

The Proliferation Challenges of Cyberspace

David Mussington*

The Emergence and Structure of Cyberspace

What is Cyberspace?

The emergence of global information networks as a venue for economic and political activity carries with it an unfortunate consequence: the potential use of these same networks for hostile political and/or criminal purposes. Because the emerging global information infrastructure (GII) is an amalgam of different national, international, public, and private communications and computing systems, there is no single authority or agency with a mandate for protecting common interests in enhanced network connectivity.¹ Instead, cyberspace — the increasingly interconnected network of computers and telecommunications systems serving businesses, consumers, and governments — is governed by an *ad hoc* framework of increasingly obsolescent legal rules, public and private telecommunications services providers, and a rapidly growing user base.²

Physical and Virtual Layers in Cyberspace

Cyberspace comprises two linked but conceptually distinct layers: (1) the physical infrastructure of copper wire, microwave, satellite, and fibre optics networks, switches, routers and bridges, and servers that make up the backbone of the GII; and, (2) a virtual or information layer, comprising the software protocols making up network operating systems and information in the form of data flowing in networks that is time-sensitive, economically valuable, and/or politically sensitive.

These layers require different treatment if threats to them are to be comprehensively understood. It is at least possible that measures taken to protect the physical infrastructure of information networks may have

*This chapter is an edited version of a presentation made to the Fourteenth Annual Ottawa NACD Verification Symposium, “Cyberspace and Outer Space: Transitional Challenges for Multilateral Verification in the 21st Century,” 12-15 March 1997, Montebello, Quebec, Canada.

¹For an early formulation of these relationships, see my “Throwing the Switch in Cyberspace,” *Jane’s Intelligence Review* (July 1996), 331-334.

²There is a danger that scientific users of information networks will be displaced by more lucrative commercial applications in broad system design decisions. This would be a tragic event, given the increasing importance of scientific collaboration on the Internet. See Herb Brody, “Wired Science,” *Technology Review* (October 1996), 42-51.

a negative impact on the flow of information within the networks themselves³. In turn, actions taken to secure the economically and politically sensitive flow of information on networks could undermine their physical security. In both cases, however, the issues determining whether the physical and virtual layers of cyberspace develop concurrently, derive from the characteristics of the two environments. This chapter offers a framework for understanding emergent network vulnerabilities, and for understanding non-network vulnerabilities that are exacerbated by the enhanced availability of information on global networks. This analysis highlights the difficult balance that must be struck between protecting critical networks, and maintaining the open access and global scope that give these networks their special value.

The term ‘cyberspace’ is used in this chapter because it encompasses a broad range of terms used to describe an emerging family of wide area networks linking advanced computing and communications infrastructures together.⁴ Because of its origins in science fiction, cyberspace is held by some observers to be little more than a fictional and ‘hype-ridden’ phenomenon, promoted by the popular media, and likely to collapse once the public’s fascination with it wears off. However, this is unlikely to be the case.

The emergence of national and, increasingly, global information networks is being underwritten by influential governmental and economic interests seeking to define new markets, and to protect hard-won technical competencies.⁵ As the extension of the ‘personal computer revolution’, the growth of the Internet is likely to cause a significant shift in patterns of economic, and eventually, political activity.⁶ This environment will likely contain significant political and social conflicts and, of course, forces favouring cooperation and conflict resolution.

³Computer Science and Telecommunications Board, National Research Council, “Application Needs for Computing and Communications,” *Computing and Communications in the Extreme: Research for Crisis Management and Other Applications* (Washington, D.C.: National Academy Press, 1996), 10.

⁴The term was first found in a science fiction novel entitled *Neuromancer*, by William Gibson. In that context, the term described ubiquitous network and direct brain-computer interfaces. While such applications are not on the immediate horizon, the societal and vulnerability consequences of network dependence are beginning to make themselves felt.

⁵A significant analog to the growth in commercial network applications is the increasing importance of information systems to national defence. These systems are not the primary focus of this analysis for a single reason — they are following, not leading — the deployment of broadband commercial networking systems. For a good summary of the technology security issues raised by these developments, see Ian Anthony, “Transfers of Digital Communication System Technology,” *SIPRI Yearbook 1996: Armaments, Disarmament and International Security* (London: Oxford University Press, 1996), 552-559.

⁶Roger C. Molander, Andrew S. Riddile and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, RAND/National Defence Research Institute, 1996).

The study from which this chapter derives focused on the problematic aspects of global networks — those that may empower new actors to threaten important societal infrastructures. The emerging threat is of two types:

- C problems arising from the increased availability of information useful to those interested in procuring materials and technologies for the creation of weapons of mass destruction; and,
- C problems created by the spread of information warfare capabilities to state and non-state actors that oppose Western interests.

Information weapons may allow terrorists — or others acting on behalf of states — to create new capabilities for blackmail or intimidation. In turn, the prevalence of complex technological systems in society — such as electric power plants, communications networks, and air transportation systems — extends this vulnerability beyond the military sphere, to include broad segments of civil society. Responses to these potential vulnerabilities must take into account the unique characteristics of cyberspace. The first section of this chapter focuses on the physical and virtual domains within cyberspace. This chapter relates the features of the network environment to the possible empowerment of new actors who may pose threats to critical societal technological systems and information resources.

Two Domains in Cyberspace

Because cyberspace has two conceptually distinct domains, threats to information infrastructures can be discussed in terms of their impact on both information flow, and decisions to deploy the new network technologies making up the GII.⁷ The physical and virtual domains within cyberspace each possess characteristics that suggest that they are potentially attractive targets for attack by those wishing to undermine the security — or credibility — of the GII as an environment for political and economic activity.

Virtual Layers Issues

The information or virtual, layer of cyberspace comprises both the software allowing the physical infrastructure of the GII to function, and the data and applications which create and transmit economic and political information among users. The three characteristics or concepts that describe the virtual layer of cyberspace are:

- C the requirement for authentication — in terms of both users and information — of the data transmitted over a network;

⁷Mussington, “Throwing the Switch in Cyberspace,” 332.

- C the necessity that information be transmitted through networks in a rapid manner for time-sensitive economic purposes and critical public safety applications; and,
- C the desire that access to the network be widely distributed, while at the same time preserving the authenticity of information and identity in cyberspace.

Authentication. This requires that authorised users and creators of information on critical networks have confidence in their ability to determine — through the use of network functionality — their mutual identities. On the Internet, authentication schemes dependent upon strong encryption seek to ensure against unauthorised use of network-carried information or applications, examples of which are: initiating transfers of funds using inter-bank funds transfer systems; the closure/opening of valves within oil and natural gas pipeline networks; and, the erroneous detection of aircraft — or the incorrect identification of some — by an air traffic control system.⁸

Timeliness. In applications that require the use of real-time information delivery, any system breakdown or fault can impede the flow of information and compromise system performance. Examples of real-time dependent applications include: financial data and electronic funds transfer systems; “just in time” inventory control systems; and, medical information systems. A subtle degradation in system performance may have significant consequences for network users. Information “outages” for such systems are intolerable, as are real-time interruptions in network control and management. Examples of network control applications include: SCADA networks — remote control and maintenance systems for oil and natural gas pipelines; digital switches underlying the public switched telephone network; and, regional and national air traffic control systems.⁹

Access. This issue differs from authentication in that it refers to “ease of use” issues deriving from the actual systems and procedures deployed in real-world networks. For many applications, restricting access undermines economic viability — i.e., as may be the case in Internet commerce. This is preeminently an issue of interface design, where the imposition of user authentication schemes begins to impede the free flow of information, or the use of network applications. Ease of access clearly has a different meaning in different segments of the GII, be they secure funds transfer systems, ordinary e-mail, or remote control and maintenance applications. Where different network applications use the same physical infrastructure — i.e., the public switched telephone network — different users of information resources may become vulnerable to impairment from a single set of vulnerabilities.¹⁰

⁸Deborah Russell and G.T. Gangemi, Sr., *Computer Security Basics* (Sebastopol, CA: O’Reilly & Associates, 1992), 124.

⁹*Computing and Communications in the Extreme*, 31.

¹⁰*Computing and Communications in the Extreme*, 47.

Physical Infrastructure Layer Issues.

The physical part of cyberspace is made up of the copper wire and fibre of the public switched telephone network, microwave and satellite communication systems, digital switches and routers allowing for isolated networks to be interconnected, and the individual servers and computers which make possible particular information-dependent applications. Three concepts describe the security issues deriving from the physical network infrastructure:

- C redundancy — the existence of multiple and duplicative network links between network nodes;
- C fault tolerance — the ability of a system to manage impairment to system function short of a catastrophic (complete) failure of critical functionality; and,
- C physical security — the robustness of critical links and servers against destruction through accident or deliberate assault.

Redundancy. This is, perhaps, the central attribute of the Internet, stemming from its origins in the original ARPANET system designed to ensure communications connectivity during and after a nuclear war.¹¹ Beyond the packet-switched architecture of the Internet, communications networks use different modalities for the transmission of information. Among the systems in use are: microwave networks; satellite and terrestrial fibre/copper wire telephone systems; conventional radio broadcast networks; and, cellular networks.

These varied systems increase the robustness of the GII to technical failure, but it remains possible that shared infrastructures supporting different parts of the GII may subject the system as a whole to the vulnerabilities of the weakest segment. It is possible, for example, that weakness in the public switched network (PSN) could propagate across the GII in novel and unexpected ways if software or other related operational factors begin to impede the operation of switches and routers. Such a situation arose on 15 January 1990 when AT&T's long distance network suffered a catastrophic failure in the United States. Flawed system software in some of AT&T's digital switches, along with operational rules that mandated that all switches receive software upgrades at the same time, created a situation many experts said could not occur. User confidence in such networks requires that multiple redundant pathways be built into both individual components of the GII and into the network as a whole. In the case of cyberspace, the varied sources of hardware and software connected to shared communications infrastructures open the possibility of nonstandard equipment causing network problems.

¹¹In many ways system security concerns for a military application are different to those of civilian systems. The working out of these differences takes place in the economic and political decision-making underlying GII development. See Russell and Gangemi, 28.

Fault Tolerance. This concept describes the reconstitution and robustness of a system in the face of software and hardware errors, unanticipated system state changes, and unauthorised interference with a network through physical assault. The question of how the network manages divergences from expected system behaviour is critical. If a system degrades gracefully, some system functionality is maintained even if the overall system architecture no longer operates within expected parameters. If the system does not manage small flaws well, then its vulnerability to the failure of a few critical components is heightened. The PSN and the Internet are said to degrade gracefully because of the number of alternate pathways through which messages can pass if critical switches and routers are no longer functioning.

Because the virtual and physical layers of cyberspace interact closely with one another, synergies — or unpredictable combinations of effects — exist in the combination of software and hardware that have the potential to:

- C render cyberspace much more resistant to sabotage and unauthorised penetration than is commonly assumed; or,
- C create unanticipated vulnerabilities, where the failure of software or a hardware component or subsystem may propagate across networks in unanticipated ways.¹²

Factors that influence this issue include: the frequency and nature of software upgrades to critical switches and subsystems; the nature of the technical standards underlying key network technologies — whether they are strong or weak; and, the extent to which economics influences network design. Concerns for maintaining system functionality encourages the building of redundant, fault-tolerant systems for critical applications. The public telephone network is the best example of this type of system. As the inheritor of the current communications infrastructure, the emerging cyberspace environment cannot help but be influenced by extant design disciplines and infrastructure resources.

Physical Security. To what degree are critical servers and communications links secured from physical damage? What is the defining method for protecting these essential elements of the physical infrastructure of cyberspace? And, is an accident viewed as the most likely threat to system integrity, or is deliberate attack viewed as a serious possibility?¹³ The protection of physical infrastructure requires

¹²See *The Hacker Crackdown* by Bruce Sterling for a discussion of the ways that a system fault can have unpredictable and multiplicative consequences. Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (New York: Bantam Books, 1992), “Part 1: Landslides in Cyberspace.”

¹³The operating security management “metaphor” for information dependent infrastructures varies widely across systems. Air Traffic Control systems focus on accident or system breakdowns as the predominant source of breakdown risk. Oil and Natural Gas pipelines are similar in this way, but have

investments in barriers to entry, redundant and fault-tolerant systems that protect networks from limited assault, and the diffusion of encryption and authentication systems that can foil “casual” penetration attempts by hackers and “experimenters.”

Each of these factors impacts the choices available to system designers and analysts concerned with protecting critical information resources. Networks, by their very nature, are both distributed computing systems and communications-centric entities. This means that maximising the usability of the network is a key system value, and not one that can be easily compromised in favour of greater security. Increasingly, internationally distributed networks open different systems to the weaknesses of other subsystems within the wider network environment. Regulatory responses to network security lapses must thus have an international component if key information networks and applications are to be adequately protected.

Types of Network Vulnerability.

Three major types of network vulnerability are likely to affect the emerging GII:

- C network failure due to technical breakdown;
- C the theft of information from the network; and,
- C the targeting of information resources for falsification or destruction.

Each of these threats to network functionality requires governmental responses. The key issue in each case is the level of severity of negative effects from the problem’s occurrence, and the appropriate policy response from government agencies.

Network Failure Due to Technical Breakdown. The growth in connectivity between previously separate networks means that minor vulnerabilities have the potential to propagate across a wide geographic area — affecting more users than might be readily anticipated beforehand. An example of such an event was the failure of the AT&T long distance telephone system mentioned above. In that case, ‘buggy’ software upgrades installed at digital switches on the long distance network succeeded in cutting data links and communications between three large airports on the U.S. East Coast — New York’s Kennedy and La Guardia Airports, and New Jersey’s Newark International Airport.¹⁴ These events caused a reciprocal slowdown in connecting air traffic in both the United States and Western Europe.

more latitude in allowing fault tolerant systems to handle problems than do air traffic controllers who are necessarily much less tolerant of system outages or operations falling outside of accepted parameters. See National Research Council Report, *Understanding the Risk: Informing Decisions in a Democratic Society* (Washington, D.C.: National Academy Press, 1996).

¹⁴Sterling, *The Hacker Crackdown*, 37-38.

The added vulnerability that flows from greater connectivity also makes it difficult to differentiate accidents from deliberate attacks on critical systems. More than anything, the AT&T incident exemplifies the relationship between access and authentication mentioned earlier. In an effort to increase the functionality of its long distance network, AT&T introduced new vulnerabilities into its systems because of flawed software in digital switches. Thus, measures taken to enhance the accessibility of the network to users — i.e., clearer voice lines, faster connections, and lowered error rates in data transfers — actually reduced the robustness of aggregate system security.

Theft of Information. The most commonly discussed vulnerability of information networks is that of the theft of information with economic, political, or national security value. Since the early 1990s, a number of arrests have been made in the U.S., Germany, and elsewhere of ‘hackers’ subsequently convicted of illegally penetrating secret government computing facilities. Attacks against economic targets are also of increasing concern, especially following the revelation in the early 1990s that the French Intelligence Service was targeting foreign — principally Japanese and U.S. — businessmen for industrial espionage.¹⁵ In this case, economic and political goals combined with one another, revealing the difficulty of separating complementary motivations.

At the end of the Cold War, many intelligence agencies have apparently shifted to economic intelligence gathering from their formerly military missions. This means that national and international policy must decide between a focus on counterespionage, and one more directly targeting criminal activity in the deployment of resources to counter system vulnerabilities. In 1990, a Russian man affiliated with Moscow organised crime groups managed to penetrate the electronic funds transfer systems of a major U.S. bank, stealing \$10 million. While most of the funds were recovered, the successful penetration of secure and private information networks highlights the increasing interconnectedness of the world’s networks. The more that these networks share physical infrastructures — and, increasingly, come to resemble each other in their virtual applications — the more vulnerable they may become to attacks that exploit small weaknesses in security preparations.

Targeting of Information Resources. Another source of cyberspace vulnerability is the potential compromise of secure and sensitive information held within networks. Theft of this information may have significant value, as the discussion above outlines. A more subtle means of attack might be to systematically compromise the timeliness or accuracy of critical data used in some economic, regulatory, or emergency medical application. Delays in the delivery of information on price movements in international stock and commodities markets could seriously disadvantage corporations and countries operating with impaired computing facilities. Similarly, the impairment of data on system behaviour in

¹⁵Winn Schwartau, *Information Warfare. Chaos on the Electronic Superhighway* (New York: Thunder’s Mouth Press, 1995), 272-273.

the SCADA system controlling natural gas pipelines could create potentially serious network management problems. In a worst case scenario, physical damage would be done to infrastructures if real-time data management systems were attacked. Lastly, a logistics system dependent upon computerised records of the disposition of physical goods and personnel might be paralysed by the introduction of erroneous information into data systems supporting military deployments. In the future, “just in time” inventory control methods may open up new vulnerabilities in governmental information management.

Understanding Vulnerability and Its Consequences

The discussion above outlines some of the vulnerabilities that characterise emerging information networks. What is the appropriate policy response to these weaknesses? The problem of detecting system flaws lies behind many of the problems outlined above. Put simply, if a system has not failed in the past, it is assumed to be “time-tested” and unlikely to fail in the future. Unfortunately, networked systems are vulnerable to the characteristics of the last piece of equipment or subsystem added to the system. This means that the exact impact of flaws in system software or in connectivity-related areas is, in many ways, inherently unpredictable. Networks are probably subject to “normal accidents,” a term coined by Charles Perrow to describe system interaction effects that are unpredictable due to the complex nature of software and hardware relationships in large technical systems.¹⁶

The complexity of networks holds a troubling implication for arms control and export control issues. The ambiguity of system behaviour intimated by Perrow’s insight means that new actors are progressively empowered with the potential to do widespread disruptive damage to critical networks. It is at least theoretically possible to reach almost any computer connected to the public switched network from any other. This multiplication of access points to the virtual layer of cyberspace means that new actors, non-state or state, criminal or terrorist, may gain the ability to stage complex and subtle attacks on critical and economically valuable activities taking place throughout cyberspace. It also means that these entities may be able to use the information available on the Internet to threaten far more destructive behaviour in the proliferation of weapons capabilities in the WMD category. The next section of this chapter expands on the nature of the actors that may be able to use cyberspace to attack civil society, and outlines the new — and not so new — nature of their motivations for doing so.

New Actors and Empowerment in Cyberspace

The broader availability of information and tools for launching “combined arms” — both disruptive and destructive — attacks on critical network systems are creating the potential for new actors to emerge as significant players in political conflicts where previously only states were of great significance. These

¹⁶Charles Perrow, *Normal Accidents: Living with High Risk Technologies* (New York: Basic Books, 1984), 17.

actors can be characterised in terms of both their phenomenology and their goals. These goals can be discussed in terms of the target of an assault, the nature and scope of destruction or disruption, and in terms of the unanticipated weapons effects that may result.

Figure 1: Characterizing Threats and Actors in Proliferation Worlds

Goals		Actors					
		Religious Extremists	Intelligence Agencies	Terrorists	Transnational Criminal Organisations	Rogue States	Individuals
Extortion				X	X		X
Promoting Anarchy		X		X			X
Other ideological goals		X	X	X		X	X
Geostrategy			X	X		X	
Economic Gain			X	X	X	X	X
Furtherance of Religious Beliefs		X		X		X	X

While this matrix of actors and goals is necessarily simplified, it suggests that the number and variety of actors who might take advantage of network vulnerabilities for political purposes are quite large. As is true in many other areas, after the Cold War, economic, sectarian, and religious motivations for group action are likely to be significant organising principles for new actors in this hypothetical networked world. Coalitions among the various actors may also be possible, making the determination of authorship of particular attacks — and of the underlying motivations behind them — increasingly difficult to achieve. The potential thus exists for “piling on” — in a way resembling the “taking of responsibility” statements released by terrorists in the aftermath of significant destructive events. Identifying the responsible party in instances of terrorism is central to governmental policy-making. Ambiguity is correspondingly likely to impede effective and rapid reactions by governments — at least those tailored to the actual perpetrators of information warfare attacks. The anonymity of network attacks — or, rather, the difficulty of tracing the geographical whereabouts of perpetrators — makes ‘hacker’ activities aimed against critical information infrastructures a likely means of terrorist exploitation.

Already, visible trends in technology diffusion and computer research point to a potentially significant expansion in the number of actors in the proliferation area.¹⁷ A number of key shifts in technology and politics will help to reinforce this trend. The long-anticipated rise of non-state actors as bearers of serious proliferation threats will likely emerge soon after the year 2000. Precursors of these new actors are already visible, with the Aum Shinrikyo cult's use of chemical agent in the Tokyo subway being the most serious and significant example.¹⁸ This group is doubly significant because its activities highlight the increased difficulties facing verification/detection agencies charged with policing the possession of potentially dangerous compounds or weapons. Two facts are key to Aum Shinrikyo's activities.

- C The cult actually launched three attacks, only one of which was ascribed to them in the first instance. The other incidents were blamed on accidents, or safety violations associated with legitimate uses of chemical compounds.¹⁹ The cult used the Internet to obtain information on bomb making and to coordinate its activities across geographically significant distances — with adherents as far separated as Japan, Russia, and South Korea.
- C Each of these factors — the Internet as a coalition support and the use of pre-tests by non-state actors to “hone” their skills — are likely to recur if such groups are active in the future.

The continuing spread of dual-use technologies means that the “ambient technological level” of proliferators will be that much higher, further empowering new actors in proliferation. Each of these factors supports the insight that these new actors will pose proliferation threats to national and global security in coming decades. Reclassifying the goals of these new actors into smaller categories yields the following array of proliferator objectives:

¹⁷Anthony, “Transfers of Digital Communications System Technology,” 554.

¹⁸“The Tokyo Nerve Gas Attack and CBW Terrorism,” in *SIPRI Yearbook* (1996), 701-704.

¹⁹*Ibid.*, 702.

