Information Warfare Arms Control: Risks and Costs

Maxie C. Thom

INSS OCCASIONAL PAPER
MARCH 2006
63

US AIR FORCE
INSTITUTE FOR NATIONAL SECURITY STUDIES
USAF ACADEMY, COLORADO

Information Warfare Arms Control: Risks and Costs

Maxie C. Thom

INSS Occasional Paper 63

March 2006

USAF Institute for National Security Studies
USAF Academy, Colorado

****

Comments pertaining to this paper are invited; please forward to:

Director, USAF Institute for National Security Studies
HQ USAFA/DFES
2354 Fairchild Drive, Suite 5L27
USAF Academy, CO 80840
phone: 719-333-2717
fax: 719-333-2716
email: inss@usafa.af.mil

Visit the Institute for National Security Studies home page at
http://www.usafa.af.mil/df/inss

TABLE OF CONTENTS

FOREWORD

We are pleased to publish this sixty-third volume in the *Occasional Paper* series of the United States Air Force Institute for National Security Studies (INSS). This paper is the fourth INSS Occasional Paper that addresses the important area of information operations and information warfare within international law and security negotiations, and within United States national security and homeland security strategy. In Occasional Paper #9 (April 1996), Richard Aldrich presented a seminal study of *The International Legal Implications of Information Warfare*. Aldrich followed in Occasional Paper #32 (April 2000) addressing *Cyberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Legal Regime*. In the companion Occasional Paper #33 (May 2000), Steven Rinaldi analyzed the issues confronting *Sharing the Knowledge: Government-Private Sector Partnerships to Enhance Information Security*.

In this Occasional Paper, Maxie Thom updates and reiterates many of the legal and policy themes developed by Aldrich and Rinaldi, this time within the context of a cost and risk analysis of an international security regime regulating information warfare. The "arms control" approach to enhancing national security has always involved balancing conflicting potentials; the potential gains from international cooperation, norms, and law versus the potential damage from others' non-compliance and one-sided advances under the cover of ignored treaty constraints. For the United States, any cyber regulation also involves complex government-private sector relationships and responsibilities, potentially magnifying the impact and complicating implementation and monitoring of any regime. Thom renews a call for careful and cautious engagement while giving full weight to a series of likely costs and potential risks as the international community continues to examine possibilities of a cyber regulatory regime that could affect the United States, and the US military, perhaps more than any other national player in this global game.

About the Institute

INSS is primarily sponsored by the Strategic Security Directorate, Headquarters US Air Force (HQ USAF/A3S), and the Dean of the Faculty, USAF Academy. Other sponsors include the Secretary of Defense's Office of Net Assessment (OSD/NA); the Defense Threat Reduction Agency (DTRA); the Air Force

Information Warfare Center (AFIWC); The Army Foreign Military Studies Office (FMSO); the Army Environmental Policy Institute (AEPI); the United States Northern Command/North American Aerospace Defense Command (NORTHCOM/NORAD); and the United States Military Academy Combating Terrorism Center (CTC). The mission of the Institute is "to promote national security research for the Department of Defense within the military academic community, to foster the development of strategic perspective within the United States Armed Forces, and to support national security discourse through outreach and education." Its research focuses on the areas of greatest interest to our sponsors: strategic security and WMD proliferation, homeland defense and combating terrorism, regional and emerging national security issues, air and space issues and planning, and information operations and warfare.

INSS coordinates and focuses outside thinking in various disciplines and across the military services to develop new ideas for defense policy making. To that end, the Institute develops topics, selects researchers from within the military academic community, and administers sponsored research. It reaches out to and partners with education and research organizations across and beyond the military academic community to bring broad focus to issues of national security interest. And it hosts conferences and workshops and facilitates the dissemination of information to a wide range of private and government organizations. In these ways, INSS facilitates valuable, cost-effective research to meet the needs of our sponsors. We appreciate your continued interest in INSS and our research products.

//signed//

JAMES M. SMITH, PhD
Director

EXECUTIVE SUMMARY

Since the end of the 1991 Gulf War, information warfare has taken a prominent role in transforming the military as envisioned in *Joint Vision 2010.* However, due to the rapid changes in information technologies and the low cost, wide availability and high payoff of information warfare weapons, some have seen it as a destabilizing influence and have called for international arms control agreements to govern its use. Although the international legal system and the modern concept of arms control were able to provide for national and international collective security during the Cold War, information warfare presents many challenges that question their viability. The most significant challenges are to the international legal system, which include undermining the ordering principle of the post-Westphalian international system. Despite these challenges, an information warfare arms control regime is still achievable; however, at potentially significant costs and risks. Although some of these costs would be similar to previous nuclear, biological, and chemical weapons arms control agreements, the lack of available data makes it difficult to determine the expected costs with any degree of accuracy. In addition, some of these costs cannot be expressed in budgetary terms; therefore, they are presented as risks and include increased proliferation, intelligence loss, cheating, and a false sense of security. Since there are also political risks by not becoming a signatory to international agreements on this issue, the U.S. would be best served by staying engaged in the discourse to shape the norm for information warfare in the international arena.

INFORMATION WARFARE ARMS CONTROL: RISKS AND COSTS

INTRODUCTION

Background

For many strategic studies scholars and Department of Defense strategic analysts, the successful integration of emerging technologies and innovative ideas in the 1991Gulf War was a precursor for a revolution in military affairs (RMA);[1] this dominated the discourse on US national security for the remainder of the 1990's. This modern RMA was characterized by the development of precision-guided munitions; improved Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities; information warfare; and nonlethal weapons.[2] DOD strategists were enthralled with the concept of a modern RMA because it could allow a smaller but more advanced and lethal military to protect US national interests with unprecedented efficiency.[3] More importantly, it could help to solve many of the strategic dilemmas for the United States in the post-Cold War international environment. In order to capitalize on the new technologies and realize the promise from the RMA, the Chairman of the Joint Chiefs of Staff produced *Joint Vision 2010 (JV2010)* to serve as the framework for transforming the military. In addition, *JV2010* provided conceptual clarity for the key to this transformation, information superiority. Specifically, it stated

> We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.
>
> Information superiority will require both offensive and defensive information warfare (IW). Offensive information

> warfare will degrade or exploit an adversary's collection or use of information. It will include both traditional methods, such as a precision attack to destroy an adversary's command and control capability, as well as nontraditional methods such as electronic intrusion into an information and control network to convince, confuse, or deceive enemy military decision makers.
>
> There should be no misunderstanding that our effort to achieve and maintain information superiority will also invite resourceful enemy attacks on our information systems. Defensive information warfare to protect