Information & Security Volume 7, 2001

The Internet and the Changing Face of International Relations and Security

Edited by Andreas Wenger

The Growth of Soft Power and the Challenges of Global Governance

The New Security Challenges of the Information Age

The Human Mind as Battlefield in the Emerging Global Information Environment

I&S Monitor

I&S Research Centers

I&S Projects

Author: **Andreas Wenger**
Title: **The Internet and the Changing Face of International Relations and Security**
Year of issuance: **2001**
Issue: **Information & Security. Volume 7, 2001, pages 5-11**
Hard copy: **ISSN 1311-1493**

THE INTERNET AND THE CHANGING FACE OF INTERNATIONAL RELATIONS AND SECURITY

Andreas WENGER

Table Of Contents:

Most experts agree today, at the beginning of the 21st century, that we are experiencing a period of fundamental change. Understandably, there is much uncertainty about what kind of world the current global transformations will produce. In order to understand these changes and adapt to them we need to develop new conceptual repertoires that will better equip us to meet the challenges posed by the speed with which the world is evolving and the extreme global complexity that is emerging. One factor that is helping to create this new environment is information technology and, most significantly, the Internet. To fully comprehend the Internet's impact on how we think about and practice international relations and security, we need to investigate the conventional approaches that have inspired practitioners and theoreticians until now.

Since its inception, the discipline of international relations (IR) has been based on a separation between internal and external state relations. This separation was bequeathed to the modern state system by the Treaty of Westphalia in 1648, which attempted to resolve the religious conflicts of the Thirty Years' War by replacing a universal religious authority who acted as the arbiter of Christendom with the state-sovereign within its own territory and with the right to non-intervention in its affairs by any other state. After 1648, the internal affairs of states were thus conceptually separated from the external arena of interstate relations. At the beginning of the 21st century, however, we have reached a point where the traditional *domestic-international* framework no longer holds.

The division between affairs internal and foreign affairs is becoming increasingly untenable in an environment where international politics are more and more driven by the forces of *globalization* and *localization*. The information technology revolution has dramatically accelerated the cross-border movement of goods, services, ideas, and capital, resulting in a huge increase in transnational cultural and political exchanges and in the emergence of many new institutions and structures that transcend state borders. Modern information technologies have minimized the previous limitations imposed by space and time on the mobility of worldwide capital and industry and have created an environment for global trade and investment decisions. At the same time, local factors like workforce skills, hard and soft infrastructure, legal norms, and political institutions allow local communities and actors to attract mobile capital, human resources, business deals, and multinational firms. The resulting complex web of relations simply cannot be characterized as either domestic or international. The key political challenge now is to strike the right balance between international and local forces.

Although there is widespread belief that the information technology revolution is restructuring the international system, there is far less consensus about the theoretical and practical impact of the often contradictory developments on international politics. Given that the world is experiencing a diffusion of territorial, societal, and economic space, the debate initially centered on the redistribution and the changing nature of power. The distribution of power has become increasingly volatile and complex, and traditional political and cultural boundaries that once defined distinct worlds are beginning to crumble. The transnational architecture of global information networks has made territorial borders less significant. War and peace in the information age are evolving in an environment in which the boundaries between the political space and the military space have become increasingly blurred, as have those between the civilian domain and the military domain.

Power in the global information society depends less on territory, military power, and natural resources. Rather, information, technology, and institutional flexibility have gained in importance in international relations. In an unpredictable and highly turbulent international environment, the soft powers of knowledge, beliefs, and ideas allow political actors to achieve their goals. Opposing powers these days are less inclined to battle out their differences in the physical arena. Rather, they focus on the information domain, and gaining access to information is now the central strategic principle. Networks wage wars, and small players can now outsmart huge opponents by using asymmetrical strategies. However, our understanding of such conflicts and their multifaceted dynamics remains limited at best.

The importance of information and knowledge today is forcing us to take a new look at the main actors in international relations. Traditionally, states have been the exclusive holders of power and authority. However, with the advent of the Internet, new and diverse actors have entered the stage, and simultaneously the speed, capacity, and flexibility in the collection, production, and dissemination of information have increased. As decentralized network-based soft power structures have gained in importance, the state’s monopoly on authority has become fragmented, and a plethora of non-governmental organizations, social movements, and other transnational non-state networks are now competing with states for influence. These new contenders rely on the power to persuade a public that is increasingly global, and they are now able to mobilize support for an array of issues, with both good and bad intentions. The huge increase in the number of actors and the potential fluidity of the international political agenda complicate considerably the conduct of statecraft and the formulation of foreign policy.

As a result of the fragmentation of authority and the altered quality of power, the traditional foundations of security have also been turned upside down. The object of security is no longer simply the territorial integrity of the state. The information revolution has dramatically increased the dependence of developed countries on efficient national and transnational information infrastructures. Modern information technologies have brought about new vulnerabilities and risks. In developed societies key critical infrastructures—electricity production and distribution, transportation, financial services, telecommunications, and the water supply—are reliant on information systems and are highly vulnerable. Threats to these structures are less likely to come from so-called rogue states than from hostile non-state actors, such as international terrorists or cyber criminals operating in a relatively opaque cyberspace that has yet to be subjected to effective regulation.

Clearly, the state is not the only international actor that provides public services such as security, welfare, education, and law. The developments of the past decade have led many observers to assume that the forces driving global change are undermining the state and its political agency. However, we are not witnessing the end of the nation state but a return to overlapping authorities. Clearly, the state has to adapt its functions to the conditions of a rapidly changing international environment. Although the growing importance of soft power presents new challenges to the state's traditional monopoly of authority, states still possess sufficient agency to influence the extra-territorial realm of action that the Internet has helped to create. Indeed, the past few years show a clear tendency towards a centralization of power, and states are increasingly acting in this extra-territorial space and are "internationalizing" some of their functions. We believe, therefore, that there is no reason to assume that the Internet is undermining the power of the state and that there is every reason to expect that states will collectively enforce their sovereignty in cyberspace.

The extent to which individual states will meet the challenge of an expanded and highly unpredictable domain of action will vary, not least because of the so-called digital divide. States will have to address potential threats to security that will likely emerge as a result of an unequal distribution of soft power. Countries, regions, and various groups already suffering economic hardship and political and cultural alienation are unlikely to feel the benefits of soft power. Thus, while developed states may be tempted to exploit the opportunities afforded to them by information technologies in order to gain advantages over their rivals, they will have to weigh this against the cost of ignoring their vulnerability to asymmetrical threats. A reduction of security risks will not only entail increased multilateral cooperation but also increased engagement with non-state actors—most notably those in the private sector who own information systems—and with people, states, and regions that already feel marginalized.

The relationship between the Internet and modern international relations is a broad and multifaceted topic. In the present publication we have assembled a series of articles that provide an overview of the scope and complexities of this area of inquiry.

The Growth of Soft Power and the Challenges of Global Governance

The first three articles deal with the broad challenges to governance posed by the growth of soft power. The first, by Giacomello and Mendez, explores the impact of the Internet on state sovereignty. The authors take issue with the widespread presupposition that the Internet entails a diminution of state sovereignty and of the state's importance as an actor. They analyze four areas in which the Internet has affected a shift in state sovereignty: ICANN, the French Yahoo!-court case, taxation on the Internet, and cyber crime. The authors conclude that although the Internet poses new challenges to conventional state authority, the state generally remains the prime negotiator of globalization and of the Internet.

The article by Brown and Studemeister focuses on the effect the Internet has had on the state practice of diplomacy. The authors claim that the empowerment afforded by networks means that states are now required to engage with a variety of non-state actors—influential multinationals, temporary and diverse coalitions, networks of citizens with various allegiances, and other non-state actors—on issues that are increasingly perceived as global and interdependent. The authors examine several recent reports produced by the US foreign affairs establishment and conclude that Washington is heeding the call to bring diplomacy in line with today’s complex and increasingly global environment.

In the third article Zinnbauer addresses the uneven distribution of soft power around the globe. The author focuses specifically on the implications of the digital divide with regard to global governance decision-making. He argues that any attempts to frame the problem in terms of resource and/or skill inequalities are misguided and lead too easily to the conclusion that the participation by grass-roots groups in global governance decision-making is a merely technical issue. The author claims that the biggest obstacle to representation in global governance is the political situation in some developing countries, not the digital divide per se. Here, he suggests, new information and communication technologies can enable grass-roots participation in issues of global governance, for example by allowing information and communication to flow from grass-roots groups to the community and from there to international advocacy groups. The author concludes that the plurality of voices in global governance decision-making depends on a mixture of old and new gatekeepers.

The New Security Challenges of the Information Age

The second set of articles deals with the security challenges posed by the Internet. The first article, by Westrin, examines some fundamental issues related to the protection of critical information infrastructures. The article looks at what or who should be secured, how security should be achieved, and where the responsibility for security will ultimately lie. The author argues that societal information infrastructures constitute an important new object of security. The article outlines the basic differences between conventional and IT-related security threats and discusses the various difficulties involved in appreciating the vulnerabilities and securing a fragmented and continually evolving resource. The article concludes with a short description of the state of critical information infrastructure protection (CIIP) research.

The next article, by Bendrath, centers on the information society as a risk society. The author stresses the novel characteristics of cyber risks: the new weapons are not kinetic but are software and knowledge; the environments in which attacks occur are not physical, but virtual; and the attacker is unknown and can hide during an attack. The author then goes on to explore the US policy response to the risk of cyber attacks on critical information infrastructures. Bendrath shows that although IT-security threats were initially framed in military terms, either as cyberwar or information warfare, the emphasis later shifted, bringing about the need to encourage law enforcement involvement, public-private sector partnership, and public and private self-help strategies. Three factors are identified as responsible for this shift of direction: differences between risk perception in law enforcement and in the private sectors; the private control of technical resources; and the constraining effect of cultural and legal norms.

The aim of the third article in this group, by N•f, is to increase awareness of the vulnerabilities of our information systems. The author does this by explaining several techniques currently used by computer hackers. The article also highlights several insecure aspects of present critical societal infrastructure, suggests some security-related developments, and makes recommendations for improving the security of information systems.

The Human Mind as Battlefield in an Emerging Global Information Environment

The remaining articles are concerned with problems arising from the dual use quality of information systems and the need to regulate the use with bad intent. The first article, by Rathmell, explores the viability of an international regime for controlling computer network operations (CNOs), defined by him as malicious computer-mediated activities. The author identifies a strategic dilemma: States are keen to exploit CNOs to gain an advantage in the military sphere, yet they also need to protect the global information environment on which so many societies depend. Underlying the dilemma are two significantly different ways in which states can understand the policy challenge that CNOs present them with: On the one hand, they might focus their policy on the interdependencies created by network-based power, which in turn have created a need for cooperation in order to ensure trust in and the survival of information systems; on the other hand, they might focus their policy on the strategic advantage that CNOs offer as a new form of weapon in an essentially anarchic environment. The author discerns a decrease in importance of the latter approach in the 1990s and a new emphasis on cooperation between the private sector and government agencies. Yet there is a schism, at the multilateral level, between NATO and the EU: While NATO is seeking to legitimize and make routine use of CNOs, the EU is seeking to de-legitimize cyber attacks and to build robust global information networks. Rathmell concludes that military thinking on CNOs, like that underpinning NATO’s position, misses important truths about the emergent global information environment and is responsible for blocking progress in developing IT-related security regimes.

The second article, by Dunn, explores the growing importance of the Internet in conflict situations. The author discusses the new conflict environment, in which there is a proliferation of voices, and where intelligence gathering, dissemination of information, and mobilization of support are carried out over the Internet. The human mind is thus a prime target on today’s battlefields. The article concludes that information attacks are likely to set precedents in approaches to CNOs, the use of the Internet as a tool of war, and international law. Dunn reminds us that we need to ensure that civilians are not made targets, either in the struggle for hearts and minds or through a possible targeting of civilian installations.

The last article, by Thomas, examines three aspects of civilian and military use of the Internet in China. The author first explores the rapid growth in Internet use by civilians, the information technologies that support the Internet, and the role of Jiang Zemin’s son in the information technology revolution. He also explores the integration of the Internet into military operations, both as a means of mobilizing the emotions of People’s Liberation Army and of providing news. Finally, the article investigates three recent Internet skirmishes in which Chinese citizens have been involved, namely against NATO in April and May of 1999, against Taiwan in August and September of 1999, and against the United States in April of 2001. The author concludes that these are dangerous precedents in cyberspace, where regulation is clearly lacking.

ACKNOWLEDGEMENT. The editor would like to thank Myriam Dunn for her support and enthusiasm for the project. She has always offered her assistance gladly and never failed to be there to see the project through to completion. Special thanks go to Lisa Watanabe, Christopher Findlay, and Michelle Norgate for their invaluable help with the manuscript.

ANDREAS WENGER is professor of international security policy and deputy director of the Center for Security Studies and Conflict Research (www.fsk.ethz.ch) at the Swiss Federal Institute of Technology Zurich (ETH). He has worked extensively in the area of security and strategic studies; US, Russian, and Swiss foreign and security policy; transatlantic relations; and Cold War and international history. His publications include *Living with Peril: Eisenhower, Kennedy, and Nuclear Weapons* (Lanham: Rowman & Littlefield Publishers, 1997), *Russia's Place in Europe: A Security Debate* (Bern: Peter Lang, 1999), and *Nuclear Weapons into the 21st Century: Current Trends and Future Prospects* (Bern: Peter Lang, 2001). He is also the author of a number of articles in scholarly journals and collections of scholarly works. Professor Wenger manages the International Relations and Security Network ISN (www.isn.ethz.ch), a leading knowledge management platform on the Internet in the fields of international relations and security. Within the ISN, he is involved in the Integrated Risk Analysis and the Critical Information Infrastructure Protection projects (www.isn.ethz.ch/crn/index.cfm). *E-mail*: wenger@sipo.gess.ethz.ch .

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Authors: **Giampiero Giacomello and Fernando Mendez**
Title: **“Cuius Regio, Eius Religio, Omnium Spatium?” State Sovereignty in the Age of the Internet**
Year of issuance: **2001**
Issue: **Information & Security. Volume 7, 2001, pages 15-27**
Hard copy: **ISSN 1311-1493**

“CUIUS REGIO, EIUS RELIGIO, OMNIUM SPATIUM?” STATE SOVEREIGNTY IN THE AGE OF THE INTERNET

Giampiero GIACOMELLO and Fernando MENDEZ

Table Of Contents:

1. Introduction

The belief that sovereignty is at the eleventh hour has become more widespread with the progress of the globalization phenomenon. The notion that sovereignty is somehow being transformed by the process of economic globalization and that this is being exacerbated by the Internet—one of the cutting-edge tools of globalization—has become an almost uncritically accepted fact. Large swathes of public opinion in industrialized democracies have been mesmerized by the pervasive equation that more globalization (and more Internet) equals less sovereignty. In this article we attempt to dissect the proposition that more Internet equals a further decrease in state sovereignty. We argue that, while state sovereignty is unmistakably declining, the Internet is, in the best case, one more element contributing to that decline. Indeed, in some instances the Internet can even strengthen sovereignty.

In this article we address the question of whether and how the Internet is affecting/changing states’ sovereignty. Our article for this special issue of *Information and Security* is best conceived as a “plausibility probe.” [1] The purpose of such a study is to enable the investigator to judge whether the potential validity of the explanatory hypothesis (or hypotheses) is large enough to justify a greater effort to produce more decisive hypotheses-testing studies.[2] The fact that the Internet is still somewhat of an unknown topic in many disciplines (including security studies) ensures that any exploratory investigation must proceed with inductive logic. This will allow us to enhance our conceptual tools with the ultimate goal of producing more systematic hypotheses in further studies.

Sovereignty (from the Latin word *super*, above) basically means authority. The notion was first developed by Jean Bodin (1530 -1596) and Thomas Hobbes (1588-1679), who identified it with the authority emanating from the sovereign. More recently, sovereignty has been defined as “... the claim to be the ultimate authority, subject to no higher power as regards the making and enforcing of political decisions. In the international system, sovereignty is the claim by the state to full self-government….”[3] Sovereignty has simultaneously an internal and an external significance, since the concept implies autonomy in foreign policy and exclusive competence in internal affairs.[4] The former attribute is thus indispensable to be a member of the international society of states; while the latter means that that authority is limited/circumscribed by borders (beyond which lays the sovereignty of others) and can be exercised only over the population residing within those boundaries. Scholars have traced the origins of the concept to the Treaties of Westphalia (M•nster and Osnabr•ck) which, in 1648, concluded the Thirty Years War (the title of this article is an explicit reference to the religious diversity also established by the treaties). The treaties established "… a secular concept of international relations replacing forever the medieval idea of a universal religious authority acting as the final arbiter of Christendom." [5] Consequently, from 1648 onwards, the particularistic interests of states became paramount both politically and legally. Given the unconditional authority that characterized the Westphalian conception of the nation-state and sovereignty, it is not surprising that an erosion of sovereignty has been steadily accruing over the centuries. In the end, the diffusion of the Internet is seen by futurologists and many technologists as a "lethal" instrument for states' authority.

2. Towards a Conceptual Framework

The contemporary debates concerning the Internet and sovereignty are characterized by what appears to be an uncanny paradox. While the new Internet technologies favor speed and decentralization, one of the most salient features of the political systems, in which they operate, is that they are simply not set up in this way. Politics tends to be a slow and consensus seeking business, it is usually characterized by uncertainty and an incredible sensitivity to particular interests. How these conflicts are resolved will have a major impact on the development trajectory of the Internet. These two conflicting dynamics are encapsulated by two radically different perspectives on the Internet.

On the one hand, the engineer/technologist perspective, views the Internet as an astonishingly elegant and seamless global information network that transcends national borders. It is because of this transnational technological attribute that the ability of nation states to regulate or control the Internet is severely curtailed, this logically entails an erosion of sovereignty. On the other hand, a regulator perspective, offers a stark contrast. Seen from this perspective, the cyberworld is presently in an anarchic state of nature. Major regulatory fault lines are emerging in relation to areas such taxation, applicable law, copyright and content, to name but a few. Political solutions to this regulatory "chaos" will have to be negotiated and to the extent that nation-states are able to create adequate regulatory regimes this does not necessarily entail an erosion of sovereignty.

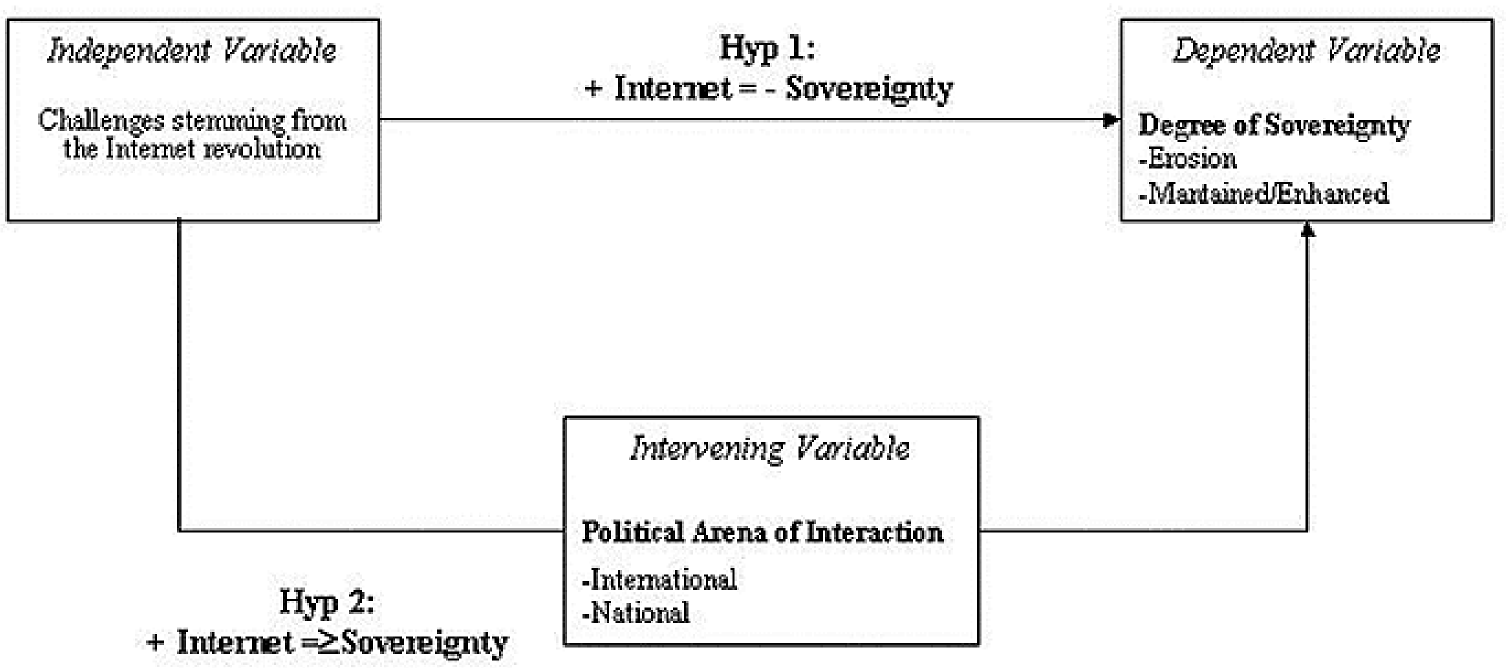
There is of course an obvious danger in polarizing what is an infinitely more complex picture. The research design and conceptualization adopted in this article is intended to principally serve as a heuristic device, it can subsequently form the basis for a more rigorous and systematic formulation of hypotheses. It is an attempt to provide a "photo-type" picture of the current state of affairs concerning the interaction between emerging digital technologies and our institutions of governance. What are the regulatory outcomes that are being produced by this interaction as policymakers respond to the challenges posed by the Internet? Has the technological juggernaut constrained policy-makers options? If this is so then one can justifiably refer to an erosion of sovereignty. Or is the nation-state adapting to this new environment and, if so, with what results?

One way in which this adaptation process works is through the mediation of disparate interests within the arenas of political interaction. The proliferation in the use of the Internet has mobilized a whole host of actors into strategic political action. These actors, ranging from business organizations and civil liberties groups to policy-makers and law enforcers, interact in different political arenas to achieve their desired goals. The outcome of these interactions usually takes the form of new rules. As new rules are created by assigning property rights, by constraining actors choices and by prescribing who can act and when, a regulatory regime begins to emerge and will affect behavior both directly and indirectly. The creation of these rules, which vary across various dimensions of formality and specificity, are central to any discussion of governance and sovereignty. Is it conceivable that as new regulatory regimes emerge, both at the international and supranational levels, states can actually enhance, or at least not suffer a serious diminution of sovereignty? In setting up the problem we are interested in examining the role of the political arena, be it national or international, in shaping regulatory outcomes.

3. Hypotheses and Variables

We can now proceed to translate these ideas into a simple causal argument using the language of variables. These can subsequently form the basis for a set of rival hypothesis that posit distinct outcomes. Our dependent variable is *changes in sovereignty*, and we wish to explain the extent to which the new Internet technologies are producing erosion in states' sovereignty. *Internet technologies* are, therefore, our independent variable. We however add another variable to the analysis, which we have referred to as the *political arena of interaction*. This acts as an intervening variable, and it has a mediating affect between the independent and the dependent variable. Does this intervening variable have a significant effect on regulatory outcomes? Can it be ignored or treated as a residual?

The aim of this—admittedly very simplistic set up—is to attempt to test for the role of the political arena. The simplicity of this set up however is justified by the purpose of this article, which is to be an “exploratory” study on this still rather indefinite and debated topic of Internet and state sovereignty. Having identified the key variables we can now postulate two rival hypotheses that differ with regard to the outcomes (see the diagram).



1) The “techno-driven” or “general belief” hypothesis: the more the Internet grows, the more sovereignty is eroded. Futurologists and large portion of the informed public (the so-called “digerati”) share this view. They maintain that technology has a strong *direct* influence on policymakers’ ability to pursue independent policy. Most techno-driven hypotheses share a similar diagnosis of the futility of attempting to steer technical change. Nicholas Negroponte, [6] one of the Information Age gurus, offers a “rosy” version of the techno-driven thesis. As we move away from the “atom” society to the ‘bit’ (i.e. digital) society the structure of society, the economy and current forms of political organization will be transformed.

One of the chief victims will be the nation-state, which will be unable to withstand the decentralizing, globalizing, and empowering potential of digital technologies. Others, such as Angell, [7] while agreeing with Negroponte as to the irrelevance of political institutions offer a much darker prognosis in which mass unemployment and anarchy will prevail. The defining characteristic of these techno-driven approaches is that they all share a similar conception of the main agent of change and the powerlessness of institutions in the face of technological imperatives. They all point to an erosion of sovereignty.

2) The “politics matters” hypothesis: Internet growth does not inevitably translate into decrease in state sovereignty. It can even lead to an increase. It thus becomes paramount to analyze the “politics” of the Internet growth. This “institutionalist” view does not necessarily treat the technological change as unimportant; rather the influence of that change will be heavily filtered by domestic political and institutional structures.

Policy responses will reflect certain cultural values. There may be a greater likelihood of international conflict in the political economy of the Internet arising, for instance, as a result of differing views as to the role of governments. It may also arise from the way in which interests are articulated within different political systems. Such analyses put the institutional and political framework at the core of the analysis.[8]

4. Cases

To support our argument, hereafter we present four examples of decrease (-) or no-change/increase (≥) in sovereignty. One example of a decrease, online tax (-) and one example of a no-change/increase (≥), Yahoo!. Furthermore, in order to maximize variation on our dependent variable we provide two additional examples, Domain Names and the management of the Internet and cybercrime. These contain elements that can be viewed both as a decrease and an increase in sovereignty. We have selected the cases on the basis of variations of our dependent variable (changes in sovereignty), which is a well-known procedure in social science methodology.[9]

4.1 Domain Names and the Management of the Internet

Since its origins, the Domain Name System (DNS) has determined on-line identities. Clearly, the DNS is vital for the private sector, where brands and trademarks are the key to business success. Companies want their names to be recognized worldwide—including the World Wide Web—and do not want unknown individuals to illegally exploit or meddle with their reputation. On the basis of a Memorandum of Understanding signed with the US Department of Commerce in October 1998 a new organization was born—the Internet Corporation for Assigned Names and Numbers (ICANN)—a non-profit, private sector corporation formed by a broad coalition of the Internet's business, technical, academic, and user communities.

ICANN, along with other similar governance organizations such as the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF) have since become the closest thing that there is to an "Internet government." [10] It appears that governments have surrendered considerable authority to these new organizations, which can powerfully influence Internet development. This in turn can lead to further erosion of state sovereignty. In the case of the W3C, for instance, governments can have the status of "members" just like a corporation or an NGO, with no special privileges attached. This process of "U.N.ization" of the Internet seems to confirm the futurologists' explanation and the general belief that the spreading of the Internet inevitably implies a reduction of states' authority.

This interpretation is only partially correct. In fact, states do "fight back" the loss of sovereignty. EU governments, for instance, have only reluctantly embraced the "privatization" process of the DNS, adopted (to some extents, imposed) by the United States, where the public tends to see the reduction of the federal state's involvement as a positive development. In fact, EU member states have tried to reverse the process, limiting ICANN's unaccountability and independence. The near-adoption of a *.eu* extension for Europe, excluded from ICANN interference is an indication of such attitude.

Other states—including less democratic ones—have adopted the same attitude. China, for instance, has undertaken a "tug-of-war with Western domain-name monitoring and registration firms over who has control of Chinese-language Internet naming rights." [11]The China Internet Network Information Center (a government agency) on 18 January 2000 initiated Chinese domain-name testing system with suffixes of Chinese-language counterparts of .cn, .com, and .net. Western registration organizations have claimed that such decision can pose a threat to the uniformity of Internet addresses. The Chinese government is thus trying to prevent Western influences and business advantage while, at the same time, preserve its freedom of action with censorship. Ultimately, "... the issue has risen alarmingly to the level of a dispute over national sovereignty rather than simple registration activity and concerns over commercial interests." [12]

4.2 Yahoo!

A recent example of a nation state asserting itself concerns the French Yahoo! Court case. It is likely to have important repercussions and has led to an important debate with regard to the governance of the Internet. In April 2000, three anti-racist and Jewish associations (Licra, Mrap and UEJF) lodged a complaint against Yahoo! before a French Court for hosting online auctions of Nazi memorabilia. French law prohibits the exhibition of objects that incite racial hatred. The Court case could be interpreted as something of a test case to see who has the power, and confidence in their legal system, to attempt to regulate aspects of the Internet.[13]

The issue arose in the context of a growing anti-globalization backlash and, in France, was allied with a general perception of the invasion of American culture. Conversely, on the other side of the Atlantic it was seen as yet another manifestation of French intransigence. In France, it was portrayed as a case of whether a nation-state can regulate within its jurisdiction, i.e. prohibit unlawful content, or whether it has to be subject to a set of lowest common denominator laws, i.e. the freedom of speech laws of the US that permit such activity. The French courts decided to hold Yahoo! responsible and gave it three months to block access to the US auction site. A raging debate ensued amongst interested parties as to the merits/flaws of the decision. Yahoo! initially argued that it was impossible to filter every piece of information. Nevertheless, in January 2001 as the profit implications and bad publicity for the company in a lucrative market sank in, it agreed to block the sale of Nazi memorabilia on its auction sites, in effect capitulating to the extraterritoriality of the French Court. The self-censorship marked a significant U-turn by the US portal, which had previously opposed the principle that it should block access.[14]

In a rather prophetic article that was written before the Yahoo!-case, Goldsmith [15] had set out the reasons why unilateral actions were likely to be a much more frequent attribute of the governance of the Internet and the conditions in which it would be successful. He argued that governments can take significant actions to regulate the flow of items within its borders, i.e. by imposing cost on persons and properties within its territories. This could take the form of punishing local assets of foreign content providers or penalizing in-state end-users who obtain foreign content. Although governments will not be able to eliminate all individual transactions they can significantly raise the cost of the activity in question to achieve their desired goals. This is precisely what occurred in the Yahoo!-case. Such events are beginning to explode the myth of the borderless nature of Internet as well overturning some of the more utopian Internet pioneer's "information libertarianism" whose unifying ideal was a desire for unfettered information flows and opposition to any forms of censorship.

4.3 Taxation on the Internet

"No taxation without representation" was a motto of the American Revolution, which implied that the imposition of taxes without proper laws passed in a parliament representing the local constituency was a despised manifestation of absolute monarchs. Indeed, since the origins of the modern state, imposing taxes has been one of the most distinctive features of sovereignty. Although, thus far, electronic commerce is still only a fraction of global trade, governments fear that that prerogative of state power could be severely limited by the fast growth of electronic commerce and began to consider ways in which to tackle such a prospect.

Tax imposition can only work within the precise limits of a state's boundaries. The Internet, among other roles, is also an "international trade route," [16] thus requiring special treatment in terms of taxation (as well as law enforcement, etc.). Quite unsurprisingly, "... the United States Treasury Department has identified the tax ramifications of such high-technology issues as transactions over the Internet as a 'top-priority' international issue ...." [17] Last but not least, to make their action even more problematic, states still use mid-twentieth century tax systems—designed largely for manufacturers and vendors of tangible personal property—to tax a technologically advanced 21st century service industry. [18]

National governments are by no means powerless: they can still track resident individuals and physical goods and tax them. However, several products are already available in digital format (from music to books to films), and this tendency will only increase in the future. It is difficult if not plain impossible (especially if they are all encrypted) to monitor the traffic of these products. The situation is even more manifest with services (including moving money tax avoidance and other criminal shifting of income), which hardly leave traces. Finally, the extreme variety and span of national tax systems makes it extremely problematic to yield international treaties that would satisfy all parties. [19] Nowhere is this more the case than with the current Internet tax state of affairs.

On the one hand, the US wants to maintain the current Internet tax moratorium, while on the other hand the European Commission is keen to apply VAT to Internet transactions. These differences will need to be ironed out and will be subject to intense negotiations. Nonetheless, there is no doubt that the Internet "... presents a serious informational and enforcement crisis to revenue authorities." [20] If governments cannot find a proper mode to answer this challenge, the erosion of the tax basis in the long run could fatally undermine the very existence of state sovereignty.

4.4 Cybercrime

The cybercrime example is illustrative of the interaction between technologies and issues of sovereignty. On one hand, cyber criminals have the potential to operate globally, while on the other hand, prosecuting agencies are bound by the principle of national sovereignty and are limited by national territory, which can only be overcome by slow and bureaucratic means of mutual assistance. Thus, in relation to cybercrime this contradiction makes international and supranational solutions indispensable since the non-coordination of national strategies could result in the proliferation of cybercrime havens. At the heart of the policy is the challenge to ensure basic rights, i.e. privacy and anonymity, while permitting restrictions to these rights in certain circumstances. How is this balancing act being negotiated?

To date some of the measures adopted to combat the potential for cybercrime by some countries have inflamed civil liberty groups both in the US and in the EU. The *Regulation of Investigatory Powers Act* [21] in the UK and the FBI's development of the Carnivore program [22] in the US are clear examples of the privacy concerns raised by legislation and the advances in technology that enhance the surveillance powers of nation-states. Is it possible that by coming together, through multilateral frameworks, nation states can actually enhance aspects of their sovereignty?

The international arena, however, poses problems with regard to issues such as sovereignty and cultural diversity as well as very different traditions of criminal law. To date there has been a degree of international activity on the issue of cybercrime, of which the most significant examples include the G8 Recommendations [23] and the OECD guidelines.[24]

By far the most important multilateral coordination is taking place at the Council of Europe (CoE), which in 1997 began negotiations to draft a treaty on cybercrime. The drafting process was conducted in a closed and secret environment with the first public draft only released in April 2000.[25] The CoE *Draft Convention on Cyber Crime* will be a defining text given that it will constitute the first international treaty on cybercrime. It is based on the premise that the risks related to cybercrime need to be addressed at the international level and, to this end, aims to create a world benchmark or minimum standard in the fight against cybercrime. Indeed, many non-European countries such as the US, Canada, Japan and South Africa actively participate in the drafting process. Most importantly, the process sets itself apart from what is occurring at other international forums such as the G8, OECD and the United Nations due to its binding nature. The draft, as it stands, aims to a) harmonize legislation on what constitutes a cybercrime, i.e. the substantive law issues; b) enhance investigative procedures, i.e. procedural law issues; and c) to develop closer international cooperation.

The aspect of the Treaty, which is most controversial given its enormous implications for privacy, is the section that deals with procedural law, i.e. interception of communications and seizure of computer data by governments. These investigative powers issues have inflamed civil liberties groups and business organizations. For instance, the Center for Democracy and Technology (CDT)—a respected Washington D.C. based civil liberties group—has condemned the unbalanced nature of the Treaty which includes very detailed procedures for interception and seizure mechanisms without any corresponding privacy standards or real limits to government powers. [26] CDT has pointed out the paradoxical nature of the draft, which is not "focused on viruses, hacking or other attacks against computer systems or the computer-dependent critical infrastructures. Instead, central provisions of the Treaty are intended to require governments to adopt laws on search and seizure of computer evidence, disclosure to governments of computerized records of any kind, and electronic interception of communications—*for all kinds of crimes*." [27]

In other words, the major focus of the Treaty is on enhancing the surveillance potential for law enforcement agencies through increased investigative powers. This has led some civil liberties groups to claim that the FBI is using a foreign forum to create an international law enforcement regime. [28] There is certainly some force to this argument given the role of the US Justice Department in the drafting process.

Law enforcement/security agencies have been mobilized into seeking preemptive action, or creating a favorable rule regime to enhance their surveillance and interception powers (not just for Internet crimes but also as a means of combating traditional crimes). The preferred arena, given the nature of the problem, is the international level. At the same time, however, another group of actors pursuing very different agendas have been mobilized to counteract the demands of the law enforcement/security agencies, which are deemed to pose either draconian privacy intrusions or disproportionate financial burdens.

The outcome of these battles between rival interests will be largely determined by the power relations between the competing organizations and the set up of the political arena in which the rules are created. Thus, the political arena can provide for varying degrees of access to power for the respective organizations. For instance, in the case of the CoE Draft Cybercrime Convention the law enforcement/security agencies—given that they had a fist mover advantage—were able to play a dominant role in the drafting of the Treaty text. They therefore played a crucial role in the agenda-setting process.

5. Conclusions

To review the central argument and by way of conclusion let us briefly revisit the hypotheses. We have argued that the simplistic proposition that more Internet equals less sovereignty seriously underestimates the ability of the nation state to adapt to a given technological reality. Thus, all we claim, at this early stage, is that nations do seem to be responding and that these responses will tend to have an influence on the development trajectory of the Internet. Whether developments in the technological domain will find a way to circumvent onerous policy decisions is, for the moment, a separate research question. The serious research agenda is to explain the conditions in which a nation state can assert itself and those where it is more difficult.

Our Yahoo! and cybercrime examples demonstrate that under certain conditions, i.e. where a nation state can punish an alleged transgressor's asset base or where agents of the nation state such as law enforcers enjoy agenda setting powers, the simplistic view of the techno-driven hypothesis begins to breaks down. Conversely, the taxation and ICANN examples are illustrative of instances where sovereignty can be called into question. Nevertheless, even in these latter cases it seems that the nation state may have more room for maneuver than is commonly assumed. The increasing politicization of ICANN's organizational structure and looming transatlantic differences with regard to online taxation suggest that politics still matters. The simplistic equation that we set out to examine should be reformulated along the following—equally simplistic but perhaps more accurate—lines: More Internet equals more politicization. We believe that examining the nature of this politicization, and the conditions in which it entails an erosion of sovereignty, constitutes a much more fruitful research agenda.

Defense operational requirements for communications support are derived from the development and fielding of warfighter information systems such as the Battlefield Command System and information services such as collaborative planning, information assurance (IA), and battlefield video teleconferencing (VTC). Non-Defense operational requirements are derived from information services such as collaborative planning, information assurance, and operational video teleconferencing (VTC). The throughput requirements and speed of service demanded by these operational requirements have made the current communications networks obsolete.

Notes:

1. Harry Eckstein, "Case Study and Theory in Political Science," in *Handbook of Political Science, vol. 7: Strategies of Inquiry*, ed. Fred Greenstein and Nelson Polsby (Reading MA, et al.: Addison-Wesley, 1975), 79-137.
2. Alexander L. George, "Case Studies and Theory Development: The Method of Structured, Focused Comparison," in *Diplomacy: New Approaches in History, Theory and Policy*, ed. Paul G. Lauren (New York: Free Press, 1979), 43-68.
3. Barry Buzan, "Sovereignty," in *The Concise Oxford Dictionary of Politics*, ed. Iain McLean (Oxford and New York: Oxford University Press, 1996), 464.
4. George Evans with John Newnham, *Dictionary of International Relations* (London: Penguin Books, 1998), 504.
5. Evans, *Dictionary*, 572. It should be noted that the concept of sovereignty was intended to be applied only to European, Christian states (later including North and Christianized Latin America), thus excluding state-like communities in Africa, Asia from benefiting from it. Furthermore, both Bodin and Hobbes lived during periods of intense clashes in the name of religion.
6. Nicolas Negroponte, *Being Digital* (New York: Knopf, 1995).
7. Ian Angell, "The Real Politik of the Information Age," *Information Strategy* (January 1998).
8. In many respects the hypotheses that have been postulated above mirror those that are fielded in the globalizations literature. The literature seems to be characterized by a similar continuum that ranges from the 'overt' thesis (the role of the nation-state in the international system has been fundamentally undermined) to the 'myth' type thesis (whereby globalization is exaggerated and nation-states have not lost their policy making autonomy).
9. See, for instance, Gary King, Robert O. Keohane, and Sidney Verba, *Designing Social Inquiry* (Princeton, NJ: Princeton University Press, 1994).
10. "Regulating the Internet," *The Economist* (June 10, 2000), 99-101.
11. Gartner Group, "A Domain-Name Battle Puts Business with China at Risk," *The Monthly Research Review*, (March 17, 2001; June 10, 2001). Available @ http://www4.gartner.com/1_researchanalysis/0301mrr.pdf .
12. Gartner Group, 17.
13. There was an earlier similar high profile case in which a Bavaria Court prosecuted Compuserve executives in relation to anti-pornography rules.
14. Jean Eaglesham, "Yahoo! Bans hate propaganda," *Financial Times* (January 3, 2001), 12.
15. Jack Goldsmith, "Unilateral Regulation of the Internet: A Modest Defence," *European Journal of International Law* 11, 1 (2000): 135-148.
16. Zak Muschovitch, "Taxation of Internet Commerce" (April 26, 1996; June 12, 2001). Available @ http://www.iprimus.ca/~zak/Taxation.html#note2.
17. "International Taxes: Financial Services, Internet, Among Top Foreign Issues, Treasury Department Official Says," *Daily Tax Report* (Taxation, Budget and Accounting, January 19, 1996), The Bureau of National Affairs, Inc., quoted in Muschovitch, "Taxation of Internet Commerce."

18. Karl Frieden and Michael Porter, "The Taxation of Cyberspace," *Cal-Tax Online* (December 1996; June 13, 2001). Available @ http://www.caltax.org/andersen/contents.htm.

19. The OECD has a "Model Tax Convention" that is highly successful (almost 2000 conventions are based on this model), but the model is used to eliminate double tax imposition, and is not tailored for the specific needs of electronic commerce. See http://www.oecd.org/daf/fa/treaties/treaty.htm.

20. Muschovitch, "Taxation of Internet Commerce."

21. The Regulation of Investigatory Powers Act was passed into UK law on the 27th July 2000. It was a controversial bill that contains sweeping powers, which cover the interception of communications, intrusive surveillance, human intelligence sources, and the compulsory disclosure of encrypted data.

22. Carnivore is a powerful computer program designed by the FBI to intercept Internet communications.

23. In 1997, the G8 adopted a number of principles and a common action program against high tech crime.

24. Further information on the OECD policy guidelines, for cryptography, privacy and security is available @ http://www.oecd.org/dsti/sti/it/secur/index.htm.

25. Available @ http://conventions.coe.int/treaty/en/projets/cybercrime.htm.

26. Comments of the Center for Democracy and Technology on the Council of Europe Draft "Convention on Cyber-crime" (Draft No. 25), Center for Democracy and Technology (CDT), February 6, 2001, June 29, 2001, available @ http://www.cdt.org/international/cybercrime/010206cdt.shtml

27. See CDT, emphasis in the original.

28. Comments from IP Worldwide available @ http://www.law.com.

GIAMPIERO GIACOMELLO has just completed his Ph.D. with the Department of Social and Political Science of the European University Institute with a dissertation on governments' control on the Internet, and is currently principal investigator on a project on "forgotten wars" with *Caritas Italiana*, Italy's most important NGO. Since 1996, he has been Visiting Professor of Political Science at the Center for European Studies of the Dickinson College, Bologna (Italy). His research interests cover research methodologies, computer networks and international relations. Giampiero Giacomello graduated (with a B.A. Hon) from the University of Padova and holds an M.A. in international relations from the Johns Hopkins University P.H. Nitze School of Advanced International Studies (SAIS). E-mail: giampiero.giacomello@iue.it.

