VIEWPOINT:

INFORMATION WARFARE: HYPE OR REALITY?

by E. Anders Eriksson[1]

Information Warfare[2] (IW) is increasingly listed alongside nuclear, chemical, and biological weapons as a potential weapon of mass destruction (WMD)—or at least as a weapon of mass *disruption*. Is Information Warfare really a significant new threat, or has the danger been overblown?

This viewpoint addresses the question in four parts. First, I provide some background on the emergence of the IW concept from various perspectives. Second, I step back and try to place this new vision of conflict and security into a broader context, arguing that the IW threat must be understood as part of a larger societal transformation. As a result, we should expect to see new categories of conflict actors and vulnerabilities as well as new methods of warfare. Third, I address specific IW security risks, and finally, I suggest measures that might alleviate them. Overall, I argue, the greatest cyber threat is probably not mass destruction, or even mass disruption, but rather precision disruption: targeted, controlled cyber attacks. Such attacks meet the needs of new security actors and exploit the characteristics of information society, whereas traditional actors with traditional goals may be more likely to opt for traditional weapons, including those that have traditionally been designated weapons of mass destruction.

THE EMERGENCE OF INFORMATION WARFARE

The 1991 Gulf War inspired widespread realization of the immense importance of information superiority in a modern conflict. In the United States, this realization had an almost euphoric quality. The notion that conflict reflects the nature of society is not new, of course, but this was the public breakthrough of the insight that Information Society warfare may be quite different from its Industrial Society counterpart.

But did the information-dominance concept capture the essence of Information Society conflict? Arguably, the Gulf War victory merely reproduced the key features of interwar military innovation—mechanized warfare and airpower—leveraged by information technology.

It is not surprising, then, that the Gulf War also saw the emergence of an alternative image—that of information vulnerability, the flip side of the information dominance coin. The perhaps most often cited (albeit far from universally accepted) example of this vulnerability was the allegation that a group of hackers in the Netherlands approached the Iraqis, offering their services as cyber warriors against the United States and the UN coalition.[3]

In spite of the lack of publicly known consequences that are truly serious, just the number of successful hacker attacks tells us to take the threat seriously. In the US-led Western security policy debate, Information Warfare is presented as an asymmetric strategy useful for the rogue state opponent typical in anticipated regional conflict scenarios, or for terrorist groups even more foreign to modern Western values.

What type of cyber attacks are such actors likely to launch? The answer provided by the current debate, particularly in the United States, is a massive attack on critical infrastructures. That is, a cyber WMD attack—with WMD here representing "weapons of mass *disruption*." (Of course, if a critical system such as air traffic control is part of the attacked infrastructure, mass disruption may result in mass destruction.)

E. Anders Eriksson is a Senior Analyst with the Defence Research Establishment (FOA), Stockholm, Sweden, specializing in technology and innovation and their relationship to national security and other public goods. Dr. Eriksson has a Ph.D. in Operations Research from the Royal Institute of Technology, Stockholm. The views expressed in this paper are those of the author, and do not represent the official policy of the Defence Research Establishment or other parts of the Swedish Government.

A significant token of this concern is the treatment of these issues by the US Presidential Commission on Critical Infrastructure Protection (PCCIP), whose findings were presented in the fall of 1997, and the ensuing Presidential Decision Directive 63.[4] Cooperation between the public and private sectors is identified as the crucial—but problematic—issue in this context. International cooperation features less prominently in the directive, but judging from conversations with US officials and commentators it is seen by many as equally important.

Contrasting the Western debate to that in many other parts of the world reveals significant differences. In countries such as Russia and other CIS nations, and authoritarian or semi-authoritarian Asian countries, many perceive information technology as a tool for Western cultural infiltration or domination. Perhaps one could describe IW, from this perspective, as "weapons of *cultural* disruption" (WCD).

Both the cyber WMD and the WCD perceptions merit serious consideration when discussing the security implications of the Information Revolution. Despite their apparent differences—or rather due to them—they point forcefully in the same direction, *viz*. a cyber version of the Huntingtonian clash between civilizations.

