THE CYBERSPACE DIMENSION IN ARMED CONFLICT: APPROACHING A COMPLEX ISSUE WITH ASSISTANCE OF THE MORPHOLOGICAL METHOD

Myriam A. DUNN

1. Introduction

The ascent of the Internet as phenomenon that affects and changes many aspects of world affairs is taking place against the broader backdrop of the so-called "Information Revolution." One of the effects of this evolutionary change is the rising importance of information next to traditional military force capabilities in the formulation of strategy and the advent of a number of new doctrinal concepts, such as "Information Superiority," that are seen as the key to winning wars. As a result, military attention focuses more on the informational aspect of conflicts. At the same time, there is a notion that an ever-widening range of actors has access to powerful tools for the rapid collection, production, and dissemination of information on a worldwide scale. Networks play a central role in this development. Usually, these intertwined systems are known as the World Wide Web, or simply www, the most popular and widespread incarnation of which is the Internet. The globalization and mass popularization of the Internet provide non-traditional actors with capabilities that were previously only available to the largest and most powerful entities, challenging the power and steering capacity of major actors.[1] This creates tensions along the intersection of newly emerging actors, the resultant power redistribution, and changes in military affairs. One emerging issue is the role of the Internet in armed conflicts, or more specifically, the role of a new dimension called "Cyberspace"; a concept that stands for the fusion of all communication networks and sources of information into a tangled blanket of electronic interchange. Cyberspace is not part of the physical world, but is detached or "virtual," existing where there are telephone wires, coaxial cables, fiber-optic lines, or electromagnetic waves—an environment inhabited by knowledge in electronic form.[2]

INFORMATION & SECURITY. An International Journal, Vol. 7, 2001, 145-158.

The role of the Internet in conflicts remains a poorly analyzed topic, even though recent developments in warfare point to its growing and manifold influence. This paper tries to show ways of dealing with the issue in a systematic way in order to gain a broader understanding of the problem, including thoughts on how, why, and with what consequences the Internet is used in today's conflicts. In the first part, the morphological approach is proposed as a method that seems promising for systematic and abstract future analysis of the problem complex. It introduces a multidimensional matrix that contains issue-parameters and assigned values. The second part explains important aspects of the morphological box in detail, with examples from Operation Allied Force in Kosovo and the Israeli-Palestinian conflict.

2. Complexity and Change: How to Approach a Multifaceted Problem

The present epoch seems to derive its order from episodic patterns and is marked by persistent opposites. It appears as if complexity and change were the two defining characteristics of the Information Age and the post-Cold War world in general. The current high degree of complexity is further enhanced by an ongoing redistribution of power relationships due to the Information Revolution that leads to skewed and volatile distribution patterns with more influential actors, significantly increasing the turbulence and unpredictability of the international policy environment.[3]

It seems obvious that highly complex issues demand methods that are at least partly capable of handling multifaceted non-linear problems. As an abstract method not dependent on case studies, the morphological approach promises to enhance the researcher's understanding of the problem complex when used for structuring and investigating the totality of relationships contained in them, and it can help to develop likely scenarios of the Internet's role and use in warfare as well as possible impacts.

2.1. The Morphological Approach as an Option

The morphological approach helps to structure and analyze complex interdisciplinary problems that incorporate non-quantifiable components. By categorizing problem fields into significant variables or parameters and ranges of conditions that can be integrated into well-defined relationships or configurations, this method not only helps to formulate problems precisely, it also facilitates the development of general or specific future scenarios, and of corresponding strategies.[4]

Fritz Zwicky, the pioneering father of the morphological method, proposes five steps in the process: The scholar first identifies and defines the parameters of the problem complex to be investigated. In a second step, each parameter is assigned a range of values, representing possible and relevant conditions. A morphological box is constructed by setting these parameters and values against each other. All the possible solutions contained in the box can then be scrutinized and evaluated—without

prejudice, in order to establish which of them are possible, viable, practical, interesting, and which are not—with respect to the purposes that are to be achieved. Last, optimal solutions are selected.[5]

This paper does not aim to execute the whole set of necessary steps. It merely suggests a matrix that might be useful for further analysis. Elements of the morphological box are partly justified in the next chapter. Four parameters have been identified as important:

- Actors using the Internet, ranging from individuals to state bodies;
- The intentions or objectives of Internet users, from the "peaceful" online collection and dissemination of information to the aggressive use of the Internet to harm adversaries;
- The "levels" on which the effort takes effect, grouped into short-term and long-term effects;
- The impact or outcome of the use of the Internet.

