Cambridge University Press: 1994).

Webster, Frank, "What Information Society?", in: Alberts, David S. and Daniel S. Papp (eds.), *The Information Age: An Anthology of Its Impacts and Consequences* (Washington D.C., National Defense University: 1997).

Webster, Frank, *Theories of the Information Society* (London, Routledge: 1995).

Wellman, Barry, Laura Garton and Caroline Haythornthwaite, "Studying Online Social Networks", *Journal of Computer-Mediated Communication*, 3, 1 (1997).

Williamson, Charles A., "Psychological Operations in the Information Age", in: Campen, Alan D. and Douglas H. Dearth (eds.*), Cyberwar 2.0: Myths, Mysteries and Reality* (Fairfax, AFCEA International Press: 1998): 179–190.

Wilson, Ernest J. III, *Globalization, Information Technology, and Conflict in the Second and Third World. A Critical Review of the Literature* (New York, Project on World Security, Rockefeller Brothers Fund: 1998), available online, URL http://www.rbf.org/pws/Wilson_Info_Tech.pdf.

Witol, Gregory, "International Relations in a Digital World", in: Campen, Alan D. and Douglas H. Dearth (eds.*), Cyberwar 2.0: Myths, Mysteries and Reality* (Fairfax, AFCEA International Press: 1998).

Wolfe, Frank, "Pentagon Analyzing Serb Attacks on DoD Web Sites", www.infowar.com, 22 June 1999.

Woods, Ngaire, "The Uses of Theory in the Study of International Relations", in: Woods, Ngaire (ed.), *Explaining International Relations since 1945* (Oxford, Oxford University Press: 1996).

Wriston, Walt, Bits, "Bytes and Diplomacy", *USIP Peaceworks*, Keynote Address from the Virtual Diplomacy Conference, June 1997.

Doctrine Publications

Army Publications:

Department of the Army, Army Vision 2010 (Washington D.C., Department of the Army: 13 November 1996).

Department of the Army, Information Operations, Field Manual No. 100–6 (Washington D.C., Department of the Army: 27 August 1996).

Joint Publications, Operations, Series 3–0:

(http://www.dtic.mil/doctrine/jel/operations.htm)

Joint Chiefs of Staff, JP 3–13, Joint Doctrine for Information Operations (Washington D.C., Department of Defense: 9 October 1998).

Joint Chiefs of Staff, JP 3–53, Doctrine for Joint Psychological Operations (Washington D.C., Department of Defense: 10 July 1996).

Joint Chiefs of Staff, JP 3–51, Joint Doctrine for Electronic Warfare (Washington D.C., Department of Defense: 7 April 2000).

Joint Chiefs of Staff, JP 3–13.1, Joint Doctrine for Command and Control Warfare (C2W) (Washington D.C., Department of Defense: 7 February 1996).

Joint Chiefs of Staff, JP 3–61, Doctrine for Public Affairs in Joint Operations (Washington D.C., Department of Defense: 14 May 1997).

Joint Publications, Joint Vision:

Chairman of the Joint Chiefs of Staff, *US Armed Forces, Joint Vision 2010* (Washington, D.C., U.S. Department of Defense: 1996).

Chairman of the Joint Chiefs of Staff, *US Armed Forces, Joint Vision 2020* (Washington, D.C., U.S. Department of Defense: 2000).

Air Force Doctrine Documents:

(http://www.doctrine.af.mil)

Department of the Air Force, Cornerstones of Information Warfare, circa 1995, http://www.af.mil/lib/corner.html.

Department of the Air Force, Air Force Doctrine Document 2–5 Information Operations, (Washington D.C., Department of the Air Force: August 1998).

Department of the Air Force, Air Force Doctrine Document 2–5 Information Operations, updated Version, (Washington D.C., Department of the Air Force: September 2000).

Department of the Air Force Air Force Doctrine Document 2–5.3, Psychological Operations, (Washington D.C., Department of the Air Force: February 1997).

Department of the Air Force Air Force Doctrine Document 2–5.4, Public Affairs Operations, (Washington D.C., Department of the Air Force: October 1999).

Primary Sources

Department of Defense, United States: News Archive, Press Transcripts, @ http://www.defenselink.mil/news/archive.html.

Joint Chiefs of Staff, *Joint Statement on the Kosovo After Action Review* (initial assessment), presented by Secretary of Defense William S. Cohen and Gen. Henry H. Shelton, Chairman of the Joint Chiefs of Staff, before the Senate Armed Services Committee, 14 October 1999.

Ministry of Defense, United Kingdom, Kosovo Background and Resources, @ http://www.kosovo.mod.uk/.