I will argue that the cyber WMD problem is likely to be transitional in the sense that as information technology (IT) matures, defense will outweigh offense. I do not, however, suggest that cyber security problems can be disregarded. First, that dominant defenses can be built against cyber WMD certainly does not mean that one can neglect to build them. Furthermore, another category of cyber threats, which I call "weapons of *precision* disruption" (WPD), are likely to prove more persistent and insidious. In contrast to WMD, WPD fully exploit the potential for diversity and innovation that constitutes Information Society, or, using the term I prefer, Network Society.

To attempt an in-depth analysis of the "WCD" view would require a different set of conceptual tools. There, in essence, the battle-space is people's minds, and criteria for winning or losing are heavily culture-dependent. In this paper I address this important theme only briefly, arguing that in the long run a *Kulturkampf* stance is likely to be a less effective strategy in defense of national or regional cultures than one that tries to exploit the room for diversity inherent in Network Society.

CONFLICT AND SECURITY IN NETWORK SOCIETY

In the view of many, myself included, we are now in the early phases of a major societal transformation, of at least the same order of magnitude as the two industrial revolutions commonly associated with, respectively, steam and railways, and electricity and the automobile. Many argue that Network Society is likely to be an even more dramatic change.[5]

I prefer the label Network Society over Information Society because by many standards the most advanced economies have been "information economies" for a long time already. For example, in large manufacturing firms, more employees have been engaged in information processing than in materials processing for decades.[6] Digital computers, too, have been around for several decades.

Network Society, in contrast, describes a situation in which the daily lives of many people are more broadly affected by information technology and network-related novelties. As an analogy, Network Society has effects similar to the changes in location and interaction patterns brought about by the introduction of railway in its time—whereas the introduction of the non-networked computer is similar to the less disruptive introduction of the stationary steam engine. Internet interaction already substitutes for physical mobility, and continuous Internet connection has the potential to thoroughly reorganize, e.g., mobility markets. Another key factor, of course, is the ability to rapidly exchange immense quantities of information across the globe.

New technology has traditionally been seen as the first mover in societal change processes. Students of societal change are now tending toward the alternative point of view provided by the Schumpeterian tradition in economics. According to this view, technology, institutions, and culture, values, and perceptions interact in more complex, unpredictable ways; taking a term from biology, they *co-evolve*. Table 1 is an attempt to summarize developments in those three arenas for the two industrial revolutions and the "Network Revolution."

Railways are a suitable point of departure for understanding the logic of the table, since many see them as the "killer application" of the First Industrial Revolution. Their development built on the steam engine—and in turn helped to improve and disseminate the steam

Table 1: Three Major Societal Transformations: Examples of Key Novelties

	THE FIRST INDUSTRIAL REVOLUTION	THE SECOND INDUSTRIAL REVOLUTION	THE NETWORK REVOLUTION
Technology	▪ The steam engine ▪ Textile industry ▪ Railways ▪ Telegraph	▪ Electricity ▪ Organo-chemical industry ▪ Car ▪ Airplane ▪ Telephone ▪ Radio	▪ Semiconductors ▪ Computers ▪ Digital networks (Internet) ▪ Modeling & simulation ▪ Modularity, interoperability through standardized interfaces ▪ Bioinformatics ▪ Telematics
Institutions	▪ The joint-stock limited company ▪ Modern capital markets ▪ Rational bureaucracies ▪ Technical universities ▪ Mass newspapers	▪ The multi-division firm ▪ The industrial R&D lab ▪ Mass political movements ▪ Cinema ▪ Broadcasting	▪ Network organizations ▪ Process- and project-oriented organizations ▪ Venture capital markets ▪ Standards coalitions and R&D consortia ▪ Issue-oriented networks ▪ Electronic commerce
Culture, values, and perceptions	▪ Uniform national culture ▪ Urbanization ▪ Literate, disciplined labor force	▪ Global popular culture	▪ Global niche cultures