The following morphological box (Table 1) summarizes the first three steps proposed by Zwicky:

The number of possible permutations is 6 x 8 x 8 x 5 = 1920, the product of the number of conditions under each parameter. A number of realistic scenarios could be identified fairly easily by hand. Examining all possible permutations, however, is best done with the help of software tools.[6]

As mentioned above, we do not aim to evaluate all the possible solutions contained in the box. The aim of the next chapter is to go into details of parameters and conditions, in order to sharpen the understanding of the problem complex by explaining step one and two of the Zwicky-process.

3. Aspects of the Internet's Use in Conflicts: Explaining the Morphological Box

This chapter wants to provide a closer examination and explanation of two of the parameters ("objectives" and "impact/outcome") and their respective values. The "actor"-parameter needs no further elaboration. Likewise, the "effects level"-parameter is not additionally explained: In the definition of the long-term effects, this papers basically follows Franz M. Aebi's suggestions of security dangers for state and society,[7] while the discussion of short-term effects applies Edward Waltz's ideas of layers of functions (both on the side of the attacker and of the attacked), described in his approach to information warfare.[8] Parameters two ("objective") and four ("impact/outcome"), on the other hand, are treated in subchapters.

Actor	Peaceful ↓ Aggressive		Objective	Effects Level		Impact/ Outcome
Individual	Collection and Dissemination activities		Gain information for personal enrichment (Gather only)	Short Term Effects	Physical System Level: Affects technical performance and capacity	Proliferation and diversification of voices
Interest group(s)			Platform of publication to spread information and opinions (Distribution)		Information Structure Level: Influence of effectiveness and performance of information functions	Undermine credibility of officials
Non-governmental organization			Gain information in order to act upon it (Exploitation)		Perceptual or Psychological Level: Causes indecision, delay of decision, or biases specific decision	Battlefield expanded to include the human mind: "Neocortical" warfare
International organization			Coordination of activist/ political/ military activities (Coordination)		Military Level: Affects military operations directly or in the long-term through changes in doctrine, organization	Blurring of boundaries between military/ civilian domains
State political body	Information Attacks Dimension		Spread of false or intentionally misleading information, propaganda (Deception)	Long Term Effects	Political Level: Affects political operations directly or in the long-term through changes in law	Blurring of boundaries between war and peace
State military body		**Hacktivism**	Hack to cause disruption (Disruption)		Economic Level: Affects production, trade resources, etc.	
			Hack to cause destruction and replacement of content (Destruction)		Social Level: Long-term effects in society	
		Cyberwar	Damage large parts of society through attacks on critical (information) infrastructure (Destruction and severe damage)		Cultural Level: Long-term effects in culture	

Table 1*:* Morphological Box for the Use of the Internet in Conflicts

3.1. Purpose of the Internet's Use: Intent and Objectives

The eight values of parameter two are grouped in four subchapters: similar aspects are treated together, though each is of distinct importance. A few examples from "Operation Allied Force" in Kosovo and the Israeli-Palestinian conflict are presented in support of the conditions selected.

Gather and Distribute with Help of the Internet

Kosovo is a precedent for conflicts in which all sides, including a variety of actors not directly involved, have an active presence on the Internet and where the network is used extensively for the exchange and publication of conflict-relevant information, some of which can only be found online. Organizations and individuals throughout the world use the Internet daily to publish information on various subjects. During times of conflict, this channel becomes even more important: While governments and government-related organizations tend to upload material that supports their official policies, individuals not only have the ability to gather more and different information even when in the conflict zone, they also have a tool with which to spread their views and opinions with little effort.