FERNANDO MENDEZ is Ph.D. candidate with the Department of Social and Political Science of the European University Institute of Science. He holds a MSc. in European Politics from the London School of Economics and is conducting research on US and EU policy responses to cybercrime and e-commerce. E-mail: fernando.mendez@iue.it.

BACK TO TOP

“Cuius Regio, Eius Religio, Omnium Spatium?” State Sovereignty in the Age of the Internet

Giampiero Giacomello and Fernando Mendez

Keywords: Internet, globalisation, Internet and governance, Internet and state sovereignty/authority.

Abstract: The belief that sovereignty is at the eleventh hour has become more widespread with the progress of the globalization phenomenon. The notion that sovereignty is somehow being transformed by the process of economic globalization and that this is being exacerbated by the Internet—one of the cutting-edge tools of globalization—has become an almost uncritically accepted fact. Large swathes of public opinion in industrialized democracies have been mesmerized by the pervasive equation that more globalization (and more Internet) equals less sovereignty. In this article, we attempt to dissect the proposition that more Internet equals a further decrease in state sovereignty. We argue that, while state sovereignty is unmistakably declining, the Internet is, in the best case, one more element contributing to that decline. Indeed, in some instances the Internet can even strengthen sovereignty. Two hypotheses have been considered: the first—the “technologist/general belief”—summarizes the view of several futurologists and technologists as well as many informed individuals. Their main claim is that the more the Internet grows, the more sovereignty will decline. The second hypothesis—“politics matters”—points out that circumstances are more complex, and that the Internet growth does not immediately translate to eroding states’ authority, but can even increase it. It is thus imperative to analyze the process of “politicization” of the Internet in order to identify the correct causal explanation. We have analyzed four cases in which the Internet has contributed to increasing and/or decreasing sovereignty: ICANN and other non-governmental organizations of Internet governance, the French Yahoo!, taxation on the Internet and cybercrime. The four cases appear to support the validity of our second hypothesis. We have however been careful in considering this paper as an “exploratory study” of the problem of Internet and sovereignty, which, in fact, require more detailed research to produce conclusive evidence.

full text

Authors: **Sheryl J. Brown and Margarita S. Studemeister**
Title: **Virtual Diplomacy: Rethinking Foreign Policy Practice in the Information Age**
Year of issuance: **2001**
Issue: **Information & Security. Volume 7, 2001, pages 28-44**
Hard copy: **ISSN 1311-1493**

VIRTUAL DIPLOMACY[1] : RETHINKING FOREIGN POLICY PRACTICE IN THE INFORMATION AGE

Sheryl J. BROWN and Margarita S. STUDEMEISTER

Table Of Contents:

Authors' note: The following article was written in August 2001, a month before the September 11 terrorist attacks against the United States. It, therefore, does not take into account many of the subsequent enhancements of the U.S. security apparatus. It does, however, identify prescient thinking about what comprises security in an increasingly interconnected world, thinking that ultimately informed much of the current administration's policies.

1. Introduction

In the first week of the presidency of George W. Bush, former Defense Secretary and National Security Advisor Frank Carlucci visited newly appointed Secretary of State Colin Powell, urging him to implement cutting-edge information technology and modern management practices to renew a department, in Carlucci's words, "in an advanced state of disrepair." Days later, a commission led by two former senators, Democrat Gary Hart and Republican Warren Rudman, offered a sweeping blueprint for transforming the national security structure of the United States, warning that "without significant reforms, American power and influence cannot be sustained." These two initiatives to revive what has been viewed as a crippling diplomatic bureaucracy come at the heels of a dozen studies, criticizing the Department of State for its staunch adherence to obsolescence—centralized decision-making, obsessive secrecy and outdated technology. This view was also evident in a letter signed by about 1,500 State Department employees, affirming that the department is unfit to meet the emerging foreign affairs challenges and calling it “the weak link in the national security chain.” At the core of the recent string of criticisms lies a paradigm shift in the diplomatic environment, influenced by the advent of revolutionary information and communications technologies. This shift has rendered irrelevant the traditional diplomacy still practiced at the department and its diplomatic missions abroad. The purpose of this article is to review some of the recommendations of experts for restructuring foreign affairs practices by the United States in light of the trends shaping the diplomatic environment.

First, however, consider the practical enormity of the reinvention, reform, and reengineering task for the United States in terms of its Department of State alone. At the turn of the century, the United States had relations with some 180 nations, maintaining about 260 posts, including embassies, consulates and other offices—some employing less than a dozen people, others more than 2,000. About 9,000 citizens and some 30,000 foreign nationals work in those posts, and over 30 government agencies are represented abroad. At headquarters, the secretary of state oversees five undersecretaries who together manage 27 regional, functional and administrative bureaus and offices, employing nearly 6,500 people. While the costs involved in the modernization of the conduct of diplomacy may be high, inattention to the vociferous calls for change would prove an even riskier gamble in the long run.

2. The Changing International Environment

Traditional diplomacy, according to Canadian diplomat Gordon Smith, is the art of advancing national interests by the practice of persuasion.[2] Today however not only the context but also the content of diplomacy has radically altered. The context of persuasion has expanded to include anyone anywhere connected to and affected by any of the information and communications media. And, even more disorienting, the realm of national interests now includes at the very least global economics, and, increasingly, international migration, environmental crises, terrorism, drug trafficking, weapons proliferation, and cyber harassment, all of which pose global threats but are suffered immediately and most profoundly at the local level. Therefore diplomacy, the practice of foreign affairs, is a subset of domestic policy, which is itself shaped by the expanded agenda of national security.

Twenty years ago, Robert Keohane and Joseph Nye labeled this new globalized epoch “complex interdependence.” [3] While acknowledging their prescience, they nevertheless point out in their subsequent 1998 *Foreign Affairs* article on the subject that information and communications technologies have not entirely transformed world politics to complex interdependence.[4] Why? Because information does not flow in a vacuum but in an already occupied political space; and because, outside the democratic zone of peace, the world of states is not a world of complex interdependence. Collective affirmations of primary identities have recently swelled around religion, nation, ethnicity, locality, all of which tend to break up societies based on negotiated institutions in favor of value-founded communities. Nevertheless, most experts recognize that complex interdependence has become increasingly costly for states to ignore. Prudent states play by the rules required by both old patterns and new constructs. This cannot be stressed strongly enough.

We are all too familiar with the old patterns, but what characterizes the new construct? According to James Rosenau, we are undergoing a decentralized fusion of global and local interests, which he calls "*fragmegration,"* a concept that juxtaposes the processes of fragmentation and integration occurring within and among organizations, communities, countries, and transnational systems such that it is virtually impossible not to treat them as interactive and causally linked." With fragmegration comes the dispersion of authority away from states and the growing role of decentralized governments, nongovernmental organizations, media, social movements and other transnational non-state networks as primary international actors.[5] What seems most to characterize this transition period and perhaps the emerging paradigm is the profusion of asymmetrical relationships between state and non-state actors, including activities sponsored or carried out by such diverse supra-individuals as software mogul Bill Gates, global financier George Soros, globetrotting diplomat and former US President Jimmy Carter, media emperor Ted Turner, and terrorist mastermind Osama bin Laden.

The new contenders for international power are information mobilizers that coalesce around issues and augur ill or well depending on one's point of reference in the global network. These contenders are most notably represented by the already internationally powerful multinational corporations and loose communities and coalitions of non-governmental and international organizations, citizens and groups displaying a variety of allegiances, including expatriates and diasporas. Although they do not have the official power to recognize or withhold recognition from states, with leverage bolstered—because extended and accelerated—by an able use of networks, they often influence states to do so. Loose coalitions, in particular, represent the international public at its most mobilized and articulate. One need only think of the landmine ban campaign, which effectively established a global policy on the basis of pressure from a network of diverse groups scattered around the world. The lack of group or community homogeneity and hierarchy among these global, popular campaigns confounds states and foreign ministries. All too often, they scramble to project an authoritative position—via competition or cooperation, or both—in this fluid international landscape.

Few thinkers have understood and written about the dialectic that informs the political transition from territory-based power to network-based power as well as French diplomat and political philosopher Jean-Marie Gu•henno. In *The End of the Nation-State* he declares, "Territorial sovereignty is no longer sacrosanct." "We have lived in the two-dimensional world of territorial power," Gu•henno asserts, "and we are entering what one could call the three-dimensional world of network power." The integrity, power, and security of the nation-state are challenged by multinationals from above and by ever-shifting coalitions of networked interest groups from below. The ability of nation-states to tax and to require duties associated with citizenship—the basis of a state's power, its treasure and its armies—is seriously threatened by opportunities afforded by information and communications technologies. On the one hand, responding to economic opportunities, multinationals locate themselves in tax friendly environments regardless of "national interest." On the other hand, individuals live conveniently or by force of economics or politics as expatriates and diasporas all over the world. Both exert political pressure not only on their native countries but also on other nation-states as well.[6]

The reigning political requirement within this shifted international paradigm is transparent and accountable governance. Transparency necessarily guides not only official relationships but also the relationships between public and private sectors and among individuals. Because each state's public has expanded far beyond the state's geographical borders and its collective values, each state, by way of accessing its citizens far and wide, renders itself accountable to all publics, not least of which is the indefinite but potent international community. The appearance of official transparency is required and at the same time states have realized that the playing field has so flattened that they must pitch their case before all of these publics, including even such individuals—the same as any other viewing constituency—like Iraqi President Sadaam Hussein or North Korean leader Kim Jung Il, who represent nations considered as sponsors of international terrorism by the United States. Thus, the potency of regimes stands or falls according to public opinion polls derived from what Gu•henno calls the mediazation of a wired world.

Although fragmegration threatens nation-states' conventional hold on power, savvy states should recognize these new conditions as an opportunity to implement revolutionary approaches to global affairs strategies and management. To date however, nation-states, confused by their loss of authoritative hold on conventional power, do not yet recognize that power as such is not devolving to other institutions but to the means to coalesce in order to pursue common interests. What states lose in control, they could regain in influence.

Thinking differently about the nature of power is perplexing to say the least. The Information Age-fostered "hard power" (or coercion) versus "soft power" (or persuasion) distinction has turned conventional theories about national security inside out. Popular persuasion in lieu of hardball coercion is neither an easy sell to nation-states (beyond a necessary overlay for optics in the toolbox of national defense) nor once grasped, learned and implemented with aplomb. According to this perspective, today, having the means to promulgate the most persuasive information to the most people the most rapidly turns out to be as important, if not more important, than a first-strike weapon system. Above all, access, information, and connectivity are essential components of wielding this new power to influence. This particular power is evanescent, associated with recognizing and pursuing a common objective, then re-forming with another collective or group in order to actualize another objective. Not so easy for a state to develop and manage a deliberately fluid and inconstant set of policies to govern theaters of operation from the local to the global.

Rosenau describes this coalescing phenomena as "spheres of authority" (SOA). He argues that SOAs have begun to supercede nation-states in terms of mobilizing and wielding effectual power.[7] Gu •henno portrays this phenomenon as the principal dynamic of a new "imperialism," which he likens to Rome's loose global empire. Instead of an authentic political space, collective solidarities will form and dissolve based on dominant perceptions and resulting interests—like multiple organisms, they morph protean-like according to conditions and needs. "It is a field of forces, of imbalances, in which the will to increase the number of one's connections is counterbalanced by the fear of losing control of the networks that have already been set up … a gigantic stock exchange of information that never closes," writes Gu•henno. "The more information there is," he continues, "the more imbalances there are: as in a great meteorological system, a wind that creates a depression here, causes high pressure elsewhere."[8]

In a similar vein, Information Age analysts John Arquilla and David Ronfeldt observe that diplomats will have to realize that a new realm is emerging—the noosphere, a global "realm of the mind"—that may have a profound effect on statecraft. Second, they say that the information age will continue to undermine the conditions for classic diplomacy based on realpolitik and hard power and will instead favor the emergence of a new diplomacy based on what they call noopolitik (nu-oh-poh-li-teek) and its preference for soft power. Noopolitik, they write, is an approach to diplomacy and strategy for the information age that emphasizes the shaping and sharing of ideas, values, norms, laws, and ethics through persuasion. “Both state and non-state actors may be guided by noopolitik; rather than being state-centric,” argue Arquilla and Ronfeldt, “its strength may well stem from enabling state and non-state actors to work conjointly.” “The driving motivation of noopolitik cannot be national interest defined in statist terms,” they opine. “Realpolitik pits one state against another,” conclude Arquilla and Ronfeldt, “but noopolitik encourages states to cooperate in coalitions and other mutual frameworks.”[9]

Noopolitik is an approach to statecraft that can be undertaken as much by non-state as by state actors. Noopolitik makes sense in today’s networked world because knowledge is the coin of the realm, permeating the multiple levels of the local to global infrastructure in ways that classic realpolitik cannot rival. That said, governments are currently structured to conceive, plan, and operate according to realpolitik within an exclusive nation-state construct. How will they, particularly the United States, make the transition between realpolitik and noopolitik policymaking and practice?

3. Peering into the Crystal Ball: Threats and Conflicts Up to 2015

If we accept the findings of intelligence analysts and independent experts, globalization and the quality of governance are shaping the diplomatic environment. Thus, transnational issues and an increasingly interconnected world require governments to develop greater communication and collaboration between their national security and domestic policies, according to this recent National Intelligence Council report entitled *Global Trends 2015: A Dialogue About the Future with Nongovernment Experts*. Furthermore, cooperation will be essential to identifying threats and to developing interdisciplinary responses to counter them.[10]

Information and communications technologies have profoundly contributed to transform the international system and not all to the good. These technologies will continue to drive the global economy, to empower non-state actors, as well, the report warns, as to facilitate illegal and destabilizing activities by rogue states, organizations and individuals. Moreover, the networked global economy distributes information, ideas, values, capital, goods and services to people unevenly. Its reach and benefits are not available to groups, countries and regions already facing economic stagnation, political instability and cultural alienation. Further distancing from the values and conventions that in effect hard-wire the world’s liberal democracies exaggerates the destabilizing conditions and violent expressions of political, ethnic, and religious extremism. Even advanced nations however will be at risk of succumbing to financial volatility and enduring a widening economic gap as they become increasingly interdependent. As a result, the United States and other developed nations will be drawn to focus on “old-world” problems at the same time as focusing on managing the “new-world” challenges.[11]

3.1 What Kinds of Threats and Conflicts Loom Ahead?

War among northern developed countries is unlikely in the future. Far more probable are frequent small-scale internal upheavals to less frequent regional interstate wars among southern developing countries. For instance, regional rivalries and antagonisms such as India-Pakistan and the Middle East will demand the attention of the international community. Internal conflicts tied to religious, ethnic, economic or political identities will remain at current levels or possibly increase. Illegal and destabilizing activities by disaffected nation-states, terrorists, arms dealers, drug traffickers and organized criminals can escalate, and the lethality of these conflicts can increase, given the availability of weapons of mass destruction, longer-range missile delivery systems and other technologies diffused or transferred unhampered across porous geopolitical borders and into their hands.[12]

Occupied with domestic issues that easily take precedence over messy international crises, which offer costly no-win engagements, developed nations will minimize their direct involvement by delegating to the United Nations and regional organizations the management of such conflicts. Growing transnational problems will require international or multilateral cooperation to handle a range of issues from economic volatility, migration, scarce resources, humanitarian, refugee and environmental crises, terrorism, all the way to cyber threats. When the international response fails, the United States will be called to broker solutions, negotiating with a wide array of state and non-state actors.[13]

The report concludes that although nation-states will continue to have a dominant role in the international system, governments will have diminished control over flows of information, diseases, migrants, weapons and financial transactions across their borders. The fate of nation-states will increasingly be linked to adaptation to the emerging global trends and to the quality of governance provided to citizens. Effective governance, in turn, will depend on the ability and agility of nation-states to engage in partnerships with non-state actors to exploit the opportunities and manage the vulnerabilities and threats in the globalized diplomatic environment.[14]

4. Institutionalizing Change: The Current State of US Diplomacy and Beyond

The two most recent calls for reform among the US foreign policy agencies, Carlucci's State Department reform proposal [15] and the *US Commission on National Security/21st Century Report*,[16] saw the light of day at an opportune time, coinciding with newly inaugurated President George W. Bush's appointment of new secretaries of state, defense, and treasury, and a national security advisor. Each proposal is the latest in a recent surge of attention to the lack of alignment between the prevailing international conditions and these foreign affair agencies' Cold War mission, practices and tools. Each proposal builds on the findings of preceding reports; accordingly, the views and recommendations made in the two pioneering reports, *Reinventing Diplomacy in the Information Age*, published by Center for Strategic and International Studies (CSIS) [17] and *Equipped for the Future: Managing U.S. Foreign Affairs in the 21st Century*, funded by the Henry L. Stimson Center, [18] both in October 1998, are adopted, adapted, and extended in the Carlucci and national security commission 2001 reports.

Reinventing Diplomacy is the product of a blue-ribbon panel under the able direction of a former administrator of the now-defunct United States Information Agency, Barry Fulton. The panel's report recommending drastic reforms in the culture, management, priorities, and information and communications technologies at the State Department has clearly influenced the Carlucci report. *Reinventing Diplomacy* offers six strategies to turn around the antiquated practices of the foreign affairs department. It calls for an end to the culture of secrecy and exclusivity that shrouds diplomatic practice, by placing greater emphasis on public awareness and opinion and on broader participation and networking, while balancing the requirements of security and openness. The second and third strategies involve reforms of management and human resources practices—replacing the hierarchical structure with a network management model, and overhauling workforce policies. These changes require a concomitant information technology strategy. The last two proposed strategies define the strategic priorities of diplomacy. Namely, the report emphatically recommends engaging publics at home and abroad and promoting US policies and values, as well as expanding global markets and supporting US businesses in activities abroad, as ways of advancing the national interests of the United States in a globalized environment.[19]

In a complimentary mode, the Stimson Center's *Equipped for the Future: Managing US Foreign Affairs in the 21st Century* makes a vigorous appeal for international engagement and a corresponding State Department reform. If "America is to be engaged in the world as it must," the report explains, "then the real questions become how it must be engaged, and what structures and institutions will most efficiently and effectively allow the nation to achieve its goals." At one point, it calls for an expanded and more inclusive promotion of national interests abroad, including tapping into, engaging with, and supporting the myriad individuals and groups conducting international relations—business people, governors and mayors, sports and entertainment figures, charitable and humanitarian organizations. It concludes with a sobering admonition to Congress about providing stable and adequate levels of funding: "Diplomacy on the cheap," the report warns, "is simply failed diplomacy," adding that "it costs money to maintain peace—that is, knowing how, when, and with whom to make the person-to-person contacts to persuade, cajole, and influence decisions in the direction of peace." Especially noteworthy in terms of the ultimate influence these two reports had on the current administration was the participation on the Stimson Center panel of Frank Carlucci, Condoleezza Rice and Colin Powell—the latter two, the new Bush administration's national security adviser and secretary of state, respectively.[20]

The report of the US Commission on *National Security/21st Century* attempts to meet the profound challenges facing conventional notions about national security implicit in the two earlier analyses. National interests and national security are the counterpoint of the nation-state's foreign policy agenda, which is itself a subset of domestic policy as that policy responds to the reality of our complex global interdependence. In other words, all government agencies in some way conduct foreign affairs and are thus foreign affairs agencies. In the commission report preface, Gen. Charles Boyd, executive director of the commission, underlines the gravity of the stakes at risk and the boldness required to meet the challenge, as he describes the commission's mission:

> "[T]hinking out a quarter century, not just to the next election or to the next federal budget cycle. … searching out how government *should* work, undeterred by the institutional inertia that today determines how it *does* work … conceiving national security not as narrowly defined, but as it ought to be defined to include economics, technology, and education for a new age in which novel opportunities and challenges coexist uncertainly with familiar ones."[21]

The commission, a 14-member expert body, was charged to take a broad view of national security during a three-year, phased process. Convened in 1997, it is the first commission to conduct an overall review of national security strategy since 1947. It sought to reverse what it perceived as the loss of global influence and critical leadership by the United States. Pointing out that "dramatic changes in the world since the end of the Cold War of the last half-century have not been accompanied by any major institutional changes in the Executive Branch," it deplores the lack of a comprehensive national security strategy to guide policymaking and resource allocation. The report decries several interrelated trends—the policymaking role that the National Security Council has gradually assumed, the continued predominance of military concerns driving the intelligence community in the post-Cold War period, the growth in size and activities and failure to privatize many support activities of the Department of Defense. It is time, the commission emphasizes, for an overarching strategy to drive the development and implementation of national security policy under the leadership of the president and in accordance to a national security budget, "focused on the nation's most critical strategic goals."[22]

That "new age" according to the commissioners requires that multilateral cooperation govern policy formulation and implementation. Recognizing the United States has a special international role because of its power, wealth, and interests, the commissioners point to the cultural and political values that promote political pluralism, freedom of thought and speech, and individual liberty that make the United States first among equals. They hastily add however that

> "as the prime keeper of the international security commons, [the United States] must speak and act in ways that lead others, by dint of their own interests, to ally with American goals. … If it is too arrogant and self possessed," affirm the commissioners, "American behavior will invariably stimulate the rise of opposing coalitions … Tone matters."[23]

In other words, noopolitik and soft power are the means by which global stability, thus national interests, is secured and national security thereby maintained.

To date, this report is the most comprehensive and far-reaching, sounding themes reminiscent of Rosenau's fragmegration and Gu•henno's three-dimensional world of network power, and proposing overarching objectives for US foreign and national security policy. While maintaining "homeland defense," the commission advises, the US government should ensure "social cohesion, economic competitiveness, technological ingenuity, and military strength." It should also seek the integration of the key major powers, particularly China, Russia and India, into the mainstream of world politics, as well as promote, along with others, the networked global economy and contribute to the effectiveness of international institutions and international law. Alliances and other cooperative mechanisms must be adapted to partners who are interested in affirming their autonomy and responsibility. Ultimately, the commissioners assure us, the United States will be best served by supporting international efforts designed to tame the disintegrative forces at work everywhere.[24]

Two particular areas illustrate the commission's understanding of what is risked if sufficient attention is not paid to current global changes. First, emphasis of "homeland defense" strategies could appear curious in the context of a serious appreciation for the effects of globalization except that physical borders and cyber borders have become more, not less, critical in protecting the infrastructures that allow the global economy to flourish. As important as the geographical integrity of the homeland is, cyber integrity links us with the rest of the globe. The geographical and the cyber entities are today inseparable. Community is lived both physically and virtually, horizontally and vertically. We are irretrievably *fragmegrated*.

The second area that receives emphasis is national education, which the commissioners go so far as to characterize as in a state of crisis. Such emphasis is reminiscent of President John F. Kennedy's concern for education as a national security issue, charging his generation to prepare to put a man on the moon. Of course, his injunction came during the hottest period of the Cold War and at time when space exploration had become a major area of contest, commonly known as the space race. The Soviet Union had launched the world's first artificial satellite in 1957, revealing a technological gap that provided the impetus for increased funding not only for aerospace endeavors, but more broadly, for technical and scientific education. This commission's call to arms is no less urgent.

National homeland defense and science education enhancement are two recommendations, which, if not understood within the context of the commissioners' overall thinking, could seem tired, even retrospective. In fact, they are the opposite and need serious, immediate attention by all US citizens, not just the government. The commission's other recommendations single out specific governmental branches as needing top to bottom reform to reengineer themselves to plan and react more coherently, efficiently, and effectively. To that end, the commission's last recommendation reminds us of the nearly forgotten, but critical role Congress plays in foreign policy development and implementation. Here the commission recommends a full review of the role of Congress in national security and foreign policy, with the objective of streamlining the budgetary process and oversight responsibilities and improving continued consultation and coordination required between the executive and legislative branches of government. This recommendation dovetails with the Carlucci report, which puts as much emphasis on congressional responsibility in guiding the State Department's reform as it does on the reform it calls for at State.

Sponsored by the Council on Foreign Relations and CSIS, Carlucci's Independent Task Force on State Department Reform inextricably ties the future successful retooling of State to Congress' oversight, making both accountable to each other and to US citizens. Carlucci's "resources for reform" plan has reportedly gathered support from Powell and members of Congress, leading to, if not optimism then, a degree of guarded hope for change. According to this plan, substantial resources will be necessary for reform inasmuch as reform will be necessary to obtain resources from Congress. It is an exchange arrangement whereby the State Department would receive the considerable funds to upgrade computers, telecommunications and security in exchange for streamlining the department's management, rebuilding its credibility as the center of foreign policy-making and implementation, and improving coordination with Congress.

The report of the task force led by Carlucci recognizes that current interagency coordination for policy development and implementation is ineffective. Additionally, bifurcation of policy-making and budget management, a culture of secrecy, low morale, inattention to staff recruitment and development, obsolete information and communications infrastructure, dilapidated and insecure facilities, and the diminished authority of ambassadors to oversee resources and staffs of many agencies housed in missions abroad plague the department. Persuading both sides of the exchange relationship would be a Herculean task even for a secretary of state of Powell's prestige and admitted interest in information and communications technologies.

Powell is said to be an avid user of the Internet and believer in the power of information and communications technologies to transform individuals, organizations and strategies through the exchange of ideas.

> "As a member of the Board of Directors of one of these transforming companies, America Online, I had a unique vantage point in which to watch the world start to transform itself," he testified to Congress. "America Online and its various services have over 100 million people connected electronically," Powell added, "[t]hey can Instant Message; they can e-mail; they can trade photos, papers, ideas, dreams, capital, likes and dislikes, all done without customs posts, visas, passports, tariffs, guard towers or any other way for governments to interfere."[25]

What is needed, exhorts the Carlucci report, is a presidential directive on foreign policy reform to emphasize that such reform is a top national security priority: "No government bureaucracy is in greater need of reform than the Department of State." Other findings call for issuing guidance to reaffirm the role of the secretary of state as the principal adviser to the president on US foreign policy and as the director of a department responsible for foreign policy-making and implementation; reinforce the ambassador's coordinating authority in their missions abroad; and reinstate the national security advisor as the principal coordinator who oversees and integrates the various elements of a national security policy and its budget.[26]

These reports necessarily involve more than the Department of State as their foci in their discussion of needed reform in the US foreign policymaking institutions. These include the US Congress, National Security Council, and US Agency for International Development. So, too, the Department of Defense, and the implications of its own internal reviews, merits a fuller discussion of its role as a foreign policy implementer. That discussion, however, is beyond the scope of this paper.

5. Seizing Foreign Affairs Reforms: What, When, and How Much?

Since the inauguration of President George W. Bush, actions taken by the White House and debates in Congress suggest that the time for foreign affairs reform has finally arrived. The fate of its depth, extent and ultimate impact remains in the hands of the leading national security decision-makers and implementers. Presently, the reorganization of the National Security Council and the willingness of members of Congress to invest in the modernization of the State Department reflect an acknowledgement of the need to reorganize, driven mostly by perceptions of threats and conflicts in the global environment. But, why would reform work now? In congressional testimony, Carlucci optimistically summed it up: "You've got the right leadership. You've got the right Congress. It's the right time."[27]

Less than a month after taking office, on February 13, 2001, Bush issued his first National Security Presidential Directive (NSPD-1) on the subject of the organization of the National Security Council (NSC), defining national security as "the defense of the United States of America, protection of [the country's] constitutional system of government, and the advancement of United States interests around the globe."[28] It reaffirmed the advisory role of the NSC and its focus on "the integration of domestic, foreign, and military policies relating to national security," according to the National Security Act of 1947, as amended.

The recent structural modifications to the NSC, also spelled out in NSPD-1 reflect, as in past presidential administrations, management styles, personal relationships and, in this discussion, more importantly, changing requirements. The new NSC has been described as a leaner and less visible body focused on both "geopolitics" and "geoeconomics," or "old world" and "new world" issues, under the leadership of Condoleezza Rice. Interestingly, today's NSC is reminiscent of that of President George H. Bush, who reorganized the body to include a Principals Committee, Deputies Committee, and eight Policy Coordinating Committees (PCCs). The current Bush administration has adopted a similar structure but instead of eight PCCs, the NSC encompasses six regional PCCs and eleven functional PCCs. The regional ones are: Europe and Eurasia, Western Hemisphere, East Asia, South Asia, Near East and North Africa, and Africa. The functional PCCs focus on democracy, human rights, and international operations; international development and humanitarian assistance; global environment; international finance; transnational economic issues; counter-terrorism and national preparedness; defense strategy, force structure and planning; arms control; proliferation, counterproliferation and homeland defense; intelligence and counterintelligence; records access and information security. As a result, the system of Interagency Working Groups adopted under the Clinton administration was abolished by NSPD-1, transferring the oversight of the ongoing interagency activities to relevant regional or functional PCCs. Also, NSPD-1 upholds an expanded attendance at NSC meetings as established under the Clinton administration. Thus, the NSC meetings include the secretary of the treasury, the president's assistant for economic policy (who is also head of the National Economic Council), the president's chief of staff and his national security adviser.

On the legislative side, the willingness of Congress to support reform of the State Department was tested during hearings on the Carlucci report earlier in 2001. Although Senate and House members expressed support for the report's recommendations, members questioned the level of the department's commitment, readiness, accountability and transparency expected by Congress. One House member pointed out that many of the reforms advocated by the Carlucci report do not require additional resources, citing the report's recommendations to right-size US missions abroad, to strengthen the authority of the ambassadors and to improve interagency coordination. The same member also noted that funding for embassy construction, security and information technology had already been provided over the last three years and criticized what he described as the department's resilience to change. "I suggest to you," the member continued, "that the most relevant question now before this committee is not, 'Have we provided enough money?' But rather, the question is, 'Is the State Department up to the task of responsibly managing the money it's been given and the mission given to it by the Congress?'" In the Senate, members affirmed the department's need for additional funding. Even so, their questions reflected a concern about issues dealing with human resources policy, internal management, roles and responsibilities among foreign affairs and defense entities, and interagency coordination.[29]

A month after these hearings, on March 12, 2001, the Bush administration proposed an almost 14 percent increase in funding for the State Department in fiscal year 2002 beginning in October 2001. The administration's budget proposal stresses two priorities, both of which affect diplomatic and consular operations—that is, hiring additional foreign and civil service officers and the acquisition of modern information technology. A third priority contained in the proposed budget is to bolster embassy security and provide for the construction of several new embassies. The proposed increase—from the current $6.6 billion to $7.51 billion—was regarded as a clear victory for Powell. Now, as the congressional member mentioned earlier inquired, “Is the State Department up to the task of responsibly managing the money ¼ and the mission given to it by the Congress?”

6. Conclusions

In the foreseeable future, although the United States will likely continue to be a hegemon with economic, technological, military and diplomatic influence unparalleled in the world, diplomacy will be even more complicated than it is today. The United States will be forced to respond to problems on both sides of the widening global gap, when the benefits of globalization will leave many behind. In this context, states and their foreign affairs ministries will encounter “old world” and “new world” threats and conflicts, and will need to practice both realpolitik and noopolitik. It is the only prudent course for them to take in this increasingly complex interdependent globe. If the current Bush administration is to succeed in the conduct of diplomacy, it must find a formula that refits the foreign affairs structure to the transforming diplomatic environment.

It is too early to tell if US foreign policy-makers have the sufficient political will to enact and implement the recommendations of blue-ribbon commissions integrated by prestigious scholars and talented practitioners. Despite worthy predecessors, neither the Carlucci nor the National Security Commission report however is ultimately sufficient in itself. The changes the world and the United States—as the principal global player—are undergoing are too fundamental and we are in the midst of them. Consequently, everything so far proposed is necessarily too little, too late. Yet we are saved by the reality that everyone is in the same situation. That said, attending to the recommendations made in the sweeping national security commission’s report and implementing the Carlucci report’s practical action plan for the State Department cannot but help aid the foreign policy establishment’s transition into the Information Age. Early indications from initial reform activities both at State and the National Security Council suggest that these reports have not fallen on deaf ears. There’s promise of a serious effort afoot, finally.

DISCLAIMER: The views expressed in this article do not necessarily reflect those of the United States Institute of Peace, which does not advocate specific policies.

Notes:

1. At its broadest, the term “virtual diplomacy” signifies the altered diplomacy associated with the emergence of a networked globe. At its narrowest, “virtual diplomacy” comprises the decision-making coordination, communication and practice of foreign affairs as they are conducted with the aid of information and communications technologies in the wake of the changes brought about by the computer and telecommunications industries.
2. Gordon Smith, “Reinventing Diplomacy: A Virtual Necessity,” *Virtual Diplomacy Series* (February 25, 1999). Available at http://www.usip.org/oc/vd/vdr/gsmithISA99.html, accessed July 30, 2001.

3. Robert O. Keohane and Joseph S. Nye, Jr., *Power and Interdependence: World Politics in Transition* (Boston: Little Brown, 1977).
4. Robert O. Keohane and Joseph S. Nye, Jr., “Power and Interdependence in the Information Age,” *Foreign Affairs* 77, 5 (September/October 1998): 81-94.
5. James N. Rosenau, “States, Sovereignty, and Diplomacy in the Information Age,” *Virtual Diplomacy Series* (February 25, 1999). Available http://www.usip.org/oc/vd/vdr/jrosenauISA99.html, accessed July 30, 2001.
6. Jean-Marie Gu•henno, *The End of the Nation-State* (Minneapolis: University of Minnesota Press, 1995).
7. Rosenau, “States, Sovereignty, and Diplomacy in the Information Age.”
8. Guehenno, *The End of the Nation-State.*
9. John Arquilla and David Ronfeldt, “What if There is a Revolution in Diplomatic Affairs?,” *Virtual Diplomacy Series* (February 25, 1999). Available at http://www.usip.org/oc/vd/vdr/ronarqISA99.html, accessed July 30, 2001.
10. U.S. National Intelligence Council. *Global Trends 2015: A Dialogue About the Future With Nongovernment Experts* ([Washington, DC: December 2000). Available @ http://www.cia.gov/cia/publications/globaltrends2015/.
11. Ibid.
12. Ibid.
13. Ibid.
14. Ibid.
15. Frank C. Carlucci and Ian Joseph Brzezinski, *State Department Reform* (Washington, DC: Council on Foreign Relations and the Center for Strategic and International Studies, 2001). Available @ http://www.cfr.org/public/resource.cgi?pub!3890.
16. U.S. Commission on National Security /21st Century, *Road Map for National Security: Imperative for Change*. (Washington, DC: March 15, 2001).
17. Richard Burt and Olin Robinson, et al., *Reinventing Diplomacy in the Information Age* (Washington, DC: Center for Strategic and International Studies, October 1998). Available @ http://www.csis.org/ics/dia/final.html.
18. Frank Carlucci, et al., *Equipped for the Future: Managing U.S. Foreign Affairs in the 21st Century* (Washington, DC: Henry L. Stimson Center, October 1998). Available @ http://www.stimson.org/pubs/ausia/#final.
19. Burt, et al., *Reinventing Diplomacy in the Information Age*.
20. Carlucci, et al., *Equipped for the Future*.
21. U.S. Commission on National Security /21st Century. *Road Map for National Security*.
22. Ibid.
23. Ibid
24. Ibid.
25. Colin Powell, “Town Hall Meeting” (Washington, D.C., January 25, 2001). Available @ http://www.state.gov/secretary/rm/2001/index.cfm?docid=24, accessed July 30, 2001.
26. Carlucci, et al., *Equipped for the Future*.
27. Ibid.
28. George W. Bush, Organization of the National Security Council System,” *National Security Presidential Directive*, No. 1 (February 13, 2001). Available @ http://www.fas.org/irp/offdocs/nspd/nspd-1.htm, accessed August 3, 2001.

29. “State Department Overhaul; Hearing of the House International Relations Committee,” *Federal News Service* (Lexis-Nexis Congressional, February 14, 2001), accessed July 30, 2001.

SHERYL J. BROWN is director of the Institute’s Office of Communications, which oversees public outreach and information services. She co-directs the Institute’s special initiative on "Virtual Diplomacy" and the Media and Conflict project. Brown came to the Institute in 1989 from Boston University’s Institute for Democratic Communication (D.C. Office), where she was deputy associate director. Among other publications, she co-edited *Resolving Third World Conflicts: Challenges for a New Era* (1992) and *Managing Communications: Lessons from Interventions in Africa*, an Institute special report. She earned a double doctorate in political philosophy and literature from the University of Dallas (1985), where she was a fellow at the Institute for Philosophic Studies. Since 1991, she has been an instructor of classical Greek history at Georgetown University. *E-mail*: sheryl_brown@usip.org .

MARGARITA S. STUDEMEISTER directs the Jeannette Rankin Library Program, co-directs the Virtual Diplomacy special initiative, and assists in coordinating and implementing Latin America and Caribbean activities at the Institute. Previously, she was director of publications at the National Security Archive, a nonprofit library, publishing, and research organization for declassified government documents, and a consultant for the World Bank. She has worked in academic, public, and special libraries, and on information technology projects. Studemeister also served as a consultant for a variety of nongovernmental organizations dedicated to human rights and community development in Central America. She holds Master’s degrees in library and information science, and in social science with an emphasis on Latin America, from the University of California at Berkeley and San Francisco State University, respectively. She has taught computer programming and database searching at the college level and for international institutions. *E-mail*: mss@usip.org .

BACK TO TOP

Virtual Diplomacy: Rethinking Foreign Policy Practice in the Information Age

Sheryl J. Brown and Margarita S. Studemeister

Keywords: Virtual diplomacy; foreign policy in information age; empowerment by networks; rise of non-state actors; realpolitik, noopolitik.

Abstract: Driven by information and communications technologies, the emerging global economy distributes information, ideas, values, capital, goods and services to people unevenly, across geopolitical borders and citizenships. As a result, the environment in which today's diplomacy must operate assumes engagement in a variety of asymmetrical relationships among and between state and non-state actors—that is, anyone anywhere connected to and affected by any of the information and communications media. Diplomatic agents range from the conventional ones—developed, stagnant, friendly, disaffected and hostile nation-states and regional and international organizations—to influential and independent multinationals, coalitions of shifting and diverse allegiances, networks of citizens of various identities and diasporas. Moreover, diplomacy increasingly involves issues that are perceived as global and interdependent but primarily experienced at the local level, including migration, environmental degradation, terrorism, drug trafficking, weapons proliferation and cyber harassment. Thus, foreign and domestic affairs are inextricably and complexly intertwined. The authors argue that this new environment demands a profound transformation of diplomatic practice within the traditional foreign affairs institutions.

Several recent studies of the US foreign policy establishment have offered recommendations to reform, reinvent, and reengineer an outdated, crippling bureaucracy. At the time of the inauguration of President George W. Bush, two more were released: one, produced under the leadership of former Defense Secretary and National Security Advisor Frank Carlucci, calls for reform of the Department of State, and the other, directed by two former senators, Democrat Gary Hart and Republican Warren Rudman, proposes a transformation of the national security structure of the United States. The authors of the article discuss the recommendations of both reports as efforts to realign diplomatic practice with emerging trends and review recent congressional debates and actions by the executive branch of the US government to renew the foreign affairs structures. The authors conclude that Washington decision-makers appear to apprehend the significance of the reports' findings and to initiate changes that will lead to a more responsive, and thus more effective, diplomacy .

full text

Author: **Dieter Zinnbauer**
Title: **Internet, Civil Society and Global Governance: The Neglected Political Dimension of the Digital Divide**
Year of issuance: **2001**
Issue: **Information & Security. Volume 7, 2001, pages 45-64**
Hard copy: **ISSN 1311-1493**

INTERNET, CIVIL SOCIETY AND GLOBAL GOVERNANCE: THE NEGLECTED POLITICAL DIMENSION OF THE DIGITAL DIVIDE

Dieter ZINNBAUER

Table Of Contents:

1. The Digital Divide

The catchphrase of the “digital divide” has evolved into a central point of reference for policymakers and IT practitioners alike. It provides an imaginative shorthand for the multiple imbalances that characterize the diffusion of novel information and communication technologies (ICTs) along income, gender, age and many other socioeconomic categories. The numbers are well-known and widely published:

- At the beginning of 2000 USA, Europe and Japan account for more than 96% of Internet hosts in the world and their combined share has even slightly risen since 1998;[1]
- The already tiny share of Internet hosts in Sub-Sahara Africa has sharply fallen between 1998 and 2000 to 0.25 % of total Internet hosts, while the growth in real terms has more or less stagnated;[2]
- 80% of Internet hosts are located in countries that speak English as their first language;[3]
- The total of international Internet bandwidth for Africa, the aggregate size of the “data pipes” to other countries is less than that of Ankara;[4]

- In 1998, 94 out of the 100 most visited websites were located in the US.[5]

Without any doubt, these numbers are disconcerting but not unexpected. They closely mirror a myriad of other global disparities with regard to income, consumption of natural resources, ownership of patents, etc.[6] Taken as stand-alone figures, these numerical snapshots of the digital divide can be even misleading. They tend to evoke strong reactions of two sorts:

- The skeptical variant, which denies the immediate importance of these ICT inequities with a strong "important are teachers and vaccines, not computers" type of response; [7] and,
- The "actionist" variant, which advocates the mobilization of resources on a massive scale and the establishment of a conducive regulatory economic environment to narrow the gap in ICT ownership and skills.[8]

These admittedly very stylized antipodes nurture each other and frame a very passionate but somewhat detached debate of the digital divide. However, in their myopic focus on the ICT resource gap they both highlight the need to move beyond the mapping of digital inequities and scrutinize both the transformational dynamics triggered and opportunities afforded by novel ICT in *concrete* applications and with regard to overarching goals of human development. This article speculates on the impact of the global digital divide with regard to participation of non-state actors in global governance processes. This specific application has been chosen for mainly three reasons:

- Much of the hopes for a benign transformative impact of ICT are pinned on this type of political grass-roots empowerment;
- The precarious temptation to infer structural social transformations from specific technological properties appears to be particularly strong in this area; and,
- The transformation of global governance regimes from state-centered systems towards greater complexity and involvement by non-state actors has received much attention and developed into a preeminent research area for International Relations (IR) research.

Given the scope of this paper and the speculative nature of the topic, it will only be able to offer a number of anecdotal observations and grainy hypothesis, that, while diverging somewhat from the mainstream thinking on the digital divide, are neither less substantiated nor less plausible than the conventional lines of reasoning. It is hoped that these think-bites will shed some light on a rarely discussed political dimension of the digital divide. The debate may contribute to a more integrative and sustained policy agenda that goes beyond mere resource mobilization if attention is drawn to some of the political and economic co-ordinates that impact the role of non-state actors in harnessing ICT for participation in global governance regimes.