Figure 2

		Actors					
		Religious Extremists	Intelligence Agencies	Terrorists	TCOs	Rogue States	Individuals
Economic Gain or Extortion			X	X	X	X	X
Ideological or Religious Goals	X			X		X	X
Geostrategic Objectives			X	X		X	

Proliferation threats in this environment change shape to resemble better understood — though not well countered — terrorist or criminal activities. As pure (ideal) types, the different cells suggest that the future will be at least as dangerous as today with serious proliferation dangers deriving from the complex combination of disruptive and destructive instruments. This combination may produce new instruments of utility to terrorists and foreign states wishing to avoid a clear ‘paper trail’ proving their responsibility for network disruption and damage.

The ambiguity of authorship in network penetrations or disruptions means that these events may be designed to resemble anticipated accidents or instances of human error. The detection/verification task in this domain thus becomes exceedingly difficult. Differentiating normal network behaviour from the deliberately induced degradation of key system functions requires that methods of investigation and verification be designed with a close eye on the nature of the networks that are under threat. Governmental concerns with political-military security merge with corporate and societal concerns with privacy and the security of intellectual property to exacerbate the difficulties of making policy in this area. Criminals or terrorists may take advantage of this yet unstructured environment to attack key information infrastructures and the accuracy and credibility of information held by government and private sector entities.

New Actors and Government: Capabilities versus Regulatory Effectiveness.

In traditional areas, states enjoy an unquestioned superiority of legal and material resources relative to any other type of actor in domestic civil or international society. Asymmetries in intellectual or technological capabilities are commonly examined within an institutional legal order that advantages governments and legitimated authorities as the ultimate arbiters of permissible behaviour. Terrorism and guerilla warfare are both classic challenges to governmental preeminence, and the new actors in the

cyberspace environment borrow some of their effectiveness from ‘unconventional’ warfare areas. The exact nature of new capabilities available to actors with network access will probably vary considerably. Network access alone does not equate to the ability to manipulate information systems and information content in ways which impact the public sphere. Because the relationship between network expansion, individual empowerment, and governmental regulation of computing and telecommunications is complex, many observers have come to inflated and unrealistic conclusions regarding the ‘end of the nation-state,’ and the ‘transcendence’ of Cold War patterns of interstate relations. One need not go to these lengths to posit that non-state actors have perhaps the most to gain — in terms of disruptive capabilities — from the spread of new network connectivity.

The opportunity for new coalitions of non-governmental organisations (NGOs) to share information and mutual support offers these groups an impressive new resource for influencing government policies.²⁰ In a variety of areas, from environmental protection to conflict resolution of sectarian and religious disputes, NGOs have become increasingly active as important players in dispute settlement. In a democratic context such activities are accepted — if not welcomed — as legitimate political participation.

However, influencing the discourse on a political topic is not the same as foreclosing through intimidation or threatened action, the options of a national government. The same network characteristics which assist protest and advocacy groups in making their voices heard also give to less peacefully inclined actors the capability to attack common infrastructures — most directly, of course, the Internet itself — as a means of fostering change in public opinion or government policy.

It is in this sense that capabilities for disruption of civil society are increasing in a manner directly related to the expansion and interconnectedness of global information networks. As critical information and communications networks come to share a common physical infrastructure, they also come to share vulnerabilities to groups wishing to disrupt them. In this sense, again, disruptive capabilities are becoming more widely distributed at the very time that regulatory frameworks for network governance are becoming fragmented under the pressure from demands for deregulation from the private sector.²¹

²⁰John Arquilla and David Ronfeldt, “Cyberwar is Coming!” *Comparative Strategy* 12:2 (April-June 1993), 141-165.

²¹The importance of business and societal concerns over network governance is focused by the fact that, for the most part, the private sector owns the information infrastructures. This means that the government must assert a sovereign interest in an area where infrastructures are becoming increasingly international, a reality that makes policy-making very difficult. See *Computing and Communications in the Extreme*, 40.

It follows, then, that the resource capabilities of governments in regulating networks in civil society are not easily translated into effective regulatory choices for guiding network development. Governments face an uphill battle in reasserting their primacy in the development of these new infrastructures. Rather than being tied to the computational and remote log in capabilities of even the most powerful personal computer, network users enjoy theoretical access to the most powerful computing and communications instruments in the networked world. Factors such as access restrictions, authentication of users, and the timeliness of delivered data, all impinge on the way that network access is administered. Each of these factors has been a target of 'hacker' attack in the past. It is to be assumed, then, that emerging networks will also be subject to attempts at illicit penetration and compromise.

The vulnerabilities of these networks thus constitute a new kind of proliferation problem. The proliferation of means of attack is matched by a parallel expansion in the number of theoretical access points from which an attack might be launched. Differentiating attacks from accident, or human error, may prove difficult. A recent example will make this point clear. In August 1996, fifteen states in the U.S. Southwest suffered serious electrical outages. Five weeks prior to this, six of these states had been 'blacked out' by what was later traced to a short in a transformer station caused by a tree limb touching an electrical wire. The second incident provided critical information that helped managers at the Bonneville Electric Power Company to characterise the first incident. Programmed system behaviour following an accident — in this case automatic shut downs of power substations and the imposition of a brownout to a large segment of the user base — produced an outcome that many analysts had previously discounted as extremely unlikely. Under tense political conditions, perhaps in a time of civil unrest or international crisis, such occurrences could produce panic among the public, and create political pressure on leaders to address an apparent weakness in national security.

The shape of the proliferation world formed by the increased disruptive capabilities of potential proliferators and the decreased effectiveness of governmental oversight is rather stark. The accelerating pace of change in network technologies means that governmental responses are particularly difficult to design, and the still largely hypothetical nature of the dangers means that public pressure to respond creatively to this problem is unlikely in the absence of a significant information infrastructure crisis.

Because most information infrastructure attacks are likely to be of a disruptive rather than destructive character, it is possible that proliferator behaviour will be channelled toward a domain where the developed taboos against the use of weapons with widespread effects are the least developed. This potential, along with the progressive empowerment of non-state groups relative to government authorities, may create the potential for novel combinations of disruptive and destructive instruments of use to those entities intent upon altering the policies and/or behaviour of national governments through deterrence or intimidation. The next section offers a framework for understanding the relationship between verification

methods and information warfare, and offers some guidelines for approaching this rapidly evolving verification challenge.

Verification Methodologies and Information Warfare

If information warfare tools are taken seriously as weapons of potentially ‘mass disruption’, then verification schemes designed to ensure against such activities are critical to international peace and security. The disruption of critical information networks could form part of a “combined arms” attack against civil society, where destructive means could be used in tandem with disruptive infrastructure assaults to intimidate the public. Verification in this context involves the maintenance of surveillance over networks on a day-to-day basis, so as to ensure that a baseline situation of “non-attack” is well understood. Clearly, international coordination of such efforts is mandatory, given the increasingly global nature of network infrastructures. The information-rich nature of cyberspace creates the parallel danger, however, that information useful to fabricating weapons of mass destruction may become more readily available on the Internet.

Controlling access to this type of information is probably too difficult an endeavour due to the sheer number of sites on the Internet where information on WMD technologies is present. The fact that much of this knowledge is dual-use in nature further complicates the determination of when information is being collected for WMD-related purposes. A less ambitious objective — assessing the distribution of information on global networks — and tracing the identities of groups collecting such information from these sites, might assist governments in their surveillance of potentially dangerous organisations and individuals. At the outset, however, the controversial nature of such surveillance over individuals who may be guilty of no criminal offense must be admitted. The surveillance of individual information gathering on the Internet is both technically difficult and politically and legally problematic. In the absence of a baseline appreciation of the information available, and of whom the consumers of this information are, it is difficult to see how investigations in this area can proceed.

Key Features of the Information Environment on Global Networks

Two features are fundamental to the workings of the Internet. First, the information available on the Internet is not under centralised control. This means that information of varying quality is available to almost anyone with network access. This also means that tracking the appearance and disappearance of new information repositories on the Internet is a very difficult enterprise. The second significant feature of the Internet is that information on almost any topic is now available to almost anyone. The quality of this information is subject to a wide degree of variation, but with skill it is undoubtedly possible to assemble very sensitive WMD-related information from public sources. The Internet adds speed and breadth to information retrieval efforts, however, increasing significantly the potential efficiency of information gathering by interested entities.

The combination of greater information access and increases in network connectivity creates a compound danger: new actor access to sensitive knowledge and materials important to the exploitation of WMD technologies, and a lucrative set of infrastructure targets where network-borne attacks can be launched against key societal assets. Verification in this environment means defining the distribution of sensitive information on global networks, characterizing the “user base” of that information, and relating this information to other investigative resources used to combat proliferation worldwide.

To secure sensitive information networks from compromise, two things are necessary.

- C Authentication systems must be deployed to ensure that only authorised users gain access to highly sensitive information resources. Such systems should probably be segregated from Internet connectivity in order to minimise the risks of remote penetration.
- C Prior to the deployment of an authentication system an attempt should be made to construct a baseline measuring the actual level of intrusion attempts, the points of origin in cyberspace of their initiators, and the degree of success intruders display in penetrating secure systems. Current estimates vary widely, and constitute little more than educated guesses concerning the level of hacker ‘probing’ of secure information networks.

Securing information that is already freely disseminated within the Internet is, as was argued above, a rather futile endeavour. Maintenance of surveillance over the distribution of that information, and over the frequency and character of information collection by suspected proliferators could help to reinforce other anti- and non-proliferation measures taken by national governments and international agencies.

Characteristics of Internet-Available Information

Internet information resources comprise collections of data and structured indices of available data. Information resources are geographically separated, and access to this information is asynchronous — that is, the placement of information on a site is not related closely to the accessing of that information by a potentially anonymous actor in cyberspace. No centralized certification authority exists that establishes the veracity of particular information or analyses on the Internet.

Evaluating the distribution of WMD-related information available on global networks could be accomplished through the design of an intelligent software agent able to “roam” the Internet in search of information of a WMD-character. This type of agent would resemble existing Internet search engines, in that it would travel the global Internet, returning to the home-site with the URLs (Universal Resource Locator) of sites containing information on WMD-related topics. An automated tool of this type would need guidance from analysts capable of selecting among the vast number of URLs returned by the agent, with a view to re-targeting the search — and honing the intelligent agent’s behaviour — to better characterize the nature of information available

on the chosen topic.

Established traditions of openness and legitimate information access, alongside a developing notion of user anonymity, may inhibit the use of intelligent agent technologies to conduct verification activities on global networks. Three factors that exacerbate the difficulty of conducting these activities are:

- C particular users of information may be difficult to identify, beyond the point of an institutional affiliation;
- C information “copying” does not clearly deprive others of access, or reveal access activity if the creation of “mirror” sites is a frequent part of network activity; and,
- C information may be derived from “processing” less sensitive network-derived data. This is particularly the case if skilled analysts are the investigators seeking the WMD-related information. It is possible that the pattern of information retrieval could be masked to conceal searches for sensitive information within more generalised searches.

If intelligent agent technologies offer the prospect of characterising the distribution of information resources on the Internet, the central domain of verification activities will most likely lie in the surveillance of accesses to known sources of sensitive information, and in the protection of content/information integrity. Three parts of the verification activity thus must be performed:

- C surveillance of access to known sites of WMD-related information;
- C protection of information integrity and security at government-controlled data centres; and,
- C the construction of analytical frameworks that establish predictive models for the way suspected proliferators utilise information to make progress toward a WMD capability.

Categorising information can be performed in a variety of ways, but a simple example of a system for categorising information, and the entities seeking it, follows.

Categorising Information Gathering for WMD Technologies on Global Networks

If intelligent agent technology is applied to the task of evaluating the distribution of information resources relating to weapons of mass destruction on the Internet, a second task still remains, that of organising the information into a structure usable by analysts to interpret possible proliferator behaviour. It should be said at the outset that such a tool could only provide an incomplete picture of the information gathering activities of suspected proliferators. Global information networks are still new, which means that established information sources aiding proliferators exist outside of their parameters. It is likely that this situation will change as the information-rich character of global networks becomes more fully appreciated. In the interim, information on the Internet relating to WMD acquisitions must be categorised in a way that makes it usable to statistical and other analyses.

A Prospective Typology for WMD-Related Information

First, the category of weapon that a particular piece of information relates to can be noted. For the purposes of verification, WMD- related information could lie in one or more of four basic categories:

- (1) technologies and materials relating to nuclear weapons;
- (2) technologies and materials relating to biological weapons;
- (3) technologies and materials relating to chemical weapons; and,
- (4) technologies and materials relating to ballistic missiles.

In turn, the information can be further categorised according to type:

- (1) dual-use technologies (system designs and subcomponents);
- (2) proprietary datasets;
- (3) test data from a weapon system; and,
- (4) analytical reports and technology assessments.

Lastly, categorising the location of the sensitive information is also important, as this gives information regarding the places on global networks where information is most freely available:

- (1) institution; and,
- (2) country.

Categorised in this way, the information on the Internet can be analysed to establish the distribution of information available to potential proliferators. Tracing information accesses by individual actors could potentially be achieved through another intelligent software agent, or classifier system, that catalogued the Internet addresses of all accesses to particular Internet information resources over a measured period of time. Agent technology of this type is still largely experimental, but offers the potential to track activity that is already pre-screened through the use of other investigative tools. This second activity is necessarily controversial if used to track the Internet activities of ordinary citizens. Care would need to be taken to minimise abuses of network trace-back techniques.

Conclusions and Policy Implications

A brief summary of the features of cyberspace of importance to verification is followed by a listing of policy issues that require consideration in the design of responses to potential problems.

Features of Cyberspace

C Cyberspace can be seen as a channel for the transmission of proscribed information relating to military technology — especially that concerning weapons of mass destruction. International

treaty or arrangement — i.e., NPT, CWC, BTWC, AG, MTCR, and the Wassenaar Arrangement — proscribes much of this information. The unprecedented access to dangerous information through cyberspace is now potentially available to a wider range of actors beyond traditional government agencies, including a host of non-state actors.

- C Cyberspace can be seen as a target or environment for new kinds of weapons and warfare — information war. There is a proliferation of ‘new weaponry’ and new vulnerabilities, which might conceivably be the subject of new non-proliferation, arms control, and disarmament measures that attempt to address these new potential threats to national and international security. Developing negotiations on responses to still hypothetical dangers may be difficult, especially given the other issues already on the international arms control agenda. A poor understanding of these issues may also impede rapid policy responses.
- C Cyberspace can be seen as a potential new verification tool, or, perhaps more accurately, a new environment for using tools to verify compliance with extant state obligations relating to non-proliferation of weapons of mass destruction. For example, cyberspace monitoring methods may offer new information regarding the activities of potential proliferators around the world.

From these insights flow a number of implications:

- C Non-state actors are likely to figure prominently in the entities that exploit the new information warfare capabilities for disruptive or destructive purposes. Economic, political, and religious stakes are the subjects likely to generate proliferation-related behaviour.
- C Non-state actors gain disproportionately from the spread of information networks to new areas of the world. The opportunity for new coalitions of NGOs to share information and mutual support offers social forces an impressive new resource for influencing government policies. In turn, new networks offer new capabilities for actors with network access to disrupt key information systems for political or criminal purposes.
- C The pace of technological change may channel proliferator behaviour in directions where few developed taboos exist against the use of disruptive weapons with widespread effects. This potential, alongside the progressive empowerment of non-state groups relative to government authorities in cyberspace, may create dangers as non-state actors use disruptive information weapons and perception management to pressure governments to change policies.

Identifying Critical Infrastructures

Thus far, the danger to critical societal infrastructures such as banking, electric power, and telecommunications applications are entirely hypothetical — in that no attacks have occurred or, at least, been detected. The critical nature of these infrastructures is not in doubt, however. Nor is their increasing use of open system architectures utilising network and Internet-related technical standards. The adoption of these systems and control protocols means that weaknesses and security shortcomings impacting the ‘known’ Internet are likely to propagate inside increasingly interconnected wide-area information networks. Investments in network security in each of these infrastructures offer the best near-term prospects for avoiding increased abuse of networked information systems. Prior to policy initiatives in this area, however, risk assessments and vulnerability analyses should be performed to evaluate information-dependent infrastructures. The following recommendations point in this direction.

- C An analysis should be undertaken of the scope and nature of critical infrastructures adopting Internet-linked remote operation and maintenance applications in Canada. In the United States, an infrastructure protection task force has been established to address some of these issues. A similar effort should be launched in Canada, with a view to assessing the vulnerabilities of key infrastructures to compromise.
- C A comprehensive survey should be undertaken of the sources on the Internet which provide weapons-related information in all areas of WMD concern. In addition, consideration should be given to applying emerging intelligent agent technology in order to characterise the information available on the global Internet in terms of both its importance and geographic location. Research could then begin to consider measures necessary to ensure that proliferator exploitation of these information resources is under the appropriate high level of surveillance.
- C While consultations on infrastructure security between countries are probably premature, efforts should be made to collate the findings of the many parallel national efforts at assessing the implications of the growth of network connectivity for infrastructure and national security. Independent efforts in this regard have been completed in the United Kingdom and the United States, but no integrative study of the cross-national growth of infrastructures — and of the parallel growth of network vulnerabilities to disruption — has thus far been attempted.
- C Because economic actors are driving the construction of cyberspace, national security and regulatory concerns are frequently forced to ‘catch up’ to the changing shape of a rapidly evolving technology. To come to terms with this situation, a forward looking study aimed at projecting the future actors likely to take advantage of network connectivity for nefarious purposes should be considered. The actor-goal matrix presented in this chapter suggests that extortion and intimidation are likely to dominate the use of information weapons by non-state

actors. This reality poses new challenges for governments in that threats to national security — interpreted as threats to critical infrastructure security — may resemble terrorist or criminal activity rather than traditional acts or threats of war.

While states may eventually achieve agreement on the sanctity of information infrastructures from attack, non-state actors may refuse to respect developing taboos. This means that states may confront a threat that is difficult to detect or fully evaluate. The danger also exists that suspected proliferators will use non-state actors as ‘fronts,’ concealing the true author of particular cyberspace exploitation schemes. Establishing the defining features of the new network environment is a critical first step to responding appropriately to the new information challenges present there. Only then will the truth regarding emerging societal vulnerability to network attack be fully appreciated.

Chapter Eight

The Information Revolution, the Military, and Arms Control

Jeffrey R. Cooper and Christopher Burton*

The “Information Revolution” is without a doubt one of the most talked about subjects of the 1990s. Newspapers, magazines, and television commentators ceaselessly discuss its technologies, its progress, and the consequences it will presumably have for every facet of life on earth. Within this bewildering ‘universe’ of subject matter, this chapter will attempt to examine only a component ‘galaxy’: it will discuss the implications of these new technologies and new ways of procuring technology for the military, and, by extension, for arms control. To do this, the chapter will proceed through four sections. First, it will position itself within the many subjects related to the Information Revolution, to make it clear which of the many implications will be further discussed. Second, it will describe how information technology is being used by the military, and how technological and economic changes resulting from the Information Revolution have affected how the military procures equipment. Third, it will describe at greater length the technological developments that together make up the Information Revolution, in order to provide a common basis of knowledge upon which to build discussion. Finally, based on this summary of the technologies of concern and how the military uses them, the chapter will conclude by discussing some of the implications of the Information Revolution, both in the broader realm of national security and in the area of arms control efforts in particular.

Broad Implications of the Information Revolution

Whatever the specific technological drivers for the Information Revolution, we can now clearly discern some of its key implications for both the military and civilian sectors in information processing, command, control, and communications. One of these impacts will dominate all others — the intermingling of civilian and military technologies and users to the point where they will be impossible to disentangle. This impact will demand dramatic changes in how we think about potential controls over the diffusion of these new information technologies.

Beyond this overriding impact, there are a number of other potential implications that deserve specific mention. First, this revolution presages a flood of information, previously unavailable, that now will be widely disseminated near-instantaneously to interested users located anywhere — and much of this information is derived from a variety of advanced sensors that are owned and operated by civil or commercial entities. Second, this information will be supplied in quantities and at speeds that were

*This chapter is an edited version of a presentation made to the Fourteenth Annual Ottawa NACD Verification Symposium, “Cyberspace and Outer Space: Transitional Challenges for Multilateral Verification in the 21st Century,” 12-15 March 1997, Montebello, Quebec, Canada.

previously unattainable, yielding completely new functionality in its use. Masses of data previously unusable or uninteresting in their discrete, atomistic form will be merged, correlated, and interpreted into useful information and knowledge. These new capabilities will raise significant economic, legal, and social issues about privacy, data security and integrity, intellectual property rights, and other appropriable benefits resulting from these activities. Third, this revolution provides significantly increased utility from even previously available processed information by synthesizing, integrating, customizing, indexing, and compressing it — changing the nature and role of data storage and archives, libraries and encyclopedias, movies and videos. Fourth, this revolution in communications technologies gives capabilities to transmit these vast volumes of information essentially on demand, with high assurance and low costs. This degree of portability and mobility for information and information users is unprecedented. Fifth, together, these capabilities allow coordination of diverse individuals and activities in ways never before possible. How these “virtual” organisations, communities, and teams will alter existing work processes cannot yet be determined. Finally, real-time encryption provides privacy and security never before available. But, at the same time, concern over vulnerability of our information systems, and about those systems dependent upon them, has never been higher.

Information Technology and the Military

For the American military, and for militaries throughout the world, the emergence of the Information Revolution portends a range of changes that will eventually reshape underlying assumptions and transform not only military operations — including both their character and execution — but military organisations as well. Throughout the Cold War, the U.S. military believed that its information, command and control, and communications needs were exceptional, if not unique, and unmatched in the civilian or commercial worlds — views probably held by most other advanced militaries. Therefore, it believed its needs demanded the most advanced sensors, the most real-time data collection capabilities, the most advanced computers, and the widest bandwidths, thereby allowing the military to set the nation’s R&D agenda and control the rate of technological change, at least in this crucial arena. However, while military users may continue to have *particular* needs, they have now lost the vanguard position so recently held, because these demands are no longer exceptional, either in quality or timing.