NATO, Operation Allied Force Video Material: http://www.nato.int/kosovo/video.htm.

NATO, Operation Allied Force: Operational Updated, Press Briefings, Morning Briefings, Maps & Aerial Views, @ http://www.nato.int/kosovo/all-frce.htm.

Office of the Secretary of Defense, *Report to Congress, Kosovo/Operation Allied Force After Action Review Report*, 31 January 2000.

In der gleichen Publikationsreihe sind erschienen:

Nr. 1 Kurt R. Spillmann: Konfliktforschung und Friedenssicherung (1987) **vergriffen**

Nr. 2 Kurt R. Spillmann: Beyond Soldiers and Arms: The Swiss Model of Comprehensive Security Policy (1987)

Nr. 3 Kurt R. Spillmann: Die Kubakrise von 1962: geschichtliche, politische und strategische Hintergründe (1987) **vergriffen**

Nr. 4 Beat Näf / Kurt R. Spillmann: Die ETH-Arbeitstagung zur schweizerischen Sicherheitspolitik vom 29. Juni 1987 – Bericht und Auswertung (1987)

Nr.5 Beat Näf / Kurt R. Spillmann: Die ETH-Arbeitstagung zur schweizerischen Sicherheitspolitik vom 7. Dezember 1987 – Bericht und Auswertung (1988)

Nr. 6 Jacques Freymond: La menace et son évolution dans les domaines militaires et civils dans l'optique de la recherche scientifique et universitaire (1988)

Nr. 7 Christian Kind: Extended Deterrence – Amerikas Nukleargarantie für Europa (1989)

Nr. 8 Franz Martin Aebi: Der Weg zum Weiterleben – Morphologische Studie zu einer zeitgemässen Planung einer Strategie der staatlichen und gesellschaftlichen Selbstbehauptung (1989)

Nr. 9 Madeleine Hösli / Kurt R. Spillmann: Demographie und Sicherheitspolitik: Nationale Aspekte – Bericht und Auswertung der ETH-Arbeitstagung vom 5. Dezember 1988 (1989)

Nr. 10 Richard D. Challener: John Foster Dulles: The Certainty / Uncertainty Principle (1989)

Nr. 11 Dominique Wisler: Vers une nouvelle politique de sécurité (1989) **vergriffen**

Nr. 12 Kurt R. Spillmann und Kati Spillmann: Feindbilder: Entstehung, Funktion und Möglichkeiten ihres Abbaus (1989)

Nr. 13 Madeleine Hösli / Kurt R. Spillmann: Demographie und Sicherheitspolitik: Rückwirkungen internationaler Entwicklungen auf die Schweiz – Bericht und Auswertung der ETH-Arbeitstagung vom 8. Juni 1989 (1989)

Nr. 14 Fred Tanner: Die Schweiz und Rüstungskontrolle: Grenzen und Möglichkeiten eines Kleinstaates (1990)

Nr. 15 Jacques Hürlimann / Kurt R. Spillmann: Der Bericht 90 zur schweizerischen Sicherheitspolitik im Urteil ausländischer Expertinnen und Experten – Bericht und Auswertung der ETH-Arbeitstagung vom 6. Dez. 1990 (1991)

Nr. 16 Urs Roemer: Die Strategie der „Flexible Response“ und die Formulierung der amerikanischen Vietnampolitik unter Präsident Kennedy (1991)

Nr. 17 Michael Fajnor: Die europäische Integration und ihre sicherheitspolitischen Folgen für die Schweiz (1991)

Nr. 18 Christof Buri / Karl W. Haltiner / Kurt R. Spillmann: Sicherheit 1991 – Ergebnisse einer Repräsentativbefragung (1991)

Nr. 19 Andreas Wenger: Kontinuität und Wandel in der amerikanischen Nuklearstrategie – Präsident Eisenhowers Strategie der massiven Vergeltung und die nuklearstrategische Neuevaluation der Administration Kennedy (1991)

Nr. 20 Kurt R. Spillmann (Hrsg.): Zeitgeschichtliche Hintergründe aktueller Konflikte I – Vorlesung für Hörer aller Abteilungen – Sommersemester 1991 (1991) **vergriffen**

Nr. 21 Stephan Kux: Decline and Reemergence of Soviet Federalism (1991) **vergriffen**

Nr. 22 Kurt R. Spillmann (Hrsg.): Europäische Integration und Schweizerische Sicherheitspolitik – Bericht und Auswertung der ETH-Arbeitstagung vom 25./26. Oktober 1991 (1992)