Table 2: Three Major Societal Transformations: Security Consequences

	THE FIRST INDUSTRIAL REVOLUTION	THE SECOND INDUSTRIAL REVOLUTION	THE NETWORK REVOLUTION
Actors, reasons of conflict	▪ Nationalistic mass movements ▪ Colonies	▪ Totalitarian political movements	▪ Niche players with a broad variety of agendas, including financial gain ▪ Rogue states, extremist movements
Methods of warfare	▪ Conscript mass armies ▪ Mass-produced firearms ▪ Railway-based logistic support	▪ Mechanized forces ▪ Air power ▪ Radio communication ▪ Radar ▪ Weapons of mass destruction	▪ High-performance special operations ▪ Precision munitions ▪ Cyber weapons
Vulnerabilities/ targets	▪ Population centers	▪ Infrastructure	▪ Knowledge and information assets

engine throughout the world, for all kinds of uses. Development and operation of railways also demanded the most advanced available solutions for the provision of capital, management, technical expertise, communication and control, and safe and reliable operation. Thus they helped create, improve, and disseminate, also for the benefit of other applications, concepts like the telegraph, the joint-stock company, modern banking, rational bureaucracies, university-trained technologists, and literate workers disciplined enough to comply with high safety standards without constant supervision. Finally, railways acted as enablers for urbanization, nationally uniform cultures, and modern newspapers.

Another feature in Table 1 that deserves special mention is the institutional framework for industrial innovation. For the First Industrial Revolution this was the technical universities, which produced the academically trained engineer by combining practical industrial skills with useful theories from calculus, classical mechanics, geology, etc. In the Second Industrial Revolution, the multi-disciplinary industrial research and development (R&D) lab, pioneered by Thomas Alva Edison, was a key enabler.[7] For the Network Revolution, I suggest that various forms of inter-firm development networks play a similar role. Further, I suggest that each step in this progression has meant that development tasks previously relying on serendipity and exceptional talent—if feasible at all—have became possible to perform in a more controlled, routinized, and speedy manner.[8]

My reason for discussing societal change processes in general in a paper on Information Warfare is that conflict and security are functions of society.[9] Table 2 is an attempt to outline the security consequences of the three major societal shifts in terms of actors and reasons of conflict, methods of warfare, and vulnerabilities and targets.

A key difference between Industrial Society and Network Society is the potential for the emergence of radically new categories of conflict actors. In Industrial Society, military strength was based on numbers of soldiers, which required a large population to recruit from, and heavy platforms, which required control over a territory for logistic support, development of operational concepts, and training of crews. Further, the development of advanced military technology—at least after the Second Industrial Revolution—required control over dedicated R&D labs and industrial facilities.

Network Society military assets, in contrast, require few personnel and will often be relatively easy to conceal, particularly considering the possibility of using computer simulations for training and development of operational concepts. Advanced military assets can be developed in network organizations drawing to a large extent on publicly or commercially available knowledge, technology, and support assets.

In the following section I will question the most extreme claims for IW as a power equalizer. Yet it should be clear from the above analysis that military power in Network Society *is* likely to be much less exclusively the realm of major state actors than in Industrial Society. The key resources for building effective military means of power are likely to be innovative understanding of operational concepts in relation to the opportunities offered by rapid technological and industrial development and, of course, substantial financial assets—rather than, e.g., a large population to sustain a large army. Already in today's world not only many states, but also many non-state actors, could meet these requirements. That states may no longer constitute the world's exclusive power elite has been argued from various perspectives; the idea of IW in Network Society provides the military component of the argument.

That states' military power monopoly is challenged is not likely to lead to their immediate demise. But to conduct their business effectively and efficiently, states as well as other actors have to adapt to changes in their environment. Among the three areas of societal innovation described above, technological innovation today is a global process. Culture, values, and perceptions are hard to change at will. Therefore, from the perspective of a state—as well as for a region, an organization, or a corporation—it can be argued that the key factor for success in Network Society is the adoption and development of effective institutions.[10] For a state, this requires finding arrangements that allow legitimate public interests to be pursued in ways that utilize, rather than hamper, the innovativeness and entrepreneurship of private actors, at home and abroad.