At the most obvious level, the Information Revolution offers militaries potentially dramatic improvements in force effectiveness from three types of potential applications. First, as foretold during the 1991 Gulf War, seamless “sensor-to-shooter” links offer the ability not just for ‘smart’ but ‘brilliant’ weapons launched from survivable stand-off ranges. Second, these same technologies can provide military commanders and decision-makers with real-time information and insights enabled by Dominant Battlespace Awareness. Finally, these technologies can allow seamless real-time integration of air, sea, and land forces in a common tactical operating environment.

Less noticeable, four key structural developments wrought by the Information Revolution upon the intelligence and communications environment, to which the military had become long-accustomed, also demand acknowledgment:

- C the opening of the military's traditionally closed, autarkic C³I environment;
- C the military's loss of technological leadership to the commercial sector;
- C the reversal of many of the long-standing technical and cost relationships that prevailed in the military sphere; and,
- C the military's need to accommodate itself to the commercial sector's pace of change.

Opening the Closed Communications Society. For most of the post-Second World War period in the communications domain, the military constituted a "closed," autarkic society. This was appropriate for the particular circumstances of the nuclear confrontation between the United States and the Soviet Union. However, since then, the military has moved rapidly from the highly secure, closed system that even five years before it controlled end-to-end — from R&D through acquisition to operational use — to today's increasingly open system. In this new environment, core military C⁴I functions are deeply embedded, if not inextricably entangled, within a web stretching from the Defense Information Infrastructure, through the National Information Infrastructure, to the global information infrastructure. Today, fully 95 per cent of day-to-day U.S. defence communications are carried by commercial channels, mostly through the public switched network.

Losing Technological Leadership. Even if the dramatic reductions in defence expenditures since the depths of the Cold War had not occurred, the civilian commercial sector might still have taken the lead in developing many of the new technologies as the opportunities for economic efficiency and profit became evident after limited commercial exploitation. Esoteric technologies that previously appeared to have few civilian applications are now being rapidly applied across a wide range of civilian activities, both for commercial and domestic purposes. These include widespread adoption of advanced telecommunications systems on a global basis, incorporating the new digital technologies in everyday appliances, application of GPS-based navigation systems to personal use, and employing extremely advanced sensors to support real-time production and control systems. These changes have substantially altered the direction of technological development in computers and semiconductors — for example, Silicon Graphics, Inc. now lists commercial customers, especially in the entertainment industry, as its key "Lighthouse Partners" for defining leading-edge technology requirements.

Reversal of Key Relationships. The military must now look toward procurement of commercial off-the-shelf, dual-use equipment, and open systems architectures, instead of relying on the classical but autarkic military R&D and acquisition systems which produced highly optimized and cutting-edge products, but at high-cost and usually with proprietary technologies. Hardware is now cheap while special purpose

proprietary software is costly, but maintenance of “legacy” systems — both hardware and software — is now prohibitively expensive.

Rapid Pace of the Commercial Sector. The military has found itself spurred into adopting more rapid acquisition processes, both to keep up with a rate of technological advance set by the commercial sector employing a common digital technology base that the military no longer dominates or drives, and to reduce the costs of its outdated, autarkic legacy system. The proliferation of new telecommunications services, such as data, cellular, and personal communications systems (PCS), has created many new companies, which not only serve these new markets, but also compete with existing services. This competition, in turn, further spurs the development of advanced, competitive-advantage producing technologies.

Together, these changes amount to the military becoming only one among many users and, in most cases, not even *primus inter pares* — a purchaser of systems rather than a developer, a follower of technology rather than an advancer of the state-of-the-art, and a buyer of services rather than an operator. The shift from a national security-dominated to a commercially dominated information environment means that the national security community will no longer drive the rate and direction of innovative activity, the types of systems produced, nor the establishment of formal or *de facto* standards. These changes will demand significant cultural adjustments, not only by militaries but by the arms control community as well.

A Constellation of Advanced Information Technologies

The technological component of what we call the ‘Information Revolution’ results from a set of related technical innovations, together yielding substantial enhancements and perhaps even the revolutionary change that the term itself promises. What we are witnessing does not appear to be a case of inexorable ‘technology creep’ but rather an explosive ‘technology rush.’ Every two years, the speed of silicon processors doubles and storage costs decline by half; every five years, compression efficiency is squeezing data to 1/30 of its size; and every three and a half years, laser diode speeds, critical for fiber optics, are doubling. Terabit transmission speeds have already been demonstrated in the laboratory.

These capabilities support a full panoply of advanced sensors that gather more and different data, new communications architectures — including “untethered” mobile systems — that change fundamental cost relationships for information storage and distribution, and mobile “supercomputer” capabilities married with seamless integration that multiplies individual component functionality and effectiveness — all based on continued progress in digital microelectronic technologies.

The Digital Revolution

Perhaps the dominant contributor to this constellation of new technological capabilities is digital technology itself. With the accelerated introduction of computer and semiconductor technologies into almost all facets of our existence, there is increasing convergence of commercial telecommunications, entertainment, home electronics, and computers.

Digital technologies give rise to two key implications that require significant changes in the information user's frame of reference. First, information in digital form is replicable at will, without degradation or change from generation to generation. Second, digital data streams are inherently encrypted by the process of converting data into streams of binary digits. Because real-time algorithmic manipulation is possible, extremely high security coding schemes are feasible at low cost. Indeed, they allow real-time on-line encryption that allows secure *synchronous* communications. Moreover, these capabilities can be applied not only to written or data communications, but to voice and video as well.

At the same time, these digital technologies are raising fundamental questions concerning ownership and control of intellectual property, privacy and security of valuable data, and equities contested between law enforcement and national security communities on the one hand and commercial interests on the other. Not only for the military, but for the national security community as a whole, these complex changes must be assimilated even as these organisations continue to adjust to the significant structural changes produced by the end of the Cold War.

Ubiquitous Computing

The second key contributor to the Information Revolution is the continuing advance of computing power. Computers are now 100,000 times faster and 1,000 times less costly than during the 1950s, with even greater increases in functionality due to graphical user interfaces, modern software, networking, and platform integration. There is little indication that Moore's Law, predicting doubling of memory chip capacity every eighteen months, is 'slacking off' very much from its historic rates of advance — it will probably continue for at least the next decade. The rate of increase in computational speed, in fact, appears to be speeding up, with recent improvements averaging about 55 per cent per year, compared with 35 per cent in 1985. Current computational power has outpaced previous predictions made in the early 1980s by a factor of more than 100.

Four technological innovations are components of this remarkable increase in computing power.

"Supercomputers" for Everyone. The use of cutting-edge machines which, just a few years ago, were available only to select military and other national security users, is now firmly established in everyday commercial use and best practices.

Embedded Computers. The same solid-state technologies — semiconductor microprocessors and memories — that allow desktop-sized supercomputers also enable the computational heart of these instruments to be embedded in other machines and systems, thereby fundamentally altering the effectiveness and usability of commonly available tools, appliances, and even complex systems.

Cheap, Random Access Mass Storage. A critical complementary technological breakthrough is the availability of high-capacity, random access mass storage, now measured in gigabytes and terabytes of instantaneously accessible data. Portable archives of this size allow complete map and geographic databases to be locally resident, requiring only change functions to bring them instantaneously up to date.

“Highly Cognitive Displays” and User-Configurable Interfaces. Perhaps the next frontier that technological advances in semiconductors, computation, storage, and software will address is effective processing, individuation, and display of complex information in order to allow it to be easily and correctly assimilated by the user. Increasingly large-scale integration of networks and synthesis of useful information from massive, complex data archives for commercial customers is providing the driving force for advanced representation and display systems. Virtual reality technology is creating new ways of displaying information other than as static data sets.

“Infinite” Bandwidth

A third key element in the Information Revolution is cheap, near-infinite bandwidth transmission capacity that creates an entirely new communications environment. Progress in this area is largely the fruit of continued advances in the same solid-state digital technologies that have increased computational and storage capabilities. Here, embodied as signal processors, amplifiers, transmitters, and receivers, these advances have continued to press usable frequencies ever higher. K_a-Band (20-36 GHz) satellite transmission capability and similarly wide-band capacities in advanced fiber-optic cables represent fundamental advances in information transmission capabilities that do not appear to be slowing down. Indeed, as mentioned above, recent laboratory work has experimentally demonstrated terabit transmission capacity using advanced laser diodes and optical fibers. In creating these systems to meet civil and personal needs, the commercial sector is constructing a global information infrastructure that meets many of the military’s demands, and in some cases, meets latent needs that have not yet even been recognised.

“Untethered” Communications

A fourth area of innovation that has contributed to the technological revolution of the present day is the advent of “untethered” communications. Historically, there were few users, other than the military community and steamship companies, who expressed a need for mobile, as opposed to relocatable communications capabilities — either to transmit orders to moving units whose location was uncertain, or to receive situation reports from those units. However, the unbelievable speed with which civil society

throughout the world has adopted cellular telecommunications and now PCS services testifies to a widespread latent demand for “anywhere, anytime” communications.

In 1995, wireless communications generated more than \$22 billion in revenues and this growth, with 20 million domestic users, outstripped predictions made less than a decade before by a factor of more than 100. By 2001, it is forecast that, worldwide, 500 million people will use mobile communicators such as cellular or PCS — whether linked through terrestrial or satellite networks. Furthermore, radio modems will link laptops and other mobile information processors and disseminators back into the entire national or global information infrastructure. To meet these demands, at least seven major space-based mobile-user communications systems are now planned, covering a variety of service features and price points.

Sophisticated Sensors and Discrimination Algorithms

The only point that must be made here is that many critical military needs can now be met by commercially available remote sensing systems. Space-based sensing, once the sole province of the two superpowers’ military establishments, is rapidly becoming an essential adjunct to day-to-day civil society, and not only for developed nations. Sensors increase the reach, decrease the time for measurement and perception, and extend the spectrum well beyond direct human senses and experience — they can make real what before was not even perceived.

Civil society has discovered the value of increasingly sophisticated information-related capabilities and commercial entities are inventing ways to turn these demands into profits by employing the most advanced sensors for data collection — previously only available to the national security community — across an extraordinarily wide range of applications. The Russians are currently selling better than one meter resolution — formerly secret compartmented data from reconnaissance satellites — and by the end of next year, a commercial American satellite will be providing similar quality data. For many civil uses, this high resolution data is essential. It has become increasingly difficult to make distinctions between civilian and military requirements and satellites.

For example, formerly secret data and classified techniques and systems are in high demand by oceanographers and oil companies. Civil or commercial systems employing extraordinarily sophisticated sensors include advanced air traffic control systems, Doppler weather radars for wind shear and storm warnings, space-based environmental monitoring systems, and supervisory control and data acquisition (SCADA) systems for monitoring and control of large-scale telecommunications, energy transmission, and continental and regional transportation networks that affect millions of people in their daily lives.

Two uses in particular stand out:

Precise Navigation. The Global Positioning System (GPS) was developed by the U.S. military to allow military units to determine their location with precision by comparing the time taken by radio signals from many different satellites to reach them, but the civilian GPS industry and the number of civilian users now overshadow the military.

Mapping and Monitoring. The rapid growth of sophisticated geographic information systems enabled by high resolution maps is resulting in a wide range of civil and commercial applications, including crop management, store location, flood control, and emergency response.

Implications of Advanced Information Technologies

Implications for the Military and National Security

These various technological developments, when considered together, do indeed amount to a revolution — the effects of which will be felt in almost all areas. Perhaps the greatest effect overall of the new information technologies is the breaking down, across many dimensions, of traditional distinctions and boundaries between different information-related elements — including those that distinguished and separated the military and civilian sectors in their demands and uses of advanced information technologies. This convergence is taking place in a wide array of different spheres:

- C in the technological dimension, underwritten by a common technical base of solid-state digital microelectronics;
- C in the user dimension, as individuals no longer want to distinguish among information sources and providers, nor employ different instruments to tap them;
- C at the system level, where network architectures increasingly must be prepared to supply seamlessly integrated multimedia products;
- C in the geographical dimension, as physical and political boundaries, time and space, lose their classical divisive impacts;
- C in the national security dimension, as the traditional distinction between raw information and processed intelligence disappears due to both the widespread availability of relevant open source information and the demands of operationally-oriented users for usable real-time actionable knowledge; and,
- C in the legal and regulatory communities, as the old distinctions and barriers between different information forms and regimes collapse.

Three overall consequences flow directly from this revolution in information technologies, capabilities, and employment. The first is that the widespread adoption of these merged, cutting-edge information technologies has created a vast commercial and consumer constituency that overshadows the national

security community, in the U.S. and elsewhere. As a result, the previous priority and obeisance accorded to national security interests is not likely to continue. Moreover, a host of controversies that would previously have been settled on terms favourable to the national security community can now be expected to be decided in favour of commercial and civilian interests.

As a second important consequence, these new information and telecommunications capabilities are creating a truly global information infrastructure and environment in which traditional notions of geography and spatial separation no longer exist. Geographic distance no longer implies time delays in communication between any two points. The increasingly intertwined nature of the “infosphere” also means that there are no impenetrable boundaries between domestic domains or even nations, and this loss of geographic reality has exposed the formerly “safe” rear areas of nations’ domestic infrastructures. Thus, there are no sanctuaries; even formerly secure rear areas are now as exposed as front-line forces to information attacks by opponents. Moreover, distinctions between military and commercial functions are increasingly meaningless when over 95 per cent of defence messages move over the public switched network, when just-in-time logistics for forces engaged in combat ‘reach back’ into contractor facilities, and when commercial contractors are providing real-time communications and analysis services in support of ongoing military operations.

A third important consequence of our Faustian acceptance of the ‘Information Revolution’ bargain is the emergence of a collective national infrastructure — electricity, telecommunications, oil and natural gas, freight, air traffic control, and so on — that is increasingly reliant on real-time scheduling and processes and is fully integrated with a national information infrastructure that is, in turn, increasingly integrated with a global information infrastructure. These systems are then in their turn often monitored and controlled remotely through SCADA systems that are themselves networked telecommunications systems tied into the same potentially vulnerable infrastructures. These trends are producing a system that is increasingly efficient, but is stable only in its dynamic configuration and may not degrade gracefully.

Another set of consequences flowing from the Information Revolution will also have an effect on the military and national security. However, these will have their effect through the intervening medium of information security. For several key reasons, the technological changes of the Information Revolution portend significant implications for effective concepts of information security and protection. First, the widespread adoption by both military and civilian/commercial users of common, commercial off-the-shelf equipment, systems, and practices decreases the difficulty that potential hackers or attackers will have in identifying entry points or finding vulnerabilities. At the same time, military communications carried over shared dual-use systems or in common frequency regimes with standardised protocols may find reduced vulnerability, both from being “lost in the noise” of a massive civilian/commercial traffic volume and from increased resiliency due to massive redundancy resulting from the complex network of alternate service providers in the commercial domain.

Second, while the military and intelligence communities have traditionally been more concerned with system security and survivability than commercial users, the development of new commercial and civil uses that are real-time and “mission critical” means that commercial users may be just as concerned in the future about privacy and security. Widespread adoption of real-time, on-line transaction services and SCADA systems for critical infrastructure systems creates a fundamentally new demand for security, privacy, and verifiability, especially where data flows involve billions of dollars or can put millions of lives at risk.

Third, widespread access by news media and others to advanced real-time sensor and communications systems may create an entirely different set of security and information protection concerns. With increasingly free access up and worldwide direct satellite broadcast down, television and radio news coverage will largely be outside of government control over content and timing. The availability of small, direct-uplink, high-capacity systems capable of supporting real-time video together with demands from news organisations for real-time information, unfiltered or uncensored by governments, is likely to produce substantial discomfort as security interests clash with claims of press freedom.

Implications for Arms Control Efforts

Just as these technologies have important consequences for the military and the practice and nature of war, so too do they have implications for arms control and disarmament efforts and regimes. The implications, however, are double-edged. First, new information technologies could prove to be important new tools in the cause of arms control, because of their potential uses for verification and information gathering. As powerful technologies spread beyond the armories of the mightiest nations into the commercial sector they also become available to the international arms control community. If sensor data can be bought, it can be bought for the purposes of arms control verification. These technologies increase information and transparency, and from an arms control perspective, that must, on balance, be good.

On the other hand, these new technologies also pose arms control challenges. The same cheap and powerful computing, communications and sensor capabilities that are revolutionising the global economy also put a whole new magnitude of military power within the reach of whomever has the knowledge and tools to take advantage of it. However, attempting to create a new arms control regime to contain these innovations — to impose old-style controls in order to limit diffusion of potentially dangerous technologies — is not likely either to be feasible or effective. Controls on railroads in turn-of-the-century Europe would have been unthinkable, despite the crucial role of railroads in the military mobilisation plans of the time — however important the railroad’s military uses, its civilian uses were of even greater importance. In the same way, restrictions upon information technologies with a view to limiting their military uses would of necessity limit their civilian uses as well.

These technologies are fast becoming the eyes, ears, and nerves of our society, and any concerted attempt to limit their spread would therefore be self-destructive as well as politically impossible. Today, mass market technologies such as desktop computers and GPS devices theoretically pose proliferation threats, but controlling such basic products would be impossible without severe economic and political repercussions. Furthermore, technological change now occurs over a cycle measured in months — far too fast for any legislative attempt at arms control to keep up with. In truth, any attempt at controlling the proliferation of information technology would be starkly irrelevant to the environment of today where the technological cutting edge moves ‘in the blink of an eye.’ It would therefore merely serve to imply progress where there was none and so disguise the futility of the underlying approach. In the end, we are better off with a real sense of vulnerability as the Faustian trade-off for technological capability than with a false sense of security bought at the price of economic progress — this, at least, should keep us on our toes.

Virtual Security: Technical Oversight, Simulated Foresight, and Political Blindspots in the Infosphere

James Der Derian*

To be means to be for the other, and through him, for oneself. Man has no internal sovereign territory; he is all and always on the boundary; looking within himself, he looks *in the eyes of the other* or *through the eyes of the other*... I cannot do without the other; I cannot become myself without the other; I must find myself in the other, finding the other in me.

Mikhail Bakhtin, *The Problems of Dostoevsky's Poetics*.

Alienation is no more: the Other as gaze, the Other as mirror, the Other as opacity — all are gone. Henceforward it is the transparency of others that represents absolute danger. Without the Other as mirror, as reflecting surface, consciousness of self is threatened with irradiation in the void... No longer the hell of other people, but the hell of the Same.

Jean Baudrillard, *The Transparency of Evil*.

In an escalating order of concern, four questions inform this chapter. How does one approach a phenomenon so ubiquitous yet so elusive as surveillance? How does one theorise — which from its Delphic origins (*thea* and *horao*) means ‘to attentively look outward at something’ — a technology that looks back at the theoriser with the reflected arrogance of science, a gaze that offers global knowledge dressed in the guise of objectivity and transparency? How does one criticise something that has been deemed vital not only to national security but also to corporate, environmental, family, and personal security? How does one offer a plausible alternative to the collective belief that we live in a world at risk, and that our ability to foresee, perhaps even to forestall, danger requires a technology of surveillance which can oversee everything and everybody?

There are some extant theoretical responses, but each comes with shortcomings. Modernism, wedded to the idea of progress through technology, is deeply implicated by surveillance in the workplace, at home,

*This chapter is an edited version of a presentation made to the Fourteenth Annual Ottawa NACD Verification Symposium, “Cyberspace and Outer Space: Transitional Challenges for Multilateral Verification in the 21st Century,” 12-15 March 1997, Montebello, Quebec, Canada. A version of this paper was presented at the 38th Annual Convention of the International Studies Association, “Coping With Insecurity: Threats More Than Enemies,” Toronto, Ontario, Canada, 18-22 March 1997.

on the battlefield, and indeed, by the mimesis of positivist modeling itself¹: it is hardly conducive to the kind of intellectual distancing needed for a critical inquiry. Pre-modernist approaches offer historical depth and narrative breadth, but cannot explain, let alone anticipate, the structural effects of rapid changes caused by innovations in surveillance techniques. Post-modernist approaches, like critical genealogies and intertextual analysis offer a deeper sensitivity for the de-territorialised, chrono-political, and global effects of surveillance, but often fall short in the area of policy alternatives.

This array of practical and political difficulties prompts many academics to take the high road of meta-theory, to theorise about theory, or, in my case, to put surveillance under surveillance. Aside from a few conceits offered as meta-theory, this will not be the strategy of this chapter — I've been there, done that.² Besides, I have come under other more powerful influences. I have been compelled to throw caution, commensurability, and the cloak of meta-theory to the winds, and to morph pre-, post-, and modernist approaches for this investigation into surveillance. I could provide a host of intellectual justifications, but the reason why has become too difficult to conceal: too many viewings of *The X-Files*. The programme's ('pre'- 'post'-erous) slogans have become my epistemological mantra: 'The truth is out there' (often *way* out there), 'Trust no one' (*especially* the truth-sayers), and 'The Government denies knowledge' (an acknowledgment of guilt, ignorance, *and* epistemic drift). Radical measures, perhaps, but after a year in which a presidential candidate exalts *Independence Day* for its American values (a movie in which a replica of the White House is bombed by aliens),³ the FBI's surveillance profiling turns a security guard at the Summer Olympics bombing 'from national hero to public zero' (a *Daily News*' headline from 15 August 1996)⁴, and International Relations (IR) continues to confront increasingly *irreal* events, there is

¹See Richard Ashley, "The eye of power: the politics of world modeling," *International Organization* 37:3 (Summer 1983), 495-535.