2. Civil Society, Global Governance and the Internet

The conjuncture of two major trends has vastly expanded the role of non-state actors in global decision-making processes. First, the proliferation of economic, social, and political transborder interdependencies has significantly diminished the autonomy of the nation state and made international co-operation a prerequisite for effective policy-making in many areas.[9] This has given rise to a proliferation of international fora and negotiations which, although primarily state centered, also serve as focal points and lobby/networking infrastructure for non-state actors.[10]

Second, civil society organizations have gained significant weight in the political process for various reasons including historical ones (their acclaimed role in toppling communist regimes across East and Central Europe in the 1980s [11]), functional ones (growing appreciation as partners for implementing policies, information providers and generators of social cohesion and trust [12]) or normative ones (shifting conception of political legitimacy, which accords a greater role to alternative forms of participation, devolved collective decision making and self-governance beyond the conventional political process)[13]. In other words, both global decision-making and the involvement of non-state actors are on the rise and inspire academic scholarship across various disciplines.[14]

Both growing interdependence and the ascent of non-state actors are interlinked with the emergence of a global information and communication infrastructure. Coordinating economic activities on a global scale is predicated upon fast and cheap global communication as is of course the globalization of the media and the working of international political regimes itself.[15] By the same token, plummeting costs of computing power, the emergence of the Internet as global information space and medium for one-to-many modes of communication have lowered the organization costs for civil society organizations and boosted their mobilizing and lobbying capacities. It is this grass-roots democratization of communication and information flows, which holds the promise to free civil society from the straightjacket of overzealous state censorship or corporately controlled mass media and equip them to successfully enter the fray of negotiations in international governance regimes.[16]

Despite being mainly relegated to consultative status, their impact should not be underestimated in a world that is more and more understood to function along lines of “softpower.” [17]The capacities to frame issues, to shape cognitive templates and agendas, to focus public attention, mobilize support and forge issue coalitions are increasingly recognized as strategic resources in a context of complex global interdependencies, where reliance on hegemonic economic or military prowess alone can be rather costly or ineffective. Information and the capacity to access, process and disseminate it with strategic timing lies at the heart of this jostling for the limelight and legitimacy on the international stage.[18] And the Internet has significantly leveraged these capacities for civil society organizations.

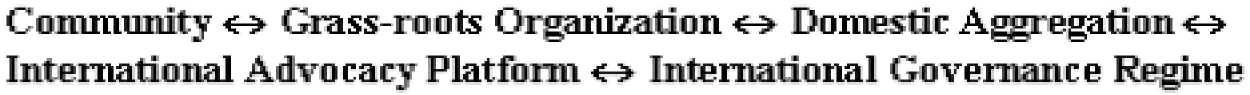
At least this is how one strand of theorizing goes—and parts of it appear to hold up well to the emerging evidence: Analyses of transnational advocacy networks for human rights, environment and gender issues find a significant impact of these coalitions on shaping international norms, regime structures and policy-making in the respective issue areas. [19] These findings are corroborated by a growing number of case studies on international regimes, including the spectacular civil society success stories with regard to banning landmines [20] and stopping the Multilateral Investment Agreement.[21] The direct causal impact of a diverse and pervasive medium like the Internet on all these activities is almost impossible to establish. Nevertheless all studies seem to agree that the Internet fulfils a significant supportive, if not necessary function.[22]

3. The Digital Divide and International Governance

What does this mean for developing countries and the global digital divide? For a start, it appears quite straightforward to argue that the lack of access to these novel communication and information technologies diminishes the possibilities to get heard and participate *relative* to stakeholders that have the resources to quickly adopt these novel technologies. One would argue that, while civil society in rich industrialized countries is able to catch-up somewhat with governments and transnational business in terms of information competence, civil society in developing countries is falling even further behind.

At closer inspection this argument needs some qualifications, since it appears to lean precariously towards an overly simplistic conception of communication and information flows. In particular it fails to consider the multiplicity of technical tools and social arrangements that process and move information, the interlocked nature of these arrangements and hence the various organizational possibilities for consolidating and articulating political claims. True, from an idealist democratic point of view the target of one voice—one computer might maximize democratic participation in electronic communication networks for global governance. Needless to say that this is not feasible. Nor would it be a sufficient condition for a substantive democratic process, given other inequities in information access, processing capacities, time resources etc.

From a strategic perspective it appears more desirable to focus on the collective arrangements that exist to pick up the voices on the ground, bundle them and feed them into the political process. This perspective directs attention to the many intermediaries that make up this communication conduit: grass-roots organizations on the village or community level that are linked with domestic advocacy groups, which in turn network with international NGOs. The mechanisms that sustain information flows across these interwoven networks are manifold: face-to-face communication in personalized interaction within social and professional networks, preparation and distribution of written material, community radio etc. In a very simplified way the corresponding information chain might look like this:



Community ↔ Grass-roots Organization ↔ Domestic Aggregation ↔ International Advocacy Platform ↔ International Governance Regime

Of course this stylized conception diverges from reality in many important respects:

Relationships are not necessarily cascading or hierarchical, the shift from local to domestic to international does rarely correspond with organizational boundaries. The chart might rather be read as the idealized procedural sequence that translates individual needs into concrete political claims to be fed into a specific international bargaining process by civil society. It shall be argued that the cluster of domestic aggregation is the pivotal sector to look at, when assessing the impact of the digital divide on voice in global governance. It is the networking of a myriad of grass-roots initiative, the bundling of voices into demands and claims and the process of feeding them into international advocacy networks, where a potential digital divide can wreak most havoc.

For the ***“community ↔ grass-roots organization”***-link, conventional modes of communication and information engrained into a fine mesh of personalized relations, social and professional networks, relative frequent contact etc. offer viable alternatives to ICT based information exchange.[24] However, these means cannot compete with the times-space compression achieved by the Internet. Information flows from remote insular communities can be infrequent; transmission might be slow relative to the chronopolitics of the global. [25] Nevertheless, complex emergencies that require immediate action aside, the absence of sophisticated Internet based technologies does not seem to stand much in the way of maintaining information flows between the community and articulating needs from the grass-roots level upwards. A digital divide might exist, but this is not automatically a broken link in communication and information flows.

Likewise, the digital divide in its common conception as ICT disparities between developing and developed countries does not appear to play much of a role in the ***“international advocacy network ↔ international regime”***- link. The argument here goes the other way round: it is not the availability of alternative established modes of communication that render the digital divide less important, it is rather that there is no significant disparities in access to ICT in the first place, when it comes to international civil society advocacy networks vis-•-vis other stakeholders such as international business etc. Building on falling ICT prices and aided by the emergence of numerous free services for E-mail, website hosting, discussion groups, the Internet has become a pervasive and ubiquitous tool for international civil society networks.

It is beyond the scope of the paper to elaborate on the available cyber repertoire, which ranges from information networking based on topic-oriented mailing lists or mobilizing via E-mail alert to building an alternative information platform on the web. The digital infrastructure to support international advocacy networks is well developed. Mailing and discussion lists exist for every conceivable topic or can on demand be set up through free, easy-to-use online services. International advocacy networks have established vast websites, compiling extensive amounts of information, providing interactive services and up-to-date news coverage.

Most importantly umbrella aggregators such as *OneWorld* or *Eldis* have evolved to provide a platform for content and web presentations by a myriad of smaller organizations. [26] Taken together free Internet services and the ICT resources of international advocacy networks provide a solid installed base of ICT infrastructure that can be harnessed by domestic advocacy groups in developing countries.

4. The Pivotal Role of Domestic Aggregation and Domestic Policies

Alternative means for information transmission on the grass roots level, on the one hand, and the availability to borrow ICT infrastructures for the last linkage between international networks and international regime, on the other hand, point to the importance of the *information and communication capacities at the layer of domestic aggregation of voices*. It is here, where the digital divide might possibly matter most.

Solid empirical evidence on the diffusion of ICT within this sector is very difficult to come by. Two general observations, which make the digital divide appear in a different light, should be borne in mind however:

- Civil society organizations in many countries around the world are over-proportionally middle-class phenomena, suggesting an above average skill and income level that put the disparaging overall inequities in Internet diffusion somewhat in perspective. This is not to say that the endowment with basic ICT is sufficient. Many organizations are woefully starved of resources. However, the gap appears to be smaller than the aggregate country-level number crunching with regard to ICT might suggest;
- More importantly, accepting the assumption that the crucial link is the domestic aggregation of voice and the embeddedness of the aggregating agents into international advocacy networks redirects the analysis of representation in global governance to the enabling and disabling factors for domestic aggregation.

In other words, the conditions for a thick and vital civil society are a great deal more important for participation in global governance than the incidence of digital inequities. Scholars from various disciplines have come to the quite consensual insight that the existence of a thriving civil society is very much a function of *domestic* factors. Explanatory power is accorded to a host of structural variables such as ethnic and socioeconomic configurations, historical trajectories of nation-building and, most importantly for our analysis, the characteristics of the political regime and the political space as shaped by the incumbent government.[27]

Domestic laws, policies and political practices pertaining to freedom of organization and expression provide the framework for civil society activities. It is quite straightforward that outright oppression of civil society organizations is severely constraining the public space for political claim making. However, the thickening of civil society and their ability to amplify grass-roots voices and feed them into international networks is also highly contingent on a variety of more subtle enabling and disabling factors, such as media policies, freedom of information practices within the domestic bureaucracy, co-operative or confrontational policy styles etc.

What are the implications of these points for the debate on the digital divide? The paramount importance of domestic factors for the functioning of civil society highlights the *domestic* political responsibility for a civil society voice in global decision-making. Domestic policy makers in repressive regimes, who routinely join in the choir of complaints about asymmetric representation of cultures and languages on the Internet, can effectively strengthen the digital engagement of their communities by removing roadblocks to civil society activity. Very often, it is domestic divides in political participation rather than inequities in the global distribution of the Internet that shape the strength of the voices of domestic civil society in global governance processes. Putting useful administrative and political information online, such as legal texts, draft regulations, proceedings of meetings and hearings, planning material or environmental indicators, creates a strong pull-effect for online political engagement. Removing legal barriers to the formation of civil society organizations, promoting a political climate of openness, deliberation and freedom of speech and involving civil society more closely in the design and implementation of public policies provide powerful stimulants for developing an organizational infrastructure for voice, engagement and advocacy. These enabling provisions will also enhance participation and visibility of domestic actors in global governance processes.

5. From Digital Divide to Digital Opportunity?

So far it has been argued that the digital inequities as referred to by the concept of the digital divide do not in themselves significantly alter the existing asymmetric patterns of representation in global governance processes and that it is the domestic conditions for civil society activity that are important in the first place. While this establishes the primary responsibility of domestic policy-making, it also raises the question to what extent a closing of the digital divide could compensate for an adverse domestic political environment and other constraints. Three interrelated effects, each discussed in more depth below, might be possible. Enhanced endowment with ICT could:

- Help to outmaneuver domestic political control mechanisms on the flow of information;
- Stimulate political engagement and civil society activity in general; and,
- Substitute for a possible weak link to international advocacy channels and disintermediate the information flows to the public and other participants in the governance regime.

ICT to Outwit Domestic Government Control on Information Flows?

Popular reviews of Internet technologies brim with enthusiasm over the alleged grass-roots empowerment the Internet offers. State control over information flows, the story goes, is rendered ineffective. “The Net routes around censorship” is a popular comment that acknowledges technical properties as inherently liberating and defying central control.[28]

However, these assumptions require some qualifications: First, the Internet, at least in its current form, is far from a non-hierarchical network. Core functions such as the Internet Domain Name System, which enables navigating in cyberspace, or the client-server architecture, with end users (client) gaining access to the Internet and sending all data through a specific gateway node (server) are essentially hierarchical or at least perform gatekeeping functions, thereby multiplying vulnerable entry points for monitoring of data traffic, surveillance of individual online behavior or interruption of connectivity to end users/websites.[29]

True, technologies exist that allow one to remain anonymous, prevent interception of E-mail communication or route around blocked websites. Most of the time however these technologies are confined to a technology-savvy cyber elite.[30] Publicly stated commitment to monitoring of the Internet coupled with often draconian sanctions and showcase seizures, provide a sufficient level of credible deterrence. The average Internet user does not command the technical competence and confidence to safeguard her information privacy and anonymity in what is often perceived as a technology race between an IT-savvy regime and the development of subversive online tools. Censorship cannot be watertight, but raising the barrier for the bulk of Internet users is possible and relatively effective.[31]

ICT as Political Stimulant?

It is very doubtful whether the Internet can act as an independent stimulant for political engagement.

A growing body of literature suggests that the Internet can act as an amplifier or inhibitor of existing predispositions but it is unlikely to create them. It might lower the transaction and organization costs for civil society and thus deliver a formidable boost to the mobilization of existing networks across vast physical spaces, but it neither appears to be a sufficient condition for the creation of these networks, nor does it automatically install a deliberative democratic culture among its users.[32]

But what about the impact of access to alternative information? Does this pull more people into civil society activism? True, the Internet can enhance the flow and distribution of alternative information, provided the state does not follow a heavy-handed regulatory approach. However, it should rather be argued that this boils down to an electronic supplement of existing political rumor mills and a gateway to alternative views for people who have been actively engaged with these issues before. The new Internet user, who is disinterested in political affairs, will rather explore the playboy- and mtv.coms than the bbc- or amnesty.orgs of the new information worlds.

Furthermore, the transformative impact of access to critical international information is often exaggerated. External information can often not be readily fed into the domestic discourse. Building on understandable post-colonial nationalist sentiments, political regimes have over time instituted a number of informal rhetoric defenses that have become firmly entrenched in the domestic political discourse. Information from external sources is branded as *neo-colonial*, infringing on state sovereignty, driven by vested interest, ignorant and disrespectful of a cultural or political otherness. While much of this rhetoric is revealed by informed civil society opinion leaders as such, it has made its mark on the domestic popular debates, instilling a great deal of suspicion about “Western” criticism, forcing even the domestic messengers to tread very carefully so as not to convey the image of a henchman of foreign powers.

In the long-term a genuine stimulant for civil society activism might arise from a very unlikely place: the very popular chat rooms and free discussion lists. While these fora are rarely explicitly political they facilitate, doubtlessly aided by the anonymity they grant to participants, informal chat and uninhibited exchange about what are often very personal issues. These acts of finding out about like-minded people with similar problems, demands and interests can support a learning process, in which problems that were previously experienced as singular and particular to one’s private lifeworld become understood as wide-spread and eventually systemic deficiencies of a specific social, economic configuration.[33] Informal apolitical anonymous chat might in the long-run build up grass-roots political ferment. This however appears to be a rather distant and long-term transformative option.

ICT to Amplify Voice in International Arena?

To what extent can increased Internet use within civil society of developing countries substitute for insufficient inclusion in international advocacy networks? This is a very interesting and important question. It relates to a concern that is often raised by critics of a strong role for civil society in global governance processes. According to this view, the structures of international advocacy have been established and continue to be operated by a number of undemocratic, unaccountable Western NGOs, which only reflect the narrow band of “luxury” values of a small elitist Western clientele. For the sake of the analysis here, the argument, which is susceptible to criticism from various angles, will be taken at face value.

Let us assume civil society organizations in developing countries want to press issues that do not befit the agendas of international advocacy networks. What are the chances to harness the Internet for creating an alternative advocacy platform and take the cause directly to the public, the media and the international policy-making forum? At first sight, it looks like the Internet provides ideal tools to cut out intermediaries of any kind: After all, setting up a website is by now relatively easy and inexpensive. As mentioned before, various free services are available online, ranging from web-based E-mail accounts and mailing list tools to website building toolkits and free hosting services. Also, many established discussion fora are un-moderated making it easy to post statements, which do not undergo editorial control. Moreover, inexpensive one-to-many communication afforded by E-mail makes it possible to distribute a statement to hundreds or even thousands of media outlets and policy makers in a relatively effortless manner.

While these scenarios suggest opportunities for a radically democratized articulation in the digital arena, two fundamental problems stand in the way of genuine disintermediation:

- *Information glut – attention poverty:* The amount of information stored on and flowing through the Internet has reached truly monumental dimensions. [34] This information glut meets a relatively constant capacity and willingness to gather and process information on the part of the user. If the bottleneck was ever availability of information, it has now shifted to attention.[35]
- Reputation problem: The democratization of online publishing has lead to an impressive but equally bewildering plurality of news sources, voices, and eyewitness reports.

Conventional systems of quality assurance and verification as cultivated and institutionalized in the editorial process and brand journalism are being bypassed. The liberation from editorial control and corporate journalism comes with a loss of reputation and trust.[36] This is not to say that the signifiers for quality information are forever linked to specific gatekeepers. But they are scarce, need to be earned hard and underscore the persisting importance of intermediaries. Taken together, information glut, attention poverty and the reputation imperative create a very difficult environment for gaining voice in the online environment as indicated by a number of worrisome trends:

The Fading Novelty of E-mail

In the early days of the Internet, E-mail appeared to be a fabulous tool to bypass hierarchies of all kinds and convey information straight to the desired contact. High-level representatives of government, bureaucracies or media would make their E-mail addresses available and invite direct contact in order to showcase their openness and progressiveness. With the popularity of E-mail rising rapidly and daily E-mail volumes for important decision makers in the hundreds, these open-access policies have become ever less feasible. It is probably fair to say that by now the handling of unsolicited E-mail has been institutionalized along the conventional lines of office routines and information consolidation through analysts and administrative staff.[37]

The Enduring Primacy of the Issue-attention Cycle

Much hope of an Internet led democratization has been fueled by some early successes of grass-root organization to harness the Internet for drawing public attention to their cause. The Zapatista uprising in Chiapas provides probably the most prominent example.[38] However, it is more than doubtful whether a similar campaign today might be able to mimic this early success story. The Zapatista uprising enjoyed a considerable first-mover advantage in the use of the new media. Rather than facing overcrowded "infotainment" spaces it found a receptive early adopter audience, excited to explore the novelty of the Internet and its applications in "meat space" struggles. Moreover, the use of highly sophisticated technology by a jungle-based, people's movement provided an unrivalled icon for the hopes and dreams associated with the magic bullet Internet, a notion that fared well at that time. The "jungle-high tech" contrast was found highly newsworthy in itself. By now all this enthusiasm has faded somewhat. In the times of cyber sobriety and ubiquitous cyber activism the rules of the news and issue-attention cycle can be expected to bite again. [39] All-out cyber mobilization in combination with significant offline activities, such as the recent Seattle activities, might manage to refocus attention on cyber campaigns for a limited period of time. The main focus at the writing of this article however has moved to alleged cyber wars and virus attacks. Internet direct actions proliferate. They become increasingly routine events from the perspective of news coverage and no longer manage to garner much attention beyond the established circles of activism and engagement

The Staying Power of Brand Names, Gatekeepers and Resource Rich Content Providers

Established information providers such as the major newswires and media conglomerates have in many cases successfully leveraged their scale advantages in news production and syndication into the online world.[40] The explosion of online information stands in stark contrast to the extraordinary concentration of web traffic on a small number of portal sites.[41] While a few new online information portals have gained prominence, they rarely build up extensive capacities for in-house content production or journalistic research, but mostly rely on news feeds from a limited number of established newswires. Likewise the proliferation of e-commerce sites has turned portal websites that aggregate large user groups into coveted online billboards. Online advertising prices have skyrocketed, making it nearly impossible for civil society content to have a link to their sites placed prominently on one of the big online portals.

The Non-Transparent Organizing of Meta-Information Online

No authoritative meta-directory structures information in cyberspace. Users navigate with the help of domain names and private search engines, which only manage to catalogue a portion of the Internet. Keyword searches operate with non-transparent index and search techniques that effectively put the visibility of websites at the discretion of search engines. Some search operators have embarked on a dubious practice to sell off premium spots in their listings rather than rely on an automated search heuristic. Often these commercial placings are poorly marked as such. The user is presented with a m •lange of search hits and advertising, while expecting an impartial execution of her search.[42]

Walled Gardens

New business models for the Internet are geared towards the creation of alliances between content and conduit providers. Internet access and service providers increasingly team up with large media conglomerates in the hope of exploiting synergies through cross-promotion and customer sharing. The recent Time Warner-AOL merger is a harbinger for the type of marriages between content and conduit to come. Through various design mechanisms Internet users are lured to spend as much online time as possible within the proprietary content space instead of clicking off into the wider Internet. These so-called walled gardens are not a distant scenario but have already become reality. As news reports revealed AOL has imposed a number of contractual obligations on Disney, a major content provider to the AOL portal site. In order to minimize the number of people leaving the AOL compound, AOL demanded that Disney keeps the number of external hyperlinks from its pages limited and included the right to financial compensation in case more than 25% of people would follow external links from the Disney site.[43] In the near future content discrimination on the Internet will go far beyond web design issues. Current mobile Internet technologies (WAP) and some forms of high speed Internet diverge from the open access principle that has laid the foundations for content plurality on the Internet in the first place. WAP gateways for example only give users access to content providers that have signed up with their mobile access operator. Similarly, owners of high-speed infrastructure are not mandated to provide open access to their networks for all Internet service providers, thereby adding another layer of gatekeeping.[44]

6. The Political Dimension of the Digital Divide

As this brief enumeration indicates, the list of barriers to stand-alone online representation is comprehensive. The hurdles for civil society organizations from developing countries to independently gain significant visibility and attention for an underrepresented standpoint are formidable. The chances to provide a widely recognized alternative framing of issues that makes its way onto the negotiation table of global governance regimes are dim.

Again the plurality of visible opinions hinges on old and new gatekeepers and is severely narrowed by the economies of news production and the well-known psychology of the issue-attention dynamics. To put it very bluntly: the fact that websites can be set up easily does *by itself* as much or little to increase media presence as the acquisition of a phone.

It is interesting to note, that, while we embarked on the argument from the perspective of underrepresented civil society in developing countries, the very same challenges also apply to the voice of civil society in general. The opportunities afforded by new communication and information technologies with regard to a voice for civil society in global governance is not so much a question of ICT resources, but of sensible media and communication policies. The Internet is not a substitute for committed anti-trust policies that curb concentration, for far-sighted communication policies that guarantee open access to the conduits, for media regulations that mandate a transparent difference between commercial promotion and impartial information.

These are just a few items for a media agenda, which in principle is not new, but has become longer and acquired a new taste of urgency through the advent of the Internet.[45] The well-known structural imbalances that have long distorted the distribution of media might around the world are not suspended but continue to mould information and communication flows in the Internet age.

Moreover, the efficacy with which civil society can use ICT to contribute to global governance processes and enhance their democratic legitimacy hinges on a conducive procedural framework underpinning international regimes themselves. A narrow fixation on electoral accountability is not helpful in this context. As Nye and Keohane have noted, the opening of a public space for deliberation, which interfaces with the actual decision making process in the broadest way possible can significantly enhance input legitimacy. On a procedural level this includes stepping up substantive consultative processes with civil society, the opportunity to file amicus briefs, [46] rigorous transparency not only for policy outputs, but also for the negotiating processes itself. ICT can greatly support these efforts through a variety of means such as online consultations, online posting of proceedings, automated notification of feedback deadlines etc. ICT however cannot substitute for reluctance on the part of governments and international organizations to increase transparency and strengthen accountability.

Summing up, policy-makers that are serious about maximizing the opportunities from ICT towards a new culture of democratic legitimacy in global decision-making process should be aware of their responsibilities:

- Domestic ones, in order to enable a thriving civil society;
- International ones, in order to increase the plurality and visibility in the global information space; and,
- Global regime ones for the case of global governance reform towards greater public deliberation, transparency and accountability.

Taken together this is the critical political dimension of the digital divide when it comes to delivering on the democratic promise of ICT in global governance regimes.

Similar points for the overriding importance of policies and regulatory frameworks could be made for other applications for ICT. Economic participation in globalized Business-to-Business marketplaces, for example, faces formidable policy challenges in the form of anti-trust issues, access to intellectual property, deployed software standards in payments systems, privacy regulations etc.

As long as the developmental rhetoric about the digital divide confines itself mainly to questions of ICT resources and market liberalization and shirks these more uncomfortable issues, it rather reeks of a project to ensure the continued growth of ICT exports than a sincere effort to bridge divides and help developing countries realize the potential of ICTs. Or to end on a more upbeat note:

The digital divide and the question of how to channel the novel information technologies towards human development could be a welcome opportunity to revisit some more fundamental structural asymmetries that are at the root of not only the digital but many other divides and hence to reinvigorate a policy debate that moves beyond simplistic ideas of open markets and limited resource transfers to sufficient guarantors to reap the benefits of technological advances on an equitable basis.

DISCLAIMER: The views expressed in this article are views of the author only and should by no means be associated with UNDP.

Notes:

1. Tim Jordan, “Measuring the Internet: Host Counts Versus Business Plans,” *Information, Communication & Society* 4, 1 (2001): 34-53.
2. Ibid.
3. Ibid.
4. Telegeography, *Hubs and Spokes: A Telegeography Internet Reader* (Washington DC: Telegeography, 2000).
5. International Telecommunication Union, *Challenges to the Network: Internet for Development* (Geneva: International Telecommunication Union, 1999).
6. Jordan, “Measuring the Internet,” provides an interesting breakdown of Internet hosts according to GDP per capita and human development level as measured by the UNDP Human Development Index. Unsurprisingly skewed host distribution mirrors human development and income distributions and the host shares for each group have not changed significantly between 1998 and 2000.
7. Emblematic for this strand of thinking is the astonishing statement by Bill Gates: “The world’s poorest 2 billion people desperately need healthcare right now, not laptops,” (quoted in: *New York Times*, November 3, 2000, A1), which has been widely picked up upon by the media and also entered professional debates about development policy.
8. See for example the widely cited e-Readiness initiative (http://www.readinessguide.org/), which provides a comprehensive but very abstract checklist for assessing infrastructure and institutional shortcomings relative to an ideal of a networked society and economy. In doing so, the guide helps draw up a sweeping agenda for resource mobilization and regulatory policy reform for the sake of bridging the divide. It barely considers socioeconomic specificities or concrete ICT applications and thus fails to identify a more integrative policy framework linked to goals of human development.
9. Robert Keohane and Joseph Nye, *Power and Interdependence* (Boston: Little Brown, 1977).
10. Sidney Tarrow, *Beyond Globalization: Why Creating Transnational Social Movements is so Hard and When is it Most Likely to Happen* (New York: Cornell University, 1999). Available @ http://antenna.nl/~waterman/Pages/general/tarrow.htm, accessed May 30, 2001.
11. John Keane, *Civil Society: Old Images, New Visions* (Polity Press: Cambridge, 1998), 19-23.
12. Robert Putnam, *Making Democracy Work: Civic Traditions in Modern Italy* (Princeton, NJ: Princeton University Press, 1993).
13. Claus Offe, “Challenging the Boundaries of Institutional Politics: Social Movements Since the 1960s,” in *Changing Boundaries of the Political*, ed. Charles Maier (Cambridge: Cambridge University Press, 1987), 63-105.
14. The proliferation of new concepts related to these phenomena is impressive. Concepts range from the seminal descriptive template of “complex interdependence” (Keohane and Nye, 1977) to bolder categories such as “world polity” (John Boli and John Thomas, eds., *Constructing World Culture: International Nonvgovernmental Organizations Since 1875* (Stanford: University Press, 1999)) and, with particular reference to the role of civil society , “cosmopolitan model of democracy” (David Held, “From City-States to A Cosmopolitan Order?” in *Prospects for Democracy*, ed. David Held (Cambridge: Polity Press), 13-52) or transnational social movements (Donatella Della Porta, et al., *Transnational Social Movements* (London: MacMillen, 1999)).
15. Manuel Castells, *The Rise of the Network Society* (Oxford: Blackwell, 1996).
16. For an enumeration of tools provided by the Internet for influencing foreign policy, see Dorothy Denning, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy” (1999) [unpublished paper online at: http://www.nautilus.org/info-policy/workshop/papers/denning.html, accessed

May 28, 2001].

17. Robert Keohane and Joseph Nye, “Power and Interdependence in the Information Age,” *Foreign Affairs* 77, 5 (September/October 1998): 88-93.

18. Contributions from various theoretical and methodological backgrounds appear to converge around a recognition of the importance of soft power. These include cognitive approaches in international relations (for an overview see Stephan Haggard and Beth Simmons, “Theories of International Regimes,” *International Organization* 41, 3 (1987): 491-517); mobilization analysis in the field of contentious politics (see Tilly, *From Mobilization to Revolution* (Reading, MA: Addison-Wesley, 1978); Margaret Keck and Kathryn Sikkink, *Activists Beyond Borders* (Ithaca: Cornell University Press, 1998) and as strongest variant, communication research in the tradition of media imperialism (Herbert Schiller, *Communication and Cultural Domination* (White Plains, N.Y.: International Arts and Sciences Press, 1976). On the applied level of policy strategizing the importance of soft power is reflected in strategies such as issue management (Phil Agre, “The Dynamics of Policy in a Networked World” (1999) [unpublished paper online at: http://www.nautilus.org/info-policy/workshop/papers/agre.html, accessed at 25 May 2001]) or “Noopolitik” (John Arquilla and David Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy*, MR-1033-OSD (Santa Monica, CA: RAND, 1999)).

19. Keck and Sikkink, *Activists Beyond Borders*.

20. Richard Price, “Reversing the Gun Sights: Transnational Civil Society Targets Land Mines,” *International Organization* 52, 3 (1998): 613-644.

21. Peter Smith and Elizabeth Smythe, “Globalization, Citizenship, and Technology: The MAI Meets the Internet” (paper presented at International Studies Association Annual Convention, Los Angeles, March 14-18, 2000).

22. Keck and Sikkink see one strategic advantage of transnational networks in their ability to move information quickly and effectively between participants, a task greatly aided by the Internet (Keck and Sikkink, 1998) and confirmed by detailed studies on the role of the Internet in toppling the MAI (Smith and Smythe, 2000), advancing the ban of landmines (Ken Rutherford, “The Landmine Ban and NGOs: The Role of Communications Technologies” [unpublished paper available at: http://www.nautilus.org/info-policy/workshop/papers/rutherford.html, accessed at 25 May, 2001]) and anecdotal evidence from various other campaigns (Denning, 1999).

23. Keck and Sikkink elaborate both on the mutual benefits of this process. While grass-roots voices and personal stories gain amplification, albeit often in a morphed and de-contextualized form, international advocacy networks gain valuable legitimizing testimony to back up their claims (Keck and Sikkink, *Activists Beyond Borders*, 18-19).

24. The literature on development communication provides an interesting strategic perspective on the multiple channels and arrangements that support information flows within communities in developing countries. For an overview see Adam Burke, *Communications and Development: A Practical Guide* (London: Department for International Development, 1999). Organizational studies emphasize the pivotal importance of communities of practice as arrangements to compare notes, exchange information, convey tacit knowledge etc. These communities of practice are not bound to a specific formal organizational structure or a specific communication medium, but thrive through various social arrangements (Etienne Wenger, *Communities of Practice: Learning, Meaning, and Identity* (Cambridge: University Press, 1998)).

25. The phrase “chronopolitics” has been coined by Paul Virilio to describe the acceleration of the political process and the increasing importance of time, timing, response time etc. as strategic resources within it. See Paul Virilio, *Speed and Politics: An Essay on Dromology* (New York: Columbia University, 1986).

26. See www.oneworld.org, which provides a metastructure for development related content from a myriad of partner organizations from around the world, and www.eldis.org, which structures development related research and links to think tanks.

27. Scholars of social movements and contentious politics stress this point. They have developed the concept of political opportunity structure, which encompasses the responsiveness to claim-making of the formal political process, as well as concrete policies and strategies adopted by the state that impinge on working of civil

society groups (Sidney Tarrow, “States and Opportunities: The Political Structuring of Social Movements,” in *Comparative Perspectives on Social Movements*, ed. Doug Mc Adam, et al. (Cambridge: Cambridge University Press, 1996)). With regard to transnational networks, Tarrow emphasizes the persistent grounding of movement agents and repertoire in domestic political configurations and domestic social networks.

28. See for example Wade Rowland, *The Spirit of the Web: The Age of Information from Telegraph to the Internet* (Toronto: Somerville House, 1997).

29. For an excellent introduction to architecture and governance of the Domain Name System see Craig McTaggart, *Governance of the Internet’s Infrastructure: Network Policy for the Global Public Network*, Dissertation (LLM, University of Toronto, 1999). The control implications of the client-server architecture are highlighted in the current discussion on novel peer-to-peer software tools that promise to threaten these hierarchical control mechanisms (for a very accessible introduction see: “Peer to peer pressure,” *Economist*, November 2, 2000). Likewise, the current discussion on law enforcement on the Internet in many countries underscores the repertoire of available tools to monitor Internet use (see for example http://www.computerworld.com/resources/carnivore/ for a resource collection on the US “Carnivore” monitoring system), whereas the debate on information warfare and critical infrastructure protection illustrates the various possibilities for disrupting connectivity (Dorothy Denning, “Cyberterrorism,” testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 23, 2000, available @ http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, accessed May 24, 2001).

30. One should not make the mistake of presupposing a large overlap between civil society activism and the IT-savvy hacker scene. The public image of a libertarian spirit among Internet activists in industrialized countries suggests a certain affinity with values that are commonly associated with some clusters in civil society. It is questionable to what extent this affinity translates into direct involvement with more organized civil society activism. This might be even more true for developing countries where hacker communities developed in different social contexts and might espouse different shared values and principled believes.

31. These arguments are based on a series of interviews the author conducted with civil society organizations in Southeast Asia from 1999 till 2001.

32. See Keck and Sikkink, 1998, for the interpersonal prerequisites for electronic advocacy networks. Norris undertakes a cross-national survey in her forthcoming book and arrives at the conclusion that “those who take advantage of the opportunities for electronic civic engagement tend to be activists who would otherwise participate via conventional channels.” (Pippa Norris, *Civic Engagement, Information Poverty and the Internet Worldwide* (New York: Cambridge University Press, forthcoming Autumn 2001), Chapter 1, 10). Denning, *Activism, Hacktivism, and Cyberterrorism*, notes the defamatory and anti-discursive nature of many unmoderated usenet discussion groups.

33. Following Ross, McAdam et al. describe this tendency to mistake systemic deficiencies for individual flaws as the “fundamental error of attribution” (Doug McAdam, et al. “Introduction,” in *Comparative Perspectives on Social Movements*, ed. Doug McAdam, et al. (New York: Cambridge University Press, 1996)).

34. See Lyman and Varian for an ambitious attempt to gauge the overall expansion of available information, which puts the annual growth rate of computer-stored information at 100 (Peter Lyman and Hal Varian,“How Much Information" [online at: http://www.sims.berkeley.edu/how-much-info on, accessed 30 May 2001]). For estimates about growth of traffic on the Internet, which is also estimated to double annually, see K. Coffman and A. Odlyzko, “Internet Growth: Is there a ‘Moore’s Law’ for Data Traffic?” in *Handbook of Massive Data Sets*, ed. J. Abello, et al. (New York: Kluver, 2001).

35. For a seminal essay on the information-attention relation, see Herbert Simon, “Designing Organizations for an Information-Rich World,” in: *Computers, Communications, and the Public Interest*, ed. Martin Greenberger (Baltimore: John Hopkins University Press, 1971).

36. Keohane and Nye, “Power and Interdependence in the Information Age,” for example link reputation to their concept of softpower and argue that “asymmetrical credibility is a key source of power.”

37. Denning, *Activism, Hacktivism, and Cyberterrorism*.

38. See for example Castells, 1996.

39. For a seminal study on the issue-attention cycle, see Anthony Downs, “Up and Down with Ecology: This Issue Attention Cycle,” *Public Interest* 28 (1972): 38-50.

40. For an overview of the extraordinary concentration in the global media market, see Robert McChesney, “The Political Economy of Global Media,” *Media and Development* 45, 4 (1998): 3-8. For early evidence on the continued market dominance of established information producers in the online world see Matthew Zook, “Old Hierarchies or New Networks of Centrality? The Global Geography of the Internet Content Market,” *American Behavioral Scientist* 44, 10 (2001): [forthcoming].

41. For recent market figures that confirm strong trends towards concentration, see for example “Four Websites Control Half of Surfing Time,” *E-Commerce Times* (June 4, 2001).

42. Inclusion and ranking of websites is even more arbitrary for directory services, which are manually referenced and do not rely on automatic indexing. (Helen Nissenbaum and Lucas Introna, “Sustaining the Public Good Vision of the Internet: The Politics of Search Engines,” Working Paper #9, Center for the Arts and Cultural Policy Studies, Princeton University, 1999). For a detailed account on the visibility of non-commercial content on the Internet and the parallels to other media, see Eszter Hargittai, “Standing Before the Portals. Non-Profit Content Online in the Age of Commercial Gatekeepers,” paper presented at conference “Shaping the Network Society: The Future of the Public Sphere in Cyberspace (DIAC2000),” May 20-23, 2000, Seattle, U.S.

43. See “AOL Restrictions Alleged,” *Washington Post* (October 10, 2000), E01.

44. For WAP and open access see Sohil Parekh, “A Close Look at the Wireless Application Protocol,” student paper for course “Autonomy and Information: The Relationship between the Individual and the Government in the Digital Age,” John F. Kennedy School of Government, Harvard University, 2000; for cable and open access see, Fran•ois Bar, et al., “Defending the Internet Revolution in the Broadband Era: When Doing Nothing is Doing Harm,” Working Paper 137, Berkeley Roundtable on the International Economy, 2000.

45. For a major international initiative to tackle information asymmetries see the debate in the 70s and 80s on a New Information and Communication World Order. For an overview see Ch. Brown-Syed, “The New World Order and the Geopolitics of Information,” 1999 Web Edition, available @ http://valinor.purdy.wayne.edu/csyed_libres3.html, accessed May 24, 2001.

46. Robert Keohane and Joseph Nye, Jr., “Between Centralization and Fragmentation: The Club Model of Multilateral Cooperation and Problems of Democratic Legitimacy,” Working Paper (Kennedy School of Government, Harvard University, 2001), available @ http://ksgnotes1.harvard.edu/Research/wpaper.nsf/rwp/RWP01-004/$File/rwp01_004_nye_rev1.pdf, accessed May 23, 2001.

DIETER ZINNBAUER is a 4th year PhD candidate at the Development Studies Institute, London School of Economics. His research focus is the use of the Internet by civil society organizations in the Asia-Pacific region. Mr. Zinnbauer has also worked as a consultant for various Internet projects for developing countries and is currently editor of the Internet Governance Information Service, which aims at facilitating information exchange on Internet policies among new Internet stakeholders in the Asia-Pacific as part of a regional Internet initiative by the United Nations Development Programme (UNDP). *E-mail*: d.zinnbauer@lse.ac.uk

BACK TO TOP

Internet, Civil Society and Global Governance: The Neglected Political Dimension of the Digital Divide

Dieter Zinnbauer

Keywords: Digital divide; civil society; global governance decision-making; grass-roots empowerment; plurality of voices.

Abstract: The author of this essay on the implications of the digital divide for civil society participation in global governance makes three points. First, he argues that the framing of the digital divide merely in terms of abstract resource/skill inequalities is incomplete and misleadingly detached. The point is illustrated by assessing the implications of the digital divide on the chances for voice and representation of civil society organizations in global governance processes. This analysis leads to the second point, that even in the digital age, it is first and foremost a number of political factors, domestic and international, that determine the chances of civil society organizations to participate in global governance decision-making. These political conditions take precedence over digital resource inequities. The primacy of the political is further corroborated by the third point. Looking at the potential of the Internet to further emancipate civil societies in developing countries from Western-established advocacy and lobbying infrastructures it is concluded that a number of—this time exogenous and international economic and regulatory coordinates—crucially shape the chances of a more disintermediated digital voice in global governance. Due to the novelty of the Internet, evidence to support this line of reasoning is still thin. Though somewhat speculative, some arguments are as plausible as the mainstream strands of thinking on the digital divide. The author hopes that this essay will inspire a fresh look at the foundations and implications of the digital divide, a debate, which has for too long been fixated on abstract resource inequities avoiding a more profound but undoubtedly less comfortable look at systemic distortions and political responsibilities

full text

Author: **Peter Westrin**
Title: **Critical Information Infrastructure Protection (CIIP)**
Year of issuance: **2001**
Issue: **Information & Security. Volume 7, 2001, pages 67-79**
Hard copy: **ISSN 1311-1493**

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP)

Peter WESTRIN

Table Of Contents:

1. Introduction

One of the remarkable features of modern, computer-based society is that so many things must *work right*. Seemingly endless small details must function correctly and in co-operation in order to maintain processes, which we take for granted. A single “bug,” the smallest aberration, so subtle as to be virtually impossible to foresee, can initiate a complex chain of events, the effects of which can manifest themselves at a national or global level.

An example of a small cause, which can lead to a large effect, is the case of the digital group selector in an electronic telephone exchange. A single erroneous binary digit in a particular shift register can instantaneously break off ongoing telephone conversations and recouple them randomly. Thousands of callers can suddenly be directing their conversations to complete strangers. The distance between a digital parity error and its social consequences may be incredibly short.

That such embarrassing situations seldom occur is because of the well-specified nature of the telephone system, its construction and rigorous built-in controls, and its careful testing before mass use. This is the case, generally, for most commercial computerized products, if we disregard computer games and related programs. If these latter systems do not function sufficiently well or otherwise lack reliability, they will soon fall to the competition. System programs inhabiting our PC's are examples of products, which are considered to function "well enough" in order to be acceptable to the average user. One reason for this is that the consequences of program failure are usually tolerable for the user.

Operating and monitoring systems for nuclear power plants, or transaction systems in the world of banking, are quite another matter and require high reliability. Even here, though, errors occur. Recently, the payment system of a major Swedish bank broke down repeatedly during a two-week period, causing considerable trouble for millions of customers nation-wide. The bank in question reported that the reason for the disruption was the "human factor." No further details have hitherto been released.

Was this too the case of a minute detail causing an entire system to collapse? Any given system can, per se, function sufficiently well and perform reliably after being tested and "run-in"—which, of course, can take its good time. It is therefore understandable that large, complex systems, which cannot be tested fully by way of simulation, often have (seemingly endless) running-in problems, in which unexpected "features" arising out of millions of minute details can lead to high-level system consequences. This is something that we will have to learn to live with. For even as our knowledge and competence in regard to system reliability increases, new demands of functionality will likewise increase, and thereby even system complexity.

However, despite the fact that breakdowns in banking and payment systems can have nation-wide consequences, or that running-in disorders in a subway system can affect millions (as was the case in Stockholm last year), such disruptions are, in substance, *local occurrences*. That is, the disruptions are contained within a given, restricted system. There is a certain delimited, more or less well defined function or service, which is affected, and there are usually more or less acceptable reserve procedures or backup-functions. In short, there are ways to get around such problems, and one can hardly maintain that they constitute a serious threat to society, let alone threaten society's very existence.

