Georg Schöfbänker

From PLATO to NATO[1]

Epistemology, Knowledge and Fantasies of cyber- and Information War.

In Search of New Threats, Threads and Cognitive Patterns after the End of the Cold War.

Introduction

Since the end of the Cold War the Western community has fought one "real classical" war with thousands of dead, though it was not a nation-state war. In terms of international law it was a "police-action" by members of the United Nations led by the US against Iraq which had invaded Kuwait, committed crimes against the civilian population and fired missiles into Israel. The air-war campaign started on Jan. 17th 1991 and lasted nonstop until the ground-offensive started on Feb. 23rd. All together the air-war against Iraq took some five weeks. The ground-campaign only lasted for four days, until Feb. 27th, when a cease-fire was announced. Kuwait was liberated from Iraqi troops, Iraq itself remained politically untouched, dictator Saddam Hussein remaining in power. Iraqi nuclear weapons and other weapons of mass destruction projects were revealed in full glory, projects which had not been detected by signals intelligence (SIGINT), e.g. by satellite reconnaissance before.

Shortly before this text was finished, India and Pakistan almost simultaneously tested twelve nuclear warheads at different development stages, including (in the case of India) a true thermonuclear device. A nuclear arms race in South East Asia is likely if it is not contained by détente and preventive diplomacy. India announced its intention to use superfast computing resources for the further simulation of nuclear tests, as do the formerly five declared nuclear powers.

Waging war against Iraq has become a paradigm in assessing new conflict scenarios and how information technology (IT) might shape future battle management. In the meantime, especially in the US governmental and military bodies, different task-force study-groups, policy-advisers in strategic affairs, security advisers to the President, the military-industrial-strategic-complex in Washington DC and related think-tanks are proliferating neologisms and acronyms, such as info(rmation-)war(fare), cyberwar(fare), netwar(fare), intelligence based warfare (IBW), electronic warfare (EW), revolution in military affairs (RMA), revolution in strategic affairs (RSA), C2W (command and control warfare), C3I (command, control, communication and intelligence, C4I (command, control, communication, computation and intelligence), C4I2 (command, control, communication, computation, intelligence and interoperability), HIC (high intensity conflicts), LIC (low intensity conflicts), OOTW (operations other than war) and so forth.

The mere fact that the discussion of these topics left the expert circles of the Pentagon and its related organizations and found a broader audience in the main US foreign-policy journals (e.g. *Foreign Affairs*) is a reliable indicator that the debate is already, or will become, a *strategic foreign policy issue* of the US and in addition, that it will come to Europe.

It is certainly not only a debate within the military elites of the US. The Swedish defense community also established a kind of *task-force* on information-war, RMA is a main driving force in reshaping NATO's military out-of-area capabilities and firepower and Russia is concerned by a perhaps not identifiable border-line between an infowar-attack and a

permanent cultural penetration of what are believed to be valuable assets in cultural, psychological and national identities and cognitive patterns.

Also, in the same time-period since the end of the Gulf war, the half-life-time of foreign policy theories, hypotheses and explanations for the post Cold War world permanently interacting on a higher scale and at a higher speed, for the system of international relations, for the interacting patterns between state and non-state actors, for *new conflict modes* and ways of resolving them, for a theory of the nature of *supremacy* and *power* in a postmodern international environment, for the *nature of state-behavior* in the international system, for the future of war-like conflicts, for *ethnicity, identity* and their impact on conflict-development– all this decreased dramatically.

A great many *trendy theories* emerged at the end of the 80s to explain the likely future of the international system, of supremacy and power: "Imperial overstretch" was an attempt to describe the assumed loss of US influence in world affairs. In 1990 President George Bush announced a "new world order", based upon the system of the United Nations, the rule of international law and global democratization of authoritarian regimes. At the final diplomatic act settling the Cold War in Europe, the Paris CSCE-Conference, 19th-21st Nov. 1990, the security of all participating nation-states in CSCE-Europe was described as "indivisible" and "…the security of each of our countries will inseparably be interconnected with the Conference of Security and Cooperation in Europe."

Shortly afterwards, theories about the "end of history" in international relations were propounded, to be replaced by Huntington in his 1993 article in *Foreign Affairs*, claiming a *Kulturkampf* (clash of civilizations) to be the most likely pattern of interstate and intrastate conflicts of the future and therefore US leadership and supremacy would be needed. The concept of a *Kulturkampf* between fundamentalist oriented rouge-states, the most hated enemy-images of US foreign policy, fits very well into postmodern subconventional terrorist threat-perceptions, using WMD.

In the mid 90s the emerging theories and concepts of cyber- and infowar started influencing the US foreign policy mainstream. From the point of a serious independent analysis it is not so important to investigate in detail how cyber- and infowar became a strategic issue, it is much more meaningful to investigate how it might become a self-fulfilling-prophecy in US terms. The question is, how do you hype a hype? How can you be a step ahead, using the rules of the game? The first hype might be the construction of information warfare as the central security thread & threat of the 21st century. The second hype might be using the US supremacy in worldwide information distribution presence to proliferate that hype and make it self-fulfilling and plausible.