In conflicts in which public opinion is the main target of political rhetoric, the Internet becomes 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 included the dishing up of rumors, wild exaggerations, denials of accurate information, and even the feeding of false and speculative stories—they looked for other ways to get relevant information. Transcripts of press briefings show that journalists actively used the Internet as a parallel source of information to the official information provided.[9]

In a case of effective distribution, Serbs used E-mail distribution lists to reach tens of thousands of users, mostly in the US. These E-mails, which were for the most part sent to American news organizations, called for an end to the bombing, some of them using heated anti-NATO rhetoric, others containing moving stories describing life under the bombs.[10] Some newsgroups were flooded with thousands of postings on Kosovo each day. Most of the contributions just aimed at fighting a war of words and abusing the other side. Others, however, contained interesting information and rumors or questioned the reliability of NATO's press briefings, pointing to inconsistencies in its story.[11]

Exploitation, Coordination, and Propaganda

Most facets of information exploitation such as intelligence, surveillance, and reconnaissance are professional military domains and require expensive hardware that

is not available to non-state actors. The Internet on the other hand is an efficient tool for gathering "open-source intelligence" during all phases of a conflict; a possibility open to the military as well as civilians as long as channels of communication stay open and phone lines remain working.

In some cases, the Internet is 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.[12] 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 sites, and networked with anti-NATO groups around the world.[13] Far more aggressive activities are pursued by Middle Eastern activists that employed the Internet's coordinating capability to gather sympathizers for E-mail flooding and Denial-of-Service (DoS) attacks against government and partisan websites. A Palestinian umbrella group called "Unity" notified hacker chatrooms and used encrypted E-mail messages to direct pro-Palestinian visitors to their website, where they were asked to "click here and help the resistance." A click on one of three links launched a DoS flood attack against Israeli websites in an effort to shut them down.[14] Hackers of the "Israel Unite" website asked web surfers to do the same. Earlier Israeli attacks had been initiated by messages circulated over the ICQ instant messaging service, which urged users to help to take the Hizbollah site down by using a ping command on their PCs, and also distributed special attack software for this purpose.[15]

A third and very important issue is the spread of false or intentionally misleading information. Neither propaganda nor outright manipulation of information are new phenomena 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. As conflicts today are turned into so-called "news and propaganda wars," the Internet with its many benefits becomes a new global propaganda tool for all sides, turning Cyberspace into a kind of ethereal war zone in which a "soft war" is waged through the use of electronic images and words.[16]

Disruption and Destruction: Hacktivism

It is striking that commentators and reporters are especially fascinated with the offensive online activity called "hacktivism." Hacktivism stands for an amalgamation of hacking and activism, covering operations that use hacking techniques for reasons of political activism, mostly directed against a target's Internet site with the intent to disrupt normal operations but not causing serious damage.[17] 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.

There are numerous examples of hacktivism incidents. Various Internet servers were attacked during the Kosovo conflict. Disruption of the NATO server began on 27 March: the attacks included so called "Ping" bombardment to cause Denial of Service, E-mail spamming attacks as well as viruses.[18] 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.[19]

More aggressive actions do not merely deny information but also cause destruction by replacing content, called "defacing": The Serb hacker group CHC, for example, replaced two US government sites with 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 Yugoslav Web servers, replacing an anti-NATO site with a pro-NATO "Help-Kosovo" page.

In the Middle East, hacktivism onslaughts broke out in October 2000 shortly after the Intifada erupted on the ground. In February 2001, a private security consultancy counted more than 90 Israeli sites, mainly business and governmental, and 25 pro-Palestinian sites that had been attacked or defaced. Prominent sites among those were the Hizbollah homepage, the Hizbollah's Al-Manar Television web page, the Israeli government portal, as well as the Foreign Ministry, Knesset, Army, and Israeli Stock Exchange websites.[20]

Denial-of-Service and defacement attacks are only directed against an organization's public face and relatively harmless, even though they are considered to be an inconvenience as well as an embarrassment. But the success of such attacks is generally limited, especially since most of the attackers involved are only teenagers. Some incidents, however, were grave enough to seriously scare officials: for example, Palestinian groups effectively shut down NetVision, Israel's leading Internet service provider, and revealed a vulnerability not realized before in Israel's Internet infrastructure and Web security.[21] After the American-Israel Public Affairs Committee (AIPAC) site was breached, the FBI reacted with warnings on potential dangers for websites in the US. A Palestinian hacker gained access to the credit card numbers of more than 200 AIPAC members, boasting of the attack in an E-mail he sent to 3,500 members.[22] There is also a likely connection between the attacks and the increased reluctance of customers of Israeli e-commerce sites to supply credit card details, as well as falling shares of Israel-based Internet companies.[23]