This also applies to efforts to contain the risk of information warfare. That in particular makes the "weapons of cultural disruption" position alluded to above problematic. I personally attach great value to European and Swedish culture, and even more so to that of my native province, Dalarna**,** and I see the Internet as an excellent arena for "defending" these against Americanization and other cultural perils, rather than simply a unilateral tool of cultural domination. For example, I was glad to find a Web site featuring texts and sound recordings of the peculiar dialect of the small Dalarnian parish Våmhus, with a population of about 1,300.[11] Hence, in societies that allow scope for innovation and initiative from below, IT can make it possible for individuals or communities to reinforce their local cultures. This feature of IT undermines the WCD argument—although it may make IT appear even more threatening to governments that seek to exercise tight control over local culture and individual initiative.

WEAPONS OF MASS DISRUPTION VS. WEAPONS OF PRECISION DISRUPTION

In discussing cyber threats it should first be made clear that the use of the Internet and its possible successors for propaganda, for coordination of terrorist and criminal activities, and for open-source intelligence collection, is a sure thing. The issue here is the possibility of using digital information networks to do harm in more direct ways—be it to the Internet infrastructure itself, to other infrastructures increasingly dependent on it (e.g., electricity, transport, and financial systems), or to other applications.

In the past, a person had to be physically present at a key point to perform sabotage, as a trespasser, an insider, or a combination of the two (legitimately passing perimeter defenses but trespassing through dedicated inner defenses). In Network Society, these categories are translated to the logical (i.e., computer code) domain.

Obviously, increasing connectivity is a key enabler of cyber attack. Admittedly, many important systems are still physically isolated from the Internet, but the trend is toward public network connection with intrusion protection at the logical rather than the physical level, even for intra-firm networks (intranets). Such linkages allow telecommuting and exploit economies of scale by utilizing public networks for communication between different physical sites. Further, the meaning of "intra-firm" has become increasingly blurred in the network economy, giving rise to the concept of the extranet, a network "internal" to an "extended organization" that also includes partners and allies.

The tendency toward technological monocultures is another enabler of cyber attack. The network economy tends to encourage "winner take all" situations in markets with high IT content. This results partly because software, once developed, can be copied and distributed at minimal additional cost, and partly because of the general advantages of standardization: e.g., economies in communication, maintenance, and training.[12] A typical case in point is the Microsoft Windows operating system. The Internet communications standard TCP/IP, also ubiquitously used in intranets and extranets, provides a nexus between the connectivity and the monoculture arguments: the technology of connectivity itself is an obvious candidate for monoculture.

Technological monoculture benefits the cyber attacker because methods and resources of attack can be freely moved to and launched from anywhere to any target. One may conceive of a piece of malicious software that affects some key function of the Internet—and then also of every intranet and extranet where the same malicious code is successfully implanted. Or think of bugs in standard programs that by necessity are well publicized, therefore inadvertently allowing a swift attacker a window of opportunity on systems where patching is lagging. One scenario, inspired by the notorious "Solar Sunrise" incident, is that attackers may exploit such windows of opportunity more or less routinely to insert "back doors" for possible future use.[13]

However, connectivity and monoculture also offer opportunities for the defender. One obvious point is that the web structure and self-routing principle of the Internet architecture itself enables resilience. By design, communication should be possible even when many nodes and links are down—this was the very idea behind the Internet's first ancestor, ARPAnet, launched as a research platform for a robust military communication system. So far, this architectural resilience has not been fully exploited. The main reason for this, in my view, is that hitherto the Internet has been used for research and leisure purposes. Now that it is increasingly being used for business-critical applications, the incentives for better exploitation of its inherent security potential should be expected to grow proportionately.