But Info- and cyberwar are just at the brink of becoming *Realpolitik*. The most influential shift in political and military terms in the 1990s in the Northern hemisphere is the collapse of the bi-polar Cold War and the *eXlargement* of NATO eastwards. Johan Galtung has called this project a type of *"megalomaniac Realpolitik"*. NATO will certainly expand eastwards, will expand its territory of potential interventions, peace-keeping, peace-making, peace-enforcement and "out-of-area-missions" and will be the Euro-Atlantic *leitmotiv* of the 21st century. The Euro- and North-Atlantic nation community will play the most decisive role in terms of military, technological and economic power on the geostrategic and geopolitical stage at the beginning of the 21st century. This seems certain. An assessment of the impacts of cyber-, info- and netwar as (geo-)political or military concepts should be made against this background. The most central questions concerning these issues are:

—How will the future of the international system look like?

— What will the future of war be? Will it be a conflict between nation-states in the "Clausewitz style" of the "continuation of politics by other means"?

— What will the future nature of *reasons for conflict* be? Will there be conflicts about ethnicity and in search for national identity, might there be some clashes along the conflict lines of a *Kulturkampf* between the Western Christian, the orthodox Christian, and the Islamic worlds?

— Will future violent conflicts mainly be of a intrastate nature, such as the recent examples in former Yugoslavia, Afghanistan, Cambodia, Rwanda, Somalia, or the current Kosovo problem?

— Who will act in these types of violent future conflicts? The only remaining super power, the US, medium powers, or subnational groups following *national-ethnic patterns*, clans, warlord regimes or criminal and violent gangs, armed with light and medium weapons, sufficient to evoke a genocide of a Bosnian or Rwandan type? Or assemblies of ad-hoc and case by case coalitions of international organizations, such as the UN, the OSCE or military alliances, such as NATO?

To put it frankly: There are no easy or likely answers to these questions. And if there were, they would risk having a very short theoretical prognostic range. In addition we have to ask if the concepts of cyber-, info- and netwars are *bottom-up* or *topside-down* approaches.

A Confusing Set of Definitions–Or What We are Talking About

In the leading US literature about political or military affairs cyberwar, infowar or netwar are used as overlapping synonyms.

Cyberwar

"Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to 'know' itself.[2]

As Arqilla & Ronfeldt's article "Cyberwar is coming" is reprinted in this publication, we are able to briefly mention their definitions here without quoting them extensively. For them, cyberwar is technology based within and outside the battlefield: "It means turning the 'balance of information and knowledge' in one's favor, especially if the balance of forces is not."

"As an innovation in warfare, we anticipate that cyberwar may be to the 21st century what *blitzkrieg* was to the 20th century. […] In a deeper sense, cyberwar signifies a tranformation in the nature of war."[3]

Netwar

"Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt or damage what a target population 'knows' or thinks it knows about itself and the world around it." In other words, netwar represents a new entry on the spectrum of conflict that spans economic, political, and social, as well as military forms of 'war.' Like other forms on this spectrum, netwars would be largely non-military, but they could have dimensions that overlap into military war. […] Netwars will take various forms. Some may occur between the governments of rival nation-states. […] Other kinds of netwar may arise between governments and nonstate actors.[4]

Or to the contrary they may be waged against the policies of specific governments by advocacy groups and movements–e.g. regarding environmental, human-rights or religious issues. […]

Most netwars will probably be non-violent […]

Some netwars will involve military issues. Candidate issue areas include nuclear proliferation, drug smuggling and antiterrorism[…].[5]

Netwars are not real wars, traditionally defined. But netwar might be developed into an instrument for trying, early on, to prevent a real war from arising."[6]

But they give just another definition of what the relationship between cyberwar and netwar may look like: "What we term *cyberwar* will be an ever more important entry at the military end […] *Netwar* will figure increasingly at the societal end […]".[7] And then: "The term *'netwar'* denotes an emerging mode of conflict (and crime) […] short of war, in which the protagonists use–indeed, depend on using–network forms of organization, doctrine, strategy, and communication."[8]

And finally: " In some cases, identities and loyalities may shift from the nation-state to the transnational level of a '*global civil society*'"[9] (emphasis added)

Further on, Arquilla/Ronfeldt[10] discuss "network principles" as a pure form of societal organization beside all technical aspects and conclude "[…] netwar is not just about new technologies."

Infowar

Arquilla/Ronfeldt refuse to use the term "infowar"[11] as being "too broad and too narrow to be appropriate". In contrast to this position the top US military authorities use a different language in explaining the concept of infowar. Both the *Joint Vision 2010*, and the *Joint Doctrine for Command and Control Warfare* (1996), unclassified doctrinal documents released by the *Joint Chiefs of Staff*, define information war(fare) explicitly and implicitly, whereas, *Joint Vision 2010* doesn't mention a definition of IW and points mainly to the military implications of the information age,

"We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information superiority will *require both offensive and defensive information warfare* (IW). Offensive information warfare will degrade or exploit an adversary's collection or use of information. It will include both traditional methods, such as a precision attack to destroy an adversary's command and control capability, as well as nontraditional methods such as electronic intrusion into an information and control network to convince, confuse, or deceive enemy military decision makers.