Cyberwar Scenarios and Media Hypes

The last step in the process of escalation is Cyberwar or full-scale information warfare. Even though the media like to hype anything involving hostile activities and Cyberspace, severely damaging attacks threatening lives or strategic information

warfare at state level still remain theory: There is also substantial evidence to disprove the rumors that during Operation Allied Force, the US launched the first 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 instrument of war would be employed in conflict. The rumors reached a first high at the end of May, when a Newsweek article reported the launch of computer attacks on Yugoslav systems by the US. According to the article, defense analysts said that US computer hackers burrowed into Serb government E-mail systems to read Belgrade's mind daily, while some infiltrated the Internet systems of banks around the world in search of accounts held by Milosevic and other Serb leaders.[24] Later that year, the *Washington Times* took the story up and wrote that details remained still classified, but that top US military officials had now confirmed that during NATO's air war, the US had 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 had catapulted the country into a military era that could forever alter the ways of war and the progress of history."[25]

Because ideas about Cyberwar are still in their infancy, the US likely found that there was neither a clear legal basis for computer attacks or for retaliation against possible Serb attacks. The uncertainty surrounding international law evoked fears that their use might make American military commanders liable to war crimes charges, especially because the effects of information attacks are still totally unpredictable.[26] Another constraint on the use of "cyber-weapons" was the fear of giving away too many secrets in this emerging technological field: widespread use of these weapons and tools would probably accelerate and focus foreign military research on them and threaten to deprive the US of its information warfare edge in a field where foes could catch up quickly and cheaply.[27]

3.2. Impacts of the Cyberspace Dimension

This chapter addresses the impact parameter. Though it really seems that the Cyberspace dimension changes several aspects of warfare, it is acknowledged that much more empirical research is needed before it is possible to move convincingly beyond the descriptive evidence that is offered here. Nonetheless, a number of careful statements can be made about the Cyberspace dimension in conflicts without adding fuel to the existing hype.

Proliferation and Diversification of Voices

The use of the Internet in conflicts leads to a proliferation and diversification of voices by allowing a variety of actors to spread their views and opinions easily. Direct channels of communication and information distribution create wider

communities of the like-minded than was previously possible. It further facilitates the gathering of information during all phases of a conflict. Traditional information monopolies cease to exist and a relative transparency is established.[28]

It might seem to decision-makers that information flows across battle lines are too valuable to be stopped. It is said that NATO did not bomb Internet service providers or shut down satellite links bringing the Internet to Yugoslavia, because "full and open access to the Internet can only help the Serb people know the ugly truth about the atrocities and crimes against humanity being perpetrated in Kosovo."[29] Serbs likely thought that it would evoke sympathy and make the Western public more doubtful of their leader's actions, eventually undermining public support, while NATO believed that communication of the Serb people with democratic voices in the West would weaken their morale and in turn their support of the regime. While the first assumption was partly right, the second was not: hopes that communication of the Serb people with democratic voices in the West would undermine their support of the regime remained fruitless; even though Serbs had access to Western news 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 just as biased as those on the Yugoslav stations.[30] First-hand accounts of events as they were being witnessed by individuals inside Yugoslavia and posted to the Internet, mostly stories of fear and devastation, might not have had a direct impact on the war or its outcome, but the Web helped to personalize the citizens of Yugoslavia in some ways.[31]

Undermine Credibility

The Internet with its ability to distribute information quickly and easily can undermine the credibility of officials and other actors. Naturally, this capacity has both positive and negative aspects, depending on the perspective and also the final consequences.[32]

The Internet's strongest effect on Kosovo was a sort of "net" surrounding the conflict, informing it and keeping other media in check. 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. As was said, journalists actively used the Internet as an alternative source of information parallel to the official briefings. It shows that traditionally "spoilt" actors facing a decline of their information monopoly might suddenly find themselves embroiled in extensive media wars, in which it is not enough to justify actions, show that right is on one's side or stress the effectiveness of military actions: alternative sources of information can seriously challenge the credibility of the authorities, causing danger of not only losing the propaganda battle against the enemy, but also the fight for public opinion at the home front.