²See James Der Derian, *Antidiplomacy: Spies, Terror, Speed, and War* (Oxford: Blackwell, 1992), 19-39; and "Antidiplomacy, Intelligence Theory, and Surveillance Practice," *Intelligence and National Security Journal* (July 1993).

³*Independence Day* also made the 8 July covers of *Time* ("Aliens have landed!") and *Newsweek* ("Out there? — from *Independence Day* to *The X-Files*, America is Hooked on the Paranormal"). And as the corner ribbon: "Terror in the Gulf: How Shaky Are the Saudis?"

⁴"From national hero to public zero," *Daily News* (15 August 1996). When asked whether there is a real *X-Files* division at the FBI, former supervisory special agent Gregg McCrary replied: "As close as we come is the unit I was in, the 'Profiling Unit.' It deals with the behavioural sciences, and bizarre and unusual crimes — sex crimes, serial killers, etc. There isn't any real need for an *X-Files* because there aren't any aliens running around — but there's enough bizarre human behaviour to keep us busy." "The War of the Worlds: In an Alien Nation, Whom Do You Trust?" *Entertainment Weekly* (29 November 1996), 35.

an even greater need for one's theoretical reach to exceed a discipline's grasp (or what's the extraterrestrial for?).

So I am a confessed *X-File*-phile. In fact, the origin of this chapter stems from an invitation for a conference on surveillance in Vancouver, the very city where *The X-Files* is taped — an invitation that I could not refuse. When I returned to Canada to attend the Annual Meeting of the International Studies Association (ISA), those tireless purveyors of truth, FBI agents Scully and Mulder, inspired new investigations. Flashing my ISA badge to gain entry into panels, plenaries, and publishers' booths, I have discovered that alien forms have infiltrated into nearly all ranks of IR theory. They have come as green-blooded, shape-shifters (a.k.a., the constructivist cabal), resistance-is-futile borgs (the critical security studies thuggees), gender-bending droids (the feminist coven), and, of course, those big-headed, bug-eyed mutants (the post-structuralist conspiracy).

This is not good news to the Syndicate: on *The X-Files*, they are those 'old white guys' who run the whole show from a smoky room somewhere on the east coast of the U.S.; in International Relations — well, just scrub the smoke from the picture. The job of the Syndicate, as one tells Scully, "is to predict the future, and the best way to predict the future is to invent it"; not too far removed from the self-fulfilling prophecies of the 'neo(realist)-neo(liberal)' Synthesis in IR.⁵ But the Syndicate has developed a peculiar relationship with the aliens. Unable to destroy what they fear, they now seek to control the aliens, first by suborning the shape-shifters — one of whom, the Bounty Hunter, becomes employed as a very scary terminator — and then by setting up a big research programme called 'Purity Control,' whose goal is to extract DNA and other vital elements from the bug-eyed aliens for the production of hybrids (check your ISA programmes for details). This season opened with an episode in which Mulder was led to a Canadian farm tended by a cult-like community of clones. All of them were dead-ringers for his sister, Samantha, who, at eight, was abducted by aliens (or was it actually by the Syndicate?). When asked what the clones were seeking to achieve, she replies, "Hegemony." By the March sweeps, however, it is no longer clear whether the Syndicate controls the aliens, or the aliens had gained control of the Syndicate. Had the aliens come to save Earth from its own kind? Extraterrestrial eco-tourists on a mission of mercy? Or had they become pawns of the Syndicate — a kind of post-war solution for the fall of the 'evil empire'? Worse, was there actually no one in control, and everyone afraid to admit it? Stay tuned for the next ISA meeting.

Aliens aside, let me get my own meta-theoretical conceits out of the way. Surveillance is Heaven (God). Surveillance is Hell (Sartre). Surveillance is fetishised desire (Freud). Surveillance is herd resentment

⁵See Ole Wæver, "Figures of international thought: introducing persons instead of paradigms," *The Future of International Relations: Masters in the Making?* Iver B. Neumann and Ole Wæver, eds. (London and New York: Routledge, 1997), 1-37.

(Nietzsche). Surveillance is patriarchal (Lacan). Surveillance is good (the V-chip). Surveillance is bad (the Clipper chip). Surveillance disciplines (Foucault), dissuades (Virilio), simulates (Baudrillard). Surveillance is everywhere (Agent Mulder). Surveillance is in your head (Agent Scully). My sole philosophical aim, to paraphrase Gilles Deleuze (and to put in a plug for the new on-line journal, *Theory & Event*,⁶ is to make theory worthy of the event, not by determining the cause of an event, but by interpreting the powerful and often ambiguous effects of surveillance.

This means that this chapter comes uncomfortably close to the kind of media spasm that reduces all phenomena and events — revolutionary or not — to superficial and ephemeral forms. Probably the greatest challenge in an age of information revolution is to slow down, to down-shift from media-hype and fast-and-easy stereotypes, to down-play crisis mongering and crisis-management for more deliberative and experiential forms of analysis and decision-making. But this is not my immediate intention. This chapter moves from screen to screen, montage to holograms, sound-bites to buzz cuts, from substance to style — for nothing is so powerfully insubstantial, multiply mediated, and simulated as information — to alert us to the dangers rather than to pretend a solution for the most profound effects of the information revolution.

The bulk of my book *Antidiplomacy* is taken up with the theme that the current effects of surveillance cannot be isolated from the effects of simulation, and that they are more profoundly produced and sustained by an acceleration of pace rather than an occupation of space. My goal is to show how simulations through surveillance, from radar gun to spy satellite to computer screen, works as a technology and works on us as a technique of power through its ability to oversee and foresee, speed-up and slow down flows of information, capital, troops, refugees, drugs, viruses, and pollutants. In short, not the deep identities of geopolitics but the transparent differences of chronopolitics, where power is more ‘real’ in time than space, it comes from an exchange of signs rather than goods, and it is transparent and diffuse rather than material and discrete.⁷

Alloyed by the always renewable threat of terrorism, surveillance, simulation, and speed form the undertheorised, overdetermined currency of the information revolution, and as such, it is inseparable from the issue of security. National security is endangered by too little (or too much) information; computer security is necessary to prevent the theft or invirillation of information; the Securities and Exchange Commission draws a line between inside and outside information, and secures the borders of high

⁶http://muse.jhu.edu./journals/theory_&_event

⁷See James Der Derian, *Antidiplomacy: Spies, Terror, Speed, and War* (Oxford: Blackwell, 1992); and James Der Derian, “The (S)pace of International Relations: Simulation, Surveillance, and Speed,” *International Studies Quarterly* 34:3 (September 1990), 295-310.

capitalism; and at conferences like the ISA's we negotiate various meanings of security through our sharing (persuasion), withholding (manipulation), or distortion (propaganda) of information. We can freeze-frame factors of surveillance, simulation, and speed in all of these forms of security. But my brief is to focus on one particular aspect, the new surveillance effects of the so-called 'Information Revolution.' Again, this is my attempt to get at the truth of the matter while trusting no single version.

Cut to CNN, General Shalikashvili, testifying before the Senate Foreign Relations Committee on the bombing in Saudi Arabia, 9 July 1996: "Terrorism will always take the most indirect approach."

Follow with Paul Verhoeven, director of *RoboCop*, *Total Recall*, and (regretfully) *Showgirls*: "The U.S. is desperately in search of an enemy. The communists were the enemy, and the Nazi's before them, but now that wonderful enemy everyone can fight has been lost. Alien sci-fi films give us a terrifying enemy that's politically correct. They're bad. They're evil, and they're not even human."

Buzzcut back to Captain Kelvin Davis inside Kuwait City: "I hate to say it, but once we got rolling it was like a training exercise with live people running around. Our training exercises are a lot harder."⁸

Buzzcut forward to now (mid-March 1997), and the National Training Center (NTC) in the high Mojave Desert, where Fort Hood's 1st Brigade of the 4th Infantry Division, kitted out with \$250 million in computers, satellites, and digital links, is about to face the Army's OPFOR ('Opposition force') for the fourth digitised rotation at the NTC. From *USA Today Online*, "Cybersoldiers test weapons of high-tech war" (6 March 1997):

The home team will try to find the Achilles' heel of the new system. On recent maneuvers, the high-tech suppliers swarming over the field headquarters, the Tactical Operations Center (TOC), make it look like a movie set with the soldiers as actors. Five dozen new devices are being prepared for action. The soldiers are making progress. In less than six hours, the sweaty troops have transformed an empty clearing into a computerized control center.

"Barnum and Bailey has got nothing on us," says Capt. Packard Mills, who oversees the TOC's operations.

Outside, the tent and camouflage look typical old Army except for the satellite dish. Inside, video screens are coming to life amid the clutter. It's a long way from chalkboards and grease pencils. And a long way from battle-ready.

"When you first set it up, it looks like a scene in Star Trek when you just got hit by the Klingons," Mills concedes.

"We've got people tripping over cables and plugging into the wrong thing. It's keeping me busy," says a harried Sgt. 1st Class Tyler Vandesteeg. He's one of an emerging class: a Webmaster of war.

⁸*Newsweek*, 11 March 1991, 17.

Cut and Paste: For the comfort of origins, I would say this investigation begins on a hilltop in the Mojave Desert, where I had been sent by *Wired* magazine to write about ‘Operation Desert Hammer IV,’ the first ‘digitised’ rotation of troops through the National Training Center at Fort Irwin. At the high end of the lethality spectrum there was the improved M1A2 Abrams main battle tank, carrying an IVIS (Inter-Vehicular Information System — ‘Knowledge is Power’ says the brochure) which could collect real-time battlefield data from overhead JSTAR aircraft (Joint Surveillance and Target Attack Radar System), Pioneer unmanned aerial vehicles equipped with video cameras, and global positioning satellite systems (GPS) to display icons of friendlies and foes on a computer-generated map overlay. At the low end, there was the ‘21st Century Land Warrior’ (also called ‘Warfighter,’ but never ‘soldier’ or ‘infantryman’), who came equipped with augmented day and night vision scopes mounted on his M-16, a GPS, 8-millimetre video camera and 1-inch ocular LED screen connected by a flexible arm to his kevlar, and a 486 Lightweight Computer Unit in his backpack, all wired for voice or digital-burst communication to a BattleSpace Command Vehicle with an All Source Analysis System which could collate the information and coordinate the attack through a customised Windows programme. ‘Using the power of the computer microprocessor and digital electronics’, digitisation was designed to be a ‘force multiplier’: the ‘horizontal integration of information nodes’ and the ‘exchange of real-time information and data’ was going ‘to establish friendly force dominance of enemy forces.’ In short, the Army was creating a C⁴I bundle (command, control, communication, computers and intelligence) of soft-, hard-, and wetware for the coming information war.

But up on that hilltop, as the simulated battle began at dawn with Black Hawks and Apaches flying so close to the deck they were below us, F-16s and A-10s roaring overhead, followed by the dust and smoke trails of M1 tanks, it was difficult to tell just what was going on. Our personable handler, Major Childress, former commander of an OPFOR unit and now head of public affairs at the NTC, did his best to explain, providing a running commentary for what we could see — and also what we could hear as we eavesdropped on the radio traffic among the combatants. Accounts of confusion and in more than one instance, fratricide or ‘friendly fire’, were overheard. But it was an aside from another member of the press that was to provide some much-needed historical perspective. For the most part my media cohort avoided me. I would like to think it was because of my intelligent questions and refusal to suck up to the brass, but it was more likely my failure to observe the press dress-code of Banana Republic safari vests, surplus fatigue pants, and desert jump boots. But at that moment, Austin Bay, ex-Army, military historian, and co-author of *A Quick and Dirty Guide to War*, turned to me and said: “It’s just like Salisbury Plain.” I knowingly nodded, but before I could ask what this had to do with lunch, we were interrupted by ‘Krasnovians’ in simulated T-80 tanks, who were about to overrun our perch as they outflanked the 24th Mechanized. We got the order to move, and during a dash through the desert in an humvee, Bay filled me in. Salisbury Plain was the British forerunner of the NTC, and it was there in the

1920s that troops, tanks, and airplanes, aided by wireless, came together for the first coordinated demonstration of mobile armored warfare. It was, said Bay, a revolution.

Flashforward. A few years later, I had the opportunity to check out his story. Killing time at the Bodleian Library at Oxford, I began searching the microfiche roles of the *Daily Telegraph*, not so much out of curiosity about the event as how it was reported: Was it recognised as a revolution at the time? I chose the *Telegraph* because I knew that Liddell Hart had been its military correspondent — and much more.⁹ Hart, a decorated officer during the First World War, had made a name for himself as an early proponent for mechanisation, for a ‘New Model’ army based on ‘tank marines’ ready to use ‘the indirect approach,’ to fight highly mobile battles on land as the navy fought at sea. At a time when Germany was disarming under the agreements of the Treaty of Versailles, and the French, under the direction of war minister Andre Maginot, were re-casting trench warfare and protecting falling birth rates by a defensive frontier of concrete, the British had the luxury (no real enemy threat), the temperament (no desire to repeat the slaughter of the previous war), and the technology (still the leader in industrial innovation) to experiment.¹⁰ From August 1927 to 1931, Salisbury Plain became the premier laboratory of a new form of warfare. Armored cars, light and medium tanks, motorized artillery, infantry in trucks and half-tracks, and even the odd horse were on the move, first during the day, later even at night. Hart’s initial reports on the first exercises in 1927 were somewhat disdainful; aircraft were simulated, coloured flags stood in for anti-tank guns, and radios, where in evidence, rarely worked. But by the ‘Armoured Force’ exercise of 1928, the tone begins to change. One hundred and fifty wireless sets were used for a maneuver which left an assembled group of brass and Members of Parliament highly impressed. Hart considered the exercises a success in 1931, when the 1st Brigade Royal Tank Regiment, taking orders by radio, managed to maneuver through the fog in concert to arrive on time before a gathering of the Army Council.

Reopen USA Today Online, “Cybersoldiers test weapons of high-tech war”

Assuming the digital force passes muster, the Army could soon be asking Congress for lots more money. The General Accounting Office estimates it would cost \$4 billion to outfit all 10 active-duty divisions. But Maj. Gen. Robert Scales, author of the official

⁹In a footnote — the *only* footnote — in his most popular book, *Strategy*, Hart’s contribution to the Salisbury Plain exercises is acknowledged: “The strategy and tactics of the Mongols are dealt with more fully in the author’s earlier book *Great Captains Unveiled* — which was chosen for the first experimental Mechanized Force in 1927.” See B.H. Liddell Hart, *Strategy*, second revised edition (New York: Signet, 1974), 62.

¹⁰See B.H. Liddell Hart, *Paris, or The Future of War* (New York: 1925); and Brian Bond and Martin Alexander, “Liddell Hart and De Gaulle: The Doctrines of Limited Liability and Mobile Defence,” *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, Gordon Craig and Felix Gilbert, eds., (Oxford: Clarendon Press, 1986), 598-623.

Army history of the gulf war, warns it will be money ill-spent if all the Army does is perfect war as we know it today. That's what France did after World War I with its Maginot line, a defence easily overrun because it failed to anticipate Adolf Hitler's high-speed mechanized attack.

From paper to film to screen to keyboard to screen to disk to screen to keyboard to disk to paper. What follows is a brief sampling of his fluent — and influential — accounts in the *Daily Telegraph* of the first exercises on Salisbury Plain in 1927. On the front pages were stories about the Naval Conference in Geneva (most notably, friction between the U.S. and Great Britain — with Japanese support — on cruiser tonnage and gun size), death sentences for Nicola Sacco and Bartolomeo Vanzetti, Italian anarchists, “Trotsky's Victory — Stalin's Move Checked — Surprise for Moscow,” ‘a world not ripe for disarmament.’ Hart's early articles were on page five or later, mixed in with military bands and tanks bogged down in the mud; gradually the articles moved up to page one. Entertainment is liberally mixed with education. They read like the bread and circus of late empires — much like our own evening news.

The Daily Telegraph, Monday 1 August 1927, “Tidworth Tattoo — Modern War Staged,”

Tidworth is the home of the mechanized force which is expected to play a great part in the future development of the Army. Therefore it is fitting that the star attraction of the Southern Command Tattoo, which commenced before many thousands of people in the arena in Tidworth on Saturday night, should be a ‘battle’ in which the latest mechanized units take part. When an interesting programme was nearing its end, the searchlights flashed on to an Eastern fort, where picturesque Eastern marauders were taking rest. Almost immediately the battle began. A signal for assistance sent by the British commander brought a reconnaissance car to the spot, and, following quickly in its wake, came the mechanized machine guns, the latest swift-moving tankettes spitting fire, with a self-propelled gun giving protection to the British force, and in doing so adding to the din. The mobility of the new armoured units enhanced the realism of the episode, and undoubtedly this battle will prove one of the most attractive features of the performances.

There is plenty of variety in the programme, for following community singing and the fanfare of trumpets, massed bands of the 2nd Cavalry and 7th Infantry Brigades enter the arena in peace-time uniform, the cavalry bandsmen mounted, and all playing delightful music... Lancer trick riders carry through amazing feats and some remarkable jumping, the obstacles including a donkey and cart, bed, fire hoop, and fire bar.... The concluding item before the reassembling of the soldier actors is a display by the Royal Air Force in illuminated aeroplanes...

The tattoo was a huge success on its first night and will be continued during the week... the railway companies are running excursions from all over the South of England and buses are expected to bring many hundreds of spectators.¹¹

¹¹“Tidworth Tattoo — Modern War Staged,” *The Daily Telegraph*, 1 August 1927, 6.

Flash sideways. To “Hearing a Face — Television Broadcast,” *Daily Telegraph* article next to Hart’s first account of the ‘Tidworth Tattoo’, 1 August 1927.

Giving a broadcast lecture at the British Empire Exhibition at Edinburgh on Saturday night, Mr. J.L. Baird, the inventor of television, said he had asked three chance acquaintances the meaning of the word ‘television.’ One said that it was an island off the Coast of Africa, the second that it was a form of telepathy, and the third that it was a kidney disease. Television meant actually seeing by wireless. The scene was first turned into a sound, which was then broadcast, and turned back into an image at the receiver. Every face had its own particular sound.

A phonograph record was then played on which the television sound of Mr. Baird’s face had been recorded. It sounded something like the rasp of a file with a peculiar rhythmic whistle underlying it. This was broadcast by the B.B.C., so that listeners for the first time in history had the opportunity of hearing what a face sounded like. The lecturer went on to describe his discovery of television, and said that the first person ever seen by television was an office boy, who had to be bribed with 2s 6d to submit to the experiment. The latest development of television had rendered it possible to see in total darkness, invisible rays being used. Steady progress was being made in developing the invention to a commercial stage, and he hoped that television would very shortly be available to the general public.¹²

Historical note. One year later, the same year that motorised and wireless transmissions were linked in simulated warfare, similar breakthroughs in television were made by engineers at General Electric. From experimental station ‘W2AXAD’ they broadcast the second-ever television image, about the size of an index card. What did they choose to broadcast? A simulation of a missile attack on New York City. The point of view was from the missile, a flight ending in an explosion, then nothing.¹³

Hammering the point of the missile home. Paul Virilio, in his preface to the English edition of *War and Cinema*, writes: “A war of pictures and sounds is replacing the war of objects (projectiles and missiles). In a technicians’ version of an all-seeing Divinity, ever ruling out accident and surprise, the drive is on for a general system of illumination that will allow everything to be seen and known, at every moment and in every place.”¹⁴

Daily Telegraph, “Tanks ‘In Action’ on Salisbury Plain” — Bombing Attack Thrills — Triumph for Mechanised Army, by Captain B.H. Liddell Hart, Tidworth, Friday Night,

¹²“Hearing a Face — Television Broadcast,” *The Daily Telegraph*, 1 August 1927, 6.

¹³Eric Barnouw, *A Tower in Babel: A History of Broadcasting in the United States*, vol. I (New York: Oxford University Press, 1966), 231.

¹⁴Paul Virilio, *War and Cinema: The Logistics of Perception*, trans. Patrick Camiller (New York: Verso, 1989), 4.

20 August 1927.

To-day the training proper of Mechanised Force was inaugurated on Salisbury Plain. More definite localization is impossible because the exercise covered too wide an area, and that is a point to the good, for an immense broadening not only of space but of mental horizons is the only way in which full value can be obtained from these tentative experiments in mechanized warfare...

Further, one discovers that common-sense again has overcome another of the apparent drawbacks of the Mechanical Force as originally constituted — by distributing this mechanical potpourri into groups according to the qualities of the mechanized units which compose it. Thus for marches it is divided into a fast group, comprising only the Armoured Car companies, whose normal rate of march is reckoned at 25 m.p.h.; a medium group, comprising light batteries, field companies R.E., machine-gun battalions, and mechanized transport, all conveyed in semi-track or six-wheeled vehicles, whose normal rate of march is reckoned at 10 m.p.h.; a slow group, composed of tanks, tankettes, and mechanised artillery, whose normal rate is reckoned at 7 m.p.h.. These normal rates are, of course, on the conservative side, with the sound object of allowing for hindrances and reducing wear and tear.

‘Attacks from the Air’

To-day’s test was a ‘peace march by day,’ a phrase which implies not that it was under peace conditions, but that it was conceived as taking place in rear of the advanced forces and so not likely to encounter the enemy. But the serpentine column which wound its length in coils over a distance of some thirty-two miles, suffered bombing and machine-gun attacks from the air, when checked by road blocks, and had also to pass through an imaginary gassed area — presumably by enemy aircraft.