There should be no misunderstanding that our effort to achieve and maintain information superiority will also invite resourceful enemy attacks on our information systems. *Defensive information* warfare to protect our ability to conduct information operations will be one of our biggest challenges in the period ahead. Traditional defensive IW operations include physical security measures and encryption. Nontraditional actions will range from antivirus protection to innovative methods of secure data transmission. In addition, increased strategic level programs will be required in this critical area."[12]

The *Joint Doctrine for Command and Control Warfare* gives an explicit definition of IW:

"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."[13]

In a broader sense *Joint Pub 3-13.1* also includes psychological operations (PSYOP), within the concept of IW and the use of the global information infrastructure (GII). In this document, IW is more comprehensively defined, by non-technical, non-military means, too. The following tables may provide some semantic templates for discussing the US concepts:

Arquilla/Ronfeldt	Cyberwar	Netwar	Infowar
conflict level	high	medium - high	
conflict reasons	not discussed	not discussed	
actors	nation-state	nation-state; societies; rouge-states; military, paramilitary; "terrorist"; NGOs; "global civil society"	
threat-perception	alarmist	alarmist	
sub-concepts	battlefield, increased lethality, RMA;	propaganda, psychological warfare, media control, "reflexive control" *Kulturkampf;*	
deep impacts	transformation in the nature of war	transformation in the nature of propaganda and psychological warfare	
channels / means	military and civil command and communication systems	computer-networks; internet; all media channels	

Joint Pub 3-13.1[14] Joint Vision 2010	Infowar. Almost no discriminations to applications other than military are made.
conflict level	high; hot and cold wars
conflict reasons	not discussed
actors	nation-state; military
foreign policy design	"Power projection, enabled by overseas presence, will likely remain the fundamental strategic concept of our future force"(*Joint Vison 2010*, 4)
threat-perception	alarmist
sub-concepts	"dominant battlespace awareness"; increased capability to kill; RMA; directed energy weapons (lasers); C2 warfare: "C2W is an application of IW in military operations and is a subset of IW."(*Joint Vison 2010*, I-4)
deep impacts	complete transformation in the waging of conventional military operations
channels / means	RMA

In *What is Information Warfare?*[15] Libicki has given a very comprehensive set of definitions including the techno-military-battlefield aspects, as well as the cultural aspects. We should like to quote these definitions here completely, in order to be able discussing the full range of impacts:

Form	Subtype	Is It New?	Effectiveness
C2W	Antihead	Command systems, rather than commanders, are the target.	New technologies of dispersion and replication suggest that tomorrow's command centers can be protected.
	Antineck	Hard wired communication links matter.	New techniques (e.g., redundancy, efficient error encoding) permit operations under reduced bitflows.
IEW		The cheaper the more can be thrown into a system that looks for targets.	The United States will build the first system of sensing systems, but stealth aside, pays too little attention to hiding.
EW	Antiradar	Around since WW II.	Dispersed generators and collectors will survive attack better than monolithic systems.
	Anticomms	Around since WW II.	Spread spectrum, frequency hopping and directional antennas all suggest communications will get through.
	Cryptography	Digital code making is now easy.	New code making technologies (DES, PKE) favor code makers over code breakers.
Psychological Warfare	Antiwill	No.	Propaganda must adapt first to CNN than to Ma-TV.
	Antitroop	No. DBS and Ma-TV.	Propaganda techniques must adapt to.
	Anti commander	No.	The basic calculus of deception will still be difficult.
	Kulturkampf	Old history.	Clash of civilisations?
Hacker Warfare	Yes.		All societies are becoming potentially more vulnerable but good home keeping can secure systems.
Economic Information Warfare	Economic	Yes.	Very few countries are yet that dependent on high bandwidth information flows.
	Techno-Imperialism	Since the 1970s.	Trade and war involve competition, but trade is not war.
Cyber-Warfare	Info-Terrorism	Dirty linen is dirty linen whether paper or computer files.	The threat may be a good reason for tough privacy laws.
	Semantic	Yes.	Too soon to tell.
	Simula-warfare	Approaching virtual reality.	If both sides are civilised enough to simulate warfare, why would they fight at all?
	Gibson-warfare	Yes.	The stuff of science fiction.

From Software to 'Soft Power'- Or in Search of New Threats?

"I'm running out of demons. I'm down to Kim Il Sung and Castro."

Chairman of the Joint Chiefs of staff, Collin Powell, 1991 (after the Gulf war), before the US Congress[16]

Yet, it is not clear what was the hen, and what the egg. Did the lack of real threats after the end of the Cold War lead to that kind of cyber- and infowar enthusiasm we now envisage as the driving force in Pentagon circles? Or was it the other way round, as Friedrich Kittler[17] has put it, that perhaps the *computer industry as a belligerent gang and camarilla* is preparing its last and final (un-?)friendly take-over, the Pentagon itself? Compared to the sales for military hardware (1 aircraft carrier 100 billion US-$, 1 hunting submarine 10 billion US-$, 1 B2 stealth strategic bomber 1 billion US-$) software and communication infrastructure are relatively cheap. But the rapid and aggressive digitalization of the armed forces of the US and the preparation for all likely and unlikely cyber- and infowar scenarios give a tremendous boost for the whole communication and computer-business. And we must not forget the strategic computing initiatives with the goal of building under DoE contracts the fastest super computers by 2004 in the 30-100 teraflop range.[18]