Blurring Boundaries Between Military-Civilian Domains Expand the Battlefield to the Human Mind

Even though modern high-tech conflicts are often pictured as being less violent than traditional forms of warfare, the expansion of the battlespace threatens to result in more civilian involvement. Future warfare scenarios picture battlefields enveloping entire societies.[33] As a result, military objectives no longer involve the annihilation of orderly enemy lines, but are aimed at eroding popular support for the war within the enemy's society. This battle for hearts and minds is seen in aggressive news and propaganda wars. Success on the battlefield means a setback for the country's efforts to manipulate its media representation and win the "news and propaganda" war. The danger in such battles for the hearts and minds of the populace lies in the difficulty of finding the right balance between countering an enemy's efforts aggressively and effectively and providing one's own true story, without using propaganda efforts that threaten to undermine and permanently damage one's credibility.

The trend towards more civilian involvement is not encouraging. Suddenly, frontlines are "everywhere." Precision-guided munitions may partially reverse the 20th-century trend towards large-scale 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 domains. The "dual use" of many assets and technologies makes distinction even harder. Applying such tools means bringing war to the civilian population, not only undermining 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. As a result, the distinction between civilian and military information systems is increasingly blurred.

Future wars that take place in an even less physical space will bring even less physical destruction, and fewer casualties – but civilians are likely to suffer differently: direct distress as a result of the cyber-targeting of civilian installations, which can be as deadly as bombs. The Cyberwar scenarios turn war into something that is no longer a last resort. Because there is less chance of combat casualties and a much lower cost of engaging in conflict, and because strikes can be carried out in blissful anonymity, it becomes much easier to commit acts of war.[34] Cyberwar also blurs the boundaries of war and peace; it begins to investigate faults and security failures in peacetime, and declaration of war is basically the first serious attack.

Inherent in many of the new military ideas is an extension of the battlefield to encompass the human mind as the ultimate target.[35] Targets may exist in physical space or in cyberspace and can include the human perception, with the objective of influencing this perception to affect decisions and resulting activities. In the new notion of "Neocortical" warfare, the military uses language, images, and information

to assault the mind, hurt morale, and change the will.[36] 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. Both the idea of "Soft power"[37] and the concept of "Noopolitik"[38] aim at spreading values, images, and ideas worldwide, and at the core are forms of domination and occupation of everyone's mind with the aid of influencing messages.

4. Conclusions

In this paper, a methodological and systematic way of dealing with complex multifaceted non-linear issues such as the use of the Internet in conflicts was shown, mainly to gain a broader understanding of the problem. It introduces the morphological approach developed by Zwicky as a method for structuring problem complexes to develop future scenarios and corresponding strategies. The morphological box introduced is only a suggestion at this stage: additional work will likely reveal more or different dimensions and parameters that need to be considered, and will surely lead to a refinement of the values assigned. In a further step, it would also be desirable to include one or more response or reaction dimensions from a policy perspective into the matrix.

The Internet as a mass phenomenon belongs to the modern face of war. It is to be expected that we will experience many future wars in which all kinds of tools and weapons are brought to bear upon the information infrastructure to affect the decision-making processes of both government leaders and the general civilian population, and the Internet plays a significant part in this. It is already making regional wars more global, as the interconnected world creates relative transparency that makes it easier for adversaries to anticipate each other's next move and also personalizes and documents conflicts in a unique way. A downside of this global village atmosphere is that every online company represents a potential target for aggressive hacktivism or Cyberwar activities. The information attack domain in particular is presently considered a pressing national and international security issue, with a lack of understanding of the real dangers and risks and steps necessary to overcome them. In the future, it is likely that aggressive online activities will set fundamental precedents for approaches to military information operations, for the use of the Internet as a tool for warfare, for the laws of war, and for international law. It is therefore clear that more systematic analysis is needed to explore the true dimensions of the problem in a political context and to establish steps towards satisfactory solutions. In particular, there appears an essential need to protect civilians from too much involvement in these new forms of warfare, otherwise they may become targets

through the targeting of civilian installations or worse, the targeting of the human mind.