‘The First Test’

...[T]he umpire created an impassable block by the declaration that a vehicle had broken down — or been blown up. It was about as severe a test as could have been imposed on a new-born force, and it was not surprising that twelve minutes elapsed before the first vehicle moved off the road to lead the way along an alternative route hurriedly reconnoitred on the flank of the sunken road a route which, incidentally, enabled the whole column to display their cross-country ability and to get on to another and wider road altogether... At this juncture flights of single-seater Gamecocks came diving over the trees and swooped down on the vehicles in the road, dropping ‘flour’ bombs and firing their machine guns. So low did they come, so spectacular was their handling of these bullet-like machines that the spectators had a series of thrills. That they would have caused heavy casualties there is little doubt, but even in a stage-managed affair they were late enough behind time to lose several minutes of their opportunity, and in war, given greater practice by the mechanised troops, it is not often that such an ideal obstacle, such

a heaven-sent breakdown, and the appearance of the enemy aircraft would all three combine...¹⁵

‘Mechanical Gods’ of Modern Warfare — Tanks in Night Move — Driving feat in the Dark, Hart, 23 August 1927.

Between 10 p.m. last night and daybreak this morning, the Mechanised Force, under Colonel R.J. Collins, carried out the second of its trial schemes — a night march along some fourteen miles of rain-steeped roads to a rendezvous near the Bustard, north-east of Shrewton, and a return in two columns across country... If the test was severe for a newly-assembled and still inchoate force, the condition increases its severity to such a pitch that even an ardent believer in mechanisation was astonished at the practically hundred percent fulfilment which was achieved.

‘Primeval Monsters’

I watched the column for a point close to Stonehenge, and in the apt and eerie setting of that dreary monolith-surmounted down, at midnight, little imagination was needed to picture it as the passage of a herd of primeval monsters or legendary dragons, with glassy eyes shining in the darkness, fiery breath, and scale-coated body. So irresistible was the impression that I pity any belated motorist who met them, unprepared on his homeward road. And the passage by Stonehenge had also a symbolical effect, for there the gods of the prehistoric past could be conceived as watching from their long-abandoned altars the procession of the mechanical gods of modern man — both equally the creation of man, but the one expressing the static mentality of the past, and the other the ever-changing, restless motion of the mind of to-day.¹⁶

Historical sidebar: The next day, Sacco and Vanzetti were electrocuted.

Impressed, but not convinced, the British general staff failed to learn the lessons of armored warfare wargamed on Salisbury Plain. Defeated, and some might even say rendered desperate by disarmament and the fiscal restraints imposed by reparations, the German staff did not. They carefully studied Hart’s writings as well as Brigadier Charles Broad’s 1929 booklet, *Mechanized and Armoured Formations*, which conceived of the tank not as a support for infantry but as a fast-moving independent force that could create shock, chaos, and demoralisation in enemy forces. In 1939, they applied those lessons with spectacular results.

¹⁵“Tanks ‘In Action’ on Salisbury Plain,” *The Daily Telegraph*, 20 August 1927.

¹⁶“Mechanical Gods’ of Modern Warfare,” *The Daily Telegraph*, 23 August 1927, 11.

Exterior. Bodleian. Film-noirish voice-over: Why, when Austin Bay looked down from the desert hillside, did he see Salisbury Plain from his desert perch, rather than Poland or France, collapsing under the speed and fury of the Panzer *Blitzkrieg*? And if we were the British, who then, or rather, who now, are the Germans?

Travelling shot. It would take a few more manoeuvres in the field before I would find an answer. Two tours at Fort Irwin; two trips to the annual Interservice/Industry Training Systems Conference in Orlando, where simulation industries like Boeing, Lockheed, Loral, Silicon Graphics, Evans and Sutherland paraded their wares to their military; Central Command in Tampa, on the heels of Schwarzkopf and the wargame that took us to Iraq, Internal Look 90; Fort Knox, home to our dwindling gold supply and to the ultramodern tank SIMNET; Hohenfels, Germany, to observe the 1st Armored Division as they ‘peacegamed’ their intervention into Bosnia; Advanced Research Projects Agency (ARPA) in Virginia, to learn how the Synthetic Theater of War (STOW) was created to integrate virtual, live, and constructive simulations of war in real time; and, finally, the Office of Net Assessment at The Pentagon, where I found the Yoda of the ‘Revolution in Military Affairs.’

Outtakes. In many ways, the itinerary for the journey was determined by an air-express package that I received from the Office of the Secretary of the Army the day before I was to leave for Fort Irwin. Although it did not come with an acronym de-coder ring, I was able to make some sense of it. Officially, it was identified as the press kit for the Advanced Warfighting Experiment (‘AWE’). But this did not do it justice. Collected in a large three-ring binder with the triangle logo for ‘The Digital Battlefield’ on the cover — satellite, helicopter, and tank in each corner, connected by lightning bolts to a Warfighter in the middle — were over thirty press releases, brochures, and articles on the Army of the future. In style and content they replicated the corporate publications that I had picked up three years earlier in Orlando. Computer-generated images were mixed in with all kinds of fonts and graphics. Indeed, it all looked a bit like *Wired*.

Leading the paper charge of the simulation brigade was a prolegomenon from the office of the Chief of Staff. It bears quotation, not just for its Toffleresque rhetoric, but for its encapsulation of the rationale behind the 21st Century Army, Force XXI:

Today, we are on a threshold of a new era, and we must proceed into it decisively. Today the Industrial Age is being superseded by the Information Age, the Third Wave, hard on the heels of the agrarian industrial eras. Our present Army is well-configured to fight and win in the late Industrial Age, and we can handle Agrarian-Age foes as well. We have begun to move into Third Wave Warfare, to evolve a new force for a new century — Force XXI.

A series of categorical imperatives for the Force XXI follow. They call for nothing short of a paradigm-shift:

Force XXI will represent a new way of thinking for a new wave of warfare. We must be strategically flexible and more lethal. We must leverage the power of the best soldiers in our history through the use of state-of-the-art simulations and realistic, simulator enhanced training. We must accommodate the wide-range of operations being demanded of us. Intellectual change leads to physical change — the mental shift goes before the software and hardware.

One brochure, slicker than all the rest, maps out how the Army was making the future present. It bears the short, yet pretentious, title: “The Vision.” It leads with the now common litany of the national security mandarins, that with the fall of the Berlin wall, the dissolution of the Soviet Union, the rise of regional powers, and the advent of MTV (reading between the lines here) no one can safely predict what is to come, nor who is to be the next enemy. The Chief of Staff, General Gordon Sullivan, asks, “What’s next?” and answers, “No one knows.” Therefore, “We are relatively safe in predicting, however, that the strategic environment in the next decade will be dynamic, uncertain, and unstable.” Military jargon married to ‘technospeak’ usually calls for high waders, so I was surprised to find, a few pages later, a box in the section on ‘Exploit Modeling and Simulation’ that read, well, like a good cyberpunk novel:

The Distributed Simulation Internet, projected for the turn of the century is a creature of another order entirely from SIMNET. Ten thousand linked simulators! Entire literal armies online, Global real-time, broadband, fiber-optic, satellite-assisted, military simulation networking. And not just connected, not just simulated. Seamless.

It gets better, and for good reason: it was written by Bruce Sterling for *Wired*. What does it mean when *Wired* is appropriated for the Army’s ‘Vision’? Perhaps in the idea-void of post-Cold War strategy, shortly after ‘enlargement’ (of democracy and free markets) is offered by the Clinton Administration as a plausible foreign policy replacement for ‘containment’ (of the ‘Soviet Threat’), it is wholly understandable that the Army’s visionary reach should exceed its rhetorical grasp. Indeed, I had come across much stranger intertexts in the course of the visit to Fort Irwin. One briefer had described the intensity of Desert Hammer as somewhere between the Gulf War and *Red Storm Rising*. Not such a surprise, considering that former Vice President Quayle had once defended Star Wars (the anti-missile system, not the movie) by citing the same Clancy novel.

Or perhaps something else was going on; something I sensed at the NTC when I was in the M1A2 tank, and again when I was granted videotaping access not once but twice to the Star Wars building, command central of the NTC from which the battles are run and to which the signals from hilltop remote video cameras and overhead reconnaissance are beamed for the after-action videotape reviews. Was my presence at Fort Irwin — no less so than Bruce Sterling’s in ‘The Vision’ — just one more tactical

exercise in the Army's much-vaunted Information War? Was journalistic simulation one more front for the successor to Salisbury Plain?

As early as 1964, after reading a breathless promotional account of the 'Cyborg' under development by General Electric and the military (from the photographs it looked like a robotic elephant), Lewis Mumford warned of the coming of a new 'technological exhibitionism.' Thirty years on, was I bearing witness to an even more powerful, possibly perverse hybrid? What happens when you combine media voyeurism, technological exhibitionism, and strategic simulations? News flash: In the 21st Century Army, you get the cyber-deterrent.

If this sounds far-fetched, remember the worst-case scenario that currently underlies strategic thinking. As CIA director James Woolsey put it at his confirmation hearings, a "bewildering variety of poisonous snakes" has sprung forth from the slain dragon. With the dragon went the mighty, if mainly illusory, deterrence value of nuclear weapons. On a quest since Vietnam (to fight only quick, popular, winnable wars), and imbued by the spirit of Sun Tzu ("Those skilled in war subdue the enemy's army without battle"), the 21st Century Army has perhaps now found in the cyber-deterrent its Holy Grail. It is fast, digitised, and as spectacular in simulation as it is global in surveillance. The digitised option also has the advantage of being out of reach of all but the richest 'rogues.' And it makes a hell of a 'photo-op.'

Moreover, the digitized deterrence machine bears an important similarity to its nuclear counterpart: it does not *necessarily* have to work in order to be effective. Its power lies in a symbolic exchange of metaphysical signs — give or take the odd reality-check in the desert to bring religion to the doubters. Hence spectacles like Desert Hammer IV, to render visible and plausible the cyber-deterrent for all those potential snakes that might not have sufficiently learned the over-hyped lessons of the first (if prototypical) cyberwar, Desert Storm.

Once again the desert functions as backdrop for the melodrama of national security. With an assist from Disneyland, Hollywood, and Silicon Valley, the National Training Center, full of video cameras, computerized special effects, not to mention thrilling rides, has superseded Los Alamos and the Nevada Test Site to become the premier production set for the next generation of U.S. strategic superiority. Can the Army go on to win the information war without firing another (real) shot? Of slightly lesser concern, can one conduct a critical inquiry of the information war without becoming, well, just another informant for it, a box in the Army's sequel issue, '(Re)Visions'?

Cut and run (and paste). Combat and Maneuver Training Center (CMTC), Hofenfels, Germany.

The U.S. Army owns, or more precisely, has 'manoeuvre rights' over a significant piece of real estate in southern Germany, 178 square kilometers worth in Hohenfels alone. Spread out over the State of Bavaria

like an isosceles triangle are the three major sites of the U.S. Seventh Army Training Command, through which the European-based U.S. troops, as well as some units from the British, Spanish, Canadian, and German armies and the Dutch marines, rotate through for some laser-simulated warfare as well as for live-fire exercises. The centres have an interesting heritage. Grafenwoehr, the oldest, was set up by the Royal Bavarian Army in 1907 to ‘play’ some of the earliest *Kriegsspiele*, or war games. It served as the southern tactical arm of the northern Prussian head, most infamously represented by Count von Schleiffen, Chief of the General Staff, who, in 1905, designed the famous Schleiffen Plan that was supposed to anticipate the next German conflict. Instead, its iron-clad ‘war by timetable’ helped to precipitate the First World War as one mobilisation triggered a cascade of others throughout Europe. The two other training centres owe their origins to Hitler’s rejection of the Treaty of Versailles, the peace of the victors of the First World War which included the humiliating 100,000 troop limitation for Germany. Rapidly filling up the ranks with new conscripts, the *Wehrmacht* found itself short on training space. Grafenwoehr was expanded, and two new sites were created: Wildflecken in 1937 for the IX German Corps, and Hohenfels in 1938 for the VII German Corps. It was here that the lessons of Salisbury Plain were applied.

The morning I drove past the front gate and into the Hohenfels Combat Maneuver Training Center, I learned a less-known part of its history. The tank-crossing sign, resembling more First World War lead toys than the M1 behemoths that skidded up the hill ahead of me, momentarily caught my attention. But it was the more conventional warning sign for “Cobblestones: Slippery When Wet” that seemed out of place. I later asked my handler, the very smart, very affable Colonel Wallace, why the short strip of quaint cobblestone interrupted the finely graded, modern asphalt road into the base. He thought it had been left intact as a tribute to the Polish construction workers. Later I filled in the blanks: Hohenfels, begun in 1938 and finished in 1940, had evidently been built by Polish *sklavenarbeiter*, slave labour. Wars, when gamed, tend to lose their history of blood and deception: “Slippery When Wet” joined ‘Trust no one’ as my coda during my visit to Hohenfels.

The reason I was there had taken on a special urgency. Two weeks before my arrival at Hohenfels, NATO air strikes on Bosnian Serb ammunition dumps triggered the hostage taking of over 300 UN peacekeepers. The ‘cold peace’ flared hot when French soldiers in Sarajevo fought back after Bosnian Serbs disguised in French uniforms and UN blue helmets tried to take the Vrbanja Bridge. Britain and France announced plans to send a rapid reaction force: debate ensued as to whether it would be under UN command — and whether the new artillery, armoured vehicles, and helicopters would be painted UN-white or sovereign-camouflage. President Clinton, breaking with the stated policy of only providing U.S. troops in the event of best and worst case scenarios — to monitor a peace accord or to cover a UN withdrawal — suddenly announced that he was ready to ‘temporarily’ send troops in support of the British and French forces. But morning-after polls and the shutdown of a U.S. F-16 pilot by the Serbs quickly reversed that readiness. In fact, as I drove through Hohenfels for my morning briefing I spied in

the *Stars and Stripes* newspaper box in front of the PX Burger King a tall headline and a big photo: “A Hero’s Welcome”...“Air Force Pilot Capt. Scott F. O’Grady looks mighty glad to be back — alive — at Aviano AB.”

It seemed like the right time to come to Hohenfels to observe an ‘Operation other than War.’ Just what that meant was supposed to be the subject of the morning brief. But there was some initial confusion, not least because somewhere between the time of my fax-barrage requesting a visit to the base and my arrival, a name-change had taken place. ‘Operations other than War’ had been replaced by the more anodyne ‘Stability Operations.’ Word had not quite made its way through the ranks, and people kept shifting back and forth between the two. The confusion mounted as I sat in a darkened theater with my two handlers, Captain Fisher and Colonel Wallace, and listened to the opening to Major Demike’s multimedia, name-negating brief. The Major was clearly in a ‘take-no-prisoners’ attitude toward the English language: ‘Army units from USAREUR (troops in Europe) rotate through the CMTC (I got that one) at least once a year for 21 days of Force-on-Opfor training’ (good guys vs. bad guys), ‘situational training with MILES in the Box’ (dial-a-scenario field exercises using lasers rather than bullets), ‘BBS training’ (not bulletin-board systems, but networked computer battle simulations with units based elsewhere), and ‘after-action reviews’ (video presentations of what went wrong on the battlefield).

It was all very impressive, but after five years of research on wargames and probably one too many jarring rides in a humvee, I had just about reached my tolerance for military speak. I had gone one brief too far, and I was ready to go in search of that faceless desk-jockey sitting somewhere in an inner-ring, windowless office of the Pentagon, whose sole mission was to regularly abbreviate and, if necessary, change the name of anything in the military that becomes decipherable to the layman before its half-life of usefulness is over.

But it would have to wait until after the ‘mother of all techno-briefs.’ Major Demike got into it with vigour: “We have at CMTC the most realistic battlefield. The instrumentation system is state of the art. No other training centre in the world has an instrumentation system like ours. It is the best in the world.” He skipped through technology like the MILES (Multiple Integrated Laser Engagement System) for firing and recording laser hits, the microwave relays which allowed for near real-time production of the video after-action reviews, and the simulated mortar and artillery fire. To punctuate the point, Colonel Wallace stepped in: “Once a unit goes into the Box, with the exception that they’re shooting laser bullets, and that a guy, instead of falling down with a gunshot wound, will read from a card he’s carrying in his pocket how badly hurt he is, virtually everything we do is real. There’s nothing simulated in the Box.”

The Major became more animated when he moved into the details of the technological capability of the CMTC. Instrumentation systems gather and process battlefield data that observer/controllers use to provide instant feedback for both sides of the operation. There is a seamless web of command and

control between Building 100 (the ‘Star Wars’) centre from which the battles are run, and the troops in the Box. For instance, simulated artillery attacks are launched via Sun Microsystem work stations, and hits are assessed according to probability software which calculates trajectories, terrain, and the grid locations of vehicles and troops which are constantly updated by Global Positioning Systems. Hits are then transmitted to each vehicle, as a ‘commo kill’ (communications knocked out), near miss, or ‘catastrophically destroyed.’ News of a simulated death comes in a female voice: the female voice gets the attention of the adrenalised or battle-fatigued soldier. My query about what happens when women eventually get to join in on the combat simulations was met with a blank stare by the Major, but the Colonel picked up on it: the female voice will always stand out from the background of male ones. My stock question about the realism of the simulated battlefield received the stock answer, but with a raising of the technological ante: the National Training Center, CMTC’s better-known state-side rival in the Mojave desert (see *Wired*, 2:09) was still using the first generation of MILES to simulate weapons effects, while they had the interactive MILES 2 with data communication interface (\$9,000 a unit). ‘Everything is wired’ said the Major, who clearly had an ear for a soundbite.

After a long slog through computer graphics on the organisation and function of the CMTC, we finally got to the geopolitical gist of tomorrow’s ‘Stability Operation.’ Up came a map of ‘Danubia,’ trisected into ‘Sowenia,’ ‘Vilslakia,’ ‘Juraland,’ and, looking like very much like a small fiefdom among them, the CMTC. The Major’s pointer started to fly: “Three separate countries have split off from Danubia — Sowenia and Vilslakia are at odds with each other. When we want to transition into high-intensity conflict, we have Juraland, which has heavy forces, come in on the side of one or other of the parties.” Prodded to just once utter the word ‘Bosnia,’ he would go no further, except to say that the scenario was based on intelligence sources, CNN reports, and the ‘threat books.’ But for my benefit he did add, “You don’t have to be a rocket scientist to figure out what this is modelled on.”

No rocket scientist, I resorted to a kind of semiotics to sort out the countries. The new countries of the disintegrating Danubia bore some obvious similarities to the region of Yugoslavia: to the former republic, now independent state of Slovenia, or perhaps the western enclave of Slavonia contested by the Croats and Serbs; and, of course, to the Jural mountain range. ‘Vilslakia’ remained a mystery. The countries surrounding Danubia were familiar enough that I sought out my own intelligence source, Microsoft’s CD-ROM version of *Cinermania ‘95*. It was not needed for the country to the northwest: ‘Teutonia’ referred back to the early Germanic tribes. However, ‘Freedonia’ to the northeast of Danubia was clearly taken from the 1933 war satire *Duck Soup*, in which Groucho Marx so effectively played the power-hungry dictator of said-country that the real dictator Mussolini banned the film from Italy. And below Danubia was ‘Ruritania,’ the country in the clouds which provided the surreal setting for W.C. Field’s 1941 classic, *Never Give a Sucker an Even Break*. What should one make of the Army’s strange choice of simulated countries? Probably nothing much, except that some wargamer had a sense of humour as well as of history. But I was left wondering: play by the intertext, die by the intertext?

The briefing ended with a short video of a ‘Stability Operation.’ By way of introduction, Colonel Wallace informed me that “none of this stuff is staged, it’s all from live footage taken by the Viper video teams in the Box.” Before I can fully enjoy the Colonel’s knack for paradox, the lights dim, the screen flickers, and Graham Nash is singing something about ‘soldiers of peace just playing the game.’ The first clip is of a confrontation between partisans and soldiers that escalates into heated words; the last is in the same tent, with handshakes and professions of friendship being exchanged. In between, UN convoys are stopped by civilians, soldiers go down, wounded or dead, a body-bagged corpse is spat upon by a partisan, food supplies are hijacked by townspeople, a female member of the media gets shoved around, an explosion and panic in the town streets, a sniper fires on a humvee, dogs sniff for explosives, infiltrators are caught in a nightscope, a UN flag waves defiantly, and an old man drops to his knees in the mud in front of a humvee, begging for food. More in the sentimental aesthetic of an AT&T ‘advert’ than an hyperreal MTV clip, it is strangely moving. I am disarmed by it.

But the mood shifts quickly when the Major concludes the briefing by handing me a three-inch thick pile of documents. The rest of the day was a whirlwind of briefs-to-go. First stop was the ‘Warlord Simulation Center,’ full of desktops and more Sun Microsystems for planning, preparing, and running simulations in the Box, out of the Box, or through the cyber-Box — that is, simulation networking (SIMNET), ‘remoting via satellite in and out of the Box to anywhere in the world.’ Next stop was a cavernous warehouse, full of MILES gear under the watchful eye of Sergeant Kraus, who probably gave the best brief of the day. A man who clearly loves his job — or just eager for some human company — he was as articulate as his lasers (“instead of a bullet it sends out 120 words on a laser beam, in the center are eight kill words, anything else is a wound or near miss”), as he made his way through the various shapes, types, and generations of laser and sensors, all set up on a variety of weapons and menacing mannequins. He was stumped only once, when I asked what would happen if a Danubian snuck up and hit one of his dummies on the head. Would any bells and lights go off? “Excuse me?” he said. “ROE?” Colonel Wallace intervened to explain: “Against the Rules of Engagement. One meter rule. No physical contact in the Box.” It seems that one conveys body-to-body harm with real words, not laser words — i.e., ‘I am butt-stroking you now, so fall down.’ I would later find out that in ‘Operations other than War,’ the Rules of Engagement were there to be broken.