Resilient connectivity can also be used to coordinate defensive and reconstitutive measures. The dominant perception today is that a static defense of information systems is not feasible against a sophisticated adversary. Static protection is meant, instead, to delay the attacker in order to allow the attack to be discovered, and to win time for the more active components of defense. One therefore talks about the defensive chain: Protect - Detect - React. Networking allows more cost-effective mechanisms for detection and reaction, and for information sharing on all three elements.

Monoculture also has a number of positive security features. In the old world of dedicated systems, there was much more scope for people with inside knowledge to perpetrate attacks exploiting specific weaknesses of each system. Now weaknesses are subject to public debate, and there is a competitive market for expertise, including expertise in fixing security problems (where the old world had locked-in customer-provider relationships). Furthermore, in an attack, all the defensive and reconstitutive resources that can be made available—subject of course to organizational constraints—are accessible to the defender.

Finally, just as the growth of the Internet into a mature business platform is likely to lead to increased exploitation of its inherent resilience, the same process will also lead to greater maturity in other aspects of information security, such as the use of authentication and encryption.[14]

On balance, then, how serious is the IW threat? According to the alarmists, almost any teenager with a computer and a modem will be able to mount significant cyber attacks on major states. I think that is hardly a probable future. I assume, admittedly, a certain degree of rationality among those making the Internet more and more critical to their businesses. But, at least under such rationality assumptions, we should expect security to become much more sophisticated. Such a development would ensure that serious cyber attack becomes the realm of the resource-rich, in terms of both funds and expertise. Still, the resources required are likely to be much lower than for conventional military capabilities. And it should be kept in mind that Network Society offers new ways of collecting funds and coordinating expertise.

So what type of cyber attacks are the members of the cyber warfare club likely to launch? The answer suggested by the current debate, particularly in the United States, is: a massive attack on critical infrastructures. That is, a cyber WMD attack, where WMD means weapons of mass disruption.

Such scenarios are worthy of the attention they now receive. I believe, however, that once the defense gets its act together—hopefully before the offense does—many of the beneficial features of the network economy will go to work for it. Many now hope for this to happen in the context of the Y2K bug. Provided there are sufficient assets for coordination, abundant human and technological resources will be brought to bear on a problem shared by virtually all members of the network economy. This is an example of "swarming," identified as an emerging key strategic principle.[15]

In any event, with no clear-cut cases to date of successful mass disruption attack, those contemplating such a course of action cannot be sure whether even an ad hoc response to attack might be sufficiently effective to defeat them. Nor would they know how the "cyber fog of war" would affect such an attack. Given these uncertainties about the chances of success in a cyber assault, therefore, traditional weaponry including weapons of mass destruction seem a more robust, and hence more likely, option for rogue states, terrorists, and others out to cause mayhem. (It should be noted that traditional WMD is also affected, to varying degrees, by the changes in technology and innovation outlined in this paper. Bioinformatics, for example, arguably has the potential to support routinized rapid innovation of biological and chemical weapons to beat countermeasures.) Of course, this assessment should be subject to revision, e.g., if the Y2K problem turns out worse than expected.

Despite the uncertainties surrounding the scope for cyber WMD attacks, I think in the long run we should take greater interest in cyber weaponry as WPD—weapons of *precision* disruption. The WPD concept is also applicable to other domains, e.g., the above-mentioned developments in bioinformatics could result in biological and chemical weapons of precision destruction.

WPD would arguably be useful to states that are relatively ruthless, yet reasonably well integrated into the world community; to relatively ruthless interest groups; and to criminal networks, typically with substantial links to seemingly legitimate business interests and perhaps acting on behalf of some other kind of actor. Such aggressors, who are potentially much more numerous than those interested in using WMD, would typically not be interested in causing disruptive chaos without control. Most certainly they would not like that to happen to their key asset, the Internet. Rather, they would be interested in paralyzing a set of carefully selected key targets at precisely the right moment (say, an important election, or the closure of a key international or business agreement), or in sustaining a controlled, low-level attack over a long period of time in order to cripple an adversary without leaving incriminating evidence. Such attacks could in many cases remain unidentified, or at least unconfirmed.