And with this in mind, we seem to have identified something of a paradox as concerns our perceptions of modern, "high-tech" society: namely, its apparent *robustness*. Certainly there are disruptions—e.g. in traffic systems, electricity distribution and banking transactions. And accidents do happen—dams burst, airplanes crash, trains collide and ships sink. But on the whole, and in light of the sheer amount of activity at hand, our modern, technology-based society would seem to function exceedingly well.

Modern technology has been developed and exploited to the affect of creating both a safer and more comfortable society. Crisis management becomes more effective when technology creates increased redundancy and flexibility. Margins of safety, buffering us from catastrophes such as floods, famine, earthquakes and epidemics, have become wider in those areas of the world where modern technology has been most widely applied to societal development. The disruptions we do experience are most often local, the consequences of which are understood and relatively limited, and with known procedures of mitigation.

Once in a while however disruptions occur which we can designate as constituting major disturbance for an entire nation or region. The power failure in Auckland, New Zealand, and the so-called ice storm in Canada in 1998 are examples of (relatively) catastrophic disruptions at the urban and regional levels, respectively. In the former event, an urban center's commercial activity was paralyzed by protracted power shortages caused by repeated power cable failures. The disruptions had relatively far-reaching economic and demographic consequences for an entire urban area.

The ice storm in Canada, in which a whole region went without electric power during severe weather conditions, involved an even greater population than in Auckland, and required rescue operations on a wartime scale in order to keep the situation under control.

Both cases involve infrastructure failure. In the case of Auckland, the cause of the disruption involved inadequate infrastructure maintenance, whereas in Canada it concerned "forces of nature" for which the infrastructure—in this case the electricity distribution system—simply was not designed to weather.

At this point, and in the context of Information Technology and Critical Information Infrastructure, the question arises: Are we evolving towards an ever more robust society, or are we heading towards a situation where the risk of *a really major, society-threatening chain reaction of IT-related events is increasing*?

2. Societal Infrastructure

All of the disruptions hitherto referred to have involved societal infrastructure systems. Although the concept of *societal infrastructure* can be defined in a number of different ways, for the present application we find it most appropriately defined as: The totality of publicly utilized functions and services which constitute the conditions for the maintenance of social and productive relationships, as well as the framework for further societal development.

Certain forms of infrastructure, or infrastructure sectors, are of special importance for modern society. These so-called *critical infrastructures,* which are also critically interrelated and interdependent, include electricity production and distribution, transport, telecommunications and water supplies. Emergency services and government or administrative services can also be included. If any of these *infrastructures* ceases to function for a prolonged period, society will be hard pressed to maintain its functioning as a whole.

With current and future rapid developments in society's dependence on IT, this list of critical infrastructures will have to be extended to other sectors. And as this very fact attests to, one of these critical infrastructures distinguishes itself from the others: data-communication and its associated computers (in the wide sense of the word) and (world-wide) networks.

The *information infrastructure* is the term usually used to describe the totality of such interconnected computers and networks, and the essential information flowing through them. The distinguishing characteristic of the information infrastructure is that it is all embracing—it links other infrastructure systems together. Take away the information infrastructure and many other critical infrastructure systems will shut down relatively quickly.

Electricity supply is in many ways as all embracing as the information infrastructure. However, one can compensate for power failures by means of reserve generators placed at strategic locations. In many cases, this is not possible with the loss of critical information flows.

There are certain parts of the information infrastructure, which are especially critical. These are the data networks which monitor and control important societal function and services. These include electricity distribution, telecommunications, banking services, rail and air traffic control and emergency management systems, as well as stock exchange and securities management. Presently, many of these systems are relatively isolated and thus (relatively) secure from intrusion. However, with the accelerated pace of development within the IT-sector it will be all the more difficult for collective systems to isolate themselves from the outside world, and to maintain the boundaries between "inside" and "outside."

2.1 The Network Society

What we call the *Internet* is the top of an iceberg, which is currently in the process of changing society the world over. While creating vast new opportunities it is creating, and will continue to create, new risks and threats that will be difficult to anticipate.

The Internet is primarily employed as a means for transferring information between people. There are also dedicated networks for monitoring and controlling all types of technical systems and computerized processes. In such networks, data flows directly into control systems and affects their physical functions. Technically, there is no obstacle to using the Internet even for such purposes. And in this event, local, dedicated networks will become integrated into the whole of the Internet.

It is in no way unthinkable that, within the not so distant future, every person on Earth can, in principle, reach and influence every other person, as well as a good portion of society's collective technical infrastructure. If, added to this, the mutual interaction between such systems and networks continues to increase at the present, or even accelerated rate, then we are going to be faced with an extremely complex system of problems which will have bearing on the function and stability of the world system as a whole.

Where does one place responsibility for the maintenance of critical societal functions if these become mutually dependent and complex to the extent that there is no longer any way to understand how such a complex will behave, or how to exercise control over it.

In his book on "normal accidents," Perrow [1] argues that in an interactively complex system two or more discrete failures can interact in unexpected ways, thereby affecting supposedly redundant sub-systems. A sufficiently complex system can in fact be *expected* to have many such unanticipated failure mode interactions, making it vulnerable to inevitable accidents.

2.2 The Threat to the Information Infrastructure

Modern society’s infrastructure has always been, and still is, vulnerable to physical threat. Severe weather conditions, earthquakes, floods and sabotage are examples. Threats of these types can be categorized and analyzed, and given their own special defensive or mitigating strategies. They can be made intelligible, their consequences described, and they originate, in a seeming well-defined way, from the “outside.”

The threats that we may face as concerns the information infrastructure are of another kind. They are not well-defined or specified beforehand, we cannot take in their potential consequences and in the developing, all embracing network society these threats may be seen as originating form the “inside.”

As concerns sabotage, the information infrastructure can be employed as a means to bring about the disruption of critical infrastructure—including the information infrastructure itself. Information can be stolen or manipulated. Computers can be infected with malicious programs, which can disrupt not only software and immediate associated hardware, but also adjoining or bordering technical systems—as well as trust and confidence in society as a whole.

The network society bears within itself the seeds of a crisis of confidence, as the individual member of that society finds it more and more difficult to gain an overall understanding of the social and technical environment, or to identify responsibility for its maintenance.

2.3 Critical Nodes and Links

An important question arises: will the IT-based network society become increasingly unstable on the basis of its increased complexity alone and, if so, how will these instabilities express themselves?

The network society is characterized by a system of integrated networks consisting of nodes and links. How can we identify those nodes, which are “critical” for the network society itself. One way is to designate a node as critical if either:

- It alone can exert such influence on other nodes that a serious disruption of societal infrastructure can occur; or
- It forms an integral part of an ensemble of nodes, which can be attacked or otherwise influenced in a similar manner, such that the aggregate malfunction can lead to serious disruptions.

An examination of all likely nodes in order to estimate criticality would however be exceedingly time-consuming and only give results with an early expiration-date, both because of the rapid rate of development within the IT-sector and the fact that such an examination would involve a myriad of details in system construction and implementation. On the other hand, it may be the case that no single node can ever be disqualified as being non-critical!

An example of the fact that many similar nodes can be critical at the same time comes from the collapse of AT&T•s long-distance telephone switching system in January 1990. Because of a “bug” in an updated portion of a systems program, put into operation on 80 of AT&T's switching systems nation-wide in the US, a chain reaction of shutdowns occurred. The culprit was a specific piece of status information exchanged between stations.

In this case, no single node was "more critical" than any other node. The defect was in the system as a whole. A penetrating account of the course of events and its underlying causes is given by Bruce Sterling.[2]

2.4 Complexity and Vulnerability

Two seemingly conflicting forces are at work in the network society. On the one hand, new means of communication make accessible to the average citizen an almost unimaginable array of new sources of information and services—as well as the prospect of becoming an active party in countless new collectivities and processes. At the same time, the increasing supply of information and the escalating technical complexity of the network society make it all the more difficult to identify potential malfunctions, find their sources and treat them in an adequate manner. The *consequences* of such potential malfunctions—above all their indirect or wider sociological effects—are becoming increasingly difficult to foresee.

The concept of the network is thus central to all discussions of society's intrinsic vulnerabilities. The combination of an exponentially increasing number of human-computer and computer-computer transactions, and the coupling of communication networks on a global scale open up new possibilities for faulty instructions or malicious code—in whatever form—to spread globally.

In the case of the above mentioned digital telephone switches, in which a single binary digit could create such bizarre effects, it is relatively easy for systems engineers to determine the consequences beforehand. For sufficiently complex systems however it is virtually impossible to anticipate all the potential consequences of errors occurring at the micro-level. Many such errors may be controllable. Some will emerge at the highest system level and give rise to local disruptions. Will some slip out of the local system and propagate unrestrained on a global level?

In two interesting articles, Pastor-Satorras and Vespignani [3] and Duncan Watts [4] address two aspects of error propagation in networks. Pastor-Satorras and Vespignani analyze cases of network virus infections on the Internet and examine their average lifetimes and persistence. On this basis, they then describe a dynamic model for virus propagation in "scale-free" networks and discover that they cannot find any epidemic threshold or associated critical behavior involved in such propagation. If this model in fact captures the essence of the dynamics of such a propagation process, then there is no "virus"—no matter how poorly constructed—which cannot propagate on the Internet.

Watts brings up another aspect of error propagation, namely, how small, local disruptions (chocks) can—in singular cases—trigger widespread cascades in a network consisting of interacting agents. A possible explanation for such processes is described in a model in which each agent's decisions are dependent upon its nearest neighbor's actions—in accordance with a simple threshold rule. Watts investigates the conditions for such a cascade and why it is difficult to anticipate. The model covers a wide range of cascading phenomena, including cultural fads, innovations and social movements, as well as error propagation in infrastructure networks.

3. How Do We Assure the Information Infrastructure?

Since the putative new societal risks and vulnerabilities are directly or indirectly related to the development and utilization of new technologies, it would therefore seem natural to follow a chain of analysis beginning with technical specifications and casually running “up” through systems, actors, threats, vulnerabilities, consequences and, finally, counter measures/ mitigation.

However, in view of the rapid technological developments constantly taking place, and the particular nature of their implementations, one can raise certain objections to such a synthetic scheme. If, for instance, one carefully examines a relatively localized subsystem from the point of view of risks and threats, thereby identifying certain of its vulnerabilities, in what way can these insights be generalized and established in order to utilize them “beyond” the subsystem itself, on a higher system level?

One might hope that certain “typical” system components or operations might be found in many subsystems, but in order to identify these one would need to have access to a good number of such systems for comparative studies. This however would be extremely time-consuming, and the rapid development of new systems and networks would quickly render such comparisons obsolete.

Furthermore, it is highly unlikely that detailed access to more than a few such systems will be available to research directed towards this end. Systems for such services as finance and security exchange, or data communication in general, will most probably remain inaccessible for analysis.

What would be required is a filtering mechanism by which the technological background noise could be eliminated to the benefit of those more enduring, central factors—which need not at all be “technical” in nature. If such a selection process is impossible to devise—perhaps because no single bit of information can, in advance, be characterized as irrelevant—then we will need to gain insights into the problem complex by working with its different levels of causal action *in parallel*, and attempt to put each of these into mutual context.

It may very well be that critical vulnerabilities, and even the worst consequences of infrastructure disruptions, will not be traceable in any useful way to single technical subsystems—perhaps as a consequence of an already overwhelming system complexity. Perhaps the analysis of vulnerability should be based instead on *functional units*, whose interactions with each other and with the environment as a whole can best be described by way of their societal manifestations as a whole, with less emphasis placed on the technical.

To the extent that this is the case, one of the most important problems for CIIP research is to identify relevant *functional units* and to describe their mutual relations. This perspective also implies that it will be difficult to differentiate between “insiders” and “outsiders”—in some sense we will all be insiders.

3.1 Unforeseeable Consequences of Disruptions in the Information Infrastructure

When we talk about the consequences of disruptions to the infrastructure, we usually think about the more established, direct effects, quantifiable in the form of injuries to people, damage to the (built up and natural) environment, and—of course—in terms of dollars and cents. Other, more indirect and/or non-quantifiable manifestations can, in fact, create the really dangerous consequences for society. One of the conditions of a secure society is a measure of basic trust among the citizenry for the mechanisms, which govern it—i.e. that one has confidence in its inherent stability.

At some point, there will be a limit to a population's tolerance towards IT-related disruptions—especially when these seem to have inexplicable or unintelligible causes. Tolerance will turn into doubt, suspicion and anger directed towards a network society seen as having become uncontrollable.

3.2 Where Rests the Responsibility for Assuring the Information Infrastructure?

Who is responsible for the Internet? This is not primarily a question of who is responsible for maintaining the Internet's *technical* functions, but rather for the enormous amount of information flowing in this worldwide network.

Since the very idea of the Internet is based on free, anonymous flows of information, every sender or poster of information is responsible for what he or she sends, and every receiver of information is responsible for interpreting and making use of this information. In this sense, everyone, and no one, is responsible.

How does this tally with other information systems and networks? The more local, bounded and (relatively) simple a system is, the easier it is to define what is *correct* and what is *incorrect* input and output. As long as there is a specification, such that any state of the system can be tested against it, and as long as it is meaningful to define an outer interface to the system, then some consequential form of responsibility for the system in question can be positioned within its system boundaries.

When systems—including infrastructure systems—begin to blend into one another due to increasing IT-utilization and increasing functional demands, then it is useless to attempt to maintain the fiction of separate systems, each with own internally demarcated mode of responsibility. The distinction between *inside* and *outside* the system, and even the concept of *systems boundaries* as such, becomes blurred.

No firewall, security system, control system or certificate in the world will help when it is no longer possible to determine what is correct or incorrect, before a disruption propagates up through the system structure and manifests itself on the social or political-ideological plane.

This argument concerns primarily so-called *soft* information. As concerns purely technical functions, we may hope that—even in the future—it will be possible to demand responsibility from an electricity supplier when the lights go out, or from the banks when your e-payments fail to go through and you end up with bad credit ratings.

The possibilities of national or local governments regulating the network society, in order to better assure future information infrastructure, would also seem to be minimal. No central authority can control a network—a state of affairs that is, so to speak, built into the very concept of network society.

4. The Vulnerability of the Information Infrastructure to Intentional Disruption

Who, can we imagine, would attempt to damage society by way of attacking the information infrastructure? The outline of possible actors includes hostile states, terrorist groups and fanatical religious movements, criminal organizations and extremist political parties as well as discontented insiders and irresponsible hackers and crackers.

An aggressor, or group of such, who would attack society through its information infrastructure has, in principle, adequate opportunities to cause major damage. However, they will be confronted by a number of difficult practical problems. Our attacker must work secretly and exploit the complexity, speed and opacity of the computerized systems at hand. He (or she) must attempt to calculate the consequences of the contemplated attack, which can itself be a very complex matter and will require a number of correct assumptions concerning countermeasures and operator intervention during the process.

One important factor, which may increase an attacker's chances of success, is that the mental preparedness of non-specialists—as concerns managing computer-related disorders—decreases in relation to increases in computer reliability, a condition that may provide a false sense of security. In addition to this, those still occurring, but all the more exceptional, computer errors often resemble one another structurally, thus increasing the risk of stereotype reaction from users, and thus rendering the discovery of, and measures against, IT-related attacks all the more difficult.

With current developments in IT, it follows that information sent from person to person is seldom sent directly, but flows through a number of anonymous, intervening links and processes. Information injected through evil intent, or even by mistake, can spread through systems in which human operator-control is becoming all the more rare, and the possibility of tracing the source of the "error" all the more difficult.

In the context of conventional threats, accessing the vulnerability of an IT-based system to "external" attacks amounts to evaluating the necessary physical violence required to penetrate a node's (physical) defense, and the effect of the information reduction resulting from its disruption. In the case of an info-logical threat, we need to know how an aggressor can penetrate the node's info-logical shell (or its "protection in depth"), the effect of reduced information—*and* the effect of (further disrupting) false information emanating from the attacked node and how this may effect a wider system context. This last point makes the problem considerably more complex, and demands much more foresight as concerns analysis and preparedness planning.

5. CIIP-Research in the Future

The question of generalizing and establishing over time the results of studies involving information infrastructure protection is itself a fundamental issue. Does the area of CIIP have a classifiable structure and content which is sufficiently stable in time, such that it will provide a foundation for durable protection and preparedness planning?

At the present time, it would appear that the answer to this question is “no.” The problem complex that CIIP deals with represents one of the most dynamic social phenomena in history. Only when this area of research has gained a more stable scientific and methodological base will we be able to change this assessment.

Thus in the short and middle term, developments may dictate that we best direct our efforts towards mitigating—i.e. diminishing the *consequences*—of disruptions to the information infrastructure, rather than attempting to totally prevent their occurrence.

The United States was the first state to take particular notice of the IT-threat to critical infrastructure. The report from the PCCIP [5] (the President’s Commission on Critical Infrastructure Protection) puts forward a complex threat assessment in order to discuss what must be done to assure critical infrastructure.

In Europe, both at the strategic/policy level and as concerns research, there are a number of activities in progress with strong association to the area of infrastructure protection. The European Dependability Forum [6] is a European Commission initiative promoting information exchange and discussions on the dependability of Information and Communications Technologies (ICT). The aim of the forum is to provide a platform for exchange of information over a wide range of technical and policy-related domains associated with the dependability of ICT-systems. One of the major concerns is the potential consequences of massive disruptions cascading through the different systems.

The Center for Security Studies and Conflict Research at the ETH in Zurich is developing the comprehensive Risk Analysis and Management Network CRN [7] —an electronic platform for promoting risk-profiling dialogue. Current project partners are the Swedish Agency for Civil Emergency Planning and the Swiss Federal Office for Civil Protection. The project is supported by the Swiss government and additional partners have been invited to participate.

At the Swedish Defence Research Agency (FOI), a long-term research program concerning “Critical Infrastructure Protection” is currently in progress. The program is sponsored by the Swedish Agency for Civil Emergency Planning and is focused on the evolution of the information infrastructure and IT-related threats and vulnerabilities.

Within a few years, and in co-operation with other research groups and other national programs, we hope to be able to establish a coherent plan of research for the study of the evolution of the IT-network society in general, and the development of threats and vulnerabilities to the information infrastructure in particular.

ACKNOWLEDGEMENT: This work is kindly sponsored by the Swedish Agency for Civil Emergency Planning.

DISCLAIMER. The opinions expressed in this article are those of the author and do not necessarily reflect the official standpoint of FOI.

Notes:

1. Charles Perrow, Normal Accidents: Living with High-Risk Technologies (New York: Basic Books, 1984).
2. Bruce Sterling, Hacker Crackdown, Law and Disorder on the Electronic Frontier (Bantam Books, 1993). Also available @ http://www.lysator.liu.se/etexts/hacker/.
3. Romualdo Pastor-Satorras and Allessandro Vespignani, "Epidemic Spreading in Scale-free Networks," Physical Review Letter 86, 14 (2001): 3200-3203.
4. Duncan J. Watts, "A simple model of fads and cascading failures," (submitted to Physical Review Letter). Available @ http://www.santafe.edu/sfi/publications/Abstracts/00-12-062abs.html, December 2000.
5. Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures, Report available @ http://www.ciao.gov/CIAO_Document_Library/Preliminary_RandD_exsum.htm.
6. European Dependability Initiative: http://deppy.jrc.it/default.
7. Comprehensive Risk Analysis and Management Network (CRN): http://www.isn.ethz.ch/crn/index.cfm.

PETER WESTRIN has a PhD in theoretical physics and long professional experience in the development and utilisation of complex simulation systems -- both in academic and industrial contexts. His earlier work in the area of electronic warfare -- which for security reasons has not be published -- has provided a special background for his present work concerning infrastructure vulnerability and the network society. He is currently director of a long-term research program for the study of critical infrastructure protection. Present affiliation: Swedish Defence Research Agency, Division of Defence Analysis, SE-172 90 Stockholm, Sweden. E-mail: peter.westrin@foi.se.

BACK TO TOP

Critical Information Infrastructure Protection (CIIP)

Peter Westrin

Keywords: Critical Information Infrastructure Protection, CIIP; security; cyber threats; conventional vs. IT-related security threats; infrastructure vulnerability; CIIP R&D; network society.

Abstract: This article treats a number of fundamental issues concerning Critical Information Infrastructure Protection, including the basic concept of CIIP as such. What are we actually referring to when we talk about a society's critical information infrastructure and against whom or what must we be prepared to protect this infrastructure? The notion of "network society" is central here, and certain aspects of societal development within the framework of CIIP are discussed. These include the issues of responsibility and trust, and whether or not CIIP is primarily a technological problem. Some basic differences between conventional threats and IT-related threats are discussed, as well as important issues concerning system complexity, error propagation and mutual dependence. Also discussed is the question of whether it is, in fact, possible to establish a solid and durable framework for research into a problem context such as CIIP, a context which is both fragmented and continually developing at a rapid pace. The article concludes with a short description of on-going CIIP-research

full text

Author: **Ralf Bendrath**
Title: **The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection**
Year of issuance: **2001**
Issue: **Information & Security. Volume 7, 2001, pages 80-103**
Hard copy: **ISSN 1311-1493**

THE CYBERWAR DEBATE: PERCEPTION AND POLITICS IN US CRITICAL INFRASTRUCTURE PROTECTION

Ralf BENDRATH

Table Of Contents:

1. The Information Society as Risk Society

"Cyberwar" has become a growth market in the US. While ten years ago the term would hardly have made sense to any expert, in the meantime attacks on computer networks and their implications for national security have received broad coverage in the media. In the broad range of service providers from technical security solutions to policy advisory groups, a whole cottage industry has sprung up. Warnings of an "electronic Pearl Harbor" or a "cyberwar" against the US' infrastructures by "rogue states" or terrorists are part of the standard repertoire in security policy analyses. Bill Clinton started the process of developing a strategy with his Presidential Commission on Critical Infrastructure Protection in 1996, and the new US government under George W. Bush is likewise trying to address the problem.[1]

As with nuclear energy production, the dangers arising from digital networking are not easily discernible for a non-expert. To detect a virus on your hard drive, you need a virus scanner as a sensory tool; to find out if there is a cracker in your network, you need an intrusion detection system or a competent system administrator with spare time. For the average user, an intentional hacker attack cannot be distinguished from a technical failure, like a hardware defect, a software malfunction or a “normal” system crash. In the case of denial-of-service attacks, it is not at all obvious whether the computer that is no longer providing its service has just crashed, whether the cable connecting it to the Internet was physically damaged, or whether it is the victim of a targeted flood of packets and requests.

The so-called “information society” is thus showing significant signs of being a “risk society.” The new risks, according to Ulrich Beck, who coined the term in the 1980s, are no longer immediately obvious, and therefore they are especially open to political interpretation and instrumentation. “It never is clear if the risks have become worse or our look at them just has sharpened.” [2] This is especially true for insecurities related to the infrastructure.

As early as 1990, the US National Academy of Sciences began a report on computer security with these words:

> “We are at risk. Increasingly, America depends on computers. [...] Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb.”[3]

This quote is typical for a whole series of warnings issued by the intelligence community, the FBI, and other government agencies in the last ten years. They focused especially on the so-called “critical infrastructures” like telecommunications, financial services, electricity, and water or fuel supply. A concerted action of qualified hackers with hostile intentions, they feared, could force a whole nation to its knees. The biggest possible damage was named “electronic Pearl Harbor.” [4]

Compared to the traditional security threat, which consists of the dimensions *actor*, *intention*, and *capabilities*, “cyberwar” threats cannot easily be categorized. First, there is no clearly identifiable *actor* who could become a possible enemy. The cyber attackers can be teenagers, rogue nations, terrorists or disgruntled insiders, even private companies or political activists like the critics of globalization. This implies, secondly, that it is very hard to get verifiable information on the *hostile intentions* of the possible attacker: Does he or she want to attack the US at all? Is he planning to use cyber attacks? This leads to the third open question: Does the possible enemy have the *capability* to wage a large-scale cyber attack against the US? It is far from clear even in the intelligence community if strategic rivals like China or Russia already have the technology and, even more important, the knowledge and qualified personnel to hack into computers that control critical infrastructures. Traditional means of intelligence do not help very much in this field, because the capabilities for an attack largely consist of software, commercial-off-the-shelf hardware components, and an Internet connection. In its 1997 report, the President’s Commission on Critical Infrastructure Protection explicitly wrote that the possible enemies are unknown, while the tools for cyber attacks are easily available.[5]

To conclude: In the case of cyber risks, almost everything is new. The weapons are not kinetic, but software and knowledge; the environment in which the attacks occur is not physical, but virtual; the possible attacker is unknown and is able to hide himself effectively even during an attack.

From a political science point of view this is an extremely interesting case. What does a state do when the strategic context of its security policy has changed radically? Which strategy will be employed to cope with the new insecurities: risks instead of threats? Which agency inside the government will become responsible for countering the risks? Will the security strategy be focused on retaliation, on minimizing the possible damage after an attack, or will it aim at preventing an attack in the first place?

The US was the first nation to address the problem of critical infrastructure protection seriously. The government put a lot of effort into thinking about it, and the newly founded agencies and institutions responsible for this task have gained some years of experience since. A detailed review of US critical infrastructure protection policy can thus help us understand the possibilities and limits of infrastructure protection in general.

The following analysis will be guided by a framework developed in a project on "international risk policy" which was conducted by the Center on Transatlantic Foreign and Security Policy Studies at the Free University of Berlin.[6] It will look at three different sets of factors that might have an influence on the formulation of any risk policy: Risk perception, resources, and norms.

2. Factors Influencing the Development of a Risk Policy

2.1. Risk Perception

Capabilities as a Starting Point

The complexity of world society after the end of the Cold War has led security politicians and experts to focus more on the capabilities of possible enemies than on their intentions. This applies just as much to nuclear proliferation or ballistic missiles as to "international terrorism." Security assessments rely more and more on the technical means that might be available to possible enemies. The new potential for cyber attacks was addressed in similar terms in the debate.

The change in the general perception of insecurity coincided with growing concerns in the Department of Defense over the vulnerability of the networked armed forces. While the debate on the "Revolution in Military Affairs" (RMA) was kicked off with extremely high hopes in the early 1990s, with trendy articles and studies on "network-centric warfare" or the real-time information flow through the global "system of systems" for C^{4}ISR,[7] since the mid-1990s one finds more and more warnings on the risks. Because a great deal of military communication is forwarded through civilian infrastructures, the risks that civil infrastructures are exposed to attacks from hackers and other intruders were also seen as a threat to military security.[8]

This analysis did not develop by chance—it grew parallel to the development of offensive information warfare capabilities and strategies in the US military (see 2.2.). As the debate on attacks against the information systems of possible enemies went further, the eventual dangers for the US' own military and civilian data networks became a major issue as well.

What makes the whole debate on the vulnerability of electronic infrastructures typical of current risk debates is the lack of experience. Many studies and warnings are filled with only anecdotal collections of well-known hacks, others try to estimate the risk based on simulations with “red teams.” The latter cannot be well compared with reality, because the “red–team” hackers were members of the attacked institution and therefore had a great deal of knowledge about system architectures or the culture of the operators. Additionally, these simulations and exercises were never held under real conditions, but on simulated systems. During the exercise “Eligible Receiver” in June 1997, which is often taken as evidence of the US military data networks’ vulnerability, only unclassified or simulated systems were attacked.[9] Furthermore, one often finds impressive data on the *numbers* of known hacker attacks, but in almost all cases a statement on the *damage* is lacking. A serious risk calculation, however, would have to include an estimate of the probability of an incident *and* of the possible amount of damage.

All statements on the scope of the danger therefore are more or less speculative. Furthermore, there are still no clear criteria for deciding what is an attack and what is not. Until 1998, the Pentagon counted every attempt to establish a telnet connection (which can be compared with a knock on a closed door) as an electronic attack.[10] As yet, there are no standard procedures for identifying and assessing the vulnerability of critical infrastructures. These have been under development by the Critical Infrastructure Protection Office’s project “Matrix” since June 2000.[11]

Due to these uncertainties, the risk estimates always move between paranoia and carelessness, without ever being precise. The relevant studies and analyses are therefore full of terms like “capability,” “possibility” or “could.”[12]

The resulting simplification of this pattern of argumentation can be seen in the simple claim voiced by Deputy Secretary of Defense John Hamre in a Congress hearing in June 1996: “Mr. Chairman, there will be an electronic attack sometime in our future.” [13] In this way, the discourse on cyber dangers has been strongly popularized, because many of the political recommendations from think tanks or staffers were derived from scenarios—and these are nothing else than claims about future events. From the mid-nineties on, the RAND Corporation and the Defense Advanced Research Projects Agency (DARPA) ran a series of exercises based on the ‘Day After’ method. In a first step the participants were taken five years into the future and confronted with a number of cyberwar attacks. They had to react under time pressure and, for example, draft a briefing and outline recommendations for the Secretary of Defense or the President. In a second step, they were taken back to the present and discussed how to prevent such events by acting today.[14]

One question is never addressed within this discourse: How plausible are these scenarios? The participants learned to deal with them as external, given realities, and the scenarios established a specific fear-driven cyber mindset in the security policy community, even though many of these assumptions have proven wrong in the long run.[15] This is a good example of how to establish a threat-based discourse in the absence of a clear danger, where there is only the risk of a potential future threat. In other words, like a member of the Syndicate once said to Agent Fox Mulder in the TV show, The X-Files: The best way to predict the future is to invent it.

However, this approach has placed cyber-risk on the political agenda. The main remaining question was: How to deal with it? Or, maybe more important in the fragmented political landscape of Washington: Who should be in charge? Should it be the classical institutions responsible for national security, like the Pentagon or the intelligence agencies? Or the FBI with its computer crime squads? Or maybe just the private companies running the infrastructures? The answer was at least partly dependent on the specific way potential enemies or damages were cast.

Military Rivals

In the summer of 1995, the National Intelligence Council reported on the information warfare capabilities of other international actors for the first time. The document is classified, but its conclusions were presented to the public. According to the report, some states are building up their capabilities for waging information warfare, but mainly focus their efforts on using them in the context of a conventional military conflict. They do not plan to attack national infrastructures, but military communications networks or air defense systems. Even after searching very hard, the National Intelligence Council found no evidence of so called "rogue states" developing capabilities for information warfare or recruiting foreign hackers for this task.[16]

In May 1998, President Bill Clinton gave the intelligence community the explicit order to collect and process information about the electronic threat from other nations.[17] Today the intelligence agencies distinguish between two kinds of threats:

> "The unstructured threat is random and relatively limited. It consists of adversaries with limited funds and organization and short-term goals. While it poses a threat to system operations, national security is not targeted. This is the most obvious threat today. The structured threat is considerably more methodical and well-supported. While the unstructured threat is the most obvious threat today, *for national security purposes we are concerned primarily with the structured threat, since that poses the most significant risk.*"[18]

The states most often named as possible sources of such a structured threat are China and Russia. The evidence for real capabilities in these countries is thin, though; it consists mostly of quotations from officers' publications about the new possibilities of cyberwar or asymmetric warfare.[19] Even Timothy L. Thomas of the Pentagon's Foreign Military Studies Office, who probably knows more than any other American about the developments in China and Russia, only lists the specialized "infowar" units of the People's Liberation Army, but cannot provide information on their capabilities. The Russian concept of information warfare, on the other hand, differs significantly from the US view, aiming more at psychological manipulation and less on computer network attacks.[20]

Another group of actors that the intelligence community is concerned with are international terrorists.[22] The National Infrastructure Protection Center (NIPC) for example warned that Osama bin Laden might possibly be planning a computerized version of the Oklahoma bombing.[23] To date, though, terrorists have not been very active in cyberspace. All that is known is that they make use of computers, the Internet or cryptography for organizational purposes.[23] "We have yet to see a significant instance of 'cyber terrorism' with widespread disruption of critical infrastructures," FBI-director Louis Freeh had to tell the Senate in February 2000.[24] Johan J. Ingles-le Nobel, deputy editing director of *Jane's Intelligence Review*, came to the same conclusion after extensive research and debates among hackers: "In theory, cyberterrorism is very plausible, yet in reality it is difficult to conduct anything beyond simple ‘script-kiddy’ DoS [Denial of Service] attacks.”[25]

What is left are the hacker attacks—in terms of the intelligence community, an unstructured and limited threat that does not pose a danger to national security. So far, there has been no incident in which hackers really damaged critical infrastructures.

Yet, this military-like discourse had much influence on Washington’s security policy establishment; CIA director John Deutch, for example, has regularly warned of threats to national security from cyber attacks since the mid-1990s. Asked in a Senate hearing to compare the danger with nuclear, biological or chemical weapons, he answered, “it is very, very close to the top.”[26] These dangers, according to the security policy agencies and departments, not only arise from states. Jaques Gansler, then Assistant Secretary of Defense for Acquisition and Technology, even called teenagers a “real threat environment” for national security.[27] George Smith of the *Crypt Newsletter* was probably right when he wrote: “Teenagers are transformed into electronic bogeymen with more power at their fingertips than the Strategic Command.”[28]

A very important metaphor in this social construction of the threat was the “electronic Pearl Harbor.” This term connected a historical trauma of American society to the new risks, thus forcing the political elite to respond somehow. The mass media gratefully took up the term and featured it prominently in almost every report on the issue.[29] The concept of an “electronic Pearl Harbor” had a great impact on the US debate, because it constructed both an agent and a structure.

In the agent dimension, it implies a danger coming from an enemy that is geographically and morally located outside of the US. This picture of a dangerous “other” reinforces the idea of the nation as a collective self. Common phrases like “our computers”[30] or “our infrastructures”[31] even amplify this effect. The reference object of security, then, is the whole American society. The logical agent of security policy acting on behalf of it is, of course, the state—not the single computer user or network provider. The logical and political implication of this is that defense against cyber attacks is a task for national security policy.

In the other dimension, the “electronic Pearl Harbor”-analogy implies a structure for security policy. Because the image is taken from military history, it implies a strategy based on analogies to physical warfare. The terms “cyberwar” or “information warfare,” which became popular in the mid-1990s, also furthered the idea of the Pentagon being the natural defender of the nation’s infrastructures. For example, the Defense Science Board in its 1996 study proposed setting up a center for defensive information warfare at the Defense Information Systems Agency (DISA). It was to be responsible for the security of the other departments’ and even of the private sector’s infrastructure.[32] Deputy Secretary of Defense John Hamre made this strategy more than clear on several occasions: “Cyberspace ain’t for geeks, it’s for warriors.”[33] In his last annual report to Congress, President Clinton’s Defense Secretary William Cohen described a role for the DoD in fighting cyber-terrorism as well.[34] This perception is typical for the military and national security policy establishment and has not changed very much under the presidency of George W. Bush. For example, his national security advisor, Condoleezza Rice, called cyberwar “a classic deterrence mission”[35] in March 2001.

Computer Crime

The risk perception of the law enforcement agencies is structured differently. Many critics of a military involvement argued that the “electronic Pearl Harbor”—should it ever happen—would take place inside the US. Thus the Federal Emergency Management Agency (FEMA) or the FBI would be better suited for preventing such an attack or hunting down the perpetrators. Additionally, the FBI was already involved in investigating computer crime and had set up a special Computer Crime Squad in the early 1990s. On the basis of the *Computer Fraud and Abuse Act* of 1986, this unit investigated more than 200 cases until the mid-1990s and had picked up a great deal of information along the way about the practical problems of the risk. Dealing with hacker intrusions, data theft and similar things had led to a more differentiated, but also less dramatic view of the risk. One point that FBI officials frequently emphasize is the practical impossibility of identifying an attacker before a thorough investigation has been conducted. “The trouble is that when an attack occurs we have no way of knowing if this is a kid in Middle America or a serious foreign threat,” said Michael Vatis, the director of the FBI’s National Infrastructure Protection Center up to March 2001.[36]

One key experience, later called “Solar Sunrise,” had a strong influence on this point of view. In February 1998, more than 500 electronic break-ins into computer systems of the US government and the private sector were detected. The hackers got access to at least 200 different computer systems of the US military, the nuclear weapons laboratories, the Department of Energy and NASA. At precisely the same time, the US forces in the Middle East were being built up because of tensions with Iraq over UN arms inspections. The fact that some of the intrusions could be traced back to Internet service providers in the Gulf region led to the initial conclusion that the Iraqi government had to be behind the attacks. A closer investigation of the case later brought up the real attackers: Two teenagers from Cloverdale in California and another teen from Israel. The law enforcement agencies took this as one more proof that one cannot respond militarily to a cyber attack as long as the attacker is not clearly identified. Then FBI director Louis Freeh told the Senate afterwards:

> “Solar Sunrise thus demonstrated to the interagency community how difficult it is to identify an intruder until facts are gathered in an investigation, and why assumptions cannot be made until sufficient facts are available.”[37]

Even intruders who try to bring down whole networks are not called “terrorists” and their activities are not dubbed “war” by law enforcement agencies. They rather call them “criminals” or “digital outlaws,” as did Attorney General Janet Reno at the Cybercrime Summit 2000.[38]

Interestingly, the law enforcement community’s perception of the problem is now being structured by private actors as well. Since 1996, the San-Francisco-based Computer Security Institute has been working together with the FBI’s Computer Intrusion Squad on conducting an annual Computer Crime and Security Survey, a widely recognized study of dangers, cases and countermeasures in IT security.[39] Here, one finds a private-public partnership that is already influencing the risk perception.

Economic Loss

Because many critical infrastructures are run by the private sector, the companies’ perception of the risk was very important as well. It is striking that completely different criteria were applied for measuring and weighing risks in the private sector. The service providers normally do not see the national implications of new vulnerabilities, and they are not overly concerned about tracking down the suspects. Therefore, it is not so important to them *who* breaks into their computers. Their main goal is to keep the systems up and running and to avoid data theft by competitors or intelligence agencies. When a hacker attack is over and the systems are restored, the companies have only a limited interest in informing the police at all.[40] Rather than cooperating with government agencies, they prefer to contract specialized IT security service providers. These normally work more efficiently and less bureaucratically and help solve important day-to-day problems.[41]

Just as important as the top management's risk perception is that of the group of persons often working "in the basement," namely the system administrators and IT experts. They have to deal with hacking attempts almost daily, and for them, the problem breaks down into single, concrete challenges. They install new virus scanners on the company's network, make sure the users change their passwords on a regular basis, try to reduce the server workload during denial-of-service attacks, or restore deleted files from the backup tapes after a hacker break-in. For this technical expert community, the problem currently discussed as a "national security threat" has existed since computers first became networked. Here it is mainly seen as a technical and practical problem, less as a political issue and much less as a question of national security policy. The operative ideas are "computer security" or "IT security," not "national security." Because these experts often are the only ones in an organization who can really assess the details and challenges, their perception also influences the way the management deals with IT security.

2.2. Resources

The Military

The US armed forces are the most advanced in the world when it comes to offensive information warfare capabilities. They are intended to serve as "another arrow in the quiver"[42] in conventional military operations, but also to give the government deterrence and strike capabilities for countering a cyber-threat. The idea is to prevent an attack through strength. It was John Hamre again who made it very clear: "That really was the message of Pearl Harbor. It wasn't that we got hit. It was that we were ready to respond," he told the public in August 1999 at the opening ceremony of the Joint Task Force - Computer Network Defense Operations Center, the central coordination point for the security of all US military networks.[43]

The US military has already been active in digital electronic warfare since the 1980s, when the armed services started their own research in computer viruses.[44] In the early 1990s, when the Gulf war showed the importance of information systems and communications lines for fighting a short, effective war, the development of these capabilities gained more momentum. A special School for Information Warfare and Strategy was set up at the National Defense University in 1994. The US military has had its own Joint Doctrine for Information Operations (Joint Pub. 3-13), which also covers computer network attacks on civilian infrastructures, since 1998.[45] The central coordination point for these activities, the Joint Task Force - Computer Network Attack, was set up and subordinated to US Space Command in October 2000. More units are located at the Air Intelligence Agency in San Antonio, Texas, among them the Air Force Information Warfare Center with more than 1,000 personnel and the

Joint Information Operations Center.[46]

In spite of the growing interest and the great efforts made in this field, the US military has not yet acquired the capability to successfully wage a large-scale cyberwar. The few cyber-missions during the Kosovo war showed this quite clearly. The Air Force waged some cyber attacks on the Serb air defense system,[47] but afterwards came under heavy criticism for the inefficiency of these measures.[48] Cascading effects of information attacks in particular are complicated to estimate, because one not only needs the know-how and technology to get into the enemy's computer systems, but also needs to know how they are embedded in his social organization and strategy.

Law Enforcement

The law enforcement agencies have been dealing with computers for some years now, because normal criminals tend to make more and more use of modern technologies as well. This led to the establishment of the National Computer Crimes Squad at the FBI as early as February 1992. In the same year, the Computer Analysis and Response Team (CART), a specialized unit for computer forensics, was set up. Each of the 56 FBI field offices has had its own Computer Crimes Squad since 1998.[49] The various activities in this field have been coordinated by the Computer Investigations and Infrastructure Threat Assessment Center (CITAC) since 1996. The efforts still are comparably weak. Only 243 out of a total of 11,639 FBI agents are designated for the investigation of computer crimes. Even this number has not been reached yet, and many federal agents are not really prepared for their task.[50]

In spite of these difficulties, the FBI's build-up of specialized computer units has shown some results. During the last year, some spectacular cases of hacking or computer fraud were solved within a very short time. These successes led to greater self-confidence on the part of the law enforcement agencies. After the FBI had caught a student who, only a week before, had circulated a fake stock exchange message intended to manipulate stock values, federal attorney Alejandro Mayorkas told the press in September 2000: "We in law enforcement can navigate the 'information superhighway' just as we can beat the pavement to detect and apprehend criminals."[51]

Private Infrastructure Service Providers

Because almost all critical infrastructures are run by local or private entities, the latter had an important role within the cyber security debate from the beginning. Only here can the technical expertise that one needs to successfully defend against an attack be found. The companies that run the systems can much more easily focus on reinforcing them than on striking back. They install firewalls, redundant emergency systems, backup facilities, and other defensive systems. With these features, they are already helping to protect the US from a large-scale cyber attack, often without viewing this as part of a national security policy strategy at all.

More importantly, the strategic resources available to the infrastructure providers include not only their staff and their firewalls, but also the virtual landscape in which a cyber attack would occur. Unlike the territorial border or the national coastline, this landscape consists of private infrastructures providing public services through the market. In a significant departure from classical territorial defense, attacks in cyberspace can only be warded off by controlling the systems of which it consists. Delegating this task to the state is difficult, if not practically impossible.