The day ended with an interview with the pugnacious commander of the base, Colonel Lenz, who made a persuasive case for Stability Operations as essential training for the increasing number of missions in that ‘grey area between war and peace.’ He would not, however, be drawn out on the relationship between Stability Operations and Bosnia, especially when I queried him about the possibility that some might find the notion of stability based on the status quo to be offensive, in both senses of word, when stabilisation is perceived to be an enemy of justice, or simply just desserts. “That’s above my pay-grade.” At the end of the interview he kindly suggested a de-brief after my visit to the Box: “I’ve got people upstairs who can suck a guy’s brain dry.”

That was sufficient incentive to stay up that night and wade through the stack of papers that I had been given. The bulk of it was a four-hundred page document called the “Coordinating Draft of the 7th Army Training Command White Paper of Mission Training Plan for Military Operations Other Than War.” A substantial part of it breaks down the ‘Critical Tasks of the Task Force,’ like the establishment of a quick reaction force, checkpoints, lodgments; conduct liaison with local authorities and convoy escort operations; provide command and control and protect the force; and, of no lesser importance, plan for media. Specific scenarios for battalions, companies, and platoons are spelled out. The philosophy of Operations Other Than War is conveyed in the introduction, and after wading through all the acronymic muck and bureaucratise (“Traditional MTP crosswalk matrixes for references and collective tasks are also included in this MTP”) — the final paragraph emerges as a reasonably clear summary of the purpose of the plan:

As we continue to maintain our proficiency in traditional wartime operations, our forces must also be ready to operate effectively in non-traditional roles. Units involved in conflicts anywhere within the full spectrum of operations will always face some elements of a complex battlefield. These elements include civilians in the area of operations, the press, local authorities, and private organizations. This White Paper is designed to assist leaders at all levels to more fully understand and prepare for these new challenges.

In other words, this ‘White Paper’ was this year’s model for the hi-tech, post-Cold War simulations and training exercises which would prepare U.S. armed forces for pre-peacekeeping non-interventions into those post-imperial spaces where once- and ‘wannabe’-states were engaged in post-war warring. In terms of past experiences rather than future threats, Somalia, Haiti, Rwanda, and — judging from the many references to the British Wider Peacekeeping Manual — Northern Ireland lurked between the lines. But in this simulated shadowland between military combat, police action, and relief aid, other ghosts could be discerned: Bosnia, yes, but why not as the next operation other than war, a counter-narcotics operation in Mexico? Or a quarantine of a paramilitary survivalist camp in Idaho? Or checkpoints and convoy escort through a persistently riotous Los Angeles? This week, however, the enemy at Hohenfels reflected the headlines.

Very early the next day I was heading for the Box, where the warring ethnic groups of a disintegrating ‘Danubia’ were about to make life very hard for the visiting 1st Armored Division. The next morning began with a low fog — confirmed by the weather report provided at the ‘Battle Update for Rotation 95-10.’ The mission: ‘to provide humanitarian assistance and separate belligerent factions.’ Computer graphics were projected in meticulous detail, breaking the mission from the highest level of ‘UNDANFOR’ (United Nations Danubian Force) commander down to equipment lists, tactical rules of engagement, task force organisation, and maps with vehicle and troop positions. A schedule of major events was put up, some of which required translation, like ‘1100 — Scud Ambush of Convoy’ (not the missile, but the ‘Sowenian Communist Urban Defenders’), or ‘2230 — Jerk Raid vs. Care Facility in

Raversdorf (again, not Steve Martin, but the 'Jurische Ethnic Rights Korps,' guerrilla forces operating in the south sector). I was in bad need of a scorecard.

Finally, we were on our way to the Box. There was a bit of delay as I struggled with the camouflaged ensemble of gortex jacket, pants, and boots (for the mud), and as my faith in our humvee was tested when the door handle came off in my hand. But Colonel Wallace proved to be as good a handle-fixer as he was a handler, and we were soon off. During the short ride through a gently sloping open terrain with trees on most of the hilltops, Colonel Wallace did the eco-army routine — "there are more trees and grass growing now than when we got here" — and as if on cue, a substantial herd of deer dashed across the road in front of us. The valleys and hillsides looked pretty chewed up by all the maneuvres, 'portaloos' dotted the landscape, but the fauna seemed to appreciate the fact that the U.S. Army — unlike the Bavarian hunters outside the Box — were shooting blanks.

The first stop was a UN checkpoint, one of many where civilians were stopped and forced to do a kind of 'self-search' for weapons or explosives. Most of the M1 tanks and Bradleys had their turrets reversed, the universal symbol of nonaggression (or surrender). We arrived with a UN food convoy which was supposed to pass through the mock-town of 'Ubingsdorf.' The town came complete with the steep-roofed houses of Bavaria, a church with a steeple (no sniper in sight), a cemetery (no names on the gravestones), a mix of 'Vilslakian' and 'Sowenian' townspeople (dressed by a retired psy-ops sergeant in what he described as 'the eastern-european, grunge-look,' accessorised with the requisite MILES vest), and a mayor in a green-felt fedora, who was insisting that the food be off-loaded for his hungry people.

Language differences, a belligerent crowd, an aggressive reporter with an intrusive cameraman, all jacked up the tension level. 'Lt. Colonel Vladimir,' commander of the local Vilslakian garrison, was refusing to bring the rabble to order. Chants for food in a kind of pidgin German — 'Essen, Essen' — made voice communication difficult. Suddenly, the crowd began to move toward the trucks, and a few rocks were thrown. The U.S. troops began to retreat back to the trucks, but already some of the townspeople were clambering up onto them. It was then that the first rule of engagement, right up there with the 'Prime Directive' of no-no's, was broken by one of the soldiers when he grabbed a civilian to toss him off. 'One meter rule, one meter rule!' was shouted by the observer/controllers on the scene. Some tanks and Bradleys, probably called up by the besieged sergeant in charge of negotiating with the mayor, came roaring up to join the convoy. The situation died down when the townspeople were rounded up and put under guard. Negotiations resumed, resulting in something of a compromise: the food would be unloaded at the local UN headquarters. But after the troops pulled out, I watched as some of the townspeople pulled off the most realistic maneuvre of the day: they scampered off with some of the large crates of food, evidently for their own purposes. Colonel Wallace later told me this was not in the script. I had witnessed some 'Box Improv.'

The script-writers clearly had it in for this convoy. At just about every checkpoint, food had to be traded for safe passage. And now, as we roared ahead in the Colonel's humvee for high ground, I noticed an observer/controller crouched in the ruins of a building probably dating back to the *Wehrmacht* days. A bad sign. As the convoy descended down the hill all hell broke loose — machine-gun fire from the hills, smoke bombs marking hits, and the light-and-sound show of MILES sensors going off. The M1 tanks and Bradleys reacted sluggishly to the ambush, not moving, and worse, keeping their turrets reversed in the defensive posture which made it impossible to identify the enemy with infra-red or thermal sights. Instead, someone called in for a Cobra helicopter gunship, breaking another rule of engagement: only 'minimum' or proportional force should be used in a counter-attack, to prevent a needless escalation of violence. From the last two engagements, it seemed apparent that the shift from war/sim to peace/sim was not going to be an easy one.

Salisbury Plains Forever. During my interview with Andrew Marshall, Director of the Office of Net Assessment, the intertext went into 'monalisa' overdrive. For five years I had managed to avoid the Pentagon. It was not just the reports of the rats in the basement that kept me away. I had learned the hard way that when it came to the Revolution in Military Affairs, the hype-to-reality ratio skewed as one went up the ranks. But at every pit-stop I got the same name, regardless of stripe on the sleeve or political colourings: go talk to Andy Marshall.

Several faxes later, I was sitting across from him in his spacious, paper-filled, very unmilitary Pentagon office. At 74 years old, Andrew W. Marshall has been around. Brought in by President Nixon, he helped set up the innocuous sounding 'Office of Net Assessment,' "to weigh the military balance in specific areas, what the important long-term trends are, and to highlight existing or emergent problem areas, or important opportunities that deserve top level management's attention to improve the future U.S. position in the continuing military-economic-political competition." His memoranda are legendary, and, for the most part, classified. They have ranged from broad politico-strategic issues like the decline of the Soviet Union, to no less important tactical debates about the advantages of sending Stingers to Afghanistan. The one that I kept hearing about bore a simple title — 'Some thoughts on Military Revolutions' — and was only seven pages long. When it was circulated on 23 August 1993, it was an idea in the wind; a year later, there were five task forces at the Pentagon alone, exploring the ramifications of the 'RMA' — the Revolution in Military Affairs.' He agreed to talk to me about it, on the record.¹⁷ Here are some excerpts:

Der Derian: Could you tell me who you are and what do you do?

¹⁷Interview, Andrew Marshall, 21 June 1996.

Marshall: Well I'll start with the history. I went to Rand at the beginning of '49 and I was there until the beginning of '72. Then I went and worked for Henry Kissinger at the National Security Council, and a couple of years later came here to set up this office.

I've been here ever since. This is the Office of Net Assessment and fundamentally what it tries to do is assess military situations with the intent of surfacing for the very top managers issues that they should pay attention to. I mean, based on emerging problems or opportunities. Of course, when I was first here we focused very much on the Soviet Union, and the more intense military, political, economic competition.

Now we really are working fundamentally on two things. One is exploring this idea of, you know, that the next twenty to thirty years may be another one of these periods where warfare changes in some very significant ways. We've done some earlier analyses of that before but, began about four years ago a much more intensive effort. I suppose we really began in '89 or so, and put out a preliminary assessment in July of '92 and have been pursuing a variety of activities to try to understand the potential character of the change, to better understand the actual nature of what the change might be.

So that is one thing we are doing and the other is trying to take a very long term view of Asia and where it may go, again, over the next twenty or thirty years.

Der Derian: Would you call it a revolution or not?

Marshall: Well, I mean, we have picked up this terminology of revolution and, I think, at one level, or in one way, that's appropriate. It turns out that tactically it gets you into a lot of arguments you don't really need to be in about whether it is a revolution, or what things can be called a revolutions. Anything that can happen over a couple of decades can't be called a revolution, for some people...

Der Derian: Would you call it a revolution?

Marshall: Yeah, I would...

Der Derian: Why?

Marshall: Well I think, again, if you look back, there is all this historical work that people have done on, way back to the fifteenth century, looking at periods where over the course of, you know, couple of decades or so many new forms of warfare emerge that just dominate whatever was dominant before and that seems, you know, reasonable to call it a revolution. It was the Russians that first brought it to my attention, the writings that they began to put out in the late seventies and early eighties.

Der Derian: You mean your counterparts in Russia were speaking about a military revolution?

Marshall: Well, yes, beginning in the '70s and on into the early '80s they began talking about the fact that we were entering, or that the world was entering, another period of what they initially called a 'military technical revolution.' And they cited two previous periods as exemplars. One was the twenties and thirties where you get the big change in many areas of warfare, because of, well, in some ways, the technologies of the internal combustion engine, radios, and so on. Then the second period, right after WWII, where it's a combination of nuclear weapons, ballistic missiles, and the beginnings of computers lead to big changes. Their function, as military intellectuals, was to diagnose when there were these periods of big change. And, so they began to say one of these periods of big change was coming, because of the micro-processor and other related technologies. It was triggered, I think, by a programme to develop a system that they called the 'assault-breaker,' that conceptually was a reasonably long-ranged rocket with a smart front-end coupled to long-range sensors.

Der Derian: I was out for the first digitised rotation at Fort Irwin when the Fort Knox brigade was out there, and did some interviews. I've been looking at this from the bottom-up, from the field, and it seems there's a lot more skepticism about a revolution going on.

Marshall: Yeah, I would think so. I wouldn't particularly expect to see it down there. It's also spotty on the top, although growing, I would say. What I tend to argue with people is that we ought to see ourselves as in something like in the early twenties where we don't fully see what the outcome would be. But there is just enough, on the one hand, to see that the technologies are moving rapidly and it's plausible that there would be a big impact. We are about in a position, where people say, at the Naval War College, were about in '22 or '23, where we now have a bunch of war games that are being played, that are beginning to explore, in some sense, the logic of the situation that would exist if you had, let's say, twenty years from now, a number of new kinds of systems.

Der Derian: Are you familiar with the exercises on the Salisbury Plain in the twenties?

Marshall: Yes, '27 and so on, oh yes...

Der Derian: Last fall I checked out the back-issues of *The Daily Telegraph*, where Liddell Hart wrote about them, and what struck me is that he didn't really call it a revolution, or understand it as such. When you are really in the middle of it, you are least aware of it.

Marshall: Yes, well I suppose to an extent there were people in the military, in the twenties that thought of things as revolutions that were primarily associated with air. Even the Germans, who really boast of being a hell of a lot better than the British, were not consciously thinking in terms of a revolution. So,

what would be unique this time, in a certain sense, I think, or more so, is that because of things that have happened since the twenties and thirties — both the historical literature that has been built up that looked at these kinds of periods and the Russians who began intellectualising about it and raising it as a kind of intellectual issue — that one of the unique things about the next twenty or thirty years, if in fact we will go through such a thing, it will be almost the first time in which it is, in a widespread sort of way, self-consciously — you know — pursued or experienced as a revolution.

Der Derian: Who do you see as our next enemy?

Marshall: Well, I'm interested in Asia mainly because of some general reasons. You look at long-range projections, that's the place where the most rapid economic growth is going to take place. Also, Asia has been dominated by the West for over 150 to 200 years and that's over. And so, exactly what Asia would be like, what kind of internal rivalry will be there is something really needs to be look at.

Der Derian: Can you really compare our times to any other? When suddenly everything is wide open, do you think a global threat is going to emerge?

Marshall: No, I think not in my time. But if you look back into history I think you can see... I think the twenties was like that. The twenties turned out to be a period of illusion about what the world was going to be like. I think we are in the twenties. Both in terms of the beginning of technical change which is working out its implications, and in terms of, well, in the twenties the United States didn't really have any big immediate threat, and the forces were very small. Whether something like the thirties is before us, I don't know.

Der Derian: But to what extent do we create our enemies? Do you think it is completely a unilateral action, or do you think it's more like the whole idea of the security dilemma?

Marshall: Well I don't see that right now. You have a little of that in Asia with the growth of China and how we react against it, and to the extent that we get to be seen as, you know, the people who are intervening in this place and that place...to the extent that we have gotten ourselves in the position of being the leader of the interventions for the UN.

Der Derian: In the way that the nuclear deterrence maintained a relative peace for some, do you think there is such a thing as a high-tech deterrent, in the way that people would see what happened in the Desert Storm and then would not want to take on the U.S.?

Marshall: I think so, I mean it's a deterrent in a sense, but it also has these other effects. I mean it deters people from taking us on in this way. But it may substantially increase incentives to go after nuclear weapons, or look for other clever ways of using the technology.

Der Derian: It's clearly part of your job here, but do you really think war is persistent; we will always have it?

Marshall: I tend to be pessimistic about it and not just because of my job. If you just look at history and human behaviour you can't be very optimistic about it...

Der Derian: You don't want to think of war as obsolescent?

Marshall: I would tend towards that view, yes.

Closing shot, a shadow looming over the White House. Ronald Reagan, at a final press conference before the National Strategy Forum in May 1988:

But I've often wondered what if all of us in the world discovered that we were threatened by a power from outer space — from another planet. Wouldn't we all of a sudden find that we didn't have any differences between us at all — we were all human beings, citizens of the world — wouldn't we come together to fight that particular threat?

Paul Virilio, from his *Popular Defence and Ecological Struggles*:

Meanwhile, damage and disaster occur just like the emergence of war populations, nihilistic spectre of the speed of those with no name, who cannot be named and who nonetheless arrive, those whom Chaucer in the fourteenth century already called "*builders of smokejails...greenish men, couriers of the Great Fear...*" The modern myth of UFO's is mixed with that of the terrifying immanence of assassination attempts, cataclysms, crime, epidemics, enemy threats.

And finally, Walter Benjamin, from *Charles Baudelaire: A Lyric Poet in the Era of High Capitalism*:

In times of terror, when everyone is something of a conspirator, everybody will be in a situation where he has to play detective.

Agent Mulder would probably agree.

Chapter Ten

Arms Control and the Future of International Security

Brad Roberts*

Arms control seems to have lost its sense of purpose and direction, at least in the United States. Many believe that arms control is a Cold War-vintage anachronism. Without strong political leadership from the executive branch of government and without a modicum of bipartisanship in the legislative branch, arms control has fallen prey to an old ideological debate between those who really care about arms control — its die-hard opponents and its passionate advocates. Today in Washington the debate over arms control is again dominated by those who see it as a dangerous delusion, a ‘sell-out’ of the national interest, and the epitome of ‘do-goodism’, and those at the other end of the spectrum who believe arms control is the only viable means of walking us back from the terrible consequences of a world of unrestrained proliferation. The combination has proven nearly fatal to the old moderate consensus that saw arms control as a useful instrument of national strategy when carefully conceived and tightly constructed.

In Washington, arms control is hostage not least to the passing of an agreed understanding of the role of the United States in the world. Containment of the Soviet threat provided a clear and straightforward understanding of U.S. grand strategy and a way to weigh the utility of various tools of policy in pursuit of that goal. Arms control’s promise was always clear, even as the utility of specific instruments was sometimes hotly debated. It seems likely that U.S. leaders will continue to invest arms control with diminished political capital so long as its utility and promise vis-a-vis new problems of national and international security remain clouded.

It is time then to return to basics. What role can arms control play in meeting the security challenges of the emerging strategic era? If it has a role to play, must it change in order to do so? In what ways? This chapter offers some speculative thinking on these questions.¹ It is conceived as a brainstorming tool, aimed at assisting the reader in rethinking inherited assumptions about arms control and in beginning to evaluate some of the new dynamics of international security. It begins with a discussion of the emerging strategic era and the specific challenges of promoting orderly relations among states. It then evaluates the utility of arms control for six specific world order tasks; this is a comparative evaluation that explores a

*This chapter is an edited version of a presentation made to the Fourteenth Annual Ottawa NACD Verification Symposium, “Cyberspace and Outer Space: Transitional Challenges for Multilateral Verification in the 21st Century,” 12-15 March 1997, Montebello, Quebec, Canada.

¹Those remarks were derived from an unpublished article entitled “Arms Control in the Emerging Strategic Environment.”

broad set of policy instruments in order to place the potential role of arms control into perspective. Finally, it explores some implications for the changing roles and functions of arms control.

World Order Tasks

Analysts have developed a number of tools for speculating about the emerging strategic era. Some look for analogies in the past, such as the decaying order of the 1920s or the swiftly rebuilt order of the late-1940s. Others construct pictures of the future by projecting forward current trends, and thus see a future dominated by transnational forces or subnational conflict. Others emphasize the transitional nature of the current era, with great uncertainty and an element of fear about what might follow, such as a renewed military competition among the major powers. This chapter adopts a different approach: it identifies six unique features of the current international system and postulates six so-called world order tasks germane to enhancing the stabilizing aspects and minimizing the destabilising ones of each of those features.

The current moment in world affairs is noteworthy for a variety of reasons. For the first time in more than a century, there is no significant prospect of war among the major powers in the interstate system. Yet relations among them — and factors within them — are changing, and other major powers are emerging. Maintaining this stability and reaping its benefits for the rest of the system is thus the first world order task.

At the same time, however, there is an unprecedented emergence of prosperous, developing, and increasingly powerful and ambitious countries in many regions of the world, which aspire to a status commensurate to their weight. The need to meet their expectations and to reinforce their stake in existing international institutions and norms is unprecedented. At issue is their ‘alignment’ and the possibility that they might become revisionist powers. Integrating these states into the existing system is thus the second world order task.

But this is also an era when localized conflicts among minor powers, or even within states, can threaten to have broad international repercussions. The advent of international terrorism and the proliferation of long-range delivery systems underscores this. Insulating the state system from the military competitions of small states and from weak and collapsing states is thus the third world order task.

Interstate aggression is an old problem of international relations but in a particular new guise. Successful aggressions threaten a principle that slowly has taken hold in international politics — that war is permissible only in self-defence. Many small and medium countries bank on this principle by not maintaining the strongest military forces within their reach and counting on the international community to come to their aid in time of need. Moreover, wars of aggression won by threats or the actual use of nuclear, biological, or chemical weapons could have a terrible impact on the proliferation problem,

especially if the power that has backed down or been defeated is an international security guarantor. Deterring aggression and punishing transgressors of agreed norms is thus the fourth world order task.

The current international system is also noteworthy for the rapid globalization of the world economy and for the associated boom in the exchange of technologies, materials, and expertise that are dual-use and thus militarily sensitive. Preventing or stopping the flows of dual-use items is impossible, especially given the evergrowing list of countries that generate those items. But preventing the proliferation of technologies from precipitating a proliferation of high-leverage weaponry, while also promoting accepted and legitimate uses of those technologies, is a more reasonable goal. Managing technology diffusion is thus the fifth world order task.

Finally, the current international moment is marked by the unprecedented role of the United States. It is the only state with a global view and the only one capable of mobilizing international institutions to deal with threats to the peace. Its military power is unmatched — but it is no more than first-among-equals politically and economically. Moreover, although the world order requires a constancy and purposefulness to the use of American power, the United States is alternatively assertive and neoisolationist. Anchoring American power in international processes and institutions in a way that is *sufficient* to the needs of their sustained functioning and to the needs of security and prosperity more generally is an urgent requirement. Thus the final world order task is engaging the United States.

Rating Arms Control's Utility

What role might arms control play in accomplishing these world order tasks? It should be obvious that none of these tasks can be accomplished by arms control in and of itself. Indeed, there is a wide variety of political, economic, and military instruments of policy germane to each. But when and where might arms control fit into the larger strategic equation?