Nr. 23 Anton Bebler: The Yugoslav Crisis and the “Yugoslav People’s Army” (1992) **vergriffen**

Nr. 24 Sabina Ann Fischer: Namibia Becomes Independent – The U.S. contribution to regional peace (1992)

Nr. 25 Dominique Wisler: La violence politique en Suisse et les mouvements sociaux: 1969–1990 (1992)

Nr. 26 Mauro Mantovani: Stand und Perspektiven der Sicherheitspolitik in Europa (1992)

Nr. 27 Kurt R. Spillmann (Hrsg.): Zeitgeschichtliche Hintergründe aktueller Konflikte II – Vorlesung für Hörer aller Abteilungen – Sommersemester 1992 (1992)

Nr. 28 Kurt R. Spillmann und Mauro Mantovani (Hrsg.): Die sicherheitspolitische Integration in Europa als Herausforderung für die Schweiz – Bericht und Auswertung der ETH-Arbeitstagung vom 26. Oktober 1992 (1993)

Nr. 29 Günther Bächler: Bosnien-Herzegowina – Friedliche Streitbeilegung zwischen Realität und konkreter Utopie (1993) **vergriffen**

Nr. 30 Ilja Kremer: Die Sowjetunion und Russland nach 1985: Von der Oktoberrevolution zur Oktoberkrise (1993)

Nr. 31 Kurt R. Spillmann (Hrsg.): Zeitgeschichtliche Hintergründe aktueller Konflikte III – Vorlesung für Hörer aller Abteilungen – Sommersemester 1993 (1994) **vergriffen**

Nr. 32 Karl W. Haltiner / Kurt R. Spillmann: Öffnung oder Isolation der Schweiz? Aussen- und sicherheitspolitische Meinungsbildung im Trend (1994)

Nr. 33 Mauro Mantovani: Nato-Mitglied Schweiz? Voraussetzungen und Folgen einer sicherheitspolitischen Integration der Schweiz (1994) **vergriffen**

Nr. 34 Michael Fajnor: Multilaterale Anstrengungen zur Kontrolle konventioneller Rüstungstransfers und die Schweiz (1994)

Nr. 35 Kurt R. Spillmann (Hrsg.): Zeitgeschichtliche Hintergründe aktueller Konflikte IV – Vorlesung für Hörer aller Abteilungen – Sommersemester 1994 (1994)

Nr. 36 Andreas Wenger / Jeronim Perovic: Das schweizerische Engagement im ehemaligen Jugoslawien (1995)

Nr. 37 Kurt R. Spillmann (Hrsg.): Zeitgeschichtliche Hintergründe aktueller Konflikte V – Vorlesung für Hörer aller Abteilungen – Sommersemester 1995 (1995)

Nr. 38 Karl W. Haltiner / Luca Bertossa / Kurt R. Spillmann: Internationale Kooperationsbereitschaft und Neutralität: Aussen- und sicherheitspolitische Meinungsbildung im Trend (1996)

Nr. 39 Ulrich Gerster / Regine Helbling: Krieg und Frieden in der bildenden Kunst (1996)

Ulrich Gerster / Regine Helbling: Krieg und Frieden in der bildenden Kunst (1996) (Bildteil)

Nr. 40 Christoph Breitenmoser: Sicherheit für Europa: Die KSZE-Politik der Schweiz bis zur Unterzeichnung der Helsinki-Schlussakte zwischen Skepsis und aktivem Engagement (1996)

Nr. 41 Laurent F. Carrel / Otto Pick / Stefan Sarvas / Andreas Schaer / Stanislav Stach: Demokratische und zivile Kontrolle von Sicherheitspolitik und Streitkräften (1997)

Nr. 42 Karl W. Haltiner / Luca Bertossa / Kurt R. Spillmann: Sicherheit '97 (1997)

Nr. 43 Andreas Wenger / Jeronim Perovic: Russland und die Osterweiterung der Nato: Herausforderung für die russische Aussen- und Sicherheitspolitik (1997)

Nr. 44 Kurt R. Spillmann (Hrsg.): Zeitgeschichtliche Hintergründe aktueller Konflikte VI – Vorlesung für Hörer aller Abteilungen – Sommersemester 1997 (1997)

Nr. 45 Kurt R. Spillmann und Hans Künzi (Hrsg.): Karl Schmid als strategischer Denker: Beurteilungen aus historischer Perspektive. Bericht und Auswertung der Tagung vom 1. Juli 1997 (1997)

Nr. 46 Derek Müller: Die Aussen- und Sicherheitspolitik der Ukraine seit 1990/91: Herausforderungen, Leistungen und Perspektiven (1998)