2.3. Norms

Neo-Liberalism and the 'Californian Ideology'

A number of strong norms have limited the efforts of the traditional security policy institutions to expand their activities into cyberspace. These norms have had less to do with questions of national security and more with the general relationship between the state and society. The so-called "neo-liberalism," that has gained much acceptance among the elites of western societies in the 1990s, calls for minimal involvement of the state, especially in economic affairs. In the field of new technologies, two additional elements added to this approach: First, a large majority in Washington was strictly against disturbing the dynamic of the 'new economy' by government interventions or regulations. "Government has largely taken a hands-off approach to the new economy," as the report "State of the Internet 2000" concluded.[52]

Secondly, high political hopes were invested in the digital communications media. Many expected that they would help the development of decentralized and self-organized social structures. This so-called "Californian ideology"[53] that also became popular in Washington in the mid-1990s promised an era of free and non-hierarchical association of electronically networked citizens. Within this technology-deterministic and anti-statist framework of norms, to which many of the high-tech companies' leaders subscribed, a strong role for the state in solving problems was hardly the right thing.

In terms of security policy theory, the debate centered on the question of the reference object of security. In plain English: What is to be secured? While the security policy elites saw "national security" in danger, the other side was concerned about the security of individual computer systems and their users. Here, the civil rights organizations played an important role in warning of the unintended consequences of a risk policy based on military strength or repression—mainly the resulting threat to privacy.

Military Identity and Professionalism

The idea of waging war in cyberspace seemed odd for many military officers in the first place. The term "cyberspace" implies a completely different concept of space and body, because the space in question consists only of symbols and their links. Because there are no linear distances like in the Cartesian physical expanse, there is no frontline anymore. The actors in cyberspace are not physically present, but are instead represented by symbols. In this ethereal cyberspace, there is no room for physical violence. The application and organization of physical violence, however, is still part of the professional military identity. "Any time things start to smell like something other than killing people and breaking things, people in the military start pointing in other directions" a Pentagon advisor described this.[54]

Only recently have the armed forces seemed able to accept computer network operations as part of their professional duties, because these have been—at least officially—limited to two tasks: The protection of their own networks and attacks against military enemies in times of war.[55]

Legal Norms

Experts in international law are still debating if cyber attacks can be considered acts of war at all.[56] But if this is the case, a strategy based on electronic counter-attacks could break the law of armed conflict. Military cyber attacks, for example, would ignore the rule that a regular soldier has to wear a uniform, but would also be at odds with more important norms codified in the Hague and Geneva conventions. These international treaties, for example, prohibit perfidious or unnecessary attacks, the use of the territory of neutral states, attacks on civilian populations or weapons that do not distinguish between combatants and non-combatants.[57] The fact that the US armed forces only reluctantly made use of their cyber arsenal was partly due to these concerns. In the Kosovo war of 1999, some planned cyber attacks against Serbia did not take place because the Pentagon's own lawyers vetoed them after having studied the international legal difficulties of cyber war.[58]

US domestic law also gave the armed forces' lawyers a few headaches, because an attack on American infrastructures could originate in Iraq as well as in the US. A military counter-strike through cyberspace might therefore unwittingly lead to an operation of US armed forces on domestic territory. This is prohibited by the *Posse Comitatus Act* of 1878.[59]

On the other hand, there have been laws against computer crime since the 1980s. The most important of these is the Computer Fraud and Abuse Act of 1984, which has been amended three times since.[60] Electronic break-ins into computer systems have been treated as crimes on the basis of this Act, and the FBI quickly used this piece of legislation for building up structures able to deal with them. The domestic laws thus gave the law enforcement agencies a strong hand in fighting cyber attacks.

One of the oldest laws governing computer security, the *Computer Security Act* of 1987,[61] points in another direction. Under this provision, the different departments of the government were directed to formulate their own plans for IT security. Here we can see an early example of handling the risks of information technology in a decentralized, preparative manner.

The legal norms, in sum, prevented a more important role for the armed forces in the protection of critical infrastructures, while giving the law enforcement community new tasks. Moreover, decentralized preventive measures were already taken in the 1980s. This is reflected today in the cooperation efforts with the private sector.

3. Policy

3.1. First Studies

President Bill Clinton set up a special study group in June 1995, the Presidential Commission on Critical Infrastructure Protection (PCCIP), whose task was to deliver a comprehensive report on the security of all infrastructure systems in the US. While this brief included not only information and telecommunications networks, but the financial sector, energy supply, transportation and the emergency services as well, the main focus was on cyber risks. There were two reasons for this decision. First, these were the least known because they were so new, and secondly, many of the other infrastructures depend on data and communications networks. The PCCIP included representatives of all relevant government departments, not only from the traditional security policy establishment. Additionally, the private sector was involved. This involvement was based on the assumption that security policy in the IT field was no longer only a duty of the government, but a "shared responsibility."[62] This decision opened up the realm of possible strategies far beyond the core measures of security policy—physical violence and repression.

Together with the PCCIP, Clinton set up the Infrastructure Protection Task Force (IPTF) to deal with the more urgent problems in infrastructure protection until the report was published. The members of the IPTF were drawn from the state's classical security policy institutions exclusively—the FBI, the Department of Defense and the NSA.[63] Insofar the IPTF can be understood as a compromise between a completely cooperative approach—including the private sector and other departments—and a classical security policy approach—giving the task to the FBI *or* the Department of Defense. The IPTF was chaired by and located at the Department of Justice to make use of the Computer Investigations and Infrastructure Threat Assessment Center (CITAC), which had been set up shortly before at the FBI.[64] Obviously, the institutional resources of the FBI were a decisive factor here. A more militant approach was still an option then, as can be seen, for example, by the appointment of former Air Force General Robert T. Marsh as PCCIP chairman.

3.2. Setting Up an Institutional Structure

The PCCIP presented its report in the fall of 1997.[65] President Clinton followed most of their recommendations in May 1998 with his Presidential Decision Directives (PDD) 62 and 63. With them, he created the position of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism at the National Security Council, who is supported by the newly founded Critical Infrastructure Assurance Office (CIAO). The Office of Computer Investigations and Infrastructure Protection (OCIIP), which had been assembled at the FBI on the basis of the CITAC, was expanded to the inter-agency National Infrastructure Protection Center (NIPC). The NIPC is located at the FBI headquarters and is mainly staffed with FBI agents, but representatives and agents from other departments and the intelligence agencies work there as well. The NIPC is responsible for early warning as well as for law enforcement and coordinates the various governmental and private sector activities. The NIPC, therefore, has a central role in the new cyber-security policy. Coordination within different high-level branches of the government has been effected by the new Critical Infrastructure Coordination Group (CICG).[66]

A number of departments act as "lead agencies", each of which is charged with the security of one sector of the infrastructure. For top-level strategic coordination between the government and the private sector, PDD 63 envisaged a National Infrastructure Assurance Council (NIAC), chaired by the National Coordinator. Additionally, new Information Sharing and Analysis Centers (ISAC) in each of the sectors were planned. They were to be run by private companies who would also determine their institutional and working procedures.[67] The close cooperation with the private sector that had begun with the PCCIP was thus continued and even enhanced. The government explicitly stressed the necessity of these non-hierarchical forms of cooperation:

> "Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private sector. To succeed, this partnership must be genuine, mutual and cooperative."[68]

Responsibility for cyber security policy no longer rests exclusively with the state, but also extends to private infrastructure providers. In a marked departure from the old monopoly of force, a networked self-help system has been established here that might be called post-modern. In some areas, the government still plays its traditional role through law enforcement and intelligence services, while in other areas it only moderates the activities of the private sector.

3.3. The "National Plan for Information Systems Protection"

The President's Commission on Critical Infrastructure Protection had explicitly described its 1997 report as a "beginning,"[69] and the presidential directives of May 1998 also acknowledged that there was no master plan for critical infrastructure protection yet.[70] Since then, a number of government departments, agencies and committees have worked on a comprehensive national strategy. On 7 January 2000, President Clinton presented its first version—under the headline "Defending America's Cyberspace"—to the public.[71] This "National Plan for Information Systems Protection" still represents current US policy with regard to the new cyber risks. The White House published a follow-up report in February 2001 after the inauguration of George W. Bush, but this document only attests to the state of the respective programs and does not include a change in strategy.[72]

The Government Only Protects Itself

The plan reinforces the perception of cyber security as a responsibility shared between the government and the private sector. The government agencies now are only responsible for protecting their own networks against intruders. Three new institutions work together for the security of the state's computer systems. The Federal Computer Incident Response Capability (FedCIRC), a part of the General Services Administration (GSA), is building a central analysis cell to investigate incidents in all of the government's non-military computer networks. For military computers, this is done by the Joint Task Force – Computer Network Defense (JTF-CND), set up in 1999. The JTF-CND is located at the Defense Information Systems Agency (DISA) near the Pentagon, but is subordinated to the Space Command in Colorado Springs.[73] The NSA's National Security Incident Response Center (NSIRC) provides support to FedCIRC, JTF-CND, DISA, NIPC and the National Security Council in case of attacks against systems that belong to the national security apparatus.[74] The FBI's NIPC is still responsible for incident warnings, strategic analyses, and law enforcement.[75]

Within the government, we now find a decentralized and cooperative risk policy similar to the one pursued between the government and the private infrastructure service providers. The FBI still has a fairly strong position compared to the Pentagon and the intelligence community. With FedCIRC, however, one central protective function is now being fulfilled by an agency that itself is an infrastructure service provider of and for the government.

Computer Crime or Cyberwar?

In spite of the FBI's strong position, the protection of computer systems is not only a question of domestic security. NIPC is located at and mostly run by the FBI, but it can also be subordinated to the Department of Defense by presidential order. The National Plan tried to maintain the traditional distinction between police and military by making such a decision dependent on an attack coming from abroad. But naturally, not every simple hacking attempt that does not originate in the US should trigger a response by the Department of Defense. The decisive criterion for differentiating between war and crime is therefore the scale of the attack.[76] This has an interesting implication: The ability to detect a large-scale attack as such now depends on the sensory instruments of the NIPC and the willingness of the private sector to share information with the government. The military is almost "blind" here and depends on the judgment of law enforcement agencies and even private infrastructure service providers. In the case of the new cyber risks, it is hard to differentiate between domestic and international security. The de-territorialized cyber-security policy blurs the line between war and crime, and the institutional responsibilities for a government response against an attack have to be established on a case-by-case basis.

Privatization of Cyber Security

The second part of the National Plan deals with the security of privately run infrastructures. It starts by stating that "the Federal Government alone cannot protect US critical infrastructures."[77] The state and local governments are also called "partners" of the federal government, but the emphasis is placed on private companies. The goal is a close private-public partnership. To ease concerns of the infrastructure service providers, the plan goes at great lengths to emphasize fundamental principles like "voluntary" cooperation or "trust" and safeguarding the companies' own interests through protective measures.[78] The government tries to make them accept its offers to check their defenses, to share information, and to further develop technical standards. Existing institutions like the North American Electric Reliability Council (NERC) are cited as good examples of this sort of cooperation.[79]

The private sector, though, is still very hesitant. The Information Sharing and Analysis Centers (ISACs) that were already planned in the 1998 Presidential Decision Directive were set up with considerable delay, and in some sectors do not exist at all to this day. The Financial Services ISAC (FS/ISAC), the first of these centers, was only set up on 1 October 1999, almost one and a half years after the presidential directives, and the IT-ISAC only started operations in March of 2001. Other sectors do not have this kind of coordination centers to this day. Besides the old NERC, there is only the National Coordinating Center for Telecommunications, run jointly by the state and the industry.[80]

This hesitation is remarkable, because the government has put much effort into achieving more.[81] President Clinton even signed an executive order in the summer of 1999 to accelerate the founding process of the National Infrastructure Assurance Council (NIAC). The NIAC had already been planned since 1998 as a forum for strategic debates among government officials and representatives of major IT companies.[82] It was finally set up in January 2001, one day before Bill Clinton left office.[83]

Many companies do not see any necessity for working with the government, and they are especially reluctant to let law enforcement or intelligence agencies know too much about their information systems. And they do not see government institutions as a real aid in tackling the new risks related to computer security. The NIPC in particular was subjected to heavy criticism after it failed to respond quickly to some E-mail worm infections in 2000 and 2001.[84] A lot of companies prefer contracting private IT security service providers, as they work faster and less bureaucratically than government agencies. These specialized IT security companies are increasingly taking on the role of traditional risk management consultants.[85]

Until an "electronic Pearl Harbor" occurs, we cannot expect the private sector to develop a keen interest in a more prominent role of the government in IT security. Instead of centralized coordination by the state, almost all the companies require private, local security instruments provided by the market.

4. Conclusions

Since the early 1990s, the debate about hacker attacks against the US has made its way from specialized expert circles to the agenda of "high politics" and national security. This in itself is remarkable because of the lack of a classical "threat triangle" consisting of actor, intention, and capabilities. There was no clear enemy and therefore no hostile intention around which such a discourse could have crystallized. Instead, the risk communication started at the last corner of the triangle, the capabilities. Here we can note something special: The potential for damage to critical infrastructures was not created by the introduction of weapons or other dangerous tools, but by the socio-technical structure of the US itself.

Until the mid-1990s, three different risk strategies were available: Repression and military strength (intervention), technical solutions for securing the systems (preparation) and awareness building (information). These strategies were linked to different actors in different institutions and cultures, who promoted them using different resources and calling upon different norms.

According to the basic tenets of risk sociology, the perception of risks plays an important role in deciding how to deal with them. The "risk communication" therefore should be an indicator for the selected security strategies. In the case presented here, the dramatization of the risk with terms like "information warfare," "cyberwar" or "electronic Pearl Harbor" was necessary to get the problem onto the political agenda. The political strategies developed should therefore have been more interventionist, using military means and approaches. The political treatment of issues such as the "war on drugs" or "counter-terrorism" is a case in point where the threat assessment was given in terms taken from military language.[86]

The risk policy selected in the case of cyber security differs significantly from these assumptions. In spite of high public interest, the military diction chosen in the early stages of the discourse could not be transformed into a similarly militant strategy. The outcome of ten years of discussion and almost five years of reforms, presented by Clinton in the National Plan for Information Systems Protection in January 2000, consists of three approaches: Law enforcement, private-public partnership, and private and public self-help. At its core, we find the strategy of preparation, meaning the preventive protection of critical infrastructures by technical means.

The study has shown the over-determination of this predominantly civilian and cooperative outcome.

Strong restrictions against a military-interventionist strategy existed in the dimensions of perception as well as of resources and norms.

In the realm of risk *perception*, two discourses were influential besides the military metaphors widely used in the mass media. On the one hand, law enforcement agencies emphasized their view of the risk as "computer crime," while on the other hand, and more importantly, the private sector running the infrastructures perceived the risk as consisting primarily of a local, technical problem or as economic costs. Therefore, the debate on cyber risks is an example of a failed "securitization."[87] The security policy institutions only partly managed to extend the concept of "security" in this case, because it was impossible to achieve a consensus between the different groups on what the word should refer to. Similar to the regulation of cryptography,[88] the debate centered on the question: Does "security" mean the security of the American society as a whole—"national security"—or the security of individual users or technical systems? Implicitly, this security policy discourse dealt with the relationship between the state and its citizens.

The distribution of *resources,* the technical and social means for countering the risk, was also important and had an impact on the discourse. Because the technology generating the risk makes it very difficult to fight potential attackers in advance, in practice, the measures taken focused on preventive strategies and on trying to minimize the impact of an attack when it occurs. Here, the infrastructure providers with their preference for decentralized and private approaches were in a strong position, because at the end of the day, only they are able to install the technical safeguards for IT security at the level of individual infrastructures.

Norms were also important in selecting the strategies. Cultural norms like the new economy's anti-statist "Californian ideology," as well as legal restrictions, prohibited a bigger role of the state, especially of the armed forces. The interventionist mindset of the security policy community gained hardly any acceptance. On the contrary, there was even much hesitation within the armed services concerning new, non-traditional military tasks. Most importantly, the general "no government regulations" approach towards the new economy, which had wide support across all political factions, strongly limited the choice of strategies. This also reflects the Clinton administration's policy of preferring economic ideas over security policy—prominently featured in the president's famous quote: "It's the economy, stupid!" Besides these cultural differences with regard to strategy, legal norms also obviated a more military strategy. The difficulties in determining whether cyber attacks constitute an act of war, the fear of committing war crimes by conducting electronic counter strikes, and the injunction against using the armed forces domestically made the Pentagon hesitate to build up its own information warfare units. On the other hand, the cyber-crime laws that had already existed since the 1980s enabled the FBI to start building up operative units very early.

Altogether, this study has shown that the public perception, which until today is full of military metaphors, only had a limited influence on the risk policy strategy. When there are concurrent discourses and viewpoints, the policy selection obviously depends upon two factors: One is the varying degree to which resources are available to the different groups, which become the more important the closer they are connected to the real (here: technical) structure of the risk. The other factor is the result of cultural and legal norms, because they restrict the number of potential strategies available for selection.

For the newer debates in other countries about the risks of the information society, this study leads to a conclusion that can shortly be described as "don't panic." The militarization of cyber security policy will be very difficult in a liberal society with private infrastructure providers. From the American experience, we should rather conclude that "cyberwar" is a fundamentally inadequate term that disrupts the discussion on useful risk policy more than it contributes.

Notes:

1. Ralf Bendrath, "Homeland Defense, virtuelle Raketenabwehr - und das schn•de Ende einer Medienhysterie," *telepolis* (28 March 2001). Available @ http://www.telepolis.de/deutsch/special/info/7234/1.html.
2. Ulrich Beck, *Risikogesellschaft. Auf dem Weg in eine andere Moderne* (Frankfurt/M.: Suhrkamp Verlag, 1986), 73, translation by R.B.
3. National Academy of Sciences, Computer Science and Telecommunications Board, *Computers at Risk: Safe Computing in the Information Age* (Washington D.C., 1990) quoted in Office of the Under Secretary of Defense for Acquisition & Technology 1996, *Report of the Defense Science Board on Information Warfare-Defense* (Washington, D.C., 1996), A-1.
4. For the origins of this term, see George Smith, "Electronic Pearl Harbor," *Crypt Newsletters•s Guide to Tech Terminology* (2001). Available @ http://sun.soci.niu.edu/~crypt/other/harbor.htm with many references.
5. President's Commission on Critical Infrastructure Protection (PCCIP), *Critical Foundations. Protecting America's Infrastructures* (Washington, D.C., 1997), 14.
6. Christopher Daase, Susanne Feske and Ingo Peters, eds., *Internationale Risikopolitik* (Baden-Baden: Nomos Verlagsgesellschaft, forthcoming 2001).
7. Command, control, communication, computers, intelligence, surveillance, and reconnaissance.
8. The actual percentage is far from clear. While many sources write about 95 percent, others only name 70 percent of the "non-essential" communication.
9. Department of Defense: News Briefing, 04/16/1998.
10. Niall McKay, "Cyber Terror Arsenal Grows," *Wired News* (16 October 1998). Richard Aldrich, Staff Judge Advocate of the Air Force Office of Special Investigations (AFOSI), in his presentation at the InfowarCon in Washington on September 6, gave another example: When asked by the Department of Justice about the number of computer security cases in 2000, the AFOSI staff counted 14 for the whole Air Force, whereas the DoD overall count for all services summed up to some 30 000. The latter had counted non-dangerous events like unidentified pings as hacker attacks, while the AFOSI only had considered serious cases.
11. Richard A. Clarke, *Memorandum. Implementation of PDD 63 through Project Matrix*, Critical Infrastrucutre Assurance Office (Washington, D.C., 19 July 2000)
12. The President's Commission on Critical Infrastructure Protection (1998), for example, wrote in its report: "We found no evidence of an impending cyber attack which could have a debilitating effect on the nation's critical infrastructures. While we see no electronic disaster around the corner, this is no basis for complacency. We did find widespread capability to exploit infrastructure vulnerabilities, … [W]e also face the possibility that someone will be able to actually mount an attack against other infrastructures by exploiting their dependence on computers and telecommunications," 5.
13. John J. Hamre and John H. Campbell, *Statement of the Honorable John J. Hamre (Deputy Director of Defense) and Brigadier General John H. Campbell (Deputy Director for Information Operations) at the Joint Military Procurement and Research and Development Subcommittee Hearing on Critical Infrastructure Protection - Information Assurance* (11 June 1998).
14. Robert H. Anderson and Anthony Hearn, *An Exploration of Cyberspace Security R&D Investment Strategies*

for DARPA: "The Day After ... in Cyberspace II" (Santa Monica: RAND, 1996); Roger C. Molander, Andrew Riddile and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica: RAND, 1996).

15. For 1999, they expected a Yen-crisis triggered by a computer virus or a "trojan" planted into the software of the Airbus A-330 by Algerian extremsists, Anderson/Hearn 1996, Appendix B.

16. John Deutch, *Foreign Information Warfare Programs and Capabilities, Testimony to the U.S. Senate Committee on Governmental Affairs; Permanent Subcommittee on Investigations* (25 June 1996).

17. White House, Presidential Decision Directive/NSC-63, *Critical Infrastructure Protection*, 1998.

18. Kenneth A. Minihan, *Prepared statement by Lt. Gen. Kenneth A. Minihan, Director, National Security Agency, before the Senate Governmental Affairs Committee* (24 June 1998), my emphasis.

19. John A. Serabian, Jr., *Statement for the Record before the Joint Economic Committee on Cyber Threats and the U.S. Economy* (23 February 2000).

20. Timothy L. Thomas, *Russian and Chinese Views of Information Warfare*, Workshop at the InfowarCon in Washington, D.C. (7 September 2001).

21. John Arquilla, David Ronfeldt and Michele Zanini, "Networks, Netwar, and Information-Age Terrorism," in Lesser, Ian O., Bruce Hoffmann, John Arquilla, David Ronfeldt and Michele Zanini, eds., *Countering the New Terrorism* (Santa Monica: RAND, 1998), 39-84.

22. George Smith, "Electronic Pearl Harbor."

23. Serabian, *Statement for the Record*.

24. Louis J. Freeh, *Statement of the Director Federal Bureau of Investigation before the Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies* (16 February 2000).

25. Johan J. Ingles-le Nobel, "Cyberterrorism Hype," *Jane's Intelligence Review* (21 October 1999).

26. CNN, "Cyberspace Attacks Threaten National Security, CIA chief says" (25 June 1996).

27. Madsen, Wayne, "Teens a Threat, Pentagon Says," *Wired News* (02 June 1998).

28. George Smith, "Electronic Pearl Harbor."

29. Infowar enthusiast Winn Schwartau, who coined the term more than ten years ago, recently even wrote a novel titled *Pearl Harbor.Com*.

30. Then Deputy Secretary of Justice Jamie Gorelick, in ABC Nightline 199, "Cyber Terror - A Consequence of the Revolution," 12/07/1997, transcript available @ http://www.infowar.com/CLASS_3/class3_011298a.html-ssi.

31. President's Commission on Critical Infrastructure Protection 1997, passim.

32. Office of the Under Secretary of Defense for Acquisition & Technology, 1996, 6-7.

33. Inside the Army, 22.4.1999, quoted in George Smith, "Eligible Receiver," *Crypt Newsletter•s Guide To Tech Terminology*, http://www.soci.niu.edu/~crypt/other/eligib.htm.

34. "DoD combats transnational threats through its activities to prevent terrorism and reduce U.S. vulnerability to terrorist acts [...]. Such activities include efforts to [...] protect critical infrastructure (including combating cyber–terrorism)," William S. Cohen, *Annual Report of the Secretary of Defense to the President and the Congress*, (Washington D.C., 2000), Chapter 1: The Defense Strategy.

35. Quoted in Kevin Poulsen, "Hack Attacks Called the New Cold War," *The Register* (23 March 2001).

36. Quoted in McKay, "Cyber Terror Arsenal Grows."

37. Freeh, *Statement of the Director Federal Bureau of Investigation*.

38. Janet Reno, *A Law Enforcement/Information Technology Industry Dialogue on Prevention, Detection, Investigation and Cooperation*, Speech at the Cybercrime Summit, Stanford, CA (05 April 2000).

39. Richard Power, "2000 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues & Trends* 1 (2000).

40. According to the Crime and Security Survey 2000 only 25 percent of the attacked companies reported these attacks to the law enforcement agencies, Power, Computer Crime and Security Survey, 13.

41. Martha Mendoza, "Valley Cool to Reno Cybercrime Plan," *L.A. Times* (06 April 2000).

42. Then Commander of U.S. Space Command and now Chairman of the Joint Chiefs of Staff, General Richard B. Myers, quoted in "Space Command Readies For Infowar," *United Press International* (05 January 2000).

43. Jim Garamone, "Hamre "Cuts" Op Center Ribbon, Thanks Cyberwarriors," *American Forces Press Service* (11 August 1999).

44. Bradley Graham, "In Cyberwar, A Quandary Over Rules And Strategy," *International Herald Tribune* (09 July 1998).

45. Joint Chiefs of Staff, Joint Pub. 3-13, *Joint Doctrine for Information Operations* (Washington, D.C., 9 October 1998).

46. For an overview see Ralf Bendrath, "Krieger in den Datennetzen. Die US-Streitkr•fte erobern den Cyberspace," in: Armin Medosch (Hrsg.), *Viren, Warez und Hoaxes – Die Kultur des gesetzlosen Internet* (Hannover: Heise Verlag: forthcoming).

47. Elizabeth Becker, "Pentagon Sets Up New Center for Waging Cyberwarfare," *New York Times* (8 October 1999).

48. Dan Verton, "DoD Redefining Info Ops," *Federal Computer Week* (29 May 2000).

49. Charles L. Owens, *Testimony of Charles L. Owens, Chief, Financial Crimes Section, Federal Bureau of Investigation, on Computer Crimes and Computer Related or Facilitated Crimes before the Subcommittee on Technology, Terrorism, and Government Information*, Senate Committee on the Judiciary (19 March 1997).

50. Suro, Roberto, "FBI Cyber Squad Termed Too Small for Hacker Threat," *Washington Post* (7 October 1999).

51. Quoted in PC World, "Feds To Net Criminals: You Can't Hide," *PC World* (6 September 2000).

52. United States Internet Council, *State of the Internet 2000* (Washington, D.C.: 2000).

53. Barbrook, Richard and Andy Cameron, "Die kalifornische Ideologie," *telepolis* (5 February 1997), http://www.heise.de/tp/deutsch/inhalt/te/1007/1.html.

54. Quoted in John Carlin, "A Farewell to Arms," *Wired* 5, 5 (1997).

55. U.S. Space Command, *U.S. Space Command Takes Charge of Computer Network Attack*, Press Release No. 15-00 (29 September 2000).

56. For a skeptical position, see Richard W. Aldrich, "The International Legal Implications of Information Warfare," *Airpower Journal* 10, 3 (1996): 99-110; for the opposite interpretation see Thilo Marauhn and Torsten Stein, "V•lkerrechtliche Aspekte von Informationsoperationen," *Zeitschrift f•r ausl•ndisches •ffentliches Recht und V•lkerrecht*, 60: 1, 1-40 (2000: 3-6).

57. Aldrich, "The International Legal Implications of Information Warfare," 104-109.

58. Associated Press, *Pentagon Ponders Legality of Cyber Weapons* (9 November 1999).

59. The text says: "Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both," 18 U.S. Code § 1385.

60. 18 U.S. Code § 1030, amended 1986, 1994 and 1996, see United States Congress, *Report of the Senate Committee on the Judiciary on the National Information Infrastructure Protection Act* (Washington, D.C.: 1996).

61. United States Congress 1988: Computer Security Act of 1987, Public Law 100-235 (H.R. 145), 01/08/1988.

62. White House, Executive Order 13010: Critical Infrastructure Protection (15 July 1996).

63. Ibid.

64. John S. Tritak, *Statement before the Senate Judiciary Committee Subcommittee on Technology, Terrorism and Government Information* (6 October 1999).

65. PCCIP 1997.

66. White House 1998: Presidential Decision Directive/NSC-63, *Critical Infrastructure Protection*.

67. Ibid.

68. National Security Council, White Paper. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (Washington, D.C., 1998).

69. PCCIP 1997, 101.

70. White House 1998, 3.

71. White House, *Defending America•s Cyberspace. National Plan for Information Systems Protection Version 1.0. An Invitation to a Dialogue* (7 January 2000).

72. White House, *Federal Critical Infrastructure Protection Activities* (22 February 2001).

73. White House 2000, 39-42.

74. Ibid., 49.

75. Ibid., 42.

76. Ibid.

77. Ibid., 104.

78. Ibid., 106.

79. Ibid., Chapter 5.

80. For an overview see Bendrath, Homeland Defense.

81. White House 2000: Chapter 5.

82. IPartnership, *President Forms Infrastructure Assurance Council* (15 July 1999).

83. Diane Frank, "IT Firms Unite to Share Security Info," *Federal Computer Week* (17 January 2001).

84. Jim Wolf, "US cyber security center lags on threat warnings – GAO," *Reuters* (22 May 2001).

85. Roberto Ceniceros, "More Consultants Offering Technical Help to Ensure Security," *Business Insurance* (3 April 2000).

86. Daase, Internationale Risikopolitik.

87. Ole W•ver, "Sicherheit und Frieden: Erweiterte Begriffe, engere Freir•ume f•r Politik?," *antimilitarismus information* 25, 11, pp. 47-53.

88. Diana Saco, "Colonizing Cyberspace: "National Security" and the Internet," in Jutta Weldes, Mark Laffey, Hugh Gusterson and Raymond Duvall, eds., *Cultures of Insecurity. States, Communities, and the Production of Danger* (Minneapolis: University of Minnesota Press, 1999), 261-291.

RALF BENDRATH has studied physics and political science in Bremen and Berlin and currently is working on his doctoral dissertation about "Information Warfare in the USA." Since 1999, he maintains the German E-mail discussion list "Infowar.de." He is a founding member of the German-Austrian Research Group Information Society and Security Policy (Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik, FoG:IS) and a frequent contributor to the online magazine "telepolis." In 2000-2001 he was a visiting scholar at the Center for International Science and Technology Policy at George Washington University in Washington D.C. *E-mail*: bendrath@zedat.fu-berlin.de.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection

Ralf Bendrath

Keywords: Cyberwar; information society; risk perception; risk society; cyber risks: physical vs. virtual; US policy response; cyber attacks; critical information infrastructures; information warfare; public-private sector partnership.

Abstract: When combating the risk of cyber attacks on critical infrastructures was adopted as part of the political agenda of the US, it was framed mostly in military terms like “cyberwar” or “information warfare.” The security strategy implemented in 1998 and elaborated in the “National Plan for Information Systems Protection” in January 2000 shows a very different direction. Instead of a military approach, it consists of law enforcement, private-public partnership, and private and public self-help. Three factors led to this outcome: Differing risk perceptions in law enforcement and the private sector, private control over the technical resources, and constraining cultural and legal norms. The American policy against cyber attacks, thus, is an example for a failed “securitization

full text

Author: **Michael Näf**
Title: **Ubiquitous Insecurity? How to “Hack” IT Systems**
Year of issuance: **2001**
Issue: **Information & Security. Volume 7, 2001, pages 104-118**
Hard copy: **ISSN 1311-1493**

UBIQUITOUS INSECURITY? HOW TO “HACK” IT SYSTEMS

Michael NÄF

Table Of Contents:

1. Introduction

> “The Internet is waiting for its Chernobyl, and I don’t think we will be waiting much longer; we are running too close to the edge.”[1]

Even though these words may not be accurate, the IT world does indeed have a security problem. There are several fundamental obstacles complicating the widespread application of security measures: There is usually no direct return on investment when it comes to security; efforts to shorten time to market impede extensive security mechanisms in the development of new products; and companies must also consider usability: how many passwords and other security measures can users—customers!—put up with?

Despite those disadvantages, people need to become aware of IT security. One way to create this awareness is to demonstrate the vulnerability of current IT systems. The main purpose of this article is therefore to vividly present a few common ways to “hack” different IT systems. The examples are deliberately chosen to be rather simple. The methods used are basic “hacking” techniques. Still, all of the techniques described are used in practice, and they are often successful. In addition to these basic “hacking” techniques described in Chapter 2, the article discusses some causes of the current security problems in our networked world (Chapter 3), lists some likely security-related developments in the future (Chapter 4), and makes a few suggestions on how to achieve greater security in IT systems (Chapter 5) before coming to an end with some concluding remarks.

Some explanatory words are necessary to clarify the use of the term “hacker.” The word originally described a computer enthusiast, a person who “experiments with the limitations of systems for intellectual curiosity or sheer pleasure.”[2] Nowadays, the term “hacker” often has negative connotations because it is used for computer criminals that break into computer systems. This article uses the terms “attacker”/ “attack” to refer to individuals that try to tamper with or break into IT systems unauthorized, or to the corresponding activity, respectively. Attackers can be categorized by objectives, access, resources, expertise, and risk. Objectives can range from personal excitement or gain to terrorism or espionage. The article uses the word “attacker” to subsume all possible variations without further distinguishing by objective or any of the other criteria.

2. “Hacking” Basics – Some Case Studies

2.1. Attacking a Specific Web Server

This chapter shows one possible simple procedure to attack a web server with the address www.xyz.ch. The goal is to actually break into the system instead of merely provoking operational problems using so-called denial of service attacks. The following shows a three-step procedure; the attacker will start off with collecting information about the system that helps him to identify its vulnerabilities, which he can subsequently exploit.

Collecting Information about the System

Telnet is an interactive communications tool that is available on most computer platforms. It can be used to simulate HTTP[3] commands. In the example in Figure 1, Telnet is used to issue the HEAD command on port 80, which is the standard port for HTTP communication. In response to the command the web server sends back some information about the requested object. Many web servers also include some information about themselves, i.e. the particular software product and version used and the platform they are running on. In this example, the following useful information can be derived from the answer:

- The server at www.xyz.ch is a Microsoft Internet Information Server (IIS), version 4.0;
- The platform is most likely Microsoft Windows NT 4.0, because IIS 4.0 is integrated with that particular operating system;
- The server makes use of ASP,[4] because the server mentions a file called default.asp in its response.

The collected information is valuable when looking for a way to exploit weaknesses in the products that are in operation. However, it is important to note that not all servers on the Internet are that “talkative” in reaction to the HEAD command, as many simply ignore HEAD commands. But there are other ways to obtain the same information. One possible alternative (among more sophisticated methods) is to visit Netcraft’s site at http://www.netcraft.com/. Netcraft regularly publishes the “Web Server Survey” which lists web server products and their respective market share. As an add-on, the Netcraft site offers a search engine that can be used to determine the server product and operating system for a given web site address.

```
> telnet www.xyz.ch 80
Trying x.x.x.x...
Connected to www.xyz.ch.
Escape character is ‘^]’.
HEAD /

HTTP/1.1 302 Object moved
Server: Microsoft-IIS/4.0
Date: Sun, 03 Jun 2001 11:42:04 GMT
Location: /default.asp
Content-Length: 145
Content-Type: text/html
Connection closed by foreign host.
>
```

Figure 1: Example of a simulated HEAD command to a web server and its response.

Looking for Vulnerabilities

Once some characteristics of the targeted system are determined, the attacker can proceed to find a way to break in. This means that he or she has to find a security-related vulnerability that can be exploited in order to get access to the web server. A simple and convenient method to find such vulnerabilities is to make use of the various freely accessible vulnerability databases on the Internet.

One of the most extensive databases is maintained by SecurityFocus.[5] This database is searchable by product name. Searching for “IIS” yields the so-called “MS IIS/PWS Escaped Characters Decoding Command Execution Vulnerability.” The discussion of this vulnerability describes a design flaw that can be exploited to execute arbitrary code on the target machine. At least a dozen exemplary code extracts are available for download [6] and show how to exploit the flaw in practice. More research in the SecurityFocus database reveals a number of potential vulnerabilities affecting the Windows NT platform or the ASP technology used.

Exploiting the Vulnerabilities Found

The attacker has now identified several potential vulnerabilities to “hack” the web server at www.xyz.ch. He will continue to modify the code example found above for his purposes and verify whether this vulnerability is actually exploitable in this particular context and setup. Maybe the system is well patched and cannot be attacked using this specific flaw, but maybe the system is indeed vulnerable and the attacker is therefore able to execute arbitrary code on it.

2.2. Attacking Arbitrary Web Servers

In the above scenario, the attack targeted a specific web server with the address www.xyz.ch. Possibly however, an attacker wants to attack a web server that is a potential target. To identify one such, he or she can again use the information that is readily available on the Internet.

Finding Vulnerable CGI Programs

A considerable number of web servers use a technique called CGI[7] to deliver dynamic web content. Once more using SecurityFocus’s database, an attacker can in no time compile a list of commonly used CGI programs with security-related vulnerabilities. The following three programs look promising:

- maillist.pl: A tool used to let web users subscribe to a mailing list;
- gbook.cgi: An implementation of a web-based guest book;
- count.cgi: Counts the number of hits to a web page and displays a dynamic counter.

CGI programs are accessed via ordinary URLs like http://www.xyz.ch/cgi-bin/maillist.pl. Once requested, the CGI program is executed by the respective server, and the program’s output is sent back to the requesting web browser. In addition, many CGI programs receive input values (e.g. form entries), which are sent from the web browser to the server. The latter then directly propagates the input to the CGI program before the program is invoked. It is this ability to receive and process input data that causes most of the problems with regard to CGI programs. Thoroughly implemented programs do not make any assumptions on the input received. However, many of the CGI programs out there falsely assume that all the input they receive is “nice.” This misconception leads to two major problems:

- *Buffer Overflows.* Consider the maillist.pl example above.[8] The tool receives an e-mail address along with additional information about a user requesting to be included in a mailing list. Maillist.pl will maybe verify the correct syntax of the e-mail address supplied, then further process the information before storing it in some location on the server. Maillist.pl makes a plausible assumption about the maximum length of any e-mail address provided and reserves some amount of memory space accordingly—something like 1024 characters seems to be a fairly conservative and safe guess. But maillist.pl may not verify whether the submitted e-mail address exceeds this maximum number of characters. What happens if maillist.pl is provided with a 300’000-character e-mail address? There are several possibilities: (1) Nothing happens, the address is written to the subscription database; (2) maillist.pl crashes; (3) the CGI program crashes and at the same time causes the whole web server or operating system to crash because of poor configuration or other reasons; (4) The last possibility is the most rewarding one for an attacker: maybe the overly long e-mail address will overwrite the part of the memory that is reserved in the server’s main memory for executing the CGI program. This may also cause the program to crash. But with a cleverly crafted e-mail address that includes executable machine instructions, an attacker is (potentially) able to feed in arbitrary code that is executed instead of the original CGI program. This type of vulnerability is called buffer overflow. Buffer overflows are among the most common vulnerabilities in today’s computer systems. Any software program—not only CGI programs—can be affected.[9]

- *Shell Escapes.* Shell escapes are another common vulnerability, which is also caused by careless or non-existent input validation. This vulnerability is relevant mostly for CGI programs and can often be exploited very easily to execute arbitrary code on a server system.[10]

Finding Instances of the Vulnerable CGI Programs

Now that our attacker has found a few vulnerable CGI programs, he or she will try to find a number of web servers that utilize those tools. This task is simple, thanks to the search engines covering the WWW that do most of the work. Table 1 shows the queries used with AltaVista[11] to find potentially vulnerable servers, as well as the number of servers found at the time this article was written.

Table 1. Number of hits reported when searching for potentially vulnerable CGI programs with AltaVista.

Search Query	**Number of “Targets”**
url:maillist.pl	39
url:gbook.cgi	1225
url:count.cgi	2342

Having finished this research, the attacker is now ready to try to break into the reported servers using the vulnerabilities identified and described by SecurityFocus. Many of the servers will not be vulnerable, however, because they run a fixed version of the respective CGI program. On others, a successful attack will be possible because they run exploitable versions of the programs and do not take any additional measures to protect themselves.

Internet search engines can also be used in a number of other ways to acquire useful information about server systems connected to the Internet. Many servers leak sensible information due to lax setup and configuration. A query for url:access_log[12] with AltaVista, for example, produces almost 1000 hits.[13]

Rattling a (Web) Server's Doorknobs: Portscanning

Abstractly, a port specifies the endpoint of a connection on a networked device. Ports are identified as numbers. Many port numbers are standardized[14] and denote a specific network or application protocol (e.g. port number 80 for HTTP or 23 for Telnet). A lot of the software components serving the respective protocols contain well-known and well-documented vulnerabilities or weaknesses (for instance, a system with anonymous login enabled). Thus, it is only a matter of finding computers that make use of those vulnerable protocols in order to try and attack the affected systems.

This search can be automated using a number of tools. One famous example is SATAN (Security Administrator Tool for Analyzing Networks). SATAN is downloadable at no charge and comes with an easy-to-use HTML-based user interface. The tool automatically and efficiently scans any given host (or the respective subnet) for a number of known vulnerabilities and produces a clear and readable report. This report can then be used as a basis to look for actual vulnerabilities.[15]

2.3. How to Write a Computer Virus

Computer viruses and worms are a common way of accessing computer systems without authorization. The effects differ: some viruses merely cause annoyance and inconvenience; others affect the functionality and stability of computing environments or compromise the confidentiality or integrity of (sometimes valuable) information. Three major aspects are important if someone wants to write their own computer virus:

- *Payload.* What does the virus do once it has infected a system? The amount of damage to be caused by the virus is arbitrary and can be freely specified by the author;
- *Delivery and Propagation.* How does the virus reach the target systems? And, in case of a (self-propagating) worm, how does the worm automatically spread to other computer systems?
- *Execution.* How is the virus payload executed on the target machine? Computer viruses are not dangerous as long as they are not executed. There are two generic methods of ensuring that a virus is executed: (1) The virus can be programmed to exploit one of the countless vulnerabilities that exist in many of today's mail clients or operating system components. Consequently, these types of viruses are executed without any form of user interaction; (2) Alternatively, the virus can rely on user interaction, in which case the virus is typically delivered as a simple e-mail attachment with a subject heading and content that invites people

to open the attachment. The virus is executed as soon as the attachment is opened.

Short Analysis of the ILOVEYOU Worm

This section gives a short overview of the infamous ILOVEYOU worm by exploring each of the three aspects identified above. The goal is to give some insights into the internals of a virus (or worm) and show how easy it is to create this digital germ.

- *Payload:* The ILOVEYOU worm is written in Visual Basic Script, an easy-to-learn and powerful programming language by Microsoft, which is often used in (dynamic) web pages or e-mails. The complete payload of the ILOVEYOU worm serves the purpose of self-propagation exclusively, and no further damage is done. Among other activities,[16] the worm searches for certain types of files on the target machine and modifies those files depending on the type of file. It will, for instance, replace all occurrences of JPEG files (a commonly used image format) with a copy of itself and add the .vbs extension (denoting a Visual Basic Script file). If the user later tries to open one of the modified JPEG files, he or she will not see the image but rather (re-)activate the worm. The respective excerpt from the worm's source code is given in Figure 2:[17]

```
[...]

elseif(ext=“jpg”) or (ext=“jpeg”) then

set ap=fso.OpenTextFile(f1.path,2,true)

ap.write vbscopy

ap.close

set cop=fso.GetFile(f1.path)

cop.copy(f1.path&.”vbs”)

fso.DeleteFile(f1.path)

[...]
```

Figure 2: Source code excerpt from ILOVEYOU worm.