In some cases, arms control's contribution is likely to be, at best, modest. For integrating aspiring powers, for example, the primary tools of policy are bilateral relations with each of the emerging powers and their enhanced economic integration with the global economy. But arms control offers some specific roles and opportunities for these powers, not available elsewhere. Arms control negotiations with them on, for example, the global treaty regimes, are a way to build consensus with the major powers on the allocation of rights, responsibility, and power in the international system. Arms control is also a tool for institutionalizing transparency within those societies, thus laying the foundations for their future, deeper integration into the global system.

In other cases, arms control's potential contribution seems likely to be more substantial. For insulating the state system, recent years have brought a recognition of arms control's utility in stemming the in-bound flow of small arms and the out-bound flow of weaponry and materials. It also has found a limited

role in disarming factions in local conflicts — in El Salvador, for example, where such controls have been applied as a part of an agreement that also arms the legitimate police functionaries of the state. Arms control also helps to ameliorate the problem of terrorist use of nuclear, biological, or chemical weaponry or materials by criminalising certain types of activities and delegitimising the use of such weapons by states. Historically, many terrorists have been unwilling to employ weapons that states consider illegitimate, because such use might alienate their perceived constituencies and delegitimise their cause.

For deterring aggression and punishing transgressors, the primary instrument of policy is, of course, the military instrument and associated alliances and coalitions. But successful deterrence requires not just an operational capability to defeat aggression on the battlefield, but a political context that delegitimises the aggressor's actions and legitimises international responses. Arms control seems useful as a tool for building consensus about what makes some states 'rogues' — by their self-selection outside of treaty regimes or their failure to comply if inside them — for utilising that consensus to assemble political coalitions against specific states, and for collective military reply to particularly egregious illegal or illicit behaviour.

For engaging the United States, arms control has a utility generally not appreciated by those in Washington. It defines commonly agreed roles for the United States, legitimises the use of U.S. military power against regional challengers on behalf of the common interests of the international community, and provides a rule-based, institutional basis for U.S. engagement — a basis for which the United States has shown an historical affinity.

Arms control also has an important potential utility for maintaining stable relations among major powers. But its actual utility is uncertain. It seems to be an essential tool for this purpose, by structuring the most volatile strategic relationships; by facilitating dialogue amongst them about changing roles, responsibilities, and ambitions; and, by harnessing their political and military power to certain common purposes. But arms control is certainly not the primary tool for any of these purposes. Moreover, arms control poorly conceived, which is to say arms control inconsistent with the interests of specific major powers or weak arms control exploited by one party to capture strategic advantage over the other(s), could prove serious destabilising.

Implications for Arms Control

If arms control is to make its contribution to these tasks, how must it evolve? Part of the answer has to do with the function of arms control. The three classic functions of arms control, as defined in the 1950s, were to reduce the likelihood of war, to reduce its scope and violence if it were to occur, and to reduce the costs of being prepared to wage it. The foregoing review of arms control utilities suggests some different ways of thinking about the function of arms control. On the one hand, it is a process of political dialogue. In the era ahead, it would appear that this process is increasingly important, not least to those who would

engage the United States in a discussion of its roles and responsibilities. On the other hand, it is a set of products whose implementation enhances stability by minimizing risks. In the era ahead, it would appear that the utility of these products will be not so much remedial as preventive. In the Cold War, after all, arms control's primary appeal was in helping the superpowers to walk back from the brink of armageddon. But is it not better not to walk to the brink in the first place by formalising patterns of restraint among nations increasingly capable of mobilising domestic resources for strategic war?

Part of the answer also has to do with utilising the existing set of arms control products for new purposes. For example, the global treaty regimes for the control of nuclear, biological, and chemical weapons are useful not just for the restraints they impose on the major powers, but also for their restraints on aspiring powers, the obligation to conduct sensitive trade under conditions of transparency and control, and the dialogue they permit among major and minor powers about the proliferation threat and the security guarantor roles of the major powers. Regional mechanisms, ad hoc and informal measures, and even unilateral restraints are familiar arms control instruments with new roles and possibilities in the years ahead. New mechanisms seem likely in certain areas, such as landmines.

This analysis points to a broader set of implications for the changing arms control agenda. First, non-nuclear matters are conspicuous on the emerging agenda. Although the arms control community in the United States remains heavily focused on nuclear matters, chemical, biological, and conventional weapons — especially small arms in local conflicts — are having a growing impact on international security and thus on the arms control agenda. Unfortunately, ways of thinking about arms control, as derived from the nuclear experience, have generally obstructed a clear assessment of the distinct arms control requirements in each of these areas. For example, the verification and compliance requirements of treaties outside of the strategic domain, where cheating does not pose risks of armageddon, are not well understood.

Second, this agenda is more multilateral and less bilateral than ever. But the new prominence of multilateralism poses a special challenge to the United States, given its past focus on bilateral measures with its superpower peer and its difficult adjustment to its role as first among equals in such fora. The absence of a sustained U.S. political commitment to multilateral institutions and processes more generally has been harmful to both the Nuclear Non-Proliferation Treaty and the Chemical Weapons Convention, for example.

Third, the arms control agenda is expanding to include not just negotiation but also implementation issues. Of course, this is a question of the relative prominence in the mix, as implementation has always been a part of the arms control agenda. Implementation poses technical, organisational, and fiscal challenges that seem likely to grow in an era of weakening political commitment to arms control and

sharper budgetary constraints. It also poses political challenges related to gaining full compliance by unwilling parties.

Fourth, arms control's normative content merits greater political attention. If arms control is useful in significant part as a political tool for building coalitions and for coping with technology diffusion, its political value derives from the shared norms of behaviour it reflects. But such norms are under challenge today, and not just from 'rogue' states at the margins of international politics. The perception in some quarters, that the United States pays only lip service to such norms and eschews the responsibilities of leading the institutions created to enforce them, only magnifies the problem.

Fifth, arms control's changing agenda raises fundamental questions about nuclear disarmament. For the purposes of maintaining stable relations among the major powers, deterring aggressors armed with weapons of mass destruction, and keeping the United States engaged, nuclear abolition seems likely to be counterproductive, at least for the foreseeable future. But abolition is just what is expected of the nuclear weapon states by those aspiring powers actively engaged in the NPT process — and urgently so. Moreover, the conservatism of the nuclear weapons states in addressing these nuclear questions is under growing assault from both civilians and military personnel within some of those countries. An increasingly sharp debate about the role of nuclear weapons in international security and the speed and direction of nuclear arms control certainly seems in the offing.

Sixth, the 'leadership needs' of the new agenda are poorly conceived. Leadership seems to be missing on a number of essential items: in the debate on the future of the NPT; in implementation of the CWC; in the use of the UN Arms Register and Wassenaar Arrangement to promote regional stability; in the North-South dialogue on export controls; in the dialogue with the smaller nuclear weapons states; and in confronting the critics of treaty norms, for example. But the leadership issue is not just *where* to lead — it is also *how* to lead. The temptation in the United States, at least, is to lead episodically and by cheerleading. But world order politics require a leadership style that matches vision, constancy, intellectual rigor, responsibility, and an ability to motivate others by appealing to shared interests as well as shared values.

Finally, the new agenda poses a large set of novel analytical questions. Yet arms control research has grown moribund. Thinking about arms control has become highly specialised and technical, when what is needed is a capacity to examine old instruments in new ways and to conceive new instruments for new purposes and in a new political context.

Conclusions

If there were no inherited arms control agenda, the international community would find it useful to create one for the strategic requirements of the new era. Arms control's potential contributions to national security and international stability seem to be expanding, not contracting, with the end of the Cold War.

But the reemergence of arms control as a major instrument of international action and of policies in Washington, cannot be taken for granted. Momentum alone is insufficient. Today, for example, seven arms control measures await ratification by the United States, with little prospect of such in the near term. A willingness on the part of senior leaders in Washington to invest political capital in arms control will not be easily rebuilt in the absence of a broadly accepted grand strategy for the United States and the West.

In the absence of concerted and effective leadership by Washington, other countries will have an opportunity to play new leadership roles. This is for the best. It provides new opportunities for the aspiring powers to take responsibility for larger international problems. It provides new roles for the emerging major powers like Germany and Japan. And it provides a way to compel Russia and China to examine their stake in the stability that existing international institutions are intended to serve. But if the new leadership team is unable to turn a commitment to arms control into the practice of arms control, other partners in the process will begin to opt out. International stability will suffer. It will be difficult, if not impossible, to turn around the disintegrating process in the absence of a major international crisis. And if weak or inadequate arms control is seen to have played a hand in precipitating that crisis, arms control may quickly be relegated to an historical footnote.

Chapter Eleven

Verification: An Active Role for the United Nations

Alan Crawford*

Introduction

The United Nations enters its fifty-second year of existence in 1997 — a remarkable achievement of longevity in the realm of international affairs. Yet the future of the organisation remains clouded. It faces, for example, even more turmoil in terms of financing and restructuring over the next few years. Perhaps even more disconcerting is the lack of a shared vision among Member States concerning the purpose and role of the organisation with respect to security affairs in the twenty-first century. This state of uncertainty applies doubly so when considering the role of the United Nations in the field of verification “in all its aspects.”

This chapter will argue that there is a legitimate and practical role for the United Nations in certain specific and carefully delimited areas of verification. After describing briefly some of the background to the United Nations’ role in verification and Canada’s involvement with it, the chapter will outline what that role seems to be today. It will then move to the more problematic question of the prospects for supporting and enhancing this role, both in terms of desirability and feasibility. Finally, it will address what Canada should and can do in this respect.

Background

Canada has, for a number of years, supported the consideration of an active role for the United Nations in verification, as indicated in **Table 1**. Beginning in 1985, when verification remained a contentious East-West issue, Canada initiated the first United Nations General Assembly (UNGA) resolution that specifically addressed the subject.¹ That resolution articulated the view that verification of arms control and disarmament (ACD) agreements was important. That initial resolution has been followed, at first annually and later biennially, by further UNGA resolutions on which Canada has taken the lead. In the initial years, these resolutions were adopted without a vote, reflecting an international consensus. More recently, this consensus has broken down.

*This chapter is an edited version of a presentation made to the Fourteenth Annual Ottawa NACD Verification Symposium, “Cyberspace and Outer Space: Transitional Challenges for Multilateral Verification in the 21st Century,” 12-15 March 1997, Montebello, Quebec, Canada. The views expressed in this chapter are those of the author alone and do not necessarily represent those of the Department of Foreign Affairs and International Trade or of the Government of Canada.

¹United Nations General Assembly, Resolution 40/152 O, 16 December 1985.

In 1987, Canada took the lead in initiating a United Nations Disarmament Commission (UNDC) working group and chairing that group.² The UNDC eventually produced, in 1988 by consensus, a report containing, among other things, a significant set of sixteen “verification principles.”³ That same year, the UNDC exercise was followed by an UNGA resolution that set up a United Nations Group of Governmental Experts Study to examine the role of the United Nations in verification.⁴ That resolution saw the first rift in the international consensus on the issue, with the U.S. casting a single negative vote on the grounds that verification was a treaty-specific exercise and a United Nations role in verification could not be examined in the abstract.

The United Nations Study Group, under the Chairmanship of Canada’s Fred Bild and comprising governmental experts from twenty countries, including a U.S. participant, still confronted much of the political ‘old-think’ of the dying days of the Cold War. Nevertheless, it managed to produce by consensus, an interesting report in 1990.⁵ The 1990 Report discussed the concept and functions of verification, described existing United Nations activities in the field, and articulated a few very modest ways to enhance the role of the organisation relating to construction of a verification database and promoting the exchange of views between experts and diplomats. The Report noted that the development of a United Nations “verification system,” a point which was promoted by several Third World members of the Group, depended on further changes in the political environment and the evolution of arms control agreements, concluding only that consideration of such a verification system should continue. On balance, given the constraints of the Cold War, this report achieved a remarkable consensus between East and West, as well as between North and South. The 1990 Study was adopted in UNGA Resolution 45/65 of 4 December 1990, which was agreed without a vote, suggesting that international consensus had been re-established.

Later, however, international consensus on the issue within the United Nations began to deteriorate again. In the aftermath of the 1991 Gulf War, the Security Council had set up the United Nations Special Commission (UNSCOM), which was tasked, along with the IAEA, to verify the disarmament of Iraq’s weapons of mass destruction and long-range missiles.⁶ UNSCOM and the IAEA were given rights to inspect and monitor Iraqi activities that were unprecedented in their comprehensiveness and intrusiveness.

²United Nations General Assembly, Resolution 42/42 M, 30 November 1987.

³*Official Records of the General Assembly, Fifteenth Special Session, Supplement No. 3 (A/S-15/3).*

⁴United Nations General Assembly, Resolution 43/81 B, 7 December 1988.

⁵*Study on the Role of the United Nations in the Field of Verification, A/45/372, 28 August 1990.*

⁶United Nations Security Council, Resolution 687, 3 April 1991.

Other international events had also unfolded since 1990 that had significant meaning for multilateral verification, including the adoption on 19 November 1990 of the Conventional Forces in Europe (CFE) Treaty.

In 1992, the United Nations Secretary General produced *An Agenda for Peace*,⁷ which was followed by several other documents dealing more explicitly with ACD issues.⁸ These documents possessed a tone, understandable perhaps in the aftermath of the successful remedial action by the international community to expel Iraqi forces from Kuwait, which seemed to favour a much more activist and interventionist role for the United Nations. The United Nations, it seemed, would no longer stand passively by to allow developments within a country to grow beyond its borders into a threat to international peace and security. The result was a growing concern among Third World states that the United Nations might increasingly interfere in their internal affairs.

Another important trend, increasingly apparent after 1990, was the success by the international community in achieving progress in reaching agreements addressing weapons of mass destruction, most notably the Chemical Weapons Convention. As a result, more attention began to turn toward dealing with the problems generated by conventional weapons, particularly the accumulation of excessive and destabilising quantities of these weapons. This was perhaps best exemplified by the creation of the United Nations Register of Conventional Arms. Also, there was increasing focus on the impact of such conventional weapons, including light weapons in local conflicts, especially where peacekeeping forces might be operating, and on humanitarian concerns generated by the mis-use of specific conventional weapons such as anti-personnel landmines. Increasingly, attention seemed to be shifting away from weapons that were largely a monopoly of the big powers — i.e., weapons of mass destruction — to those used by smaller and poorer countries — i.e., conventional weapons. The result was a heightened sense of unease on the part of the latter's governments.

At the same time, many of the big powers increasingly questioned any enhanced security role for the United Nations, including in the field of non-proliferation, arms control, and disarmament (NACD). In part, this reflected dissatisfaction with the perceived inability of the UN to work effectively in this area and with the 'messiness' of United Nations politics. In addition, it may well reflect an antipathy toward creating a strong supra-national organisation that would have the power to constrain the big powers'

⁷Boutros Boutros Ghali, *An Agenda for Peace*, A/47/277, 17 June 1992.

⁸Boutros Boutros Ghali, "New Dimensions of Arms Regulation and Disarmament in the Post-Cold War Era," A/C.1/47/7, 23 October 1992; and *idem*, *Supplement to an Agenda for Peace*, A/50/60, 3 January 1995.

freedom of action. As a result, the U.S. and some other states displayed an increasing hostility to studying an effective United Nations role in verification, or even further consideration of the subject.

Finally, the mid-1990s saw the United Nations — as well as its main donors — facing an increased financial crisis. There was less money to support an enhanced role for the UN in security affairs, let alone verification. Indeed, given the greater number of local conflicts to which the United Nations was being called upon to send peace operations, there was growing concern that the UN would not be able to perform its traditional security functions, much less expand its responsibilities.

Against this background, in 1994, Canada initiated another United Nations Group of Experts Study to explore a UN role in verification. The rationale was that the international environment had changed greatly since the end of the Cold War, at the end of which the 1990 Group had conducted its work, and that verification of multilateral NACD obligations was becoming increasingly important. The establishment of this new Group of Experts Study was resisted by many of Canada's traditional allies, including the U.S. and European Union (EU) states, primarily on the grounds that it was too soon, examining UNSCOM's experience was too sensitive, and it would be too expensive. From a purely research perspective, all three excuses were suspect. Through perseverance, the Group was established by UNGA Resolution 48/68 of 16 December 1993. Under the Chairship of Canada's Peggy Mason and with only a Dutch and Swedish expert from other developed countries, the Group reached a consensus report in 1995.⁹ That report was not, however, adopted by consensus in the General Assembly: the United States, Iraq, and North Korea, among others, did not support it.¹⁰ In a welcome gesture, Germany, after abstaining on the resolution in the First Committee, changed its vote to an affirmative in the Plenary of UNGA, after having had an opportunity to evaluate the report more carefully.

The 1995 United Nations Study introduced an important conceptual refinement to the concept of verification: it expanded the application of the concept beyond formal NACD "agreements" to encompass "obligations," reflecting, in part, thinking that was present in previous UNGA resolutions concerning compliance with NACD obligations. This expanded concept of verification now applied to obligations imposed by the United Nations Security Council (such as in Iraq), including arms embargoes, and to less formal agreements as might occur in the context of the operation's peacekeeping missions. The 1995 Study also outlined a more ambitious — though still modest and very qualified — set of recommendations for an enhanced United Nations role in verification. These are summarised in **Table 2**.

⁹*Verification in All Its Aspects, Including the Role of the United Nations in the Field of Verification*, A/50/377, 22 September 1995.

¹⁰United Nations General Assembly, Resolution 50/61, 12 December 1995.

Verification Activities of the United Nations Today

In theory, the United Nations has a major role in international security deriving from its Charter — in practice, this role has been and still is subject to major restrictions imposed by Member States, especially by the big powers. However, the very nature of the international system and its focus on sovereign states also constrains UN activities in international security and, by extension, in verification. Traditional concepts of national sovereignty favoured by both big and small powers limit the role the United Nations can play.

Norm-Building

One role about which there appears to a fair degree of international consensus and one where the United Nations has made some important contributions is in the development and articulation of international norms relating to verification. The UNDC sixteen principles mentioned above are an example of this. One might also hope that the expanded definition of verification outlined in the 1995 United Nations Study would also prove to be an example, though this remains to be seen.

This is an important role, though one that is often underrated. Despite fatigue on the part of many with rhetorical pronouncements or the ‘lowest common denominator’ character of many United Nations documents, most people would recognise the need for some body that can make authoritative statements that represent the consensus, or at least majority beliefs, of the international community. In the context of verification, the UN has succeeded in increasing international recognition of the importance of verifying compliance with NACD agreements and obligations: relying on good faith declarations is simply not enough when important issues relating to security are at stake. The need to balance the requirement for verification with concerns about national sovereignty and other legitimate matters is an example of an important general principle about which there is also broad international agreement. The United Nations can claim considerable credit for helping to develop, articulate, and maintain international consensus about such ideas.

However, norms are not built and do not endure by grandiose statements of principles alone. They are generated and gain much of their meaning by the practice of Member States. The United Nations has had less success in contributing directly in this area.

Verification Infrastructure

Both the 1990 and the 1995 United Nations studies suggested that the UN can play a useful role in contributing to the development of what might be called a “verification infrastructure,” by which is meant certain shared management and coordination functions on behalf of the international community. These functions are usually conceived in much less treaty-specific terms, in contrast, for example, to the tasks that the Verification Implementation and Coordination Staff of NATO performs for the Parties to the CFE Treaty. Instead, the United Nations’ role is seen as applying generically across treaty regimes. Among

the functions suggested are support for verification research, training, and the exchange of views/communication between treaty regimes and between Member States. Because of its universal membership, the UN is thought by some to be in a better position to see the broader picture and to be better able to exploit potential synergies that might not be apparent to a treaty-specific organisation or to individual Member States.

Such a role for the United Nations may be useful in certain narrow contexts and may be very important to some Member States, particularly those lacking national capabilities. Success in this role, seems to be a matter of the UN carefully identifying and focussing on specific requirements in this area. However, it must be recognised that the United Nations is not alone in undertaking such “infrastructure” activities. Non-governmental organisations, including research institutes and also some Member States, also make important contributions. It is debatable, therefore whether the UN really has a *unique* role to play in developing an international verification infrastructure at this time.

Operational Activities

The real ‘meat and potatoes’ of NACD verification is in operations. It is in this area that the UN’s role is, ironically, both very restricted and almost pre-eminent.

It is useful at this point to digress briefly, to outline some of the advantages that have been advocated in the past for a comprehensive international verification organisation — that is, one that would undertake verification of a variety of NACD agreements. These advantages might also suggest a more robust role for the United Nations in operational verification activities. Among these advantages are the following:

- C verification by such an international body can achieve economies of scale and thus be cheaper than by groups or individual countries;
- C for smaller countries in particular, which lack national capabilities, an international body can help provide a vehicle for meaningful participation in verification activities;
- C important synergies and cross-fertilisation can be achieved because of the international body’s broader scope of coverage, with the result that it can verify compliance more effectively than can a number of treaty-specific organisations or individual countries; and,
- C such a role for an international body helps promote the rule of law and international governance.

Returning to the question of the United Nations’ current verification role in the realm of traditional NACD, by which is meant verification related to specific formal NACD agreements, the UN has little operational responsibility. There are two exceptions to this general statement. First, the United Nations has undertaken and still does perform some fact-finding activities with respect to compliance with the 1925 Geneva Protocol dealing with chemical and biological weapons use. This function is expected to be largely taken over by the Organization for the Prohibition of Chemical Weapons (OPCW) when the

Chemical Weapons Convention comes into force. Second, if one considers the International Atomic Energy Agency (IAEA) to be part of the United Nations, then the UN does have a central role in verifying the Nuclear Non-Proliferation Treaty (NPT). However, this is, at best, a quasi-exception, because the IAEA operates, for the most part, quite independently of the central United Nations organs.