Nr. 47 Andreas Wenger und Jeronim Perovic: Russland zwischen Zerfall und Grossmachtanspruch: Herausforderungen der Regionalisierung (1998)

Nr. 48 Andreas Wenger, Christoph Breitenmoser, Patrick Lehmann: Die Nato-Partnerschaft für den Frieden im Wandel: Entwicklung und Zukunft eines kooperativen Sicherheitsinstrumentes (1998)

Nr. 49 Christof Münger: Ich bin ein West-Berliner: Der Wandel der amerikanischen Berlinpolitik während der Präsidentschaft John F. Kennedys (1999)

Nr. 50 Christian Nünlist: Kennedys rechte Hand: McGeorge Bundys Einfluss als Nationaler Sicherheitsberater auf die amerikanische Aussenpolitik 1961–63 (1999)

Nr. 51 David C. Atwood / Shahram Chubin / Pál Dunay / Jozef Goldblat / Martin Schütz / Heiner Staub: Arms Control and Disarmament: Revised version of papers Papers Presented at the 3rd International Security Forum Zurich, 19–21 October 1998 (1999)

Nr. 52 Andreas Wenger: Herausforderung Sicherheitspolitik: Europas Suche nach Stabilität (1999)

Nr. 53 Kurt R. Spillmann / Andreas Wenger / Stephan Libiszewski / Patrik Schedler: Informationsgesellschaft und schweizerische Sicherheitspolitik (1999)

Nr. 54 Kurt R. Spillmann / Andreas Wenger (Hrsg.): Zeitgeschichtliche Hintergründe aktueller Konflikte VII – Vortragsreihe an der ETH-Zürich – Sommersemester 1999 (1999)

Nr. 55 Daniel Möckli: Neutralität, Solidarität, Sonderfall: Die Konzeptionierung der schweizerischen Aussenpolitik der Nachkriegszeit, 1943–1947 (2000)

Nr. 56 Andreas Wenger / Jeremi Suri: The Nuclear Revolution, Social Dissent, and the Evolution of Détente: Patterns of Interaction, 1957–74 (2000)

Nr. 57 Jon A. Fanzun / Patrick Lehmann: Die Schweiz und die Welt: Aussen- und sicherheitspolitische Beiträge der Schweiz zu Frieden, Sicherheit und Stabilität, 1945–2000 (2000)

Nr. 58 Vojtech Mastny: Learning from the Enemy: NATO as a Model for the Warsaw Pact (2001)

Nr. 59 Daniel Maurer: Europäische Sicherheit: Konfliktmanagement am Beispiel „Ex-Jugoslawien“ (2001)

Nr. 60 Kurt R. Spillmann / Andreas Wenger (Hrsg.): Zeitgeschichtliche Hintergründe aktueller Konflikte VIII – Vortragsreihe an der ETH-Zürich – Sommersemester 2001 (2001)

Nr. 61 Fred Tanner (ed.) with the assistance of Joanna Schemm: The European Union as a Security Actor in the Mediterranean. ESDP, Soft Power and Peacemaking in Euro-Mediterranean Relations (2001)

Nr. 62 Judith Niederberger: “Making the Difference between Mutual Destruction and Survival”. Amerikanische Rüstungskontrollpolitik unter Dwight D. Eisenhower, 1953–1960 (2001)

Nr. 63 Daniel Trachsler: Neutral zwischen Ost und West? Infragestellung und Konsolidierung der schweizerischen Neutralitätspolitik durch den Beginn des Kalten Krieges, 1947–1952 (2002)

Nr. 64 Myriam Dunn: Information Age Conflicts. A Study of the Information Revolution and a Changing Operating Environment (2002)

Nr. 65 Kurt R. Spillmann / Andreas Wenger (Hrsg.): Zeitgeschichtliche Hintergründe aktueller Konflikte IX – Vortragsreihe an der ETH-Zürich – Sommersemester 2002 (2002)

Nr. 66 Kurt R. Spillmann: Von Krieg und Frieden – Of War and Peace. Abschiedsvorlesung – Farewell Address, ETH Zürich, 3. Juli 2002 (2002)

Eine Gesamtübersicht über alle bisher erschienenen „Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung“ ist einsehbar im Internet unter www.fsk.ethz.ch.

Die Beiträge können bei der Forschungsstelle für Sicherheitspolitik und Konfliktanalyse, ETH-Zentrum SEI, CH-8092 Zürich, Tel. 01/632 40 25, Fax: 01/632 19 41, bezogen werden. Es ist auch möglich, die Bestellung online auszuführen unter www.fsk.ethz.ch/publ/order_publications.htm.