"The transformation of U.S. military forces goes well beyond gaining information superiority and developing new technologies. Through a wide variety of analyses, wargames, studies, experiments, and exercises, the Department is systematically and aggressively investigating new operational concepts, doctrines, and organizational approaches that will enable U.S. forces to maintain full spectrum dominance of the battlespace well into the 21st century"[19]

Theories about arms races discriminate between two fundamental explanations or a combination of both. Simplifying, one theory explains arms races with an action-reaction pattern in regard to potential adversaries. This action-reaction-system finds its prerequisites and its final explanation and justification in the system-inherent production of mutual threat perceptions. The theoretical answer in the Cold War was mutually assured destruction (MAD) by nuclear weapons. In a strictly epistemological interpretation of the theorem that states arm because other states arm as well and may pose a threat to national security (neo-realistic approach), this may not be proved wrong; instead, it is tautological. It was not the military, but politicians that cut off this pathological cycle of each others´ misperceptions by confidence-building measures.

Another approach tries to explain armament efforts by lobby-interests, by the inertia of bureaucracy and the dynamics of the scientific-industrial-military complex, a danger to a democratic nation, as former US. President Eisenhower warned about in his final speech before retirement in 1961.

However, a third and new set of explanations seems necessary to explain how and why an information-war arms race might be imminent, and it has to go back to Clausewitz.

Most scholars engaged in the theory of international relations and in peace research agree that a nation-state war between democracies in the sense of bloody fighting over territory, resources and other assets is very unlikely. These findings are also shared by "cyber-theorists", e.g. the Tofflers who stated:

"The world, thus, is entering into a global order–or disorder, as the case may be–that is post-Westphalian, and post-Clausewitzian. It is something new. In a dialectical sense, it bears some resemblance to the pre-Westphalian order of diverse kinds of politics, but it involves a much higher order of complexity among actors, and, above all, it changes at hyper-speed."[20]

There are three plausible assumptions that may mean that western-style democracies won't fight wars against each other:

a) They are able to settle their conflicts by other than military means.

b) Globalization leads to such an irreversible dense interdependence as to avoid any "real‘ military conflict.

c) The "third wave" or the "third industrial revolution" is taking place right now and transforming the industrial nation-state into a global information-age society, where more and more goods and services are traded and sold within the global information infrastructure. (Although emerging technologies are seen as a prime force of change, there is an alternative point of view provided by the Schumpeterian tradition in economics. According to this view, technology, institutions, and culture, values and perceptions interact in more complex, unpredictable ways.)

So, Clausewitz will perhaps come back, not through the "industrial age front door", but through the "information age, infowar back door", even among western-style democracies as infowar is being defined by elites as "the "continuation of politics by other means".

If one looks at the above templates, psychological warfare, *Kulturkampf*, techno-imperialism and info-terrorism may be the most probable candidates on the *non-bloody* battlespace of infowar[21], or–as the Russians call it: "information psychological struggle", or the Chinese: "people's information warfare".

From an US American point of view Joseph Nye & William Owen have described this approach as a geopolitical tool and not only as a military asset in an 1996 article in *Foreign Affairs,* the *Zeitgeist-Zentralorgan* of US foreign policy thinking.

"Knowledge, more than ever before, is power. The one country that can best lead the information revolution will be more powerfull than any other. […] The information edge is equally important as a force multiplier of American diplomacy, including "soft power'–the attraction of American democracy and free markets"[22]

whereas "soft power"is defined as

"the ability to achieve desired outcomes in international affairs 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."[23]

After mentioning all "advantages" of American popular culture[24] and world wide information dominance, Nye & Owen conclude:

"In truth, the 21st century, not the twenties, will turn out to be the period of America's greatest preeminence. Information is the new coin of the international realm, and the United States is better positioned than any other country to multiply the potency of its hard and soft power resources through information."[25]

This view is widely shared. The Tofflers speak of "media howitzers' of the US (Hollywood, CNN) that nobody else has[26]. Panarin[27], a Russian Academician and governmental expert on info-war dates back the concept of info-war as an US foreign policy strategy to the era of the "Hollywood-presidency" of Ronald Reagan and the SDI-project, after having identified four components of US national security and national interests strategy: diplomatic, economic, military and information.

What has been elegantly formulated in diplomatic language (information superiority, "soft power") has been put bluntly during the last two years in the main US military and political doctrine papers[28], dealing with the structure, the shape and the mission of the US armed forces in the 21st century: The *unconditional will* for political and military world-supremacy, -hegemony, -dominance and -domination (e.g., the metaphor "full spectrum dominance" is used in a twofold way: as the domination of the full electromagnetic spectrum for reconnaissance, surveillance, blinding, jamming and intercepting and as a full dominance for "power projection" in the "national interest") by (not only, but increasingly importantly) cyberwar means, certainly in a defensive, but also in an offensive way. Just to give some examples, along and beside the "cyber-debate":

— The quadrennial defense review of May 1997 to the US congress[29], as well as Joint Vision 2010, still demand the capability to "fight and win" two large conventional simultaneously waged wars in (e.g.) Persian Gulf and Asian theaters.