Notes:

1 Among the important proponents of this view are James N. Rosenau, *Turbulence in World Politics: A Theory of Change and Continuity* (Princeton: 1990); David S. Alberts and Daniel S. Papp, eds., *The Information Age: An Anthology of Its Impacts and Consequences* (Washington D.C.: National Defense University, 1997). Available @ http://www.ndu.edu/inss/books/anthology1/.

2 John Arquilla and David F. Ronfeldt, "Cyberwar is Coming!" in John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND Corporation, 1997), 23-60. Available @ http://www.rand.org/publications/MR/MR880/MR880.ch2.pdf.

3 James Rosenau, "Global Affairs in an Epochal Transformation," in Henry, C. Ryan and Edward C. Peartree, eds., *Information Revolution and International Security* (Washington: 1998), 33 –57.

4 Maria Stenström and Tom Ritchey, *Morphological Analysis as a Method for Evaluating Preparedness for Accidents Involving Hazardous Materials*, Methodology Report (Swedish Defence Research Establishment /FOA/, September 2000), 11.

5 Fritz Zwicky, *Discovery, Invention, Research through the Morphological Approach* (Toronto, 1969); Hermann Holliger-Uebersax, *Handbuch der Allgemeinen Morphologie, Elementare Prinzipien und Methoden zur Lösung kreativer Probleme* (Zürich: 1982).

6 One example for such tool is the computer support program developed by the Swedish National Defence Research Establishment (FOA) called CASPER (Computer Aided Scenario and Problem Evaluation Routine). Note that not all combinations of conditions are logically consistent or plausible. These are usually weeded out by using a process called "cross-consistency assessment," in which pairs of conditions are identified that do not represent a consistent relationship. All those conditions containing these pairs are considered internally inconsistent and excluded from the final analysis.

7 Franz Martin Aebi, *Der Weg zum Weiterleben. Morphologische Studie zu einer zeitgemässen Planung einer Strategie der staatlichen und gesellschaftlichen Selbstbehauptung*, Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung, Heft Nr. 8 (Zürich: Forschungsstelle für Sicherheitspolitik und Konfliktanalyse, 1989), 13-14.

8 Edward Waltz, *Information Warfare. Principles and Operations* (Boston: Artech, 1998), 148-152.

9 For example Jake Lynch (Skynews) during a Press Conference by NATO Spokesman, Jamie Shea and SHAPE Spokesman, Major General Walter Jertz on 14 May 1999, NATO HQ, Brussels, available @ http://www.nato.int/kosovo/press/p990514b.htm: "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."

[10] Dorothy E. Denning, "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, available @ http://www.nautilus.org/info-policy/workshop/papers/denning.html, 5-8.

[11] Ros Taylor, "UK: Partisans Wage Virtual War," *The Guardian* (April 22, 1999). Available @ http://www.infowar.com/mil_c4i/99/mil_c4i_042399b_j.shtml.

[12] Denning, Hacktivism, 11.

[13] Michael Satchell, "Captain Dragan's Serbian cybercops. How Milosevic took the Internet battlefield," *U.S. News* (May 10, 1999). Available @ http://www.usnews.com/usnews/issue/990510/10info.htm.

[14] John Galvin, "Cyberwars Bring real-world Conflict to the Web" (February 16, 2000), http://www.zdnet.com/zdnn/stories/news/0.4586.2687046,00.html. Unity website @ http://www.ummah.net/unity/ .

[15] Fadi Salem and Fawaz Jarrah, "Israeli Palestinian Clashes Spur Hacking Attacks" (October 18, 2000), *IT News*, DITnet, http://www.dit.net/itnews/Article.asp?Article=139; Hacker of Israel Unite @ http://www.israelhackers.cjb.net/ .

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

[17] Ralf Bendrath, "Der Kosovo-Krieg im Cyberspace. Cracker, Infowar und Medienkrieg," *telepolis* (19 July 1999). Available @ www.iwar.org.uk/iwar/resources/kosovo.htm.