- *Delivery and Propagation:* The worm uses several techniques to infect computer systems. The most important way is via e-mail. End users receive a copy of the worm in their inbox. It is an e-mail with the subject line “ILOVEYOU” and just one line of text: “kindly check the attached

LOVELETTER coming from me." But the attachment contains the worm's code instead of the expected love letter. This code is executed as soon as the affected user opens the attachment, e.g. by simply clicking on it. After that, the worm rapidly spreads to other users' systems by sending itself to all the entries in the address book of Microsoft's Outlook application. This has the advantage that the worm sends itself to valid e-mail addresses. The perfidious detail is that the recipients think they have received the mail from an acquaintance and are therefore tempted to open the attachment without a second thought. In addition to the mail functionality, the worm also spreads via IRC (Internet Relay Chat), or if another user executes an infected file on a shared file system.

- *Execution:* As explained above, execution of the ILOVEYOU worm is triggered by the user on opening the mail's attachment.

Any attacker wanting to write their own virus/worm can use the same or similar techniques found in the ILOVEYOU worm or any other mechanism that seems promising. To make things easier still, the author can use one of the dozens of virus construction kits available on the Internet.[18] Many of those construction kits come with user-friendly, Windows-based user interfaces and enable a user to build a virus or worm with just a few mouse clicks. The virus writer does not need to have substantial technical expertise.

2.4. Intangible Security: "Drive-By Hacking" and Other Wireless Attacks

One current tendency is to connect computers without using physical wires. Wireless LANs have the security-relevant drawback that it is harder to keep the physical signals under control. As a result, wireless networks often give attackers an easy opportunity to overcome all physical and logical (e.g., firewalls) access control mechanisms of a company's or an organization's local network. This is possible because wireless LANs are often set up as a wireless extension of the existing wired network, without further access control.

A modern form of attack in this area is called "war driving." Attackers basically just need a few laptops with wireless network interface cards built by the major manufacturers in that sector, and a van to carry the equipment around. Then they choose a few companies or other organizations that seem to be valuable targets and drive their van in front of a suitable building containing a WLAN access point.[19] Once in place, they use their laptops and the corresponding wireless network adapters and try to connect to the access point. Maybe the attackers also have to sort out some details like community strings that work like passwords. But often these passwords are set to the factory default or they can be snooped from the existing wireless traffic.

Of course, this attack is not possible as soon as WLANs are used with encryption turned on. In this case, the (symmetric) keys used for the encryption at the same time serve to authenticate devices that try to connect to the access point. However, many WLANs are still operated without this security measure because the necessary key management is considered to be too tedious and error-prone. Under these circumstances, WLANs are a convenient way to access internal networks without having to bother with physical access control, firewalls, or similar measures.[20]

Wireless attacks are not limited to attacks against WLANs described above. Every electronic device creates electromagnetic emissions. This radiation can be detected. Therefore, using the right equipment (and being sufficiently skilled), it is possible to read the contents displayed on a computer screen from a remote location or to intercept information from cell phones, network cables, or computer keyboards.[21]

2.5. Tampering with Tamperproof Hardware – Attacking Smart Cards

Tamperproof devices are an important element of many security-related environments. Take PKI[22] solutions as an example: Using a tamperproof piece of hardware called smart card is a common way to protect the important private key against theft or unauthorized access. Smart cards are becoming ever more important with the introduction of digital signature legislation in many countries.

The problem is that tamperproof hardware does not exist. It is not possible to make a device that cannot be tampered with. The correct term is tamper-resistant hardware, because tampering with so-called tamperproof hardware is just a matter of equipment and creativity. Let’s assume a smart card is used to store a private key that in turn is used to sign e-mails and other digital documents. The following are two possible ways of accessing and/or using the private key unauthorized:[23]

- *Side-Channels Attacks.* Side channels are characteristics of a system that are not directly related to the system’s intended purpose. Examples include timing characteristics, power consumption, and radiation emission. These side channels can be systematically measured and used to obtain valuable information about the targeted smart card in order to gain access to the information contained. Take timing information as an exemplary case: The attacker can (systematically) perform a multitude of cryptographic operations with a smart card and measure the processing time needed. It will take many attempts, but eventually the attacker might be able to derive the secret information stored on the smart card based on the timing characteristics.
- *Subverting the Device Accessing the Smart Card.* Usually, a smart card is inserted into a smart card reader, which is connected to a personal computer. When a user wishes, for instance, to digitally sign an outgoing e-mail, the mail client transmits the mail message to the smart card in order to have it signed. The attacker simply needs to write a Trojan Horse[24] that hooks itself into this process and covertly replaces the mail message to be signed with a different document. Using this technique, it is possible to sign arbitrary information with a user’s private key, and without the user even noticing.

2.6. “Hacking” Humans: Non-Technical Attacks

This article has a clearly technical focus. Nevertheless, it is important to note that one of the most promising methods to attack IT systems is not technical at all. “Social engineering” is the common term to describe attempts to influence people and get them to reveal valuable information (e.g., passwords) or take security-related action (e.g., open a new computer account for the attacker).[25]

3. Ubiquitous (Digital) Insecurity – Some Causes

We know a variety of crimes that can be committed in the offline world: theft, voyeurism, fraud, money laundering, child pornography, intellectual property theft, identity theft, privacy violation, etc. All of these crimes can be committed in the online world too. The Internet does not introduce new types of crimes. The motives and goals of criminals do not differ. However, there are some fundamental differences when it comes to tools and techniques. The list given below presents a few essential properties of a networked world with regard to IT security.

- *Intangibility.* Information in the digital world exists independently of any physical object that carries the information. Information cannot be "imprisoned" and is therefore easily copied, modified, destroyed, or stolen, usually without leaving any traces. This fact has important implications for information theft, identity theft, intellectual property right theft, and many other aspects of information security;
- *Complexity.* As Admiral Grace Hopper put it: "Life was simple before World War II. After that, we had systems." Every IT system contains bugs (i.e. software or hardware faults). The more complex an IT system is, the more bugs it contains. Not all of those bugs are security-related, but some of them are and can be exploited by a potential attacker. An IT system's security is hard to control or manage. IT systems interact with other systems or with people, and they have emergent properties that were never considered when the system was originally designed;
- *Automation.* One important property of the computerized world is the huge potential for automation. Computer programs can automate many arduous tasks and thus provide a high degree of efficiency and accuracy. But automation can also make the process of breaking into an IT system easier and faster. Some examples: (1) Password cracking: It is possible to write a software tool that simply permutes all possible combinations of letters, numbers, and special characters in order to find a valid password to a computer system. A more elaborate variant of the same tool would make use of a number of (freely downloadable) dictionaries to speed up the process, based on the assumption that people often choose variations of existing words as their passwords. (2) Port scanning: A port scanner is a program that runs on a computer with a network connection and independently sweeps the Internet searching for computers or devices with active services that are known to be vulnerable (see above). The port scanner then produces a report with all potentially vulnerable systems and how to attack them. (3) Search Engines: Traditional Internet search engines can support an attacker in that they are able to provide plenty of information about the targeted company or system (see above);
- *Global Networking.* In contrast to the offline world, an attacker in the online world can (potentially) connect to the Internet anywhere he or she chooses and nevertheless reach any other system that is online—regardless of its physical location. This global connectivity makes attacking easier and less resource-intensive. In addition, the tendency towards globalization has a negative impact on criminal investigation and prosecution, because several jurisdictions are typically involved;
- *Rapid Knowledge and Tool Propagation.* Only a relatively small number of people possess the skills required to attack an IT system. However, once an attacker succeeds in finding a particular vulnerability that can be exploited, he or she can easily encode his or her knowledge into a software program. The newly developed tool can then be published on the Internet. Thus, every Internet user—regardless of skill level—is able to download the tool and use it against an IT system.

4. Security-Related Visions for the Future

The following list offers only a selection of possible future security-relevant developments.

- *Ubiquity of Computing and Networking.* There is a clear tendency towards “connecting everything to everything.” The most important security-related implication of the mobility and ubiquity of IT devices is that they pose risks in new areas and to a much wider spectrum of targets. A few visionary but nevertheless plausible examples: Virus-based attacks against mobile phones and PDAs,[26] denial-of-service attacks against Internet-enabled refrigerators, burglary alarm systems, or cars, privacy-violating attacks against electronic butlers (including webcams in people’s homes) or against wearable electronic devices that monitor the wearer’s body condition;
- *Trusted Third Parties.* PKIs already work with trusted third parties that, for instance, issue digital certificates. Trusted third parties help to reduce the trust problem. Instead of having to extend their trust on a peer-to-peer basis, people (or machines) “only” have to trust a few selected trusted third parties (e.g., certification authorities);
- *Tamperresistant (Hardware) Devices.* Tamperresistant devices delegate the security/trust problem from a large, complex, and uncontrollable system (e.g., a personal computer) to a smaller, less complex and easier-to-secure (hardware) device (e.g., smart cards and smart card readers);
- *Software/Hardware Liability.* Companies in the offline world are liable for the products or services they deliver. Many software companies are known to ship bug-infested products and officially deny liability. Users of those products are accustomed to encountering many faults. Still, it is feasible that this may change in the future and that software or hardware companies will be held liable for the products they ship;
- *Increased Security of Network Protocols.* A lot of the security-related problems with the Internet originate in the fact that the Internet was not designed with security in mind. Many communications protocols currently in use will be revised or replaced by other protocols that feature more sophisticated security mechanisms;[27]
- *Biometrics.* Biometric techniques for authentication have some very promising advantages. At the same time, they have some problematic characteristics. Two examples: (1) Biometric techniques have no potential for something like “pseudonym authentication.” It can be a serious privacy issue if people are forced to use fingerprints, iris scans or DNA samples to identify themselves. (2) If a user’s password is corrupt (i.e. stolen), he or she sets a new password. If a user’s private key is corrupt, she revokes the corresponding certificate and is issued a new one. But a user only has nine fingers left if one fingerprint (or, to be exact, its digital representation) is stolen;
- *Security Outsourcing.* Many (smaller) companies are considering IT security outsourcing as an option, because they cannot afford their own security department. In addition, security outsourcers can fully concentrate on security issues and are able to relate security-relevant information from several sources (i.e. monitored networks) in order to optimize their activities;

- *IT Insurances.* It is feasible to assume that, at some point in the future, companies will deploy firewalls, intrusion detection systems, public key infrastructures, or other security mechanisms because insurance companies offer according discounts on their insurance rate. Insurance companies will then dictate the course of IT security to some degree.

5. What Can Be Done? Possible Solutions

Chapter 2 mentions a few aids that help people obtain security-related information about systems. However, it is crucial to understand that tools like SATAN, SecurityFocus or AltaVista are of course not the problem. The first two are intended to help system administrators and security professionals track down problems with their systems. The latter is a general-purpose tool for information retrieval on the Internet. IT systems would not become more secure if these services and tools were shut down or prohibited. But there are other ways to achieve greater security in the IT world. Three suggestions:

- *Reduction.* Complex systems are much harder to secure than simple and manageable ones. Many of today’s IT systems are way too complex. It is therefore advisable to realize simpler systems, even if this means having to do without some cutting-edge functionality;
- *Careful Systems Design.* IT systems must be built with security in mind. Careful systems design is necessary in order to reduce the number of (security-related) bugs and design faults in a software or hardware component;
- *User-Based Risk Management and Education.* There is no need and no way to provide absolute security. Therefore, users must understand the risks they take in a digital and networked world in order to decide which risks they are willing to take. Those decisions are only possible if users are aware of and educated in various aspects of IT security.

Conclusions

The main goal of this article was to show a number of common ways to attack IT systems. The “hacking” methods presented were deliberately chosen to be rather simplistic. However, the examples were described in some detail in order to give the average reader a vivid and accurate impression of the various vulnerabilities inherent in current IT systems. In addition, the article presented some possible causes of security problems in the digital and networked world, and a few perspectives and possible countermeasures for the future. The massive complexity of modern IT systems was identified as one of the most important causes for security-related vulnerabilities. Hence, a crucial prerequisite for more secure IT systems is to reduce this complexity, even if that means having to put up with reduced functionality. Furthermore, there is a need for more careful systems design, and appropriate education on all levels—end users, developers, management, etc.

Notes:

1. Peter G. Neumann, “Internet security experts of SRI International”, in *New Yorker* (28 May 2001).

2. Bruce Schneier, *Secrets & Lies—Digital Security in a Networked World* (New York: John Wiley & Sons, 2000).

3. Hypertext Transfer Protocol, the protocol used for the WWW.

4. Active Server Pages, a technique to realize dynamic content.

5. http://www.securityfocus.com/.

6. E.g. http://www.securityfocus.com/data/vulnerabilities/exploits/execiis.c.

7. Common Gateway Interface.

8. Maillist.pl is used as an illustration to explain buffer overflows. It was not verified whether the vulnerability described in this paragraph actually exists in that particular CGI program.

9. For a more thorough discussion of buffer overflows, see Mudge, "How to Write Buffer Overflows" (1995). Available @ http://www.insecure.org/stf/mudge_buffer_overflow_tutorial.html (all URLs accessed July 21, 2001); Aleph One, "Smashing the Stack for Fun and Profit." Available @ http://www.cs.ucsb.edu/~jzhou/security/overflow.html.

10. For more information see Simson Garfinkel and Gene Spafford, *Web Security & Commerce* (Cambridge: O'Reilly, 1997); and Lincoln D. Stein, "The World Wide Web Security FAQ" (2000). Available @ http://www.w3.org/Security/faq/www-security-faq.html.

11. http://www.altavista.com/.

12. Apache (one of the most popular web server products) stores log information in a file called "access_log" by default.

13. Paul Heely, "Search Engines: The Ignored Threat" (2001), available @ http://www.sans.org/infosecFAQ/casestudies/search_engines.htm, describes more security-related aspects with regard to search engines.

14. Reynolds, J. and J. Postel, "Assigned Numbers (Request for Comments RFC 1700)" (1994). Available @ http://sunsite.cnlab-switch.ch/ftp/doc/standard/rfc/17xx/1700.

15. See Anonymous, *Maximum Security*, 3rd edition (Indianapolis: Sams Publishing: 2001) for a more thorough discussion of SATAN and plenty of other scanning tools.

16. See CERT Coordination Center, *CERT Advisory CA-2000-04 Love Letter Worm*, 2000, available @ http://www.cert.org/advisories/CA-2000-04.html for a detailed discussion.

17. See http://www.nettime.org/rohrpost.w3archive/200005/msg00059.html for the complete source code.

18. Numerous virus construction kits are listed on e.g. http://members.tripod.com/internet_sicherheit/virendatenbank.html.

19. The WLAN access point is a device that provides wireless connectivity to the wired part of the network.

20. SeeJohn Leyden, "War driving—the latest hacker fad" (2001), available @ http://www.theregister.co.uk/content/archive/17976.html; Kevin Poulsen, "War driving by the Bay" (2001), available @ http://www.theregister.co.uk/content/archive/18285.html for more information on war driving.

21. C.f. Gary Kelly, "TEMPEST" (2000), available @ http://www.sans.org/infosecFAQ/casestudies/tempest.htm.

22. Public Key Infrastructure.

23. See Schneier, *Secrets & Lies.*

24. A Trojan Horse is a program with hidden, malignant functionality.

25. Social engineering is covered in John Palumbo, "Social Engineering: What is it, why is so little said about it, and what can be done?" (2000). Available @ http://www.sans.org/infosecFAQ/social/social.htm.

26. Personal Digital Assistants.

27. See for example R. Thayer, N. Doraswamy and R. Glenn, "IP Security Document Roadmap (Request for Comments RFC 2411)" (1998). Available @ http://sunsite.cnlab-switch.ch/ftp/doc/standard/rfc/24xx/2411.

MICHAEL NÄF studied computer science and didactics at the Swiss Federal Institute of Technology in Zurich. After his internship with Digital Equipment Corp. in Hudson, MA, working in the field of optimizing compilers and high-performance microprocessor design, he returned to Zurich and now works as an IT security engineer with Telekurs's Payserv AG, a major Swiss financial services provider. In his spare time he works with infoSense (http://www.infosense.ch/) as a consultant, instructor, and publicist in various areas of ICT. He is a co-author of two educational books on information retrieval and IT security. *E-mail*: naef@infosense.ch.

BACK TO TOP

Ubiquitous Insecurity? How to “Hack” IT Systems

Michael Näf

Keywords: Information systems vulnerability; hacking; hackers; IT-security; critical societal infrastructure.

Abstract: There are several important obstacles to IT security: there is no direct return on investment, time-to-market impedes extensive security measures, and security mechanisms often have a negative impact on usability. On the other hand, today’s IT systems are undeniably very vulnerable and users—regardless of their profession or position—need to be aware of IT security to some degree. One way to create this awareness is to demonstrate the vulnerability of currently used IT systems. The article shows various examples of “hacking” techniques along with a few statements on the causes of the currently experienced “ubiquitous insecurity,” some security-related perspectives for the future, and a number of general suggestions on how to increase security in our networked world.

full text

Author: **Andrew Rathmell**
Title: **Controlling Computer Network Operations**
Year of issuance: **2001**
Issue: **Information & Security. Volume 7, 2001, pages 121-144**
Hard copy: **ISSN 1311-1493**

CONTROLLING COMPUTER NETWORK OPERATIONS

Andrew RATHMELL [1]

Table Of Contents:

1. Introduction

This article is concerned with the prospects for the emergence of an international regime for control of Computer Network Operations (CNO). CNO are a subset of a broader set of malicious computer-mediated activities.

According to draft British military doctrine, CNO comprises: Computer Network Exploitation (CNE), namely: "the ability to gain access to information hosted on information systems and the ability to make use of the system itself;" Computer Network Attack (CNA), namely: the "use of novel approaches to enter computer networks and attack the data, the processes or the hardware;" and Computer Network Defense (CND), which is "protection against the enemy's CNA and CNE and incorporates hardware and software approaches alongside people-based approaches."[2] In turn, CNO are one element of Information Operations (IO).

The precision of the military definition is not yet matched by internationally agreed definitions in the civil and criminal domains. The EU is now moving towards the concept of “cyber-abuse” as an overarching term to include activities ranging from privacy violations to attacks on computer systems.[3] The Council of Europe’s Cybercrime Convention, with which EU approaches are likely to be harmonized, encompasses CNA under “category 1” offences, i.e. offences “against the confidentiality, integrity and availability of computer data and systems.”[4] The G-8 Government-Industry Conference on High Tech Crime has however proposed that two major categories of threat be agreed upon, namely computer infrastructure attack and computer assisted threat. The former is defined as “operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Malicious acts, unauthorized access, theft of service, denial of service.”[5]

This article does not seek to examine the details of any prospective regime or convention. Possible approaches using either criminal law [6] or arms control [7] have previously been examined in detail. Instead, this article critically examines current approaches to the problem as embodied in the paradigms that dominate Western strategic thought. The article argues that a more holistic understanding of the emerging global information environment [8] is required in order to better guide Western strategic interests and policy development.

The article begins by framing the strategic dilemma of how to characterize and hence approach control of CNO, it then points to the “routinisation” of CNO within emerging NATO doctrine at the same time as multilateral efforts to secure cyberspace are gathering momentum. The article then draws attention to the institutional disconnects that are hampering coherent Western policy-making before focusing on two central features of the emerging environment that are insufficiently accounted for by strategic policy-makers: interdependencies and the private sector. The article concludes by arguing that Western strategic and economic interests can best be fulfilled by developing norms of military behavior in cyberspace.

2. The Strategic Dilemma

The central argument of this article is that NATO states face an increasing tension between exploiting their CNO advantage in the military sphere and protecting the global information environment.

Led by the USA, NATO nations are moving apace to develop doctrines and capabilities that will allow them to exploit cyberspace for military advantage. Within the broad rubric of IO, increasing effort is being devoted to integrating Computer Network Operations (CNO) into routine military planning. At the same time, these nations are becoming increasingly concerned at the dependency of their militaries, governments, economies and societies on the networked information systems that are emerging as the nervous systems of post-industrial society. They are taking a range of actions, both unilaterally and multilaterally, to mitigate the resultant risks.

The desire both to exploit and to restrict CNO is a paradox that needs to be addressed before an international regime can be developed. Underlying this paradox are two divergent approaches to characterizing the policy challenge.

2.1. Characterizing the Problem

One approach defines the CNO threat as originating from organized crime, electronic vandalism, corporate espionage and sub-state terrorism. The threat is defined as being to the economic prosperity and social stability of all nations plugged into the global information infrastructure. In this paradigm, all nations have an interest in working together to devise international regimes that will ensure the trustworthiness and survivability of information networks. It is a non-zero sum game.

From this perspective, a range of mechanisms can be used to mitigate the risks. International organizations can promulgate infosec standards and industry can be encouraged to make its information systems more secure and dependable. International law enforcement mechanisms, such as Interpol, can be used for information exchange and investigations while multilateral conventions on computer crime, such as the Council of Europe convention, can be negotiated similar to those that deal with hijacking and other forms of criminality. While transnational investigations and traceback will always be a problem, at least the appropriate mechanisms exist through which such problems can be addressed.

The other approach treats control of CNO as a zero sum game. The focus is on the threat from nation states; IO and CNO are perceived as tools of strategic coercion. Although it may not be realistic to control CNE as an intelligence gathering tool, CNA that do breach the confidentiality, integrity or availability of information systems could in theory be treated as weapons of war and brought within the scope of arms control or the laws of armed conflict. In this approach, existing mechanisms and methods such as the Laws of Armed Conflict and arms control/verification regimes could be applied to this new “weapon system.”

The contrast between these two approaches can be seen in the debate over the Russian UN General Assembly resolution that seeks to develop arms control approaches to IO and CNO. Russia’s draft resolution, UNGA 53/70, called upon member states to “promote at multilateral levels the consideration of existing and potential threats in the field of information security” and requests progress on “developing international principles that would enhance the security of global information and telecommunications systems and help combat information terrorism and criminality.”[9] Pointedly, Russia’s submission to the UN Secretary General called for “acknowledgement that the use of information weapons against vital structures is comparable to the consequences of the use of weapons of mass destruction.”[10]

The important point is that the Russian submission was made to the General Assembly’s First Committee, dealing with disarmament issues. The USA has consistently urged that the matter be referred to the Second Committee (economic issues and financial matters) and/or the Sixth Committee (legal). This apparently abstruse bureaucratic point highlights the divergent paradigms in play.

2.2. Framing the Dilemma

The problem of how to treat CNO is recognized by the US military, which is at the cutting edge of military CNO developments.

A US Air Force-sponsored workshop held in March 2000 concluded that international efforts to tackle cybercrime and cyberterrorism "could hinder US information warfare capabilities, thus requiring new investments or new research and development to maintain capabilities."[11] The dilemma was summed up in 1999 by the US Department of Defense whose legal counsel argued that:

> "the United States has not yet addressed fundamental policy decisions about where its long-term interests lie in connection with the possible international legal restriction of information operations. On the one hand, there is an obvious military interest in being able to interfere with an adversary's information systems … On the other hand, as the nation that relies most heavily on advanced information systems, the United States has the greatest vulnerability to attack. This concern would seem to drive US policymakers to consider the merits of international restrictions on information operations."[12]

That this policy dilemma remains unresolved is evident from the variety of activities in the Western world both in the military IO sphere and in the CND sphere, both civil and military. Whilst there is some coherence to current approaches, there is likely to be increasing tension between the multilateral institutions that are pursuing the military (offensive) and civil (defensive) tracks. An underlying problem is that existing state-led approaches to the military dimension of CNO fail to recognize the nature of the globally interdependent network environment and the leading role of the private sector in this domain.

3. Vertical Proliferation

Although great play is given by US defense analysts to potential CNO threats from nations such as China and Russia, it is the US, supported by its NATO allies, that is leading the way in turning CNO into a sophisticated and integrated strategic tool. Although CNO has played only a marginal role in recent operations such as Kosovo, the US and several NATO nations are moving to develop the capabilities, doctrines and organizational structures to operationalize CNO. Increasingly, IO is being regarded as "an integrating military strategy." Within this context, NATO planners are routinizing CNO as part of military planning, doctrine and capability development.

3.1. The US Leads the Way

The United States Army was the first branch of the US Armed Forces to publish a doctrine on Information Operations, back in 1996.[14] The doctrine was operationalized with assistance of the Land Information Warfare Activity (LIWA) during the tenure of Multinational Division North in peacekeeping operations in Bosnia. Lessons learned studies however demonstrated that an integrated doctrine, at the level of US forces, let alone that of a multinational coalition, was lacking.[15]

Whilst the US Air Force had deployed operational IW units at Kelly AFB and Shaw AFB since 1993, it was only in 1998 that USAF doctrine on IO, *Air Force Doctrine Document (AFDD) 2-5, Information Operations*, was released. In the same year, Joint Doctrine was also published under the authority of the Joint Chiefs of Staff. US Joint Publication 3-13 characterizes Information Superiority

(IS) as one of the cornerstones of US doctrine for the 21st century. IS is defined as “the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same.” Within this framework, JP3-13 sets out the importance of an integrated use of IO in all aspects of a military operation.[16]

Joint and Air Force doctrine emerged in time for the 1999 Kosovo Campaign. Although the IO campaign against Serbia went a step further than the Bosnian campaign, there was still a lack of integrated planning and operations. As an element of IO, CNO and Special Information Operations (SIO) were used only to a limited extent. This was due to a combination of factors, including: lack of integration into overall campaign planning; uncertainty as to the legality of such operations; disagreement between intelligence and military personnel over whether to exploit or attack networks; unwillingness to expose US capabilities to the coalition; limited Serbian reliance on vulnerable networks.[17]

Further to this experience, in 1999 Computer Network Defense was handed to US Space Command (SPACECOM).[18] In October 2000, SPACECOM took over the CNA mission. The 609th Information Warfare Squadron was also moved to SPACECOM’s area of responsibility.

3.2. The Europeans Follow

Leading European military powers have followed the US lead and are beginning to see IO (and CNO) as a routine part of their military operations. However, differences over definitions and limited resources to invest in new capabilities have meant that integration has been gradual and haphazard.

The United Kingdom’s 1997 *Strategic Defense Review (SDR)* recognized IO and CNO as a military activity of growing importance.[19] MoD recognized the advantages that digitization could bring, but pointed out that this created new dependencies which meant forces were much more susceptible to IO and CNA by malicious actors. Although the MoD carried out some elements of IO in the Kosovo campaign, it acknowledged in subsequent reviews that “our capabilities for conducting information operations need to be further developed.”[20]

Since 1999, the UK’s Joint Doctrine and Concepts Center has been drafting a doctrine, which is likely to be approved in late 2001. The draft doctrine defines IO as the military component of affecting the enemy’s perception, but points to the need for an integrated IO campaign to be coordinated across government departments.

France has been behind the United Kingdom in official development of organizational capabilities for IO. Although there have been speeches given by relatively senior figures in the French defense establishment, there have been no public statements that an IO doctrine is under development. Nonetheless, two research centers appear to be the focal points of French IO work. CELAR (Centre d’Electronique de l’Armament) specializes in the study of the application of IW techniques and the Ecole de Guerre Economique takes an interesting view of the application of IO by including economic vulnerabilities, as well as psychological warfare and information security. The main declaratory statements have been at conferences, where theories on the ‘Mastery of Information’ have been developed.[21]

German doctrinal thinking on the importance of IO in modern warfare was originally crystallized in a draft document entitled the *First Position of the German MoD on InfoOps*. A concept for IO is under development and is likely to be ready for political approval in the autumn of 2001. This concept paper, or Teilkonzeption bereichs•bergreifende Aufgaben (TKBA) may well feed into the future overall Bundeswehr strategy Konzeption der Bundeswehr (KdB). While the current TKBA on IO has not been released, a 1999 Bundeswehr draft paper touched on CNO by referring to the importance of developing: “capabilities to manipulate, interrupt, compromise, ... an adversary’s information and information systems.”[22]

3.3. NATO Catches Up

NATO developed a draft policy on IO in 1997, based in part on a recognition of the crucial importance of this activity in the context of IFOR and SFOR. This policy defined IO as “actions taken to influence decision makers in support of political and military objectives by effecting the other’s Information and/or Information Systems, while exploiting and protecting one’s own Information and/or Information Systems.”[23]

However, by the time of Operation Allied Force (OAF) in 1999, NATO had not moved from the conceptual stage to developing an agreed IO doctrine or to including IO in its exercises or planning. NATO planners recognized that their failure to implement an effective IO campaign reduced the effectiveness of OAF. They have acknowledged that “doctrine on information operations needs to be developed further.”[24] A NATO doctrinal working group on IO was subsequently established but appeared to have made little progress by the summer of 2001. Nonetheless, NATO military planners recognize that IO will be used more and more in MOOTW (Military Operations Other Than War) where the ‘center of gravity’ of allied and enemy forces will be psychological and therefore a prime candidate for CNO.

At a higher level, the NATO Parliamentary Assembly has been discussing the issues of Information Warfare since 1997, when the Science and Technology Committee presented a report on *Information Warfare and the Millennium Bug*. In 1999, this same committee reported on *Information Warfare and International Security*. The Committee argued that “the possibility that the United States (or any other Western country) would develop and deploy offensive information warfare techniques has not been adequately discussed in public forums. This can be essential in order to build a national and possibly international consensus about the role of offensive information warfare and to clearly define its policies of use.”[25]

4. Protecting Cyberspace

International businesses, governments and multilateral institutions have for some time been concerned by the implications of a growing reliance on information systems for critical business processes. In the past two decades, a variety of initiatives have been undertaken to improve the security and dependability of systems, of management practices and of international policing efforts. However, it was the rapid expansion of the Internet, of e-commerce and the promises of e-government in the 1990s that put security, reliability and privacy firmly onto the international policy agenda.

By 2001, European and US policy-makers at the highest levels were expressing their concerns that insecure information systems threatened economic growth and national security. President Bush's National Security Adviser Condoleezza Rice noted in March 2001 that "it is a paradox of our times that the very technology that makes our economy so dynamic and our military forces so dominating also makes us more vulnerable." She warned, "Corrupt [the information] networks, and you disrupt this nation."[26] The European Commission warned in March 2001 that "the information infrastructure has become a critical part of the backbone of our economies. Users should be able to rely on the availability of information services and have the confidence that their communications and data are safe from unauthorized access or modification. The take up of electronic commerce and the full realization of Information Society depend on this."[27]

As a result of these concerns, a complex and overlapping web of national, regional and multilateral initiatives has emerged.[28] A common theme behind these initiatives is the recognition of the inadequacy of existing state-centric policing and legislative structures to police international networks and the importance of ensuring that private networks are secured against disruption. One way of grouping these initiatives is to use the standard information security paradigm of Deterrence; Prevention; Detection; and Reaction.

- *Deterrence:* Multilateral initiatives to deter CNA include harmonizing cyber-crime legislation to promote tougher criminal penalties and better e-commerce legislation (Council of Europe Convention, UNCITRAL).
- *Prevention:* Multilateral initiatives to prevent CNA center around promoting the design and use of more secure information systems (e.g. R&D initiatives between the US and EU; Common Criteria) and better information security management in both public and private sectors (e.g. ISO and OECD standards and guidelines initiatives). Other measures include legal and technological initiatives such as the promotion of security mechanisms (e.g. electronic signature legislation in Europe).
- *Detection:* Multilateral initiatives to detect CNA include the creation of enhanced cooperative policing mechanisms (e.g. G-8 national points of contact for cyber-crime). Another important area is the effort to provide early warning of cyber-attack through exchanging information between the public and private sectors (e.g. US Information Sharing & Analysis Centers, FIRST, European Early Warning & Information System).
- *Reaction:* Multilateral initiatives to react to CNA include efforts to design robust and survivable information infrastructures; development of crisis management systems; and improvement in coordination of policing and criminal justice efforts.

In toto, these initiatives involve significant investments of time and effort from a variety of government departments in many nations, from numerous international organizations and from numerous companies, large and small. Many initiatives are pre-existing; many are being pursued in isolation. Nonetheless, there has emerged a coherent and effective set of initiatives involving states and businesses, not to mention some NGOs that are focused upon improving the security of the emerging global information environment.

5. A Joined Up Approach?

Upon surveying the parallel developments in the military (offensive) and defensive or protective spheres, an analyst could conclude that what we are seeing is a sophisticated twin track approach on the part of the leading global powers, notably the US national security community. Moreover, it is possible to understand the terms of the strategic debate in realist terms. As with any new military technology, the party that is most advanced wishes to retain that unilateral advantage by restricting opportunities for use of the capability against itself. Its potential adversaries will seek asymmetric responses.

The Bush Administration, which, at the time of writing is finalizing a new national security approach within which to encapsulate Critical Infrastructure Protection (CIP), has been clear about its strategic vision. While it reinvents US armed forces for an era of Revolution in Military Affairs (RMA) operations, the Administration has made economic and homeland defense a priority. As the US seeks to make itself invulnerable from conventional threats by adopting RMA-era armed forces and from ballistic missiles through the National Missile Defense, its information infrastructure remains its soft underbelly. Hence, efforts to protect both the US infrastructure and those global infrastructures on which it is dependent are logical extensions of economic and homeland defense. The most effective way to stimulate defensive measures by government, industry and international organizations is to characterize the threat as coming from non-state actors, hence the hacker/cyber-terrorist paradigm.[29]

One asymmetric response to military weakness is to seek to use international legal instruments to restrain vertical proliferation on the part of a rival. Hence the Russian gambit at the UN. Russia’s attempts to ban IO make strategic sense and mirror its efforts to restrict nuclear weapons in the early years of the Cold War. Russia recognizes that, as it struggles to rebuild its economy, it is vulnerable to the advanced tools and doctrines of IO that its Western rivals are developing. Unable to counter in kind, or to afford comprehensive defensive measures, Russia is seeking to use international law to reduce America’s military advantage.

Another response is indicated in recent Chinese military writings. The widely-quoted People’s Liberation Army (PLA) publication *Unrestricted Warfare* makes the point that emerging international norms and rules are shaped to fit the interests of the USA. Therefore, a weaker power must subvert these rules. This goes for operations in cyberspace as much as in other spheres. As the book puts it: “strong countries make the rules while rising ones break them and exploit loopholes. … The United States breaks [UN rules] and makes new ones when these rules don’t suit [its purposes], but it has to observe its own rules or the whole world will not trust it.” Therefore, “the first rule of unrestricted warfare is that there are no rules, with nothing forbidden.”[30] Thus, a weaker power should realize that: “all these non-war actions [hacking, financial manipulations, perception management] may be the new factors constituting future warfare.”[31]

Unfortunately, if strategists in Western capitals, mirrored by their counterparts in Moscow and Beijing, believe that they are merely engaging in the time-honored game of seeking strategic advantage from a new technology, they fail to perceive crucial elements of the new environment in which they are operating. The problem is that both sides of the argument are working within a set of paradigms that are outdated in the globalized and networked world. The most important aspects that are being missed are the nature of interdependency and the role of the private sector.

Before elaborating on this point, it is worth noting that, even within the current paradigm, there are serious inconsistencies in both institutional and conceptual terms that are undermining Western policy.

5.1. Multiple Agencies, Multiple Agendas

On an issue as complex as CNA/CND, which cuts across so many traditional bureaucratic and sectoral boundaries, it is not surprising that there are institutional schisms. Underlying the institutional issues however are questions of the extent to which policy-making is really joined up and, hence, intellectually coherent.

In simple institutional terms, it is evident that it is the military and national security institutions in the USA and its allies that are pursuing the development of CNO. It is the civil government/commerce and law enforcement institutions that are devising and implementing defensive policies.

Clearly, within countries, there is some involvement by the military in protection of national infrastructures. Indeed, the military drove much of this original work as they were concerned at their dependence on insecure civil infrastructures. Nonetheless, the military role has declined since the late 1990s as the focus has shifted to the private sector and to civil government agencies.

The institutional schisms at the multilateral level can be seen most clearly in the form of NATO and the EU. For the purposes of this argument, the membership of the two groupings can be regarded as overlapping. Apart from the fact that the leading European players in CNO and CIP are in both organizations, the USA also has a growing role in EU deliberations on cybercrime and network security.[32]

Despite this overlap in membership and an obvious shared interest in protecting NATO and EU networks, the policy agendas being pursued are radically different. NATO is seeking to legitimize and routinize CNO as a military instrument of coercion. The EU is seeking to delegitimize cyber-attacks and to build robust global information networks that will make cyber-attacks harder to conduct, easier to trace and easier to recover from.

A conspiracy theorist, or believer in government as a rational actor, would argue that this represents a sophisticated, multilateral sword and shield approach in which NATO forges the CNO sword and the EU deploys the CND shield. In this case however the cock up theory holds more water than the conspiracy theory. NATO and the EU represent different bureaucratic constituencies, which are often not joined up at home. Whilst NATO discussions on CNO involve primarily the military, with support from intelligence agencies, EU discussions on dependability and cybercrime involve commerce ministries and law enforcement.

The translation of institutional disconnect into incoherent policy is not just a potential problem. A good example of the problem on the domestic scene was found in recent UK legislation. In short succession, the Department of Trade & Industry sponsored a minimalist, pro-business Act promoting e-commerce (Electronic Communications Act) whilst the Home Office sponsored the regressive and intrusive Regulation of Investigatory Powers Act. Unfortunately, the consequences of policy incoherence and of divergent agendas at the multilateral level undermine the framework of trust upon which the emerging global Information Society is being built.

6. An Interdependent World

Of the two elements of the global information environment paradigm that are missed by Western strategists, it is the notion of interdependency that current military thinking on CNO mostly fails to appreciate. In short, there is a disjunction between the technological and market realities of a globalized, interdependent and networked world and emerging military doctrine on IO and CNO. Constrained by a focus on delivering "effect" to a particular geographic conflict zone and within existing "kinetic-era" legal paradigms, militaries are trying to exploit CNO for precise targeting of enemy infrastructures.

Unfortunately, the attempt to squeeze CNO into existing conventional force paradigms misses important truths about the *emerging* global information environment. It is not enough to devise military policy for today's rather rudimentary cyber-environment, it must take into account the next generation Internet and information environment that will emerge over the coming 5-10 years. The Next Generation Internet that will form the backbone of this information environment will provide always on connection through multiple devices embedded in all aspects of business, public and personal life.[33] Online computing will be pervasive.[34]

As today's Internet evolves into the Next Generation Internet (NGI), businesses, consumers and governments will depend upon the Internet even more than they do today. The Internet will become as ubiquitous as electricity and will have to be as reliable. With the advent of mobile computing and the micro applications of Information Technology, concepts like IBM's Intelligent Kitchen will be realized. This envisages an environment in which even household appliances are connected to 'the Grid' and where devices use networked information technology in a pervasive and ubiquitous manner to find and use services as and when they need them. In this way the whole Internet melts into one giant computer. This means that the Internet will be not only interdependent, but super–dependent.[35]

Three aspects of this future environment are of particular significance:[36]

- <u>High powered, embedded computational capability will become pervasive in the civil sector</u> … localized wireless communication devices will dominate the consumer electronics sector within the next 5 years. This will become an enabling technology for the wide-scale adoption of … "ubiquitous computing." This … will dramatically increase the level of connectivity and lead to new, ill understood, systems behavior.
- <u>The emergence of a highly connected Global Information Infrastructure (GII)</u>[37] with converged broadband computing, media, telecommunications capabilities … will greatly complicate interdependency analysis.
- <u>Greater interconnectivity between traditionally separate information infrastructures</u> may drastically alter overall systems behavior. Particularly worrying is the potential emergence of

infrastructures with in-built instability, critical points of failure, and extensive interdependency.

6.1. The Blowback Effect

These features of the emerging information environment make it extremely unlikely that any but the most limited and tactically-oriented uses of CNO could be contained as called for by current military doctrine. There are a number of ways in which military use of CNO could "blowback"[38] on Western societies through the interdependencies that will characterize the new environment.

The most obvious route is through direct network interdependencies. Even in today's environment, relatively innocuous cyber-weapons such as viruses and worms "in the wild" can cause considerable disruption to businesses, governments and consumers. This risk is parallel to that with Biological Weapons, any use of which has always faced the risk of infecting friendly populations.

Another "blowback" channel is via second and third order dependencies. In today's globalized, liberalized and just-in-time economy, governments and companies have found it almost impossible to map and understand their wider dependencies.[39] As the discussion above highlights, the emerging information environment is likely to exacerbate these interdependencies and to make systems behavior even harder to predict. The most sophisticated attempt yet to model these interdependencies, by the US Department of Energy, is increasingly turning to chaos theory for assistance in its task. Against this background, Western militaries cannot responsibly claim to be able to predict the knock-on effects of large-scale CNO use in the context of a wired world.

A more intangible blowback effect is that the routine use of CNO risks undermining trust in cyberspace. Across the developed world, a lack of trust and confidence in information networks is already a barrier to the rapid take-up of e-commerce and e-government. Trust is being undermined by cyber-vandals (hackers and virus writers), by cyber-criminals, by cyber-espionage[40] and by companies that abuse online privacy. The knowledge that global information networks are being routinely exploited by Western militaries would lead users to question whether data and systems were trustworthy and whether information was being polluted. The damage to consumer and business confidence could well undermine efforts to promote a trusted Information Society.

Finally, another intangible effect has already been considered by the US military. For the US, one reason for not using IO more aggressively in the Kosovo conflict was the fear that this could set a legal and operational precedent. Routinisation of CNO as a military tool by NATO states will remove any legal, political or operational barriers to its routine use by other states and groups. Given that the balance in CNO is likely to favor the offence for some time to come, it is not at all clear that the routine adoption of CNO would be in the West's strategic advantage.

7. Bringing in Business

The other element of the new paradigm is the increased part played by the private sector.[41] Policy-makers dealing with CIP have come to recognize that defensive policies are untenable without active participation by the private sector since this sector owns and operates the networks and knows what is going on in cyberspace. The US is addressing this problem by inviting industry to participate in writing its *National Plan for Infrastructure Protection*. The European Commission explained the problem succinctly:

> "whilst security has become a key challenge for policy makers, finding an adequate policy response is becoming an increasingly complex task. Only a few years ago, network security was predominantly an issue for state monopolies … Establishing a security policy was a relatively straightforward task. This situation has now changed considerably because of a variety of developments in the wider market context, amongst them liberalisation, convergence and globalisation … these developments constrain the ability of governments to influence the level of security of the electronic communications of their citizens and businesses."[42]

The recognition of the central importance of the private sector in the formulation and implementation of policy in this domain has long been recognized in some multilateral fora, such as the OECD.[43] There is however a long history of clashes between states' perceptions of their national security needs and of businesses' perceived needs to secure their international operations.