— The QDR insists on keeping 12 aircraft carrier battle groups operational, whereas the IISS's *Military Balance 1997/98*[30] counts one (not operational) Russian, two French, three British and one Indian in the rest of the world.

— The US is the only country still having deployed about 150 nuclear weapons–free falling bombs of the type B-61 -, outside its territory in seven European NATO countries, Belgium, Germany, Greece, Italy, Netherlands, Turkey, United Kingdom, to be operated by US and NATO forces. NATO countries–including the US–recently condemned India's and Pakistan's nuclear tests, but insist, at least in June 1998, "that NATO's nuclear forces […] continue to *play a unique and essential* role in Alliance strategy."[31] (emphasis added).

— The US nuclear arsenal is within a multi million US $ upgrade which will enable it immediately to shift among a large number of contingencies all over the world. Two days after the U.S. Joint Chiefs of Staffs released their *Joint Doctrine for Command and Control Warfare (C2W)*[32], the *Doctrine for Joint Theater Nuclear Operations*[33] was put into force on 9th Feb 1996. Later on, in November 1997, President Clinton issued a highly classified Presidential Decision Directive (PDD-60) with new guidlelines about the targeting of nuclear weapons. Information from this classified directive (Kristensen 1998) and from the unclassified *Joint-Pub 3-12.1* paints a dramatically *new and unique picture of further nuclear targeting by the US*. As the only country which ever used two types of weapons of mass destruction in war (nuclear and chemical weapons)[34], it may use a new type of earth penetrating nuclear weapon in the sub-kilton range against "rouge-states" or even on the battlefield.

In detail the objectives are: "belligerent response", (nuclear reprisals against non-nuclear states who use weapons of mass destruction), "agent defeat" (the incineration of chemical and biological agents on the ground and in flight), the destruction of facilities and operation centers in the hands of "non-state actors" and last, but not least, preemptive strikes against nuclear, chemical, and biological installations and command and control centers. These concepts go far beyond what was "deterrence" in the Cold War or what was intended to counter attacks of perceived superior conventional forces in an over-all block confrontation or on the battlefield. Under the title: "Desired Results from the Use of Nuclear Weapons"[35] the following objectives are pointed out:

— Decisively change the perception of enemy leaders about their ability to win.

— Demonstrate to enemy leaders that, should the conflict continue or escalate, the certain loss outweighs the potential gain.

— Promptly resolve the conflict on terms favorable to the United States and our allies.

— Preclude the enemy from achieving its objectives.

— Ensure the success of the effort by US and/or multinational forces.

Inventing the New Military and Non-Military Threats

A military threat to the American homeland is not in sight. Only Russia, China, France and the UK have ICBM capabilities to strategically threaten US territory. Maybe India will come up with its own ICBMs, but the "rouge-states" Iraq, Iran, Libya, North Korea, Syria and whoever else might be a new member in this club, are far, far away from that competence. But, following the *Quadrennial Defense Review of 1997* (QDR 1997) "new threats and

dangers–harder to define and more difficult to track–have gathered on the horizon." These threats range from the use of weapons of mass destruction (WMD) by terrorists, a scenario Hollywood has been massively hyping in the few last years,[36] psychological warfare and info-terrorism (the latest *James Bond*-movie), as well as cyber-terror attacks on the US national information infrastructure. Only the latest Hollywood hype (*Deep Impact*), an asteroid incident with the earth in about 2010 is right now not included in QDR.

One may however expect this to be implemented soon, because it was the favorite hobby of Edward Teller to deploy nuclear weapons in outer space orbits after the initial SDI project did not take off. But the succeeding project, "the National Missile Defense (NMD) remains a high priority. The Administration and Congress have agreed to keep this program on an accelerated research and development path aimed at creating the option to make a decision on deployment possible as early as the fiscal year 2000, if the threat warrants." (QDR 1997). The most convincing combination for the Pentagon's plans would surely be an attack by "communists from outerspace". When the first Hollywood movie about this comes out, you can be sure that the Pentagon has set up a task-force on this issue. (NASA had already such a task force for asteroid watching, before *Deep Impact* came out.)

To be serious again, the QDR seeks to lead the US into the 21st century with a defense budget only 23 per cent lower than the average for the Cold War period of 1976-1990[37]. Latest official NATO data on the declared overall US and NATO defense budgets give the following figures for the US defense budget (in current prices and exchange rates, to the nearest billion US-$)[38]:

So, the declared overall US defense budget in 1997 is 15 billion US $ higher than in 1985 and only 33 billion lower than in 1990, at the "official end" of the Cold War.