[18] Press Conference by NATO Spokesman, Jamie Shea and Air Commodore David Wilby, SHAPE, Transcript 31 March 1999, updated 31 March 1999, NATO HQ, available @ http://www.nato.int/kosovo/press/p990331a.htm.

[19] Bob Brewin, "Cyberattacks Against NATO Traced to China," *Federal Computer Week* (September 2, 1999). Available @ http://www.infowar.com/mil_c4i/99/mil_c4i_090299a_j.shtml.

[20] Galvin, Cyberwars.

[21] Ibid.

[22] AP Message, "Mideast Cyberwar Spreads to U.S. Pakistani Hackers Attack American pro-Israel Web Site," *USA Today* (November 3, 2000). Available @ http://www.usatoday.com/life/cyber/tech/cti762.htm.

[23] Fadi Salem and Fawaz Jarrah, "Escalating Middle East Cyberwar may Prove too Costly for Israeli Business," *IT News* (December 6 2000). Available @ http://www.dit.net/itnews/Article.asp?Article=408.

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

[25] Lisa Hoffmann, "U.S. Opened Cyber-War During Kosovo Fight," *Washington Times* (October 24, 1999), C1, available @ http://www.potomacinstitute.org/press/Cyberwar.htm. See also Robert Burns, "Computer Warfare Used in Yugoslavia," *AP* (October 7, 1999), available @ http://www.infowar.com/mil_c4i/99/mil_c4i_100999b_j.shtml.

[26] Steven Metz, "The Next Twist of the RMA," *Parameters* 30, 3 (Autumn 2000), 40-53. Available @ http://carlisle-www.army.mil/usawc/Parameters/00autumn/metz.htm.

[27] Julian Borger, "Pentagon kept the Lid on Cyberwar in Kosovo," *The Guardian* (November 9, 1999).

[28] This does not say that these voices will be heard, believed, or understood though: the Internet is by itself no more than a vessel, a means to distribute meaning and content that has been added. It has no ability to change human basic psychology.

[29] James P. Rubin, spokesman for the US State Department cited in Denning, Hacktivism, 1.

[30] 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 Michael Satchell, Cybercops; see also Denning, Hacktivism, 4.

[31] Ellen Goodman, "Kosovo – our first Internet War," *Reporternews.Com* (Friday, April 9, 1999). Available @ www.reporternews.com/1999/opinion/good0409.html.

[32] Robert O. Keohane and Joseph S. Nye, Jr., "Power and Interdependence in the Information Age," *Foreign Affairs* 77, 5 (September/October 1998): 88-93.

[33] C.f. web resource on "Fourth Generation Warfare" available @ http://www.d-n-i.net/FCS_Folder/fourth_generation_warfare.htm.

[34] Lisa Hoffmann, "Computers Change Rules of War, Civilians Still Get Hurt," *The Washington Times* (October 24, 1999), C8. Available @ http://www.potomacinstitute.org/press/Computers.htm.

[35] Top level, attacked in Information Operations, is the perception or the knowledge of an adversary with the objective to influence decisions and behaviors. See Waltz, *Information Operations*, 151.

[36] Richard Szafranski, "Neocortical Warfare? The Acme of Skill," in Arquilla, *In Athena's*, 395-416.

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

[38] Cf. John Arquilla and David Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy* (Santa Monica: RAND, 1999). Available @ http://www.rand.org/publications/MR/MR1033/MR1033.pdf/.

MYRIAM DUNN is trained in modern history and international relations at the University of Zurich. She is an editor of the International Relations and Security Network (ISN), Center for Security Studies and Conflict Research, Swiss Federal Institute of Technology, Zurich. Her major responsibilities are in the field of information brokering and webpublishing, including research for and maintenance of online services in international relations and security policy. She is also in charge of co-organizing and running IT courses on the use of the Internet for professionals in the defense or diplomatic communities in Partnership for Peace countries. In her PhD project she explores methodologies for measuring interdependencies and vulnerabilities in Critical Information Infrastructure. *E-mail*: dunn@sipo.gess.ethz.ch