There has been a marked lack of enthusiasm among the parties to formal multilateral arms control agreements for giving the United Nations a role in the verification of those agreements. In fact, it is hard to avoid the impression that parties have gone out of their way to prevent UN involvement. Why is this the case? Perhaps there are several reasons: disillusionment with the perceived inefficiency and ineffectiveness of the United Nations; fear of strengthening the United Nations' power and promoting a supra-national government; and, the desire to ensure the requisite technical expertise. Another important consideration is the fact that each separate arms control agreement is composed of a different set of parties — sets which do not coincide with the membership of the United Nations. In other words, giving the UN authority with respect to verification of a specific NACD agreement would mean allowing non-parties to that agreement to have a say in its verification. A valid point; however, it has not prevented the IAEA from being assigned responsibility for NPT verification. The membership of the IAEA includes non-parties to the NPT.

Also, Third World countries, as mentioned above, may fear that an activist United Nations might be used to interfere with their internal affairs and weaken the traditional concept of national sovereignty. Finally, some may be concerned about the financial implications in an era of tight United Nations budgets. It is also worth mentioning that there has been no interest on the part of Russia/USSR and the United States for a United Nations role in verifying their bilateral NACD agreements. Clearly, the question of superpower status and power are key in this context.

This situation with regard to formal traditional NACD agreements contrasts sharply with the more informal NACD verification in peace and security operations, by which is meant United Nations peacekeeping, peace building, peace enforcement, etc. The 1995 United Nations Experts Study pointed out that peace operations often involve an important NACD component and that the UN has a great deal of experience in this area. More recently, the term “micro-disarmament” has been introduced to describe this activity.

For peace operations, neutral third party verification is a key idea — that is, involvement by a trusted third party which undertakes a verification role in lieu of or in addition to activities by the adversaries. Of course, there are peace operations where the United Nations has no role — for example, the Dayton Accords where the OSCE is playing the role of third party verifier in some ways. Another example is that of the Multilateral Force and Observers with respect to the Egypt-Israel Peace Treaty. Moreover, there has been at least one important instance wherein this third party verification role was undertaken by an

individual country: the U.S. during the Sinai Disengagement process between Egypt and Israel. Nevertheless, the UN can rightfully claim pre-eminent experience in this area.

A unique case of United Nations involvement in verification is that of UNSCOM/IAEA in Iraq. Clearly, this is not a situation of verifying a traditional NACD agreement, or even of United Nations micro-disarmament activities. For a number of reasons, this case is special: it involves a unique United Nations Security Council mandate; the weapons involved are weapons of mass destruction, unlike the case in micro-disarmament; it is decidedly compulsory in nature; and, the degree of intrusiveness and intensity of the disarmament involved is unprecedented. Nevertheless, the ongoing experience in Iraq has much to teach about the methodology of verification — indeed, the 1995 United Nations Study described it as a “verification laboratory.”

Another area where the United Nations has extensive involvement is one that it is often overlooked: that of arms embargoes. Because the *monitoring/verification* element in embargoes is intimately intermingled with the *enforcement* of the embargoes, and because arms embargoes are also intertwined with more general economic embargoes, such cases have special characteristics. Nevertheless, as the 1995 United Nations Study recognises, arms embargoes are a form of arms control in the sense of having an obligation relating to the acquisition of weapons and monitoring compliance with that obligation. Monitoring and verification in this area is most often *ad hoc*, rudimentary, and inefficient — it is left up to Member States to implement, for the most part. There are many political and technical complications — especially demands for the compensation of economic losses by innocent parties and the involvement of customs controls. Verifying arms embargoes is also a costly activity. As a result, there has been little political will to improve the capability of the United Nations in this regard, and little research has been done in this area.

One great difficulty in describing the foregoing activities by the United Nations — peace operations, UNSCOM, arms embargoes — as NACD verification is that the peacekeeping and diplomatic community tend not to think of them as involving arms control, verification, or even monitoring. This is largely a result of a preoccupation with formally negotiated agreements and a question of terminology, as well as, perhaps, bureaucratic mindsets. All the basic functional elements of NACD verification seem to be present in micro-disarmament, the UNSCOM experience, and monitoring arms embargoes, despite their special individual characteristics.

The foregoing suggests that, despite the traditional wisdom on the subject, the United Nations today has an important role in certain types of NACD monitoring and verification. This is not the old idea of the UN as a supra-national verification organisation, but it is nevertheless a very important role.

Prospects for Enhancing the United Nations Role in Verification

Norm-Building

Verification is on the agenda for the next United Nations General Assembly in October 1997. However, while the UN still has a role to play in promoting international consensus about verification of NACD obligations, there is decidedly little interest among Member States in pursuing this agenda item at this time. Most do not see it as a priority. Most, while paying ‘lip-service’ to verification of traditional NACD agreements, do not really see it as critical and, for reasons outlined above, are unlikely to see the United Nations as having a central role in this area. As well, most Member States have trouble seeing the NACD element in peace operations and, if they do accept this conceptual leap, see peace operations as being so different from traditional NACD that there is nothing to be learned from one to the other.

Apart from a modest resolution reiterating the importance of verification, it is difficult to see where the UNGA can go on this matter. Certainly, any reference to the 1995 United Nations Study will cause a break in consensus, as occurred in 1995. Proposing further United Nations consideration of verification principles and guidelines is also unlikely to be met with much enthusiasm because this is not seen as a priority. One possibility might be to try to push for greater recognition of the United Nations’ role in monitoring and verifying the NACD element in peace operations and arms embargoes. However, a great deal of political baggage will have to be overcome if such an effort is to be successful.

In terms of norm-building, a more important effort might be to focus on regional organisations such as the ASEAN Regional Forum (ARF) and the Organization of American States (OAS). Such a regional focus would concentrate on emphasising the important role that NACD can play in regional security affairs and the critical nature of effective verification for successful NACD.

Verification Infrastructure

While improvements in this area might be a useful task for the United Nations to undertake, it is hard to justify them as essential or a priority, especially in the environment of severe resource constraint faced by the organisation. If anything is to be done in this area, it will likely have to be financed by special efforts of Member States. Despite the recommendations of the 1990 and 1995 United Nations studies, the organisation has done little to develop a United Nations verification database. One possible action might be for Canada to press ahead, perhaps with United Nations Institute for Disarmament Research (UNIDIR) assistance, to create such a database.

Another idea might be to promote a “verification fellowship” or training programme especially intended for Third World diplomats and officials. This might best be done with the support of a consortium of Member States following the model of the United Nations Disarmament Fellowship.

Finally, thought might be given to establishing a regular process or forum under the rubric of the United Nations for promoting the exchange of views among various NACD verification regimes. The easiest

thing to do in this regard might be to establish an annual, or perhaps biennial, conference where representatives from various treaty bodies — i.e., IAEA, OPCW, CTBT Organisation — peace operators — i.e., UNSCOM, UN/Department of Peacekeeping Operations — regional organisations — i.e., Organization for Security and Cooperation in Europe, NATO/Verification Implementation and Coordination Staff — as well as others involved in verification/monitoring, could meet to share informally their views on operations and concepts.

Needless to say, any of these undertakings would not be cheap. On the other hand, we are not talking about an outrageous expense. Moreover, such modest initiatives might have a real benefit in terms of promoting NACD verification expertise, cross-fertilisation of ideas, and building an international verification infrastructure.

Operational Activities

In the realm of traditional NACD, apart from the special case of the IAEA, there seems very little likelihood for enhancing the role of the United Nations in verification. Most Member States seem very wary of this idea: the big powers because they don't want to give the United Nations real independent power over their own activities; and smaller less-developed states because they fear an interventionist United Nations that would be used by the big powers against their interests. Moreover, there is a natural reticence by the parties to formal NACD agreements to allow non-parties (under the guise of the UN) to have a say in verification of those agreements; the United Nations is not seen as a neutral third party, as it might be by adversaries in peace operation contexts. There is also some logic to the contention that verification operations are essentially "agreement specific," because it is the obligations of a specific agreement that are being verified, perhaps involving unique methodologies. On the other hand, does this really mean that one organisation cannot verify obligations deriving from different agreements? Do the RCMP, FBI, or customs officials, for example, only enforce one act of legislation? Whatever the merits, the "agreement specific" argument will be used to constrain expansion of a United Nations verification role. Finally, the poor reputation of the UN for inefficiency and ineffectiveness is a severe constraint for many Member States. In sum, a United Nations-based international verification organisation covering existing NACD agreements remains a remote possibility.

One potential exception to this general statement is the United Nations' residual role in dealing with cases of non-compliance with NACD obligations that are referred to the Security Council by treaty-specific organisations or by Member States. The Security Council has already stated that it will consider proliferation of weapons of mass destruction as a threat to international peace and security.¹¹ One idea suggested to facilitate this UN function has been the development of a Security Council capability to

¹¹United Nations Security Council, "Note by the President of the Security Council," S/23500, 31 January 1992, 4.

investigate or verify non-compliance — an idea sometimes linked to UNSCOM or a successor body. In addition, the Secretary General already has an investigative power which has been used in the past — i.e., with respect to the 1925 Geneva Protocol case — and could be used in the future in a NACD verification context. Both the 1990 and 1995 United Nations Verification Studies called for the strengthening of this fact-finding capacity. In some limited ways this has been done through the establishment of rosters of national experts, though the impression remains that this process is still largely *ad hoc* in nature and not as efficient as it might be. Reliance is still placed on contributions from Member States rather than an independent UN capacity.

In a related vein, there have been suggestions for improving the capacity of the United Nations to analyse verification-like data, such as that flowing from various NACD registers like the Conventional Arms Register, or information related to conflict prevention/crisis management situations. The analysis of overhead imagery might form one dimension of such a capability. The recent DFAIT report on a United Nations Centre for Information, Training, and Analysis (CITA) is one example of such ideas.¹² Canada's proposals regarding a United Nations Rapid Reaction Capability also incorporates similar notions.¹³

As publicly available information grows in volume and technical nature, traditional United Nations analytical processes may no longer be adequate. Clearly, there is a perception by many that the UN needs to strengthen its ability to collect and analyse in a timely fashion information relevant to its peace and security functions, independent of the contributions that Member States might choose to make. Such a capability could, among other things, be used to address NACD verification questions. But this development would entail giving the UN an *independent* capacity to analyse and come to conclusions. It is far from clear that Member States want this and it seems unlikely that it will happen, at least in formal terms, in the near future, except perhaps in strictly defined *ad hoc* situations such as UNSCOM. It is possible, nevertheless, that such a capability might evolve *informally* within the United Nations simply because it is essential if the UN is to function in a meaningful way in the peace and security field.

In the realm of non-traditional NACD verification operational activities, the United Nations will remain an important player. There are probably a host of practical, if mundane, ways why the United Nations' capability to undertake NACD verification in peace operation contexts should be strengthened. The 1995 United Nations Study suggested a few. This is probably an area where significant research and action can

¹²Patricia Bliss McFate, F. Ronald Cleminson, Sidney N. Graybeal and George R. Lindsey, *Verification in a Global Context: The Establishment and Operation of a United Nations Centre for Information, Training and Analysis (CITA)*, Arms Control Verification Studies No. 7 (Ottawa: Department of Foreign Affairs and International Trade, February 1996).

¹³Canada, *Towards a Rapid Reaction Capability for the United Nations* (Ottawa: September 1995).

be expected, even in these tight financial times. However, while there might be an even greater recognition of the value of such improvements, they are unlikely to be seen in NACD terms.

Future cases of peace enforcement will probably be rare, but important when they happen. Can the UN's capacity in this area be improved? Probably, but given the unpredictability and limited likelihood of such operations, it is difficult to see specific actions being taken in this regard. Any United Nations capacity to verify NACD obligations deriving from peace enforcement will more likely derive from capacities developed for other contexts — such as peacekeeping — or be *ad hoc* in nature, as is UNSCOM.

With respect to arms embargoes — one type of peace enforcement, if you like — the United Nations will probably remain an important actor, but there seems to be little prospect for improvement of the chaotic state of embargo monitoring/verification. This area too is not usually seen as being a case of NACD verification. Nevertheless, there is a crying need to undertake serious research into this area, if only because more effective embargoes might be an effective tool for the international community short of armed intervention.

There may well be an NACD dimension to cyberspace. Whether there will be an important United Nations involvement in this context is not at all certain. A UN role in verifying NACD obligations with respect to outer space seems unlikely in near future. In the longer-term, a more active United Nations role might be conceivable.

Canada and the United Nations' Role in Verification

It would be easy to question why we should waste our time and resources on a United Nations role in verification, especially in the face of the indifference of the international community. But NACD will continue to be an important dimension of international peace and security. The parameters and nature of some NACD obligations may be changing in some respects, but monitoring and verifying of compliance with such obligations remains vital. It is just as true today as it was during the Cold War that declarations of good behaviour are not sufficient. Moreover, increased pressures to develop innovative and cost-effective approaches to monitoring and verifying NACD obligations can be expected.

There is a Canadian bias toward improving the United Nations role and capacity in the security field in general. The UN has long been seen as central to Canadian interests, including in the area of international peace and security. This perspective is not, however, shared by all Member States, affecting what action is feasible.

Whether NACD verification is one area of the security field where the United Nations role and capacity should and can be enhanced is a difficult question to answer. An effort has been made in this chapter to outline areas where the United Nations already has a legitimate role and where it is active. In some of

these areas, there are possible avenues where the UN could improve its performance; in some areas there appears to be a fair degree of agreement though not necessarily consensus that the United Nations needs to do so. With respect to verification norm-building and infrastructure functions, some activities could be pursued, which are not too expensive and which would have some positive impact. But the question remains as to just how important these functions are. The answer is probably that they are useful but not essential.

With respect to verification operations, enhancing the role of the United Nations with respect to traditional formal NACD agreements is probably a non-starter. Despite reasonable arguments that there might be real cost savings and synergies to such a role for the UN, it is not politically feasible at this time or in the foreseeable future.

Perhaps the most important area where the United Nations' role can and should be enhanced relates to NACD in peace operations. This will likely happen regardless of whether the NACD community is involved or not. A significant constraint on inputting an NACD perspective into this process is that those who are responsible for peace operations, both within the United Nations and within national bureaucracies, are different from those dealing with NACD. This different bureaucratic structure follows from traditional categories of security thinking. There is a need for better communication and integration of these processes and structures. While the need may be present to improve United Nations verification of arms embargoes, there seems little likelihood of much progress in this area, though further research activity would be beneficial.

What is the bottom line? It probably relates to whether the international community wants a norm-based international system and whether it is willing to pay the price of achieving this aim. In domestic society, monitoring and verification of compliance with norms goes on all the time, whether the issue is criminal or contractual in nature. If we want a similar norm-based international society, then verifying and monitoring compliance will also be an essential ingredient. Without this function, it is difficult to see how such a system could operate — good faith is simply not enough. To quote from the first submission to the United Nations by Canada on the question of verification:

[Verification] should meet the need to institutionalize in the context of relations among states the kind of accepted rules, procedures and expectations as those that govern the conduct of relations among individuals in all civilized societies. Such rules and procedures do not presume bad faith or malevolent intent on the part of others, but they allow for such a possibility and provide a framework in which unjustified accusations

could be authoritatively rebutted, misunderstandings clarified and resolved, and non-compliance objectively established.¹⁴

To the extent that the United Nations is a key player in the peace and security dimension of the international system, and it seems likely to continue to be so, then the organisation should have an active role in certain carefully defined areas of verification.

¹⁴Canada, [Response to Resolution 40/152 O], in United Nations Secretary General, "Verification in All Its Aspects: Report of the Secretary General," A/41/422, 11 July 1986.

Table 1: A Brief Overview of United Nations Treatment of the Issue of Verification

YEAR	NAME	DESCRIPTION	OUTCOME
1978	Second UNGA Special Session on Disarmament (UNSSOD II)	Included some basic verification concepts in its Final Document.	Adopted by consensus.
1985	UNGA Resolution 40/152 O	First UNGA resolution devoted to verification exclusively. Emphasised importance of verification. Initiated by Canada.	Adopted without a vote.
1986	UNGA Resolution 41/86 Q	Requested UNDC to consider the subject of verification. Initiated by Canada.	Adopted without a vote.
1987	UNGA Resolution 42/42F	Requested UNDC to continue its consideration of verification. Verification became an independent item on the agenda of the UNGA. Led by Canada.	Adopted without a vote.
1988	UNDC Working Group Report on Verification (A/S-15/3)	The UNDC report contained sixteen agreed verification principles, a section on provisions and techniques of verification, and views on the role of the UN and its Member States in verification. Canada chaired the UNDC Working Group on Verification during 1987 and 1988.	Adopted by consensus.
1989	UNSSOD III	Deliberations focussed on the question of the role of the UN in verification.	No Final Document adopted, although there seemed to be a consensus emerging on verification.

YEAR	NAME	DESCRIPTION	OUTCOME
1988	UNGA Resolution 43/81 B	Acknowledged that the UN was already playing a useful role in verification and can make a significant contribution; endorsed the UNDC sixteen verification principles; and, requested the UN Secretary General to undertake a Group of Experts study on the role of the UN in the field of verification. Canada and Sweden led on this resolution.	Recorded vote of 130 to 1 (U.S.) with no abstentions. The U.S. stated it voted no because verification arrangements must be developed and agreed by negotiating parties and it did not see how the Secretary General could undertake a study on the role of the UN in verification in the abstract.
1990	UN Group of Experts Report on the Role of the UN in the Field of Verification (A/45/372)	The report analysed the concept of verification including its definition and functions; described a range of verification methods and techniques, as well as existing activities of the UN in verification; and, made three general recommendations concerning improvements to the UN role: (1) a UN data-bank on verification, (2) promotion of exchanges between experts and diplomats, and (3) support for the Secretary General's fact-finding activities concerning compliance with ACD agreements.	Report adopted by consensus.
1990	UNGA Resolution 45/65	Welcomed the Group of Experts report and requested Secretary General to take appropriate action within existing resources on the report's recommendations. Led by Sweden	Adopted without a vote.

YEAR	NAME	DESCRIPTION	OUTCOME
1992	UNGA Resolution 47/45	Requested Secretary General to seek views of Member States <i>inter alia</i> on how verification can facilitate UN activities in peace operations, and on additional actions concerning the role of the UN in verification, including further UN studies. Led by Canada.	Adopted without a vote.
1993	UNGA Resolution 48/68	Requested the Secretary General to undertake a follow-on Group of Experts study, in view of significant developments in international relations since 1990, that would examine the lessons from recent experience, with particular attention to ways verification can facilitate UN activities in confidence-building, conflict management, and disarmament; explore further development of guidelines and principles; and, review the conclusions of the 1990 Study. Led by Canada.	Adopted by 145 to 0 with 22 abstentions (incl. EU members and U.S.). In explaining its abstention, the U.S. said it was premature to undertake a new study; it was too sensitive to examine work of UNSCOM and UNSCOM experience had doubtful relevance to arms control and other UN activities; and, the expense of a new study should be avoided in view of the financial burden on UN of new peace operations. Belgium, on behalf of EU members, explained their abstentions in similar terms and added that it was inappropriate to deal with verification in the abstract outside treaty specific contexts.

YEAR	NAME	DESCRIPTION	OUTCOME
1995	UN Group of Experts Report on Verification in All Its Aspects, Including the Role of the UN in the Field of Verification (A/50/377)	The report expanded the 1990 Study's definition of verification beyond formal agreements to include "obligations"; reviewed the conclusions of the 1990 Study and implementation of its recommendations; described UN verification and other relevant international developments since 1990; explored possible future activities by the UN in verification; and, made recommendations concerning the role of the UN in verification in three general categories: (1) facilitation/coordination, (2) common services, and (3) operations.	Adopted by consensus.
1995	UNGA Resolution 50/61	Took note of the 1995 Group of Experts report and commended it to attention of Member States, and encouraged Member States to assist the Secretary General in implementing its recommendations. Led by Canada.	Adopted 157 to 1 (U.S.) with 6 abstentions (DPRK, France, Georgia, Israel, Monaco, UK). In explaining its negative vote, the U.S. reiterated it had not supported setting up the study and could not endorse its conclusions or recommendations. The UK also said it could not endorse the study's recommendations which ran counter to the view that verification measures should be treaty-specific.

Table 2: A Synopsis of the Results of the 1995 United Nations Group of Experts Study

<p><u>Ideas for Verification Guidelines and Principles:</u></p> <ul style="list-style-type: none">C the importance that transparency has for verification;C the importance of verification for providing early warning of non-compliance with obligations;C the role that neutral third party verification can play, particularly when there is hostility among the parties to a conflict;C the need to verify the absence of <u>un</u>declared activities inconsistent with obligations, as well as verifying declared information;C the growing importance of cost-effectiveness in verification as well as of using the synergies between verification methods and between verification organisations to improve verification;C the value of pooling verification resources among parties and of common services by an international organisation;C the need for suitable start-up periods and joint training and research;C the benefits of sharing information from national and multilateral sources; and ,C the importance of independence and impartiality for international verification organisations.
<p><u>Recommendations:</u></p> <ul style="list-style-type: none">a) facilitation/coordination:<ul style="list-style-type: none">C promotion of the exchange of verification experience; and,C encouragement of cooperative monitoring and verification experiments.b) common services:<ul style="list-style-type: none">C development of a number of databases relating to verification;C establishment of a modest, operationally-oriented centre for information, training, and analysis;C development of standard procedures and channels for, as well as encouragement of, sharing with the UN of national source verification data;C development of a training programme for verification implementers; and,C expansion of existing agreed verification guidelines and principles.c) operations (neutral third party verification):<ul style="list-style-type: none">C provision by the UN of verification assistance on request;C exploration of better preparation and systematisation of verification in peace operations and in sanctions;C systematic collection of verification experience deriving from UN peace operations; and,C investigation of the leasing or purchase of commercial remote sensing aircraft for UN verification activities.