1975	1980	1985	1990	1993	1994	1995	1996	1997
88	138	258	306	298	288	278	271	273

It is at present not at all clear how much of this expenditure goes directly or indirectly into cyber- and infowar projects, if one includes e.g. the Visions 2010 campaign for joint real time warfighting on a global scale, the space based projects for C2W (satellite surveillance and reconnaissance), the space and land based projects for theater and strategic missile defense, or the RMA initiatives.[39] Beside this, the strategic computing initiatives for computer nuclear weapons test simulations[40] under the "Stewardship Stockpile Program" are not listed in the DoD budget, but in DoE's. The 26.7 billion US $ budget for the fiscal year 1997 for secret service activities including CIA, NSA and other services is not inculded in the official defense figures, either.[41]

As the "real threats", possibly deterred by military means, more and more disappeared at the end of the Cold War, "wild card" scenarios for military threats and legitimization threads emerged. "The agnosticism of the uncertainty hawks extends not only to the specifics of discrete future events […] but also to the general character and magnitude of possible threats."[42] The US staggers in the twilight of uncertainty, and this prevailing feeling quickly took root in NATO bureaucracy. The answers are not preventive (e.g. by technology control export regimes, preventive diplomacy), but counter measures, counter-proliferation, counter WMD, including strikes out of area, but within the national interest. It demonstrates that the US national interest is now global, not only including the "old oil supplies" in the Persian Gulf, but perhaps soon the "new oil supplies" in the Caspian Sea basin (one of the hottest regions between Russia, Kazakhstan, Azerbaijan, Iran and Turkmenistan, arena of a

Kulturkampf between Russia, the US and the Islamic world). Not surprising, the main, straight and clear answers for geoeconomic- and geopolitical challenges for US foreign policy are technology based.

To enable Joint Vison 2010 which is politically intended to "respond to the full spectrum of crises that threaten US interests"[43] a new acronym-monster was created recently in Pentagon brains and confirmed in April 1998 by Secretary of Defense, William S. Cohen. Not cyberwar, not infowar, not C2W, not C3I, not C4I, no. *C4ISR* is the latest level of discussion and Pentagon demands: command, control, communications, computers, intelligence, surveillance, and reconnaissance.

The Pentagon recently set up the "most important C4ISR architecture initiative", the "Joint Technical Architecture"[44] which is to be a "backbone of the revolution in military affairs". The six principal components of the evolving C4ISR architecture for 2010 and beyond are:

— "A robust multisensor information grid providing dominant awareness of the battlespace to U.S. commanders and forces.

— Advanced battle-management capabilities that allow employment of globally deployed forces faster and more flexibly than those of potential adversaries.

— A sensor-to-shooter grid to enable dynamic targeting and cuing of precision-guided weapons, cooperative engagement, integrated air defense, and rapid battle damage assessment and re-strike.

— An information operations capability able to penetrate, manipulate, or deny an adversary's battlespace awareness or unimpeded use of his own forces.

— A joint communications grid with adequate capacity, resilience, and network management capabilities to support the above capabilities as well as the range of communications requirements among commanders and forces.

— An information defense system to protect globally distributed communications and processing networks from interference or exploitation by an adversary."[45]

Conclusion–Cyber- and Infowars, Hype or Reality?

Some questions have been asked here. The relationship between the foreign policy design of the US and the boosting of cyber- and information war issues–is it "grand design", or simply the result of erratic decisions by different bureaucracies and the current administration? It seems to be much less than a conspiracy and much more than only a new trend in military affairs.

If information warfare is defined as being everything between gossip, C-something-W and supercomputing, there is nothing new on earth beside the advanced channels of distribution and facilities processing data.

If information and cyberwarfare are concepts to change the mind, the consciousness, the perceptions of the enemy elites prior to or in combat about their reality and selfunderstanding, it is as old as Sun Tzu's aphorisms about the "art of war", approximately 2000 years old and heavily quoted in US papers. In the 20th century this approach has been called psychological warfare or reflexive control.

If the debate is about the real battlefield in the sense of all subtypes of cyberwar, from C2W… to… C4ISR and RMA, it is mainly about *increased lethality* over long distances and in real-time. Political and military power, and the ability to kill become in the clearest philosophical meaning literally 'virtuell.'

It is about power-projection without physical presence. This intention is in all aspects most advanced by the US. And it implies a political notion.

Cyber- and Netwar in the sense of hacking global or national information infrastructures (no matter if they are civilian or military) by individuals, NGOs or nation states and causing severe damage to lives are not easy to assess. But probably it is an intended alarmist view and *perhaps a hype of extraordinary dimensions*. A discrimination between facts and fiction is urgently needed. The *real* armed conflicts of the 1990s *in the real world* were fought by light and medium fire-arms (in some cases by heavy arms as well) and land-mines and *really* killed about 2 million people, mostly innocent civilians. DARPA's scenario of the exercise "The Day After", reported by Anderson & Hearn[46], taking place in May 2000, in which hacker attacks effect damage in the US and by allies in Europe and the Gulf region to the financial, ground transport, electric and air traffic systems, to oil supplies and CNN broadcasting does not provide any plausibility as to how or on what technical scenarios these attacks might be based on, or conducted. The only assumption is that there are low barriers to enter the networks.

There are mainly four arguments rejecting netwar as life-threatening dangers on a larger scale: (a) large scale attacks, as described by "the day after" scenario cannot be conducted by individuals or even large scale NGOs or subnational entities; (b) if such scenarios indeed could become real, then most likely in the morning twilight of a large scale war, when the political tensions and the actors would be known; (c) everybody who attacks information systems in that style leaves an electronic trace and may be identified; (d) to back up widely dispersed IT and communication systems is much easier and cheaper on the carrier level as well as on the software level, than to defend closed systems. Open systems based on universal protocols, such as TCP/IP or derivates, used in internet, intranets and extranets, are in many ways redundant from their principle architecture. (Even NATO considers operating "hidden" WEB pages with classified information for the members of the Partnership for Peace Program. Successfully hacking those pages would cause not more "damage" than revealing classified information.)

To sum up: In my view WMD, poison gas, biological or radiological weapons or crude nuclear weapons in the hands of terrorists[47] would constitute a much severer threat to security than hacking NII's or GII. There are only a very few speculative scenarios which all revolve around the nuclear weapons of the US and Russia that really could cause disaster:

> Fifth, it is important to recognize that soon both sides (US and Russia) will have the ability to use holograms and other IT manifestations that will offer the opportunity to completely fool one another both on the battlefield and through the airwaves […] A hacker simulating an incoming ICBM nuclear attack on the radar screens of the military of either Russia or the United States is but one manifestation of this threat.[48]

Hacking the launch codes of strategic nuclear weapons which might effect paralysis of either Russian or US ability to launch a counter strike, the attempt to gain positive control over each other's nuclear arsenals, the attempt to achieve electronic control over early warning satellites, or finally to retaliate against a "real" or "perceived" hacker attack on the nuclear command and control chain by nuclear weapons–all these belong to the same category of hyper-alarmist views.

No one can really tell if these scenarios pose a real danger to mankind. Only little is known in unclassified literature about the real technical nature of the nuclear command and control chains of the US and Russia. The danger is much more about the nature of nuclear weapons themselves.

Coming to final conclusions, Plato said in his "Gorge-Allegory" that cognition and knowledge are always a "shadow" of reality. In this sense he was an early "constructivist" meaning that differentiating between a "real" reality and a "constructed" reality is very hard to, if not actually impossible. Psychological and sociological theories in the 20th century go as far as claiming the construction of social "reality" is only a function of perception. Putting Plato on a modern language track in cyber issues would mean finding the border line between hype and reality. Günther Anders, an Austrian philosopher, forecasted in 1960 the principal vulnerability and all related follow-on problems of technical-based and interconnected networks in his equation "Apparat=Welt"[49]:

Die katastrophische Gefährlichkeit einer solchen Universalmaschine liegt auf der Hand. Würde nämlich — was bei der Degradierung aller Apparate zu Apparatteilen der Fall wäre — die totale Interdependenz zwischen allen ihren Teilen Wirklichkeit werden, dann würde jedes Versagen eines Teiles automatisch den ganzen Apparat in Mitleidenschaft ziehen, also still legen[50].

There is almost nothing more to add, apart from my assumption that more empirical research seems necessary to understand the interaction between the military and the new information technologies. It is important as well to establish an early warning system of "watchdogs" to identify *as early as possible* any incipient information war arms race.

[1] Van Creveld, *Command in War*, Harvard Press, Cambridge/Mass., 1985, p 264, quoted after Arquilla, John & Ronfeldt, David: "Cyberwar is Coming!", in: Arquilla, John & Ronfeldt, David (eds.): *Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica 1997, 58, Footnote 11, has put it this way: "From Plato to NATO, the history of command in war consists essentially of an endless quest for certainty […]"

[2] Arquilla/Ronfeldt, *Cyberwar is coming*, in: *In Athena's Camp*, 30

[3] ibid, 31

[4] ibid, 28

[5] ibid, 29

[6] ibid, 30

[7] ibid, 275

[8] ibid, 277

[9] ibid, 278

[10] ibid, 285

[11] ibid, 279

[12] *Joint Vision 2010*, 16

[13] *Joint Pub* 3-13.1, GL-8

[14] George J. Stein has argued in *Information Warfare: Words Matter* ### that both documents are essential in understanding the doctrinal level of IW. In addition he discriminates in the sub-concepts: "There might be other applications of IW in military operations and there might be applications of IW in other than military operations. Likewise, C2W now applies 'across the range of military operations and at all levels of conflict.' That is, it is not restricted to a simple battlefield objective of disrupting the enemy commander's command and control of his troops. The Joint Doctrine for Command and Control Warfare, then, is probably the best window through which to observe the evolution of InfoWar."

[15] Quoted on the Web under:

[16] Quoted after Conetta, Carl & Knight, Charles: "Inventing Threats", in: *Bulletin of the Atomic Scientists*, March/April 1998, 32

[17] ### Friedrich Kittler, "On the history of the theory of Information Warfare", in: *infowar*, Springer, Wien-New York 1998, pXXXX

[18] In Feb 1998 IBM got from the Department of Energy (DoE) the contract to develop the world's fastest super-computer with a 500 million US-$ budget for nuclear weapons-test simulations under the stockpile stewardship program. The computation power will, it is claimed, reach 30 teraflops by 2001 and 100 teraflops by 2004.

[19] William Cohen in a report of the US Department of Defense to the US Congress, April 1998, chapter 15. Cohen, William S. (1998): Annual Report to the President and the Congress. U.S. Department of Defense, April 1998. Quoted at http://www.fas.org/man/docs/adr_99/index.html

[20] Toffler, Alvin & Toffler, Heidi (1997): "The New Intangibles", in: *In Athena's Camp*, xx

[21] Which might turn out as "bloody" later on.

[22] Nye, Joseph & Owen, William (1997): "America's Information Edge", in: *Foreign Affairs*, March/April 1996, 20

[23] ibid, 21. By the way: Russians have called the attempt to influence others in their behavior and against their will in the tradition of Ivan Pavlov "reflexive control".

[24] What one might reduce to a terrible triple M stultification, Mc Donalds, Michael Jackson and Madonna.

[25] Nye, Joseph & Owen, William (1997): in: *Foreign Affairs*, March/April 1996, 35

[26] Toffler, Alvin & Toffler, Heidi (1997): "The New Intangibles", in: *In Athena's Camp*, xvi

[27] Panarin, Igor Nicolaevich: "The Information-psychological Struggle and the authority", in: infowar, Springer, Wien-New York 1998, ###

[28] Namely: Joint Pup 3-13.1, the Quadrennial Defense Review of 1997, the Joint Vision 2010 concept and the April 1998 report of the DoD to Congress.

[29] Quoted at: http://www.fas.org/man/docs/qdr/index.html

[30] IISS, International Institute for Strategic Studies, *The Military Balance 1997/98*, London 1998

[31] NATO Press Communiqué M-DPC/NPG-1 (98),72, 11. June 1998

[32] Joint Pub 3-13.1

[33] Joint Pub 3-13.1

[34] The nuclear weapons used against Hiroshima and Nagasaki are well known. In addition US armed forces used "agent orange‘ a chemical weapon in the Vietnam war and even the poison gas sarin in Laos, as Time Magazin reported on June 15, 37-39.

[35] *Joint Pub* 3-12.1, p. I-2

[36] Gen. Eugene Habiger, head of the U.S. Strategic Command, toured weapons sites across Russia over the past week to learn more about how the world's other major nuclear power controls its most lethal weapons. `I want to put to bed this concern that there are loose nukes in Russia,' Habiger said in an interview with The Associated Press before flying back to the United States. `My observations are that the Russians are indeed very serious about security.' (Associated Press, June 7, 1998).

[37] Conetta, Carl & Knight, Charles (1998): "Inventing Threats", in: *Bulletin of the Atomic Scientists,* March/April 1998, 32

[38] NATO Press Communique M-DPC-2(97)147, 2nd Dec. 1997

[39] These, e.g., are just selected topics of the budget of DARPA (Defense Advanced Research Projects Agency) for fiscal year 1998, US-$ millions. Source: http://www.arpa.mil/documents/98_budget.html

Title FY 1996 FY 1997 FY 1998 FY 1999

Defense research sciences 76.459 90.701 76.009 80.936

Next generation internet 0.000 0.000 40.000 40.000

Computing sys & comm technology 361.528 314.969 341.752 371.471

Tactical technology 120.440 121.520 155.329 177.995

Integrated command & control tech 44.395 59.672 37.000 40.000

Advanced electronics technologies 389.610 360.288 277.044 282.668

Command, cont'l & communications sys 0.000 102.996 163.800 172.600

Sensor & guidance technology 0.000 108.360 166.855 200.582

Agency total 2.269.202 2.140.436 2.204.403 2.271.934

[40] For an overview see: 'Explosive Alliances. Nuclear Weapons Simulation Research at American Universities,' compiled by the Natural Resources Defence Council. http://www.nrdc.org/nrdcpro/expl/eainx.html

[41] As CIA stated, this budget increased in 1997 slightly (about 0,2 per cent) compared with fiscal year 1996. It was the second time since 1945 that this well buried expenditure had been released. Neue Zürcher Zeitung, 25. März 1998, 4.

[42] Conetta & Knight, ibid, 34

[43] Cohen, William S. (1998): *Annual Report to the President and the Congress.* U.S. Department of Defense, April 1998. Quoted at http://www.fas.org/man/docs/adr_99/index.html

[44] Cohen, ibid, chapter 8

[45] Cohen, ibid, chapter 13

[46] Anderson, Robert H. & Hearn, Anthony C., National Defense Research Institute, RAND: "An Exploration of Cyberspace Security R&D Investment Strategies for DARPA", in: Arquilla, John & Ronfeldt, D. (eds): *In Athena's Camp. Preparing for Conflict in the Information Age*, Santa Monica 1997, 1-19

[47] I want to mention that especially in case of scenarios like the theft of nuclear weapons by terrorist of subnational groups, the alarmist position also seems much exaggerated.

[48] Thomas, Timothy L. (1998): *Information Technology: US/Russian Perspectives and Potential for Military Political Cooperation.* In: Cross, Sharyl; Zevelev, Igor; Kremenyuk,Victor & Gevorgian, Vagan (eds): Global Security Beyond the Millennium: American and Russian Perspectives, MacMillan Press (forthcoming), 69-89.

[49] Anders, Günther: *Die Antiquiertheit des Menschen*, C.H. Beck, München 1986, 111

[50] Anders, Günter, ibid., 114