7.1. A Troubled Past

The debate over cryptography policy provides the most obvious examples of these clashes. In the 1990s the use of cryptography spread from a few specialized, civil applications such as banking, and Western governments became concerned about the impact of widespread, strong cryptography on their intelligence activities. The business view was that strong cryptography was vital for the success of e-commerce and the growth of the Internet. Civil liberties groups supported liberalization in the name of privacy. The US government however sought to control the proliferation of strong cryptography, arguing that putting cryptography into the hands of criminals would make the tasks of law enforcement much harder.[44] European governments took varying positions.

Throughout much of the 1990s the US government engaged in various efforts to control cryptography, to ensure that weak crypto was used at home and abroad and to ensure government retained access to encryption keys. The Clipper Chip was the most notorious but key escrow mechanisms such as Trusted Third Parties were intensively discussed. In Europe, there were both very restrictive policies (e.g. in France) and more liberal approaches (e.g. in Ireland and Belgium).

On the multilateral level, the issue was dealt with through the Wassenaar Arrangement, the 33 nation successor to COCOM that was founded in 1996. Wassenaar imposes controls on exports of dual-use goods and munitions; including certain encryption products. It declares that "the export of encryption technology will remain possible without depositing keys with government agencies" but that asymmetric encryption procedures appearing under the dual use list, category 5, part 2 (Information Security) are restricted.[45] The debate has been over the strength of the encryption allowed, measured in bits.

By the end of the 1990s, the debate had shifted in favor of liberalization. As a 1996 report by the US National Research Council concluded, "on balance the advantages of more widespread use of cryptography outweigh the disadvantages."[46] In 2000, the Clinton administration revised export regulations on high grade encryption, permitting exports to EU member states and Australia, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland and Switzerland without a government license.[47] This paved the way for Wassenaar restrictions to be lifted from 56 bits to 512 bits, meaning that everything but extremely sophisticated military encryption was liberalized. This harmonization of international approaches was reflected in individual European states; even France made a dramatic U-Turn and adopted an approach of almost complete liberalization.[48]

Whilst this shift in policy did to some extent represent the victory of the views of business and civil liberties campaigners over those of national security establishments, the debate is far from over. For instance, the EU's directive on electronic signatures was only finally concluded once state and business parties to the negotiations had agreed to focus on one application of cryptography – authentication – rather than to include confidentiality. The problem of how to ensure that strong encryption for confidentiality does not undermine law enforcement intelligence efforts remains undecided. The UK's *Regulation of Investigatory Powers Act* uses legal sanctions to ensure "escrow by intimidation."[49] The Council of Europe Cybercrime Convention adopts a similar model.[50]

7.2. A Clouded Future

The crypto debate has in part been resolved in favor of business but serious differences remain between states and businesses. As CNO becomes a more prominent issue, it is likely that a new source of tension will emerge between states and businesses.

This time, though, government strategists on all sides will find it much harder to enforce their positions on the private sector. The fact that the private sector now leads in developing, deploying and operating the information networks in question poses challenges both to states such as the USA who want to exploit CNO and to states such as Russia who seek to control this capability.

Insofar as military exploitation of CNA is concerned, there is a growing recognition by businesses, that are becoming reliant on the global network of networks, that the fragile commodity of trust could all too easily be undermined by military uses of CNO. Even if individual global or Western businesses are not the direct targets of CNA in a military campaign, the potential for knock-on effects as outlined above is disturbing. In the debate over key escrow, a central concern of business has been that even the *perception* of the *possibility* that data could be accessed by a third party such as a government could undermine trust in e-commerce. The same argument applies many times over if information networks are routinely exploited by NATO militaries for purposes that will, necessarily, remain undisclosed.

As for those who seek to limit CNA proliferation, the arms control community has a problem in that state centric arms control approaches have traditionally not had to engage with business, except in a prescriptive manner through export control regimes, e.g. MTCR, NSG. The Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BWC), both of which deal with dual-use goods in a globalized industry, provide both positive and negative lessons for any arms control initiatives in this sphere. As will be discussed below, though, the conceptual and practical problems in designing an arms control regime for CNA are much more complex.

8. Developing Norms

If the proliferation and routinization of military CNO pose a danger to the information society, then it is important to examine ways of limiting the vertical and horizontal proliferation of CNO. Before outlining possible approaches, it is worth addressing the common argument that the current structure of the international system will void any such effort.

8.1. Power Politics

Surely, it is commonly argued, the US “hyperpower” will not agree to have its hands tied by its rivals and by idealistic arms controllers. There is little point developing norms and regimes for controlling CNO if a convincing argument cannot be made to US strategists that these may, in fact, be in US national security interests.

In fact, such an argument can be made. While there is a clear strategic advantage to the US to remain the dominant power in the field of IO and CNO, it is not in US strategic interests to allow the unfettered proliferation and use of CNO, even if the US retains the offensive lead. An obvious reason is US national vulnerability to CNA. It remains a moot point and the subject of numerous wargames whether unconstrained use of CNO in a future conflict would be to the net benefit of the US. Rather, widespread use of CNA may give opponents an asymmetric tool by which to undermine the US’s conventional, nuclear, economic and diplomatic might. As John Arquilla has argued, it is in the USA’s strategic interests to pursue cyber-arms control as “we are such a broad and rich target.”[51]

More fundamentally however by engaging in the building of norms that restrict the use of CNO, the US will be able to use its leading military and technical position to shape the international agenda, customary law and practice and to lay out the bases of discussions. As Neal Pollard has argued, it would be in the interests of the US to adopt an open declaratory policy on strategic CNA in order to raise the deterrent threshold. A unilateral declaratory policy would provide “a nexus around which the international community can consider strategic CNA in conflict, perhaps providing a starting point for a normative framework.”[52]

8.2. Arms Control

Although arms control approaches to controlling CNO have begun to be discussed, it is hard to envisage traditional capability-based arms control being of much utility due to the impossibility of verifying limitations on technical capabilities possessed by a state. As Anders Eriksson put it: “generally speaking, the avenues available for “arms control” in this arena are primarily information exchange and norm-building, whereas structural approaches—trying to prohibit the means of information warfare altogether or restricting their availability—are largely impossible due to the ubiquity and dual-use nature of information technology.”[53]

The CWC and BWC have also dealt with dual-use technology but the current struggle to develop a verification regime for the BWC indicates some of the problems that would be faced by any cyber-arms control verification regime.[54] While it is true that the creation of organized military IO/CNO units could be monitored with the assistance of Western intelligence services, the proliferation of CNA capabilities in themselves could not really be monitored since the technology required (hardware, software and “wet-ware”) is inherently globalized. The fact that existing multilateral and national arms control regimes are only beginning to grapple with the export of intangibles such as software and know-how[55] indicates how difficult any controls would be in an era when cyber-attack scripts reside on Internet hosts computers around the world.

Even if approaches to cyber-arms control could be conceived and verification regimes designed, arms controllers would face two enormous challenges. First, even more than with the BWC, any regime would need the involvement and support of the private sector from the start. The globalized Information & Communications Technology (ICT) industry is not one to which top-down mandatory regulations can be easily applied, unlike, for instance, the more traditional, nationally-based defense manufacturers.

The other key problem would be the need to ensure that restrictions on state proliferation did not disadvantage states vis-•-vis sub-state groups. Given the potential that CNO provide for sub-state groups to wreak serious damage on states, multilateral controls on sub-state and criminal behavior would have to be reinforced before states are likely to accept controls on their own capabilities.

8.3. Norms and Codes of Conduct

Whilst arms control may not be a feasible approach for the time being, an approach that seeks to develop norms of use and non-use is certainly worth exploring. The aim of developing explicit norms of behavior would be to govern the new risks by making behavior more predictable and so enhancing business and citizen trust and confidence. The case for norms was made by Jack Mendelsohn, speaking to the NATO Parliamentary Assembly in May 2000, “if we were to … drift toward an increasingly opaque world, without structure, without norms and without predictability, where nations would be seeking unilaterally to ensure their own security, how could you hold out any hope to your constituents for a more peaceable, stable and secure world.”[56]

These norms may well include definitions of when and how CNO could be used (for instance as part of enforcement mechanisms under UN auspices). This debate would have to take careful account of the “blowback” risks identified above but could thereby ensure that some of the perceived military advantages of CNO were exploited in the interests of the international community rather than for, destabilizing, unilateral advantage.

Norms for CNO are, by default, already being developed by the leading powers. As they develop their IO doctrines, NATO militaries are examining existing legal restrictions on use and restrictions on targeting under the Laws of Armed Conflict.[57] Information Warriors are seeking to ensure that IO and CNO meet the classic requirements of military necessity, humanity and chivalry. There is also a vibrant debate over the extent to which cyber-attacks can be classed as armed attacks under international law and the terms of the UN Charter.

Efforts have also been made in multilateral fora to develop norms that could put NATO doctrine into a wider context and influence the global development of IO and CNO capabilities. The most significant effort has been within the EU, where Germany, Sweden and Austria jointly sponsored efforts to apply military codes of conduct to IO. Although the initiative was reportedly blocked by the UK, this route retains a great deal of potential.[58] Codes of conduct are used within the OSCE to encourage harmonization of military practice and civil-military relations across OSCE member states, notably in the former Eastern Bloc.[59] Codes of conduct provide a mechanism by which states with current IO capabilities can ensure that both their own use of IO/CNO and that of future proliferators will be regulated and within agreed boundaries.

If the development of codes of conduct is to be successful however four factors need to be integrated into the process as soon as possible:

- First, any norms and restrictions must be developed in light of the likely future market and technological environment. It will be important to understand the risks outlined in chapter six above and to ensure that the norms are framed broadly enough to be frequently updated since CNO will not be carried out within a stable and predictable environment.
- Second, advantage should be taken of likely harmonization within OSCE member states and indeed globally as multilateral initiatives on CND and CIP progress. In the short term, EU associate nations are likely to be engaged in EU efforts to secure regional information infrastructures. In the longer term, legal and other measures are likely to move towards global harmonization as more countries join the fight against cyber-crime. Since the defense is inseparable from the offence, defensive harmonization can advance convergence on norms for offensive operations.
- Third, advantage should be taken of emerging plans for internationally coordinated Alert, Warning and Response (AWR) systems to counter cyber-attacks. The G-8, EU, US and international policing and industry groupings are making progress towards the development of standardized and integrated systems to ensure detection of cyber-attacks.[60] These systems can contribute to the verification and enforcement of norms since most nations will be subject to network monitoring and reporting.
- Fourth, and perhaps most importantly, the private sector needs to be engaged up front in development of any norms or codes of conduct. The necessity of engaging the private sector in policy development is recognized in the field of CIP and domestic CND. However, in a multilateral context, businesses and NGOs must be given a central role since they understand the infrastructures, are already setting international standards and are designing alert and warning systems.[61]

9. Conclusions

The benefits of e-government, digitized battlespaces and e-commerce are evident to the advanced nations; less developed states also recognize the importance of plugging into the emerging global information environment. It is equally evident that, without trustworthy systems and survivable infrastructures, the information revolution will not progress. Hence an increasing number of governments are grappling with the problem of building secure electronic commerce environments and of ensuring protection of their critical national infrastructures.

America and its strategic partners will have to decide how they wish to balance contradictory requirements. On one hand it is in their economic and security interests to see the emergence of robust international conventions and mechanisms that protect the global information environment. On the other hand, their investment in military technologies and doctrines designed to disrupt the infrastructures of rival nations is a comparative strategic advantage that they will be loath to give up. Nonetheless, there is a strong argument that it would be to the overall strategic benefit of the Western powers to accept internationally agreed norms of use for CNO.

As with cryptography, the particular interests of warfighters and intelligence agencies do not outweigh the broader societal benefits of a secure information environment. The adoption of multilateral norms such as codes of conduct provides one way ahead. To be effective, such norms must be designed with an eye to a dynamic future and must engage the private sector from the start.

Notes:

1. Neil Robinson, also of RAND Europe and IAAC, contributed extensively to the research for this article.
2. Ministry of Defence, *Draft doctrine for Information Operations; Joint Doctrine Pamphlet XX-01* (Shrivenham: Joint Doctrine and Concepts Centre, March 1, 2001), 8.
3. http://www.jrc.deppy.it.
4. The other categories of offences are: 2) Computer-related offences; 3) Content-related offences; 4) Offences related to infringements of copyright and related rights.
5. G8 Government/Industry Conference on High-Tech Crime, *Report of Workshop 3: Threat Assessment and Prevention* (Tokyo, May 22-24, 2001), 1-2.
6. Abraham D. Sofaer and Seymour D. Goodman, *A Proposal for an International Convention on Cyber-Crime and Terrorism* (Stanford: Center for International Security and Cooperation, Stanford University, August 2000).
7. See the conference organised by the Heinrich Böll Foundation, *Arms Control in Cyberspace: Perspectives for Peace Policy in the Age of Computer Network Attacks* (Berlin, June 29 - 30, 2001).
8. The concept of global information environment is used here rather than the narrower concept of the global information infrastructure (GII). As today's GII evolves, the focus will shift from the Industrial Era concept of infrastructure protection/attack to the Information Age concept of information protection/attack. Britain's Defence Evaluation and Research Agency (DERA) coined the term "national digital environment" to replace the term NII. DERA, *An Analysis of the Military and Policy Context of Information Warfare*, June 1997, (DERA/CIS3/58/8/5).
9. UN General Assembly, draft resolution 53/70, *Developments in the field of information and telecommunications in the context of international security*.
10. *Note from Permanent Mission of the Russian Federation to the United Nations to the Secretary-General* (June 9, 1999), 4.
11. USAF Directorate for Nuclear and Counterproliferation and Chemical and Biological Arms Control Institute, *Cyberwarfare: What Role for Arms Control and International Negotiations?* (Washington, D.C., March 20, 2000), 4.
12. Department of Defense, Office of the General Legal Counsel, *An Assessment Of International Legal Issues in Information Operations* (May 1999).

13. Andrew Garfield, "Information Operations as an Integrating Strategy," in Alan Campen and Douglas H. Dearth, eds,, *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict* (Fairfax, VA: AFCEA International Press, 2000), 261-274.

14. Department of Defense, *FM 100 – 6 Information Operations Doctrine* (Washington DC: Headquarters, Department of the Army, August 1996). Available @ http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/100-6/toc.htm.

15. LTC Garry J. Beavers and LTC Stephen W. Shanahan, "Operationalizing IO in Bosnia – Herzegovina," *Military Review* 77, 6 (November-December 1997).

16. Department of Defense, *Joint Publication 3-13*, *Joint Doctrine for Information Operations*, United States Joint Chiefs of Staff, Washington D.C., October 9, 1998, Chapter 4, Information Operations Organization, IV-1, available @ http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

17. http://www.airpower.maxwell.af.mil/airchronicles/apj/apj00/sum00/pounder.htm; Andrew Rathmell, "Information Operations: Coming of Age," *Jane's Intelligence Review* (May 2000).

18. http://www.peterson.af.mil/usspace/new19-99.htm.

19. Ministry of Defence, *Strategic Defence Review* (London: The Stationary Office, 1998), 10.

20. Ministry of Defence, *Kosovo, Lessons from the Crisis* (London: The Stationary Office, 2000), 5; House of Commons, *Defence Select Committee Fourteenth Report* (London: The Stationary Office, October 2000), chapter 3, "The Conduct of the Campaign: Information Operations," available @ http://www.publications.parliament.uk/pa/cm199900/cmselect/cmdfence/347/34718.htm#a53.

21. Jean-Pierre Meunier, "Le CELAR, centre technique de la guerre de l'information," *L'Armement* 60 (Dec 1997-Jan 1998), 84-88; Col Jean-Luc Moliner, "La guerre de l'information vue par un opérationnel français," *L'Armement* 60 (Dec 1997-Jan 1998), 11.

22. Susanne Jantsch, "Comparative Approaches to Critical Infrastructure Protection - German Approach," presentation at 22nd National Information Systems *Security Conference* (Washington, D.C., October 1999).

23. MC 422.

24. Vice Admiral Haddacks (UK Military Representative to NATO), *Minutes of Evidence to the Defence Select Committee* (London: The Stationary Office, May 2000), available at http://www.parliament.the-stationery-office.co.uk/pa/cm199900/cmselect/cmdfence/347/0051704.htm.

25. NATO, *Information Warfare and International Security*, NATO Parliamentary Assembly Science and Technology Committee (Brussels, October 6, 1999). Available @ http://www.naa.be/publications/comrep/1999/as285stc-e.html (visited 08/08/01).

26. Associated Press AP, "National Security Adviser sees cyberterrorist threat," March 26, 2001.

27. COM(2000) 890 final, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime.*

28. A comprehensive review of activities is presented in Rathmell, et al., *Information Operations: A Global Perspective* (Coulsden: Jane's Information Group, 2000).

29. Nonetheless, Western security agencies are really concerned about foreign state CNE and potential CNA which they see as having much greater capabilities in the longer term.

30. Editors note in forward to Liang, Qiao and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999), 2.

31. Ibid, 12.

32. For instance, the US Department of Justice played an important role in the development of the Council of Europe Convention and the US State Department and defense research community have growing links to the European dependability R&D community.

33. For instance, the advent of Personal Area Networks (PAN) will embed the human user firmly within the Internet infrastructure.

34. Global Internet Project, *A Primer on the Security, Privacy and Reliability of the Next Generation Internet* (November 6, 2000).

35. "Computing Power on Tap," *The Economist* (June 23, 2001).

36. Abstracted from IAAC, *Information Assurance & Security Research & Development Policy Paper* (July 2001). Available @ http://www.iaac.ac.uk.

37. The GII can be defined as "that system of advanced computer systems, databases and telecommunications networks … that make electronic information widely available and accessible. This includes the Internet, the public switched network and cable, wireless and satellite communications." Adapted from definition of NII in: US Senate Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace" (5 June 1996).

38. Peter Feaver, *Information Warfare and the Political Control of Coercion* (Duke University, Durham, 1997), 16.

39. The fuel crisis that almost brought the UK to a halt in 2000 is a good example of these interdependencies, if in the physical world.

40. For instance, see European concerns over "Echelon." Temporary Committee on the Echelon Interception System, '*Draft Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System)*' (Brussels: European Parliament, May 18, 2001). Available @ http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon_en.pdf.

41. Taken here to mean primarily private business but also NGOs and individuals as users of networks, as citizens and as consumers.

42. *Network Security Communication*, 3-4.

43. For instance, the Business & Industry Advisory Council was extensively involved in the development of OECD *Guidelines for the Security of Information Systems.*

44. Though, as Ross Anderson argues, the primary motivator for the position of the US Government was concerns over national security intelligence collection rather than criminal intelligence collection. Ross J. Anderson, *Security Engineering: A guide to Building Dependable Distributed Systems* (Chichester: John Wiley & Sons, 2001), 461-464.

45. List of Dual Use Goods and Technologies and Munitions List * WA LIST (00) 1 01-Dec-00 Category 5 Part 2 – Information Security, available @ http://www.wassenaar.org/list/Cat%205P2%20-%2099.pdf.

46. Brian Gladman, *Wassenaar Controls, Cyber-Crime and Information Terrorism, Cyber Rights and Cyber Liberties (UK)* (London, September 1998), available @ http://www.cyber-rights.org/crypto/wassenaar.htm.

47. http://www.bxa.doc.gov/Encryption/19Oct2KFactsheet.html.

48. Assemblée Nationale, Document no. 314, *Projet de Loi sur la Societe de l'Information*, Assemblée Nationale (Paris, June 14, 2001). Available @ http://www.assemblee-nationale.fr/projets/pl3143.asp.

49. Anderson, 467.

50. "[Each party shall] adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable [authorities to access stored computer data]" Council of Europe, *Draft Cyber-Crime Convention*, Committee of Experts on Crime in Cyber-Space (PC-CY), Strasbourg, June 29, 2001, Article 19.4, available @ http://conventions.coe.int/Treaty/EN/cadreprojets.htm.

51. Stephen Green, "Pentagon Giving Cyberwarfare High Priority," *Copley News Service* (December 21, 1999).

52. Neal Pollard, "The Mouse that Leaves Something to Chance: Deterrence and Computer Network Attack," unpublished draft paper (2000), 49.

53. Anders E. Eriksson, "Information Warfare: Hype Or Reality?," *The Non-Proliferation Review* 6, 3 (Spring-Summer 1999).

54. "Bugs in the System," *The Economist* (June 16, 2001).
55. House of Commons, *Export Control Bill* (London: The Stationary Office, June 2001). Available @ http://www.publications.parliament.uk/pa/cm200102/cmbills/005/2002005.pdf.
56. J. Mendelsohn, "Does Arms Control Have a Future?," NATO Parliamentary Assembly 46th Rose Roth Seminar, *Non-Proliferation and Arms Control: The Agenda for the 21st Century* (Portoroz, Slovenia, May 4-6, 2000).
57. Richard W. Aldrich, *The International Legal Implications of Information Warfare* (Colorado Springs: US Air Force Academy, 1996); Mark Russell Shulman, *Legal Constraints on Information Warfare* (Maxwell Air Force Base, AL: Air University, 1999).
58. Johannes Bertholdt, *Arms Control in Cyberspace* (Berlin: Department of Arms Control, Federal Ministry of Foreign Affairs, June 29, 2000). Available @ http://www.boell.de/downloads/medien/bjohannes.pdf.
59. OSCE, *Towards a Genuine Partnership in a New Era – Decision No IV; Code of Conduct on Politico – Military Aspects of Security*, Budapest Document 1994, adopted at the Budapest Summit 1994 (Budapest, 6 December 1994). Available at: http://www.osce.org/docs/english/1990-1999/summits/buda94e.htm#Anchor_COD_65130.
60. Andrew Rathmell, "Building Partnerships to Protect Europe's Infrastructures," *Information Systems Security Europe Conference* (London, September 28, 2001).
61. "What's in a Scan?" *Canadian IO Bulletin* 2, 2 (June 1999).

ANDREW RATHMELL is a Senior Research Fellow at King's College London where he directs work on the Dependability Development Support Initiative (*www.ddsi.org*), supported by the European Commission's IST Programme. Dr Andrew Rathmell is also Chief Executive Officer of the Information Assurance Advisory Council (*www.iaac.ac.uk*). IAAC is a unique public-private forum dedicated to building partnerships across sectors in order to find solutions to the challenges of Information Assurance and Critical Infrastructure Protection. In October 2001, Dr Rathmell will take up a position as a Research Leader in the ICT Policy Research Programme at RAND Europe (UK) (*www.randeurope.org*). Within the ICT Programme, he will direct research on Information Assurance & Security Policy. Prior to joining RAND Europe, Dr Rathmell was Executive Director of the International Centre for Security Analysis (ICSA) at King's College London. ICSA is an interdisciplinary research center, which conducts scholarly and consultancy research on technology and public policy issues. A recipient of numerous academic and government grants, he has been a Principal Investigator on an ESRC project into Early Warning for cyber-threats; an EPSRC grant into fraud detection and a NATO Research Fellowship into Critical Infrastructure Protection policies. He has also served as a specialist adviser to the House of Commons and serves on the editorial boards of a number of scholarly journals. Dr Rathmell is a regular contributor to media outlets, including the BBC, Channel 4, ABC, CNN, Sky, *The Economist*, *Janes Intelligence Review* and is the author of a number of monographs and numerous articles. *E-mail*: andrew.rathmell@kcl.ac.uk.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Controlling Computer Network Operations

Andrew Rathmell

Keywords: Dual use information systems; regulation; computer network operations, CNO; malicious computer-mediated activities; interdependencies created by network-based power; private sector - government cooperation; IT-related security regimes.

Abstract: The development of Information Operations and, more particularly, Computer Network Operations (CNO), has been paralleled by calls to control both the military and the criminal/terrorist use of these capabilities. The need for multilateral action to control criminal and terrorist activity is acknowledged and being pursued through mechanisms such as the Council of Europe. Efforts to control military use of CNO through arms control or multilateral behavioral norms are however being undermined by an unresolved dilemma faced by the leading powers; whether to exploit their CNO advantage for strategic purposes or to protect the global information environment on which they depend. In resolving this dilemma, Western strategists need to take into account two important new features of the security environment-interdependency and the role of the private sector.

full text

Author: **Myriam A. Dunn**
Title: **The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method**
Year of issuance: **2001**
Issue: **Information & Security. Volume 7, 2001, pages 145-158**
Hard copy: **ISSN 1311-1493**

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

Myriam A. DUNN

Table Of Contents:

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]

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

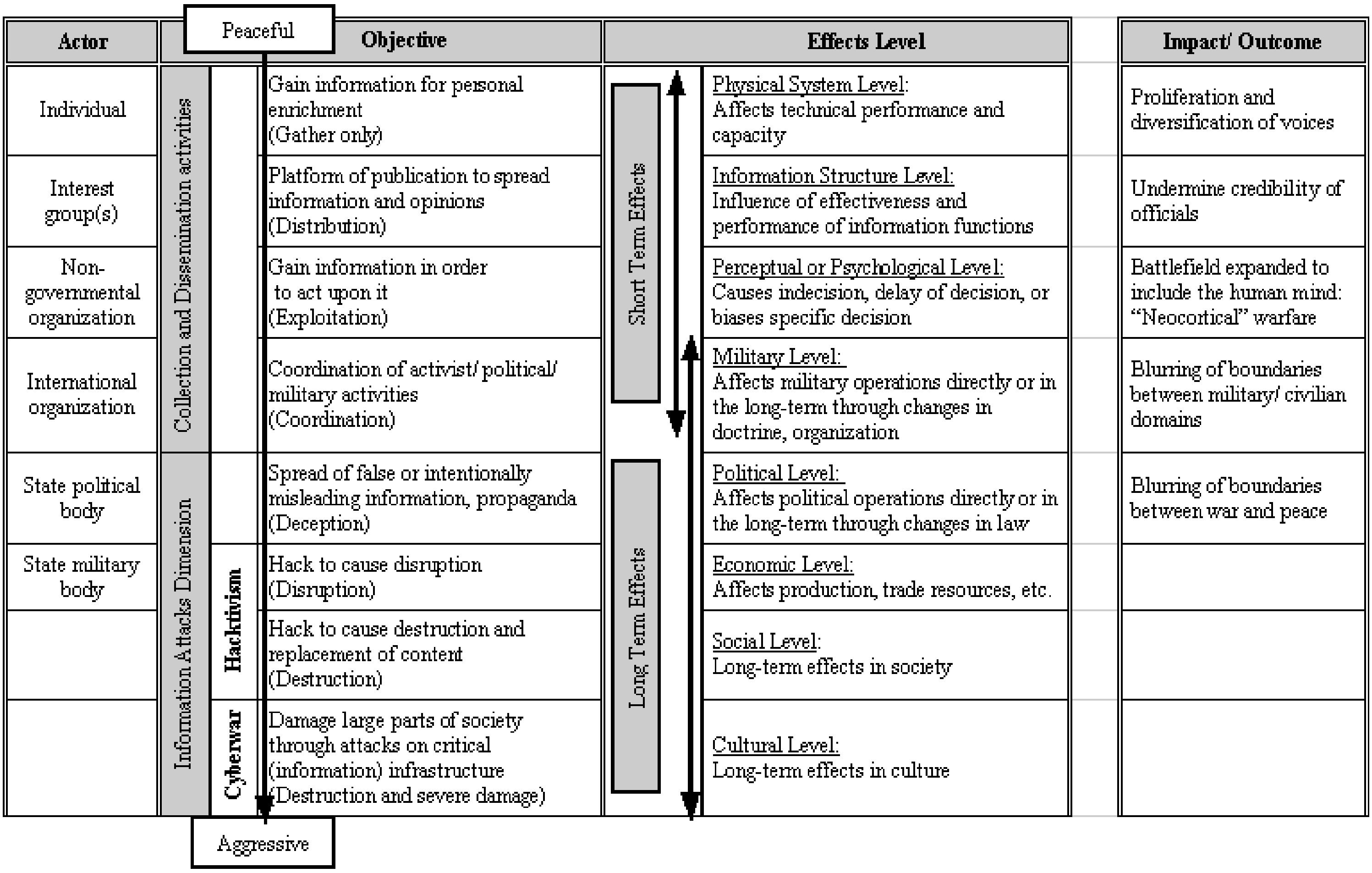
The morphological approach helps to structure and analyze complex interdisciplinary problems that incorporate non-quantifiable components. By categorizing problem fields into significant variables or parameters and ranges of conditions that can be integrated into well-defined relationships or configurations, 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:



Peaceful

Actor			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	

Aggressive

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

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.

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 Stenstr•m 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 L•sung kreativer Probleme* (Z•rich: 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 zeitgem•ssen Planung einer Strategie der staatlichen und gesellschaftlichen Selbstbehauptung,* Z•rcher Beitr•ge zur Sicherheitspolitik und Konfliktforschung, Heft Nr. 8 (Z•rich: Forschungsstelle f•r 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.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method

Myriam A. Dunn

Keywords: Internet in conflict situations; new conflict environment; proliferation of voices; information operations; information warfare; cyberspace, cyber warfare; morphology; human mind as target; neocortical warfare; information attacks; international law.

Abstract: In recent years, newly emerging actors, an ongoing redistribution of power relationships with volatile distribution patterns, and changes in military affairs have created a variety of fascinating multifaceted issues. One emerging topic is the role of Cyberspace in armed conflict, a complex problem that incorporates various non-quantifiable technical, social, and cultural components. The domain of information attacks, in particular, is presently considered a pressing national and international security issue, especially in the absence among many actors of any understanding of the real dangers and risks and steps necessary to overcome them. There is a demand for systematic exploration of the role of the Internet in the future of warfare in order to develop likely scenarios for its use and impacts, to sharpen the understanding of the issue and to facilitate necessary policy decisions. The morphological approach that is proposed in the article can overcome some of the methodological difficulties inherent in multipart problem complexes, as it is used for structuring and investigating the totality of relationships contained in complex interdisciplinary problems.

The paper suggests a morphological box for additional analysis of the topic and subsequently justifies the selection of the four parameters - 1) actors involved; 2) intentions/ objectives; 3) level at which the effort takes effect; 4) impact of the use of the Internet - and the value of each parameter. It seems that the information attack dimension is especially likely to set fundamental precedents for approaches to information operations, the use of the Internet as a tool for warfare, the laws of war, and international law. There appears to be an essential need to protect civilians from too much involvement and from becoming targets of new forms of warfare featuring the targeting of civilian installations or worse, the targeting of the human mind. More systematic analysis is needed to explore the full extent of the problem in a political context and to establish steps towards reaching satisfactory solutions.

full text

Author: **Timothy Thomas**
Title: **The Internet in China: Civilian and Military Uses**
Year of issuance: **2001**
Issue: **Information & Security. Volume 7, 2001, pages 159-173**
Hard copy: **ISSN 1311-1493**

THE INTERNET IN CHINA: CIVILIAN AND MILITARY USES

Timothy THOMAS

Table Of Contents:

Introduction

During the past five years China has developed an impressive telecommunications industry with the potential to become the world's largest communications market. At the end of the year 2000, there were 22 million Internet users, while projections for the year 2005 estimate 130 million users. Optical fiber now joins the capitals of all of China's provinces and its 1.3 billion people together, providing the integrating factor for such growth in users.

Of equal importance is how the Chinese government plans to utilize the Internet for military purposes. According to Chinese information warfare specialist Shen Weiguang, the Internet can be used to implement Chinese strategies to destroy or deface private and official web sites. Shen wrote in his book *The Third World War—Total Information War* that the Shenyang Military region organized

> "… military exercises in IW [Information Warfare] using live soldiers … On the computer, people have come up with 36 ways to disrupt the Internet and 36 ways to defend against such disruption. There are also proposals to create a social order for the future information world."[1]

According to Shen every computer chip is a potential weapon, every computer may become an effective fighting platform, and every citizen may develop a war plan and use the Internet to launch a special war. Internet war is a part of peacetime IW in Shen's view, making the purpose of war "controlling the enemy and preserving oneself" through Internet confrontations and online military exercises. Shen also noted that the Internet is a "New World" with no border and no treaties.[2]

This article addresses three aspects of the civilian and military use of China's Internet. First, it looks at Internet use by China's citizens, and the information technologies that support it. This includes an examination of the role of President Jiang Zemin's son in this process. Second, it examines how the military has implemented the Internet into its operations, both as a mobilizer of People's Liberation Army (PLA) emotions and as a provider of news, and as a new tool for political officers. Finally, the article looks at three recent Internet skirmishes—China versus NATO in April and May of 1999, China versus Taiwan in August and September of 1999, and China versus the United States in April of 2001, the latter the Chinese response to the April 1 collision of a US Navy surveillance and reconnaissance plane and a Chinese fighter.

1. The Internet in China

Over the past few years, use of the Internet has skyrocketed in Mainland China. While a February 2000 *Jane's Intelligence Review* article on China and Taiwan stated that China had 4 million Internet users, a survey for Greater China (China, Hong Kong, and Taiwan) in the fourth quarter of 2000 conducted by the online research company Interactive Audience Measurement Asia (Iamasia) found that there were 15.2 million Internet users in China, 2.2 million in Hong Kong, and 6.4 million in Taiwan. In the classroom, "Iamasia" noted Taiwan has 40% of its students using school facilities to go online, while only 21% do so in Hong Kong and only 8% in China.[3]

The web site Muzi.com noted in early 2001 that according to the China Internet Network Information Center (CNNIC) Internet users reached 22.5 million at the end of 2000, up from 8.9 million at the end of 1999 (when the *Jane's* article mentioned above was probably written).[4] The Internet service ChinaOnline considers these numbers dubious since CNNIC counts all regular users, not just online consumers. CNNIC is a semiofficial nonprofit organization that is run by the Chinese Academy of Sciences and handles Internet issues within the purview of the Ministry of Information Industry (MII). The Center manages and oversees English and Chinese character domain names ending in ".cn". It also maintains a database of Internet protocol addresses, provides information on Internet-related policies, and conducts surveys on Internet development, among other jobs. The center estimates that there are now 122,099 domain names registered under ".cn" and 265,405 websites in China.

According to one survey, Sina.com was listed by 68.1 % of netizens (a Web surfer who spends no less than two hours online during a session and surfs no less than twice a week) as the most influential Web site in China, followed by Sohu.com with 53.3 %, Net Ease with 40.7 %, and Chinese Yahoo! with 16 %.[5] However, when using e-mail, most users preferred Sina followed by NetEase. When searching, 60.3 % like Sohu and 54.7 % preferred Sina.[6]

Finally, the journal *Red Herring,* in its special Asia issue of October 2000, was even more optimistic. It listed Internet use in China, by the year 2005, as nearing 9.2 % of the population. This would put the Internet use figure somewhere around 125 million people.[7] Even if these figures are off by millions of people, the underlying idea is clear—the utilization of the net is widening quickly. For example, the US Embassy in China, on a web site article on "The Growing Influence of the Internet in China," noted that the Feiyu Net Cafe (www.feiyu.com.cn) near Beijing University has one thousand computers.

Even the government has pushed to go "on-line." As Nina Hachigian noted in *Foreign Affairs*, the "Government On-Line Initiative," launched in 1998, aimed to ensure that 80 % of all government agencies—local and national—had Web sites by the end of 2000. State-owned China Telecom lowered its access charges and is adding two million new lines each month to meet demand for network access. Other state-owned telecommunication providers are encouraged to build their own networks.[8]

Beijing-based telecoms consultancy BDA stated that 69 million people in China would access the Internet over their phones by the end of 2000, and there will be 236 million wireless subscribers and 120 million Internet users by 2004. China Mobile, China's largest mobile phone operator, said it would charge fees for wireless application protocol (WAP) services.[9] In March of 2000 it was announced that China would link four backbone Internet networks. These four are CSTNET (China Science and Technology Network), ChinaNET, CERNET (China Education and Research Network), and ChinaGBN (China Golden Bridge Network). Circuit capacity was not listed, however.

ChinaNET is a public network that connected to the Internet in early 1995. It now covers all of China's provinces and autonomous regions, and all municipalities under the central government. It has monopolized the market. CSTNET is a national Internet network constructed by Tsinghua University and Peking University. It launched its Internet access service in 1994. It networked 100 institutes by 1995, and by 1998 had connected more than 100 Ethernets, 3,000 computers and 10,000 users. CERNET began in 1994 and it has also linked more than 100 institutes. ChinaGBN is a state public economic information network under the control of the former Ministry of Electronics Industry. It is still weak and competes only against ChinaNET in limited areas. The networks currently can access one another only at very slow speeds. Access to ChinaNET from CERNET is possible only through an 8 Mb/s bandwidth. The integration of the nets will increase speed to 155 Mb/s it is believed.[10]

Use of the Internet has also spawned a growth industry of Internet police. The authorized size of this unit is more than 300,000 personnel. The police are designed to fight the flow of "harmful information" nationwide, to fight viruses and Internet crime. Organized into public information network supervision departments, the goal is to manage the Internet in accordance with the law, strengthen supervision, focus on prevention, ensure the stability of key points, and promote development while guaranteeing safety. College students have been recruited to help where possible.[11] Police control of the Internet, or at a minimum its monitoring, appears to be vital for future success in the opinion of most Chinese leaders. On 19 June 2001, newspapers carried an account of a Chinese businessman who was sentenced to three years in prison for posting articles critical of Chinese leaders and the ruling Communist Party on the Internet. He was charged with incitement of subversion, according to a report from the *Xinjiang Daily*.[12] Earlier, on 7 January 2001, another control mechanism was under consideration. Several unidentified companies agreed to form the China

C-Net Strategic Alliance, a second-generation Internet-like network for China's government and industry. No start dates for construction or completion were offered. The *Xinhua News Agency* release noted that "the current one [Internet] has too many faults and is incapable of satisfying the needs of the Chinese government and companies as they enter the digital age." It is unknown whether foreigners will have access to the net, or if it will be compatible with the existing net.[13]

In October and November of 2000, the Chinese government established laws governing ownership, content, and other aspects of Internet use. The October set of laws limits direct foreign investment in Chinese Internet companies, requires companies to register with the Ministry of Information Industry and apply for permission before issuing stock or signing any agreement with a foreign investor, and bans the dissemination of any information that might harm unification of the country, subvert the government, or endanger national security. All Internet service providers (ISPs) must monitor content and restrict controversial topics in their chat rooms. Thus, the providers turn into *de facto* spies for the government.[14] In November, regulations emphasized that special licenses must be obtained by sites desiring to publish news. These sites may not generate their own news content, and can publish only stories from official sources.[15]

Shanthi Kalathil has provided the most interesting report on state controls over the Internet in China. Controls are necessary since China's educated professionals now have access to the Internet and are becoming more and more aware of the disparities between China and the rest of the world. Private sector development can also challenge state control in the economy and political spheres. Finally, the Internet offers dissidents and activists an unexpected outlet for their platforms. Kalathil listed both reactive and proactive responses. For reactive measures, she cited the desire of Chinese authorities to filter material and promote self-censorship. The latter includes "encouraging" Internet caf• owners to keep a close eye on web surfers. For proactive measures, she noted that the government is becoming "informationized" since an e-government plan was devised. Further the government has learned how to distribute on-line propaganda and encourage what Kalathil calls "thought work." China is also considering the creation of a Chinese Intranet, is developing an information warfare strategy, and is using web access as a means of gaining popular support and legitimacy from the population.[16]

2. China's Information Technology Sector

The Ministry of Information Industry (MII) formulates national strategies and policy and plans for China. It also oversees special military networks and supervises telecom and information service markets. A military electronics industry bureau is part of the Ministry's internal setup. MII was created in 1998 by combining the Ministry of Post and Telecommunications and the Ministry of Electronics and Information. As a super-agency, it oversees telecommunications, multimedia, broadcasting, satellites, and the Internet.

A survey of China's information technology industry was completed in June 2000. It was divided into four parts: (1) telecom products and services, which were subdivided into four parts in 1999, China Telecom, China Mobile, China Satellite, and China Unicom; (2) computer products and services; (3) information appliances; and (4) audio-video entertainment. This and similar surveys will serve as the "investment guide" for the industry according to the report. Simultaneously,[17] China has increased its share of the domestic market for geographical and mapping software. Five years ago, domestic software companies held almost no portion of the Chinese market for these products, but today that share has increased to 28.9 %.[18] In February of 2001, Culturecom Group announced it would develop alternate versions of Chinese 2000 (Linux) to meet the needs of specific linguistic and cultural groups among the Chinese-speaking population.[19] Beijing has reported that the municipal government has approved 221 new software companies in 2000, positioning it to soon become China's largest software production center.[20]

China's State Council has invited investment in the software and integrated circuit industries. The 10th Five-Year Plan (2001-2005) plans on earmarking funds for the software and integrated circuit industries, as well as tax breaks for software enterprises. The integrated circuit industry will also receive preferential treatment, although not to the extent that the software industry will enjoy.[21] The 10th Five-Year Plan also envisages the infusion of $ 500 billion into the information technology sector. Development strategy is focused on e-commerce, broadband infrastructure construction and information development. Liu He, vice director of the State Information Center, added that relevant laws and regulations should be improved, as well as the transparency of market rules. Protection of intellectual property and increased investment in human resources should be expanded too.[22] The information technology industry surpassed the power industry for the first time and is now the most profitable industry in China; and China's Minister of Information Industry Wu Jichuan predicted that China's information sector would grow by 20 % in the next five years.[23] The world's largest information technology center recently opened in Guangdong province on 19 December 2000 in Dongguan. The new center is both traditional and virtual, with clients able to view products, place orders and make payments online.[24]

One of the people most responsible for breaking up telecom monopolies, opening the Internet to China's massive middle class, and steering hundreds of millions of dollars of state money to venture investments is a rather unlikely source. He is Jiang Mianheng, son of President Jiang Zemin, and he is helping to modernize China from behind the scenes, outlining strategy and securing funding. His flagship company is China Netcom, which is building a 5,300 mile fiber-optic network linking 50 million people in 17 of China's most prosperous cities. China Netcom was originally created to build a broadband IP network. Rupert Murdoch and Michael Dell have invested $ 325 million in China Netcom. Jiang got his doctorate in high-temperature superconductivity from Drexel University in Philadelphia in 1991, and then worked for Hewlett-Packard for 18 months.[25]

Jiang hopes to set up a communications network to turn China into one of the countries with the highest density of Internet users in the world. In November of 2000, Jiang broke ground with Winston Wang, son of Taiwan private industrial chairman Wang Yung-ching, after coming to an agreement on a $ 1.63 billion computer-chip plant. There has never before been an economic bond of this magnitude that could eventually become the bridge for a political settlement between Beijing and Taipei. China already has six semiconductor foundries that make circuit-etched silicon wafers. NEC of Japan built one plant in Shanghai two years ago, and Motorola is building a plant in Tianjin. The Jiang-Wang plant is the first of four that the two plan to build on a 60-acre plot Shanghai.[26]

3. The Military and the Internet

The growth of the Internet in China also included the military sector. Reports out of China indicated in August 2000 that there were more than 400 military websites. Some support the PLA directly, such as the PLA internal information network. This "Intranet" has found a place in the political room of many units. Now, instead of reading Marxist-Leninist tracts soldiers can look up foreign military equipment on the web and read other interesting military-related information. Former PLA officers are establishing some sites[27] and the PLA reserve forces have web sites too (i.e., http://ezarmy.net, the web site of the Echeng Reserve IW unit). *Jiefengjun Bao* established an Internet version of the PLA General Political Department's newspaper (www.pladaily.com) on 1 October 1999. The site discussed topics as varied as the 50th anniversary of National Day, the return of Macao, China's successful launch of the Shenzshou spacecraft, sessions of the National People's Congress, the development of the Western region of China, the study of the "three represents," the Taiwan issue, and criticism of the Falungong. This made one PLA officer stationed abroad proclaim, "we are very close to Beijing all of a sudden."[28] The paper also maintains links with journals such as the *Chinese National Defense Journal*, *Militia of China*, *Journalism* and *Self-Cultivation*, and *PLA Pictorial*.[29] WebPages on the Internet Version include Military Observation, Military Science and Technology, Joint Logistics for the Three Armed Services, Political Work, Weaponry, Windows on Foreign Armies, Military Pictures, Chinese Military Academies, Armed Police of China, Militia of China, Military Projects for National Defense, Military Circles History, Noted Military Surgeons, and Military Bookstore, among others.