Further, a key technological feature of Network Society is the ability to put together novel systems and concepts rapidly, utilizing interoperable generic technologies and simulation-supported systems engineering. This means that an attacker may be immediately ready with new attack concepts to replace any that become compromised.[16] Also, because the number of victims for any single WPD attack would typically be quite limited, prospects for volunteers swarming against the attack are reduced. In my view these properties are likely to make weapons of precision disruption a more formidable challenge to Network Society than weapons of mass disruption.

So, if I am right, Information Warfare is not hype, but it is a somewhat different kind of reality than most voices in the debate suggest. Taking the WPD threat seriously should lead us to demand new—and higher—standards for defense innovation. If not, with the type of routinized rapid innovation I have outlined, the first-mover advantages classically exemplified by Germany's preeminence in mechanized warfare early in World War II will exist for potential future cyber attackers as well. Furthermore, in the Industrial Society context, lock-in effects tended to slow down those with a head start in a new field and allow competitors to catch up, at least until the next wave of major innovation hit some decades or so later. In Network Society, a structurally more innovative actor may have a perpetual advantage.

An important question is what cyber weaponry will do to conflict dynamics. Perpetrator ambiguity is a problematic feature in this regard, with a clear potential for conflict aggravation through mistaken attribution of responsibility for attacks and retaliation against innocent parties—perhaps as an intended effect by the real perpetrator. The potential for rapid innovation of new concepts is potentially destabilizing in the sense that escalation through many, small steps may lead to situations quickly getting out of hand—perhaps to the level of WMD deployment. This is particularly pertinent in connection with value-driven and decentralized actors—idealistic "hacktivists" turning into cyber terrorists. On the other hand, as we have seen, many probable WPD perpetrators are likely to show the restraint necessary for successful parasitism. This would be particularly likely for those operating under a covert action or organized crime paradigm, and under strong organizational or cultural control.

COMING TO GRIPS WITH WEAPONS OF PRECISION DISRUPTION

Can we cope with the type of emerging threats I have tried to outline in this viewpoint? And, by the way, who are "we"?

To summarize, the new threats posed by cyber weapons of precision disruption—but also by other types of weapons of precision disruption or destruction—are characterized by the ability to rapidly develop and deploy novel, customized weapon systems and operational and tactical concepts; to do so in organizational settings other than states—including emerging issue-oriented or "for-profit" networks; and to do so in disguise.

"We"—the community that has legitimate interests in coping with these threats—should be taken to include states, but also businesses and NGOs. The relatively ruthless members of this community may be susceptible to moral hazard stemming from perpetrator ambiguity. But perpetrator ambiguity may also have an upside: establishing non-state origin as the default presumption for WPD-related activities should enable the application of international law enforcement cooperation to the problem. 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.[17]

How to deal with the potential for rapid radical innovation is one of the outstanding challenges for public policy posed by Network Society. The security domain is arguably one of the most affected areas, because "competitors" face one another directly rather than in a marketplace with a more or less inert customer base, and because government itself is a "competitor," not only a rule setter or a customer.

Public policy has a proactive side, building infrastructure in the broadest sense of the word, as well as a reactive side. In the present context, infrastructure could include such items as standardization, legislation, international regimes, regulatory agencies, and structures for warning, alerting, and crisis response. Network Society's innovation potential requires that infrastructures be built to manage a broad variety of potential future developments, the vast majority of which will never materialize. To do this will require extensive use of scenarios and other qualitative foresight methodologies.[18] Furthermore, purposeful crisis response against an innovative adversary requires that the knowledge created in scenario exercises and forecasts on possible attack concepts be retrievable and useful to analysts.

[1] The origin of this article is a presentation at the international conference on "Information Technologies, Security, and Conflict Resolution," Moscow, April 28-30, 1998. I am indebted to the editors and two anonymous reviewers of *The Nonproliferation Review* and to Malin Johansson for very useful comments and assistance.

[2] In official US and NATO documents the term now preferred is "Information Operations," with "Information Warfare" being reserved for war and crisis.

[3] John J. Fialka, *War by Other Means: Economic Espionage in America* (New York: W.W. Norton, 1997) is one example of an influential commentator disseminating the Dutch hackers working for Saddam story (p. 104f). Rop Gongrijp, in an oral presentation at infoWARcon VI (Brussels, May 1997), presented a compelling argument for the story being largely an urban myth. US government officials present in the room did not dispute this. They said that Dutch hackers *did* penetrate information system assets used for Coalition campaign logistics. The purpose of these attacks, however, could well have been just the usual in such cases, i.e., to boost the hackers' self-esteem and reputation among their peers.

[4] See "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," May 22, 1998, <http://www.ciao.gov/63factsheet.html>.

[5] There is a vast literature on societal transformations inspiring this paper. Here and in the following endnotes it is only feasible to mention a few representative works, e.g., Manuel Castells, *The Rise of the Network Society* (Malden, MA, and Oxford: Blackwell, 1996).

[6] Daniel Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting* (New York: Basic Books, 1973).

[7] Richard S. Rosenbloom and William J. Spencer, eds., *Engines of Innovation: U.S. Industrial Research at the End of an Era* (Cambridge, MA: Harvard Business School Press, 1996).

[8] E. Anders Eriksson, "National and International Security in Network Society: The Need to Re-Invent Military Innovation," *Militært Tidsskrift* 128 (March 1999), p. 43.

[9] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the Twenty-First Century* (New York: Little, Brown and Company, 1993); John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997).

[10] There is a vast literature arguing that this has also been the case historically, an early classic being Douglass C. North and Robert Paul Thomas, *The Rise of the Western World: A New Economic History* (London: Cambridge University Press, 1973).

[11] <http://w1.250.telia.com/~u25000104/vsockeng.html>.

[12] W. Brian Arthur, "Increasing Returns and the New World of Business," *Harvard Business Review* 74 (July – August 1996), p. 100.

[13] "Solar Sunrise" was an incident in February 1998 involving numerous intrusions into US defense computer systems. There were serious suspicions of a major cyber campaign, but eventually the perpetrators were identified as two Californian teenagers with an Israeli teenager as their mentor. The intruders exploited a well-known—but apparently unattended in many systems—vulnerability in the Solaris operating system. They introduced backdoors and patched the vulnerability they entered through. See Bradley Graham, "US Studies New Threat: Cyber Attack," *Washington Post*, May 24, 1998, p. A1, and Mike Vatis, "The use of the Extranet to combat cyber attacks on national infrastructure," keynote address delivered to 3rd Annual SMi Conference on Information Warfare, London, March 10-11, 1999.

[14] These interrelated areas are unfortunately very good examples of the hardships of defining mutually acceptable public and private sector roles in a Network Society setting.

[15] John Arquilla and David Ronfeldt, "Looking Ahead: Preparing for Information-Age Conflict," in Arquilla and Ronfeldt, eds., *In Athena's Camp*.

[16] Eriksson, "National and International Security in Network Society."

[17] E. Anders Eriksson and Malin Johansson, "IT-relaterade hot i nätverkssamhället: förslag till en svensk proaktiv agenda," ("IT Related Threats in Network Society: Proposal for a Swedish Proactive Agenda"), mimeo, FOA Defence Analysis, May 1999.

[18] One such methodology is "The Day After," developed by RAND and used in many cyber threat exercises. The idea is to subject a group of decision makers to a crisis scenario, and then use this experience to address policy and strategy. Applications include the already classic cyber WMD-oriented work, Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: RAND, 1996); our own somewhat WPD-ish E. Anders Eriksson, Malin Johansson, Birgitta Lewerentz, and Eva Mittermaier, "Information Warfare and National and International Security Challenges in the Information Age," mimeo, FOA Defence Analysis, March, 1998; and the WPD-like problematique of money laundering in David A. Mussington, Peter A. Wilson, and Roger C. Molander, *Exploring Money Laundering Vulnerabilities through Emerging Cyberspace Technologies: A Caribbean-Based Exercise* (Santa Monica, CA: RAND, 1998).