For a period of time the number one site was Knowledge about Vessels (KAV) but the site soon merged with China's number one civilian site, Sina.com. After the KAV-Sina union, Chinese Youth Online began a military site named Chinese Youth Beacon on 1 August 2000. KAV has six "mottled bamboos" in its military forum. They are designed to check up on web users to ensure that secrets are not being passed around without notice. Another very popular web site is PLA pictures (www.plapic.com.cn), which has a huge variety of photos of military exercises, current events involving the PLA and President Jiang, photos of Chinese landscapes, and sixteen Internet connections. Some of the sixteen sites include:

- www.pladaily.com
- www.peopledaily.com
- www.sina.com.cn
- www.china.net
- www.xinhua.org
- www.globalizationforum.org
- www.top81.com.cn, and
- www.999junshi.com.

The site is updated with new pictures and with new current events on a frequent basis.

The military has become a popular topic lately, especially in light of Chinese reactions to the continuing tension with Taiwan, the war in Kosovo, and the recent incident involving the US reconnaissance and surveillance aircraft. Some non-military web sites have added military pages, such as Xinhua Net's Junshi Tiandi (Military Sphere), Zhongxin Net's Junshi Tiandi (Military Sphere), Zhong Qing Zaixian's Zhong Qing Genghuo (China Youth Beacon, at www.cyol.net), and the military section of Xinlang Net (New Wave Net).[30]

There are several additional reasons for this popularity. First, the military sphere is changing quickly. There are new local wars and conflicts, and new generations of weapons. Due to the net, military news is not as opaque or semi-transparent as it once was. Second, the people are simply more interested in military affairs now that China has stepped into the center of world attention. On occasion it has happened that the more military information a site publishes the more hits it receives. Third, many military enthusiasts in China have never had an opportunity to publish about military affairs before the advent of the net. This offers many such individuals a chance to air their own point of view. Finally, several military news media and scientific research and teaching units are using the net. This includes *Jiefengjun Bao* (Liberation Army Daily), and the *Jiefang Huabao* (PLA Pictorial) of the Academy of Military Sciences.[31]

Fan Tao of the Military Law Department of the Xi'an Academy of Political Science believes that people's increased concern over national defense, and the diversification that the web offers to military education are other reasons for the web's popularity. Increased interaction among young web participants, that free one from time and space restrictions, increase its influence as well. However, not all web sites are as responsible and regulated as they should be. Some publish false information and irresponsible political views. Author Wei Daqing, writing in the newspaper *Zhongguo Guofang Bao* (sponsored by the PLA Daily three times a week), recommended increased control by network monitoring and management departments, and information security departments.[32] On 10 February 2001 *Jiefangjun Bao* noted that the Central Military Commission went a step further. It issued Provisions to the four general departments of the PLA on the Security and Confidentiality of Computer and Information Systems. The Provisions were designed to boost Internet security as well as military computer security.[33] On 2 May this warning was repeated in *Jiefangjun Bao*. Reporter Li Min stated that comrades of "network management" departments must conduct thorough investigations, issue warnings in a timely manner and expel from the Internet those who refuse to correct mistakes after repeated disciplinary action.[34]

Finally, the Internet has provided the means for PLA war games on occasion. For example, in July of 2000, the Chengdu Military Region conducted a confrontational campaign exercise on the Internet. The three training tasks associated with the exercise included organizing and planning the campaign, striving for air and information control, and making and countering breakthroughs. Over 100 terminals were linked for the exercise.[35]

4. Two 1999 Internet Wars: China vs. NATO and China vs. Taiwan

In May 1999 a US guided missile slammed into the side of the Chinese Embassy in downtown Belgrade, Yugoslavia. The Chinese Liberation Army Daily (LAD) disclosed on 27 July 1999 that a "network battle" was fought between Chinese and US hackers following the 8 May bombing of the

Chinese embassy. US hackers, according to the report, aimed their counterattack at the following web sites: Xin Lang Wang or Sina (http://home.sina.com.cn), Zhongwen Re Xun or Yesite (http://www.yesite.com), and Shanghai Wang Sheng or Shanghai Web Boom (no URL listed). The Chinese initiated the US hack by altering the home page of the US Embassy in Beijing, writing on it "down with the Barbarians."[36] The Chinese also report causing a blackout at a few US political and military web sites, and some 300 civilian web sites. In all Chinese hackers broke into nearly 1,000 US civilian web sites and coordinated an attack on NATO computers.[37]

The methodology for performing these hacks, according to the LAD article, was the mobilization of thousands of net users to issue a ping command to certain web sites at the same time. This caused servers to be overloaded, and paralyzed these websites. In addition, thousands and thousands of e-mails were sent daily to the opposite side, thus blocking mail servers. Viruses were sent via e-mail, and attacks were launched with "hacker tools" hidden in certain programs. The LAD article called for developing a computer network warfare capability, training a large number of network fighters in PLA academies, strengthening network defenses in China, and absorbing a number of civilian computer masters to take part in actions of a future network war.[38]

There was also an Internet war with Taiwan. In June Of 1999, Taiwanese President Lee Teng-hui stated that PRC and ROC ties should be based on special state-to-state relations. This infuriated the PRC, with Beijing calling Lee a "demented test-tube baby." Nearly two months later, on 8 August, a cyber war started between the two. Taiwan blamed China for starting it, and China blamed Taiwan. Taiwan's hackers reportedly attacked the PRC's State Tax Authority website and the Ministry of Railways site. One hacker threat was that on 1 October, China's National Day, all Chinese web sites with simplified Chinese characters would be hit with viruses. Chinese hackers, for their part, broke into Taiwan's Inspector General web site, and the web sites of the Investigation Bureau of Taiwan's Justice Ministry, the Ministry of Economic Affairs, the National Assembly, and the American Institute in Taipei, the unofficial embassy of the US in Taiwan.[39] The MSNBC website estimated that, in all, Chinese compatriots launched more than 100,000 attacks on Taiwan government sites.

5. The Internet War with the US over the EP-3 Reconnaissance and Surveillance Aircraft

On 1 April 2001, a US EP-3 reconnaissance and surveillance plane approached China's Hainan Province via the South China Sea. Two Chinese F-8 jet fighters scrambled to meet it. Unfortunately, one of the planes, piloted by Wang Wei, collided with the US plane. The latter and its crew, due to damage done to the plane, was forced to land on Chinese territory at Lingshui Airport in Hainan. Initially, discussion about the incident was centered in chat rooms in China and the US. In China, citizens expressed their indignation and offered potential solutions to this situation in chat rooms throughout the country. Sina.com, Sohu.com and Chinadotcom Internet chat rooms were the most popular web sites in China. Chinadotcom conducted a survey to find out the feelings of citizens. Some 60,962 citizens reportedly participated. The survey indicated that 18 % felt China should remain unyielding, 15 % took the action as an act of war, 22 % said keep the plane for examination, 25 % said free the plane, and only 3 % recommended getting to the bottom of the incident with an investigation.[40] Some of the comments reported in the chat rooms included:

- "This is the third time the American imperialists have dumped crap down China's neck."

- “We can forego joining the WTO but we cannot afford to loose face.”
- “We should calm down and find out the truth.”[41]
- “Why can’t the US show any human rights concern to the poor missing pilot?”
- “The whole nation is waiting to see if China can play hardball with the US.”[42]

Two hacker groups took center stage in the US, Pr0phet and Poizonb0x. On 11 April, the first Pr0phet political reference was made, and on 14 April the first Poizonb0x defacement of a Chinese site occurred. One attack site read “bagel-morning coffee-and a Chinese website. Nice little routine.” Concern was great, and the National Infrastructure Protection Commission’s Watch and Warning Unit gave out its phone number (202-323-3204/05/06) and a web site (NIPC.Watch@fbi.gov). Hotlines were established at http://www.fbi.gov/contact/fo/fo.htm and http://www.NIPC.gov/incident/cirr.htm . A list of many of the hacks is available at http://attrition.org/mirror/attrition.[43]

In China, there were three groups responsible for most of the defaced web sites. They included Honker Union of China, Hacker Union of China, and China Eagle Union, a civilian nonprofit organization of part-time network enthusiasts. Provincial groups organized some Chinese attacks. They included the provinces of Fujian, Hubei, and Guangdong among others. Perhaps these groups included the PLA reserve groups of IW battalions, but this was never made clear. The Chinese used several hacker tools such as killUS and DNSKiller. The State Computer and Network Emergency Handling and Coordination Center, China Computer Network Emergency Center (www.cert.org.cn) handled the Chinese web problems.[44]

Soon, Netor.com, a leading host of mourning sites in China, established an online shrine to Wang Wei. Here citizens could light a virtual candle, leave digital flowers, dedicate digital melodies ranging from traditional Chinese music to the theme songs from Titanic or Ghost, or offer written expressions of their grief online. “We salute the hero in the sky,” wrote one, while another citizen said, “You have fallen but millions like you live on to fight for the motherland.” In just three days Wang’s site received the third most visits of any of the nearly 5,000 hosted by Netor.com.[45]

Slowly, the defacing increased and a hacker war was declared for the dates of 30 April to 8 May. Pamela Hess reported on 30 April in Infospace.com that spokesman Lt. Cdr Reif stated that the Navy was at INFOCONALPHA, a cyber version of the physical threat condition. The Navy’s Fleet Information Warfare Center announced its status on 26 April, and the JTF CND on 30 April. So both governments were taking this small cyberwar between individuals very seriously.

Individuals from many nations participated, with Saudi Arabia, Pakistan, India, Brazil, Argentina, and Malaysia on the US side and Korea, Indonesia, and Japanese hackers supporting China. Some, such as Brazil, supported both. It was clear that a cyber mob mentality had developed. Chinese hacker Jia En Zhu, who lives in a Beijing suburb, wrote, “Many people here are frustrated with America.” China’s attack was planned for 1-7 May, peaking on 4 May, a Chinese holiday commemorating the country’s first major student demonstration that took place, ironically, in Tiananmen Square 82 years ago.[46]

A Chinese National Defense University Professor dubbed this cyber war “extremely important” on 11 May. Professor Zhang Zhaozhong, a renowned military expert and director of the Military and Equipment Teaching and Research Center, stated that the cyberwar

> “… presented a modern format of warfare, alive and kicking, before the eyes of the netizens, and invented many a combat method through practice, amassed abundant experience, expanded the contingent of hackers, tempered their mettle for cyberspace fighting, and made an impressive show of the wisdom and abilities of the Chinese netizens to the netizens around the world. … This cyberwar was by nature a counteroffensive for self-defense and was an act of defensive counterattack compelled by the strong offensive from hackers of the opposite side.”[47]

6. Conclusions

This overview of the civilian and military aspects of the Internet in China reveals several interesting issues. First, of course, is the rapid growth of Internet users in both sectors. If *Red Herring* is correct, the figure of 130 million Internet users by the year 2005 is simply astounding for a nation often accused of being too backward to present any type of threat in the immediate future. China also appears capable, with the work of Jiang Zemin’s son and others, of putting together a formidable computer industry that will be home grown. The sheer number of Chinese software writers and mathematicians should ensure a healthy future for the Chinese computer industry.

Second, the idea of 130 million potential Internet users coupled with the idea that the Internet might be used by the military, as Shen suggests, as a means to implement 36 ways to disrupt the Internet is worthy of much closer inspection. Perhaps the reserve IW forces of the PLA that are currently used by the military as an opposing force in military exercises will bear the brunt of the mission to perform the disruptions. It is doubtful if foreign military observers will be able to distinguish between civilian hackers and reserve force hackers in a future Internet confrontation. It should be remembered that the IW reserve force in Xian has already become somewhat infamous for its development of 10 methods to attack computers. These ten methods are: planting information mines; conducting information reconnaissance; changing network data; releasing information bombs; dumping information garbage; disseminating propaganda; applying information deception; releasing clone information; organizing information defense; and establishing network spy stations.[48]

Third, the military has found several uses for the Internet other than providing an OPFOR mechanism for reserve forces. The Intranet in political rooms offers young soldiers a chance to use computers, and to actually access PLA databases of foreign military equipment. In one instance, the Internet served as the mechanism for an entire IW exercise in the Chengdu military region. Important academies and institutes in China maintain several other military sites.

Finally, the Internet battles that have erupted between China and NATO, Taiwan, and the US are worthy of our immediate concern. They demonstrated the ability of citizens (or military members cloaked under the guise of civilians) to conduct cyber attacks on one another’s systems, and to increase tensions between two sides. This is a dangerous precedent in a world sadly lacking in regulation in this area, if indeed regulation is even possible. The involvement of the FBI and the raising of the threat status among US Navy personnel to INFOCONALPHA, a cyber version of the physical threat condition, are indicative of the growing seriousness of this issue.

What does the future hold? Clearly it appears that the future will offer even more problematic scenarios for military forces around the world. The inability to determine who initiated an Internet attack and what is the intent of the electrons involved in the attack will continue to haunt intelligence and operational staffs in the coming months and years. The Internet may indeed play a bigger role in our military future than any of us originally believed.

DISCLAIMER: The views expressed in this report are those of the author and do not necessarily represent the official policy or position of the Department of the Army, Department of Defense, or the US government. The Foreign Military Studies Office (FMSO) assesses regional military and security issues through open source media and direct engagement with foreign military and security specialists to advise army leadership on issues of policy and planning critical to the US Army and the wider military community.

Notes:

1. Shen Weiguang, *The Third World War—Total Information War* (Xinhua Publishing House, January 2000), as translated and downloaded from the FBIS web site on May 17, 2000, http://199.221.15.211/.
2. Ibid.
3. "Greater China online population hits 24 million," *Taipai DPA* (January 23, 2001).
4. "China Internet Users grow to 22.5 million," *Muzi.com Website* (January 17, 2001), http://www.muzi.com/.
5. "Portal Personification: Survey Tracks Netizens' Use, Opinion of Net," *Inside China Today* (May 3, 2001), http://www.europeaninternet.com/china/.
6. Ibid.
7. "Asia at a Glance," *Red Herring* (October 2000), 115. Available @ http://www.redherring.com/.
8. Nina Hachigian, "China's Cyber-Strategy," *Foreign Affairs* (March/April 2001), 119, 120.
9. "69 million mobile Internet users in China by 2000," *Muzi.com Website* (November 16, 2000).
10. "China to Link Four Backbone Internet Networks," *ChinaOnline Website* (March 23, 2000). Available @ http://www.chinaonline.com/.
11. "Internet police ranks swell to 300,000," *'Ming Pao' web site* (Hong Kong, December 8, 2000), www.mingpao.com/newspaper/.
12. China Sentences Critic," *The Kansas City Star* (June 19, 2001), A8.
13. Beijing, *The Associated Press* (January 8, 2001).
14. "Cracks in the Great Firewall," *World Press Review* (May 2001), 11, 12.
15. Hachigian, "China's Cyber-Strategy," 124.
16. Shanthi Kalathil and Taylor C. Boas, "The Internet and State Control in Authoritarian Regimes: China, Cuba, and the Counterrevolution," *Carnegie Endowment Working Papers*, Global Policy Program, Number 21 (July 2001), 6-10.
17. "China completes nationwide IT survey," *ChinaOnline Website* (June 5, 2000).

18. “China puts itself on the software map,” *ChinaOnline Website* (August 16, 2000).

19. “Survival of the Linux: Software adapted to meet different cultural needs,” *ChinaOnline Website* (February 28, 2001).

20. “Bejing moves to upgrade software industry,” *ChinaOnline Website* (March 20, 2001).

21. “State Council encourages development of software, integrated circuit industries,” *ChinaOnline Website* (July 14, 2000).

22. “U.S. $500 billion slated for IT sector by ’05,” *ChinaOnline Website* (April 23, 2001).

23. “China Targets 20% Annual Growth for Information sector in Five Years,” *Chinatopnews.com* (May 8, 2001), http://www.chinatopnews.com/.

24. “World’s largest IT center opens in Guangdong,” *ChinaOnline Website* (December 27, 2000).

25. Joanne Lee-Young, “The Digital Prince of China,” *The Industry Standard* (2000).

26. Craig Smith, “A Chip Plant That is Full of Symbolism,” *The New York Times* (November 24, 2000), from the New York Times web site on 24 November 2000.

27. Wei Daqing, “On the Sudden Emergence of Military Websites,” *Zhongguo Guofang Bao* (November 6, 2000), 4, as translated and downloaded from the FBIS web page on 14 December 2000.

28. Li Guohua, “Open Up New Field for Dissemination of Military News,” *Jiefangjun Bao* (October 4, 2000), 2, as translated and downloaded from the FBIS web page on 4 October 2000.

29. Ibid.

30. Ibid.

31. Ibid.

32. Wei Daqing, “On the Positive and Negative Aspects of Military Websites,” *Zhongguo Guofang Bao* (November 6, 2000), 4, as translated and downloaded from the FBIS web site on 14 December 2000.

33. “Managing Internet According to Law is a Must,” *Jiefangjun Bao* (February 10, 2001), 1, as translated and downloaded from the FBIS web site on 12 February 2001.

34. Li Min, “Network Mangers should Exercise Strict Management,” *Jiefangjun Bao* (May 2, 2001), 1, as translated and downloaded from the FBIS web site on 2 May 2001.

35. Xu Wenliang and Wan Yuan, “Chengdu Military Region Conducts Long-Range Confrontational Exercises on Internet,” *Beijing Jiefangjun Bao*, Internet version (July 10, 2000), as translated and downloaded from the FBIS web site on 10 July 2000.

36. “Military Forum” page, *The Liberation Army Daily* (27 July 1999), report obtained via e-mail from Mr. William Belk (June 1, 2000).

37. “Collision could Launch Wave of Hackers,” *thedailycamera.com* (April 4, 2001).

38. William Belk’s e-mail (June 1, 2000).

39. Damon Bristow, “Cyber-warfare rages across Taiwan Strait,” *Jane’s Intelligence Review* (February 2000), 40.

40. Rachel Morarjee, “AFP: PRC Web surfers call for PRC to ‘Play Hardball’ with U.S. on Air Collision” (Hong Kong, April 4, 2001), as translated and downloaded from the FBIS web site on 4 April 2001.

41. “AFP: Chinese Websites Protest U.S. Plane Incursion” (Hong Kong, 2 April 2001), as translated and downloaded from the FBIS web site on 2 April 2001.

42. Rachel Morarjee, “AFP: PRC Web surfers call for PRC to ‘Play Hardball’ with U.S. on Air Collision.”

43. Carl O. Schuster and Anthony Miccarelli, “Special Press Summary: China’s May Day Cyber War,” a product of the Virtual Information Center (no date).

44. Ibid.

45. Clay Chandler, “For Chinese Pilot, Martyrdom on Earth and in Cyberspace,” *The Washington Post* (18 April 2001).

46. Michelle Delio, “Technology: U.S., Chinese hackers vow to wage online war,” *Agence France-Presse* (April 21, 2001).

47. Interview with Zhang Zhaozhong, “Military Expert Comments on ‘May Day’ Cyber War between China and the United States,” *Guangzhou Ribao* (May 11, 2001), as translated and downloaded from the FBIS web site on 12 May 2001.

48. *Qianjin Bao* (December 10, 1999), provided by Mr. Belk via e-mail.

TIMOTHY L. THOMAS is an analyst at the Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas. He retired from the US Army as a Lieutenant Colonel in the summer of 1993. Mr. Thomas received a B.S. from West Point and an M.A. from the University of Southern California. He was a US Army Foreign Area Officer who specialized in Soviet/Russian studies. His military assignments included serving as the Director of Soviet Studies at the United States Army Russian Institute (USARI) in Garmisch, Germany; as an inspector of Soviet tactical operations under CSCE; and as a Brigade S-2 and company commander in the 82nd Abn Division. Mr. Thomas has done extensive research and publishing in the areas of peacekeeping, information war, and political-military affairs. He is the assistant editor of the journal *European Security*; an adjunct professor at the US Army’s Eurasian Institute; an adjunct lecturer at the USAF Special Operations School; and a member of two Russian organizations: the Academy of International Information and the Academy of Natural Sciences. You may forward comments referencing this study to: FMSO, ATZL-CTL, Mr. Thomas. 101 Meade Avenue, Ft Leavenworth Kansas 66027-2322. *E-mail*: ThomasT@Leavenworth.army.mil.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method

Timothy Thomas

Keywords: Internet in China; growth in Internet use by civilians; integration of the Internet into military operations, Internet skirmishes.

Abstract: China is promoting widespread use of the Internet. Not only are there more users, there are also more companies and conglomerates (some government sponsored) establishing a Chinese Internet backbone for the nation. The Ministry of Information Industries makes strategies, policy, and plans for China. However, even though embracing economic reforms, China continues to try to limit the challenges presented by the Internet through some creative controls. The military uses the Internet to conduct exercises and as a training device. There are reportedly over 400 military web sites. To date, Chinese citizens have been involved in three Internet "wars," two with the U.S. and one with Taiwan. China's expanding Internet use should be closely monitored by other nations in the coming years.

full text

Author: **Information & Security**
Title: **Center for Security Studies and Conflict Research**
Year of issuance: **2001**
Issue: **Information & Security. Volume 7, 2001, pages 177-186**
Hard copy: **ISSN 1311-1493**

CENTER FOR SECURITY STUDIES AND CONFLICT RESEARCH

Table Of Contents:

Address: Center for Security Studies and Conflict Research
Seilergraben 45-49
ETH-Zentrum/ SEI
CH - 8092 Z•rich
Switzerland
Director: Prof. Dr. Kurt R. Spillmann
Deputy Director: Prof. Dr. Andreas Wenger
Phone: (+41 1) 632 40 25
Fax: (+41 1) 632 19 41
E-mail: postmaster@sipo.gess.ethz.ch
Web address: http://www.fsk.ethz.ch

The Center for Security Studies and Conflict Research specializes in the field of national and international security studies and conflict analysis. Activities include research, teaching, and information services. The center has developed and maintains two major electronic information services - the International Relations and Security Network (ISN) and the Information Management System for Mine Action (IMSMA).

The center is the only one of its kind in German-speaking Switzerland and plays an important role as a complement to similar academic institutions in French-speaking Switzerland. It is part of an international network of scientific institutions and organizations and cooperates with numerous partners. The center's expertise has made it an important resource for public administrators and the media, and the center functions as a political consultant to the Swiss Federal Government.

The Organization

The center, which is located at the Swiss Federal Institute of Technology (ETH) in Zurich, was founded in 1986 by its current director, Professor Kurt R. Spillmann. Since 1997, Professor Spillmann has shared the responsibility of directing the center with Professor Andreas Wenger, deputy director. Due to steady growth in research activities and an increasing number of tasks and functions it undertakes, the center now has a staff of about 70 persons working in research, teaching, administration, the electronic information services, the reference library, and documentation. The library can be accessed by the public and contains 14 000 books, 120 current periodicals and newspapers, and a document collection. The library is an important source of information in the fields of international relations, security policy, and conflict research.

In 1997 the Center for Security Studies and Conflict Research joined together with the chairs of international relations at the Swiss Federal Institute of Technology and the University of Zurich to form the Center for International Studies Zurich (CIS) (http://www.cis.ethz.ch). The CIS specializes in the fields of international relations, security studies, and conflict research.

Research

Research work at the center follows a broad, interdisciplinary approach appropriate to the real-world analysis of security policy and conflict management. Research is based upon an expanded conception of security that transcends traditional military conceptions to encompass political, economic, social, cultural, regional, and ecological aspects. Research is conducted by project teams, and members of the center pursuing individual projects. The projects are carried out in cooperation with international and national partners. The main foci of research are:

- Swiss security policy: Conceptual and practical issues of Swiss foreign and security policy;
- International security policy: Global security issues; security-related aspects of the foreign policy of nations; transatlantic relations and the architecture of European security;
- Conflict research: Basic research on the rise of violence and armed conflicts; the dynamics of conflicts; the theory and practice of constructive conflict resolution.

Major Projects

Parallel History Project on NATO and the Warsaw Pact (PHP)

In response to the declassification of NATO documents and the steadily growing availability of documents from the archives in Eastern and Central Europe, the Parallel History Project seeks to collect, analyze, and interpret these premier resources for the study of contemporary international history. As a cooperative undertaking of institutions and individuals dedicated to independent scholarly inquiry, the PHP brings together archivists, historians, and government officials. They locate, declassify, copy, translate, evaluate, and prepare for publication with commentaries documents from archives in Europe and North America.

The growing international network of PHP partners and associates benefits both the specialist academic community by providing new scholarly perspectives on the Cold War period and the wider public by multiplying the results of research in a readily accessible form. The findings are presented at conferences and published in print and multimedia volumes, as well as on the PHP's website http://www.isn.ethz.ch/php). Since its establishment in 1999, the project has collected thousands of pages of relevant material on the military aspects of the Cold War and published several online collections with revealing documents highlighting mutual threat perceptions and the "parallel" history of the Cold War alliances.

- URL: http://www.isn.ethz.ch/php
- Contact: php@sipo.gess.ethz.ch

Regionalization of Russian Foreign and Security Policy

The objective of this international research project is to analyze regional dimensions of Russian foreign and security policy, an aspect of center-periphery relationship that has not yet been researched systematically. The aim of the project is to determine whether and how the central state understands the specific interests of Russian regions and to what extent regional processes have an impact on Russia's external relations and on integration processes within the CIS space and beyond.

A main task of this project consists in establishing profiles of selected Russian regions in order to examine their international security environment and relationship to the Moscow center. In order to present a true picture of Russia's uneven regional landscape, the regions have been carefully selected according to various criteria. Border regions and central regions, ethnic republics and oblasts and krais, poor agrarian regions and rich oil- and gas-producing regions are among the regions selected.

Apart from field research, several studies are planned to further elaborate on issues of a more general and/or theoretical character. Problems such as the regions' place in a globalizing world, the understanding of "sovereignty" from a regional point of view, the importance of external factors for Russia's regionalization, the impact of information and communications technology on center-periphery relations, and the role and political orientation of Russia's regional elite will, among others, be the issues included.

- URL: http://www.isn.ethz.ch/russia/
- Contact: perovic@sipo.gess.ethz.ch

Integrated Risk Analysis - Comprehensive Risk Analysis and Management Network (CRN)

New or newly recognized vulnerabilities of modern societies and the rising complexity of causal circles involving various kinds of risks call for an intensified international dialogue and more co-operation in the field of national risk profiling—to be undertaken in an open structure, and not a hierarchical one. A new knowledge, a better understanding of new risks, their causes, interactions, probabilities and costs is needed. The "Comprehensive Risk Analysis and Management Network" (CRN) is a future-oriented initiative launched by Switzerland (Center for Security Studies and Conflict

Research, ETH Zurich) and Sweden (ÖCB, The Agency for Civil Emergency Planning) to cope with the complexity and multidimensionality of the threats we are facing.

The risk analysis initiative is based on the Comprehensive Risk Analysis Switzerland Project, which was commissioned by the Swiss parliament and launched in 1991. In 1999, the project was transferred from the Central Office for General Defense to the Center for Security Studies and Conflict Research at the Swiss Federal Institute of Technology (ETH) in Zurich.

The purpose of the project "Integrated Risk Analysis" is to develop methodological expertise for the identification, evaluation and analysis of national collective risks that modern society in general, and Switzerland in particular, is facing. CRN was developed in order to support the dialogue between governmental and academic risk specialists and professionals in the areas of security risk analysis, assessment and profiling. As an electronic platform promoting the dialogue on risk profiling, the CRN site offers methodologies, procedures, tools and case studies for the security risk profiling process at the national, sub-national and local levels.

- URL: http://www.isn.ethz.ch/crn
- Contact: metzger@sipo.gess.ethz.ch

Electronic Services

The center has developed and maintains two major electronic information services—the International Relations and Security Network (ISN) and the Information Management System for Mine Action (IMSMA).

International Relations and Security Network (ISN) (http://www.isn.ethz.ch)

Parallel to the end of the Cold War and the breakdown of political barriers between East and West, the Internet has opened up new opportunities for interactive work across political and institutional borders. The new challenges presented by the information revolution demand knowledge, competence, and ethical awareness from the international security community. The International Relations and Security Network (ISN) is a unique instrument in these momentous times. Dozens of research institutes and international organizations, and hundreds of professionals working in the security community linked and supported by the ISN, create knowledge and facilitate information exchange, dialogue, and cooperation. They and the ISN are part of a vast network of cooperative relations that literally reaches around the globe. The ISN's services provide various open-source resources. While the ISN strives to foster an international, multidisciplinary dialogue, it also knows the importance of staying abreast of fast-paced developments in information technology. For and with its partners, the ISN produces new knowledge, creates dynamic forums, defines high-quality standards, and continually improves its service offerings. The ISN is an essential component of Switzerland's participation in NATO's Partnership for Peace initiative and is the leading electronic information service for the fields of international relations and security policy.

Information Services

The ISN holds a leadership position in information technology (IT) for the international relations and security policy community. Its Internet-based services allow professionals to access, retrieve, and use information any time, anywhere. The ISN provides information solutions on the broadest range of IT services and content, customized to users' individual needs and interests. The ISN leverages Internet-based technologies designed to deliver user-centric information for efficient and responsive knowledge management in international security. The ISN is unique in its ability to provide this kind of package, both by itself and together with its extended networks of international partners.

Limited Area Search Engine (ISN LASE)

The ISN LASE is the most prestigious information service that the ISN provides to the international security community. The service enables users to access all available electronic documents in the fields of international relations and security from one site on the Internet. A high-quality index serves the sophisticated needs of professionals. Adopted as a tailored search interface by renowned institutions in the Partnership for Peace area, the ISN LASE provides an individualized and specialized service to partner organizations. The ISN LASE is a state-of-the-art search engine, designed by Eurospider, that supports text analysis and multilingual searches in several European languages, highlighting of matched terms, relevance feedback, and other advanced features. As a brand new feature, the ISN LASE offers a push functionality, which delivers information preconfigured according to a defined set of subscription criteria. Quality control of the ISN LASE content is guaranteed by its editorial board.

Links Library

The ISN Links Library provides an outstanding collection of annotated links in the fields of international relations and security. As a searchable clearinghouse, the ISN Links Library provides a high-quality online reference directory of all relevant international organizations, governmental and non-governmental bodies, research institutes, journals, armed forces, and the full range of subject categories in international relations. Notable features include strong regional collections and extensive specialized holdings.

Conference Calendar

With its online Conference Calendar, the ISN provides an outstanding database of conferences in foreign affairs and security policy searchable according to 18 subject categories, all world regions, conference organizers, and country venues. The Conference Calendar demonstrates the ISN's commitment to delivering a high-quality public service to the international security community. The service is operated in cooperation with Columbia International Affairs Online (CIAO-Net).

Facts in International Relations and Security Trends (FIRST)

FIRST provides a sophisticated collection of statistics and data, including chronologies of conflicts and peacekeeping activities, arms transfers, military expenditures, and country profiles. Professionals will appreciate the authoritative and structured factual reference system of an integrated database supported by the world's leading research institutions in international relations and security policy.

FIRST is run in cooperation with the Stockholm International Peace Research Institute (SIPRI) and other international partners.

Security Watch

In today's fast-moving and ever-changing security environment, professionals, researchers and the public at large need to know on a daily basis what is going on. They need to receive both global and national security news, reference and background information, and analyses in real time and on a continuing basis. The ISN addresses these pressing information needs through its Security Watch, an exclusively Internet-based news service focusing on the Partnership for Peace (PfP) region. Security Watch is unique in its coverage and scope in that it concentrates on security policy germane to the PfP community and is supplemented by links to background resources, documents, and further references.

Research and Publications

The key to the ISN's success as a leading Internet-based network of electronic services is its close collaboration with its international partners. The quality and commitment of the ISN's partners is nowhere more evident than in the ISN Research and Publications section. Here the ISN provides for its users a range of high-quality documents in full text, including academic books and papers, regular journals and bulletins, and documentation to Partnership for Peace (PfP) activities. The Research and Publications section is used primarily by policy makers, academics, students, journalists, and other professionals in the fields of international relations and security who need up-to-date, relevant, and reliable information.

Learning Material

The ISN produces first-class e-learning environments in the fields of international relations and security studies. Our efforts aim at high-quality content, sound didactical approaches, and cutting-edge electronic environments. The target audience comprises students from the Swiss Federal Institute of Technology and teachers who use ISN products for their own educational needs. These products are available on CD-ROM or on the Internet; they are designed either as stand-alone programs for self-study or to support tutored online and residential courses.

e-Learning

The demand for educational services and the supply of educational programs and courses on the Internet is growing considerably. The ISN helps potential students to find appropriate distance-learning courses, produces its own multimedia educational programs, and provides support to its partners in designing and programming Internet courses. The ISN is also setting up an Advanced Distributed Learning (ADL) service within the Partnership for Peace Consortium of Defense Academies and Security Studies Institutes.

Advanced Distributed Learning (ADL)

Collaboration in the Partnership for Peace (PfP) transcends cooperative exercises. Education and training are key to the Extended and More Operative Partnership (EMOP). The PfP Consortium of Defense Academies and Security Studies Institutes, with its ADL working group, is the leading European promoter of an initiative that will bring web-based learning to all the PfP countries. Switzerland and the US have agreed to support this initiative with substantial resources. Eventually, the ADL working group will present a platform for the distribution of exchangeable web-based courses. It will also provide a set of courses from different nations that represent the core curriculum in security policy to every European civil servant and military officer.

Vision

Learning is becoming a life-long activity and is no longer restricted to specific locations like the classroom. The ADL working group is striving to build a common web-based platform for all European educational institutes in the field of security policy. This platform will allow for learning anywhere at any time. It will also enable institutes to:

- Distribute their courses over the web;
- Support the learning process with the most advanced web-based services;
- Put together their own courses, based on modules from different sources.

Open Source Platform

Key to the special environment of the PfP Consortium is a solution that keeps infrastructure and systems costs for partners down and at the same time draws on available high-skill labor in Central and Eastern Europe. A so-called “open source” solution provides an optimal basis for such a process. At the core of the solution is the PfP Learning Management System, or PfP-LMS, which is being developed on behalf of and within the context of the ADL working group. Interested parties can use and expand the core system at no charge under the condition that, in return, all developments to the system are made available at no cost.

Content

The leading partners in the ADL working group maintain a cooperative development team (CDT) to help partners convert their content into an online format. The CDT focuses on didactic support and technical services to convert existing courses into well-structured and comprehensible multimedia online courses. The CDT is happy to assist any interested parties with their course conversions.

The Information Management System for Mine Action (IMSMA) (http://www.imsma.ethz.ch)

IMSMA is an information management system that improves capabilities for decision-making, coordination, and information policy related to humanitarian de-mining (Mine action). Since January 1999, IMSMA has been the UN-approved standard for information systems supporting humanitarian de-mining. Collection of standardized data in a comprehensive information system improves data evaluation using powerful statistical and geographical tools.

Set-up as a networked multi-user system, IMSMA enables several users to enter and evaluate their data simultaneously. The system consists of two modules, since information management capability in Mine action is needed at two different levels: Data is collected and evaluated in mine-affected countries at Mine Action Centers (MACs) and entered into the IMSMA Field Module. Using this system, countries possess improved capabilities for coordinating, prioritizing, and executing de-mining activities.

In addition to local data management capabilities, information can be transferred in the future to the IMSMA Global Module (GM) where consolidation and analysis will be performed. Results of this process can be used at a regional and global level to support strategic decision-making and provide information for the general public on the scale of the mine problem and the progress of mine action activities over the Internet. Mine action centers will be able to directly profit from the Global Module technology with the GM Country Edition that brings dynamic mapping and explorative statistical analysis to their website and improves the countries information dissemination possibilities.

The Geneva International Centre for Humanitarian Demining is providing the IMSMA Field Module free of charge to the mine action community. Using IMSMA as the UN (as well as the de-facto) standard in mine action enables for the first time to collect and evaluate data in a standardized form. This supports a better and more comprehensive capability of data evaluation on a national, multinational as well as multi organizational level.

Analyzing the requirements of the international Mine community demonstrated the need for Information Management capabilities at two different levels. Country and regional mine action centers require a powerful system for gathering and evaluating data at country and regional levels, while at the international level a decision support system, as well as a system that provides information to the general public is needed. IMSMA takes these requirements into account with the development of two independent but inter-linked systems: the Field Module and the Global Module.

The Field Module

Development of the IMSMA Field Module began in fall 1998. While the first release of the Field Module concentrated on covering the urgent need for providing humanitarian demining operations with IT support, the current version and future development is designed to provide information management and operational support to all aspects of mine action.

The Field Module was defined and developed for use at country Mine action Center (MAC) and regional center levels. To fulfill the specific requirements of coordinating and performing Mine action activities, the United Nations developed and approved new international standards for humanitarian demining. The IMSMA Field Module was used as reference system for defining the new standards and is the only system available that complies with these standards. The IMSMA Field Module is the UN standard for Information Management at Mine action Centers.

The Field Module allows the Mine action Center to record, evaluate and visualize information.

Considerable effort has gone into developing a comprehensive but easy to use system. Colors, pictures, tool-tips and graphic- as well as menu-driven system navigation support the user. In addition, the Field Module is fully multilingual and can be translated by the user.

Global Module

The IMSMA Global Module (GM) was initiated and is under development to address the need for data aggregation at national, regional and global level. For the first time in the history of mine action, the IMSMA Global Module will provide the possibility for systematic data consolidation, aggregation, and analysis using a comprehensive data warehouse solution. This process aims to support strategic decision-making for the United Nations and other interested parties and to provide information on the scale of the mine problem and the progress of mine action activities to the general public over the Internet.

Development of cutting-edge technology by the Center for Security Studies and Conflict Research permits the IMSMA Global Module to provide dynamic mapping capabilities as well as exploratory statistical analysis tools (Online Analytical Processing or OLAP) over the Internet directly to the desktop of its users. It also provides a comprehensive view of multiple aspects of Mine action by providing an extensive link library to relevant information that exists on the Internet.

As part of the Global Module, a data warehouse to support strategic decision-making is being developed in order to achieve the important goal of providing relevant information on the mine situation and on the progress in mine action to the user. In order to provide dynamic mapping and exploratory statistics to the users, the development of GIS and statistical reporting mechanisms has been undertaken. These mechanisms use the same base data originating from IMSMA Field Modules, other operational databases, UN databases, or other information sources. The user accesses the GIS as well as the statistical tools over the Internet by accessing the central webserver of the IMSMA Global Module. The exploratory analysis capability with online GIS tools was awarded ESRI’s prestigious “Special Achievement in GIS” award in 2001.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Author: **Information & Security**
Title: **Advanced Information and Communications Technologies in Sub-regional Security Cooperation**
Year of issuance: **2001**
Issue: **Information & Security. Volume 7, 2001, pages 187-188**
Hard copy: **ISSN 1311-1493**

ADVANCED INFORMATION AND COMMUNICATIONS TECHNOLOGIES IN SUB-REGIONAL SECURITY COOPERATION

Modern information and communications technologies have considerable, and as yet – largely underutilized, potential to contribute to security cooperation. This short paper provides an introductory presentation of a project, aimed at utilization of technology, including Internet and Web technologies, to enhance effectiveness and efficiency of security cooperation in South East Europe (SEE). More complete presentation of the project will be published in one of the coming issues of "*Information & Security*." Updates will be available trough Internet at www.GCMarshall.bg.

The project is entitled "*Cooperative C4 Systems Development in South East Europe: From Coordination to Joint Procurement*." It builds on the encouraging developments in the Balkans and the demonstrated willingness of SEE countries to cooperate in conflict prevention and crisis management and to take responsibility for security and stability in their own home.

The overarching concept is that SEE countries need to develop and maintain, in cooperation, *common crisis management capacity*. The challenge is to build and sustain cooperative crisis response capabilities while efficiently using limited financial resources.

The project is intended to devise feasible regional strategies for evolutionary C4 systems development in support of cooperative crisis management and other regional security initiatives. Among expected results are policies for coordinated, and in the future – joint, procurement of technologies and systems for information collection, situational awareness, distributed decision making, communications, command and control in managing multinational multi-agency crisis prevention and response. We shall cover potential regional actions to crises of political-military nature, natural disasters, industrial accidents, and humanitarian crises, as well as organizational and technology solutions to combat arms proliferation, illegal trafficking of people, drugs and goods, money laundering, and terrorism. Of particular interest will be the areas requiring advanced technology implementation in close civil-military cooperation, such as emergency management, aerospace management, control of maritime and river traffic, and coastal zone management.

To achieve this goal the research team will pursue the following objectives:

1. Create a data bank of existing C4 systems, C4 development proposals, initiatives, and projects

in SEE and overlapping regions.

2. Create a system model of cooperative security arrangements in SEE, accounting for existing consultations mechanisms, organizational/ command arrangements, crisis management capabilities (military forces, paramilitary formations and civil organizations), and implemented, or potentially implemented, technology.
3. Devise and test, through simulations, a flexible and efficient operational architecture, system and technical architecture, as well as a blueprint of a notional "desired end state" to serve as benchmark.
4. Propose principles, procedures and system for coordinated/joint acquisition of C4 systems.
5. Devise a resource constraint strategy for cooperative C4 development and coordinated/joint procurement.

***Points Of Contact*:**

Dr. Todor Tagarev
Director Programs, Center for National Security and Defense Research
Bulgarian Academy of Sciences
1, "15 November" Str.
Sofia 1040, Bulgaria

Tel.: +359 87 244810

E-mail: Tagarev@space.bas.bg

http://www.icsr.bas.bg/cnsr

Dr. Velizar Shalamanov
Chairman
"George C. Marshall – Bulgaria"
3, Sheinovo Str., et. 6
Sofia 1504
Bulgaria

Tel.: +359 87 954770

E-mail: Shalamanov@GCMarshall.bg

http://www.GCMarshall.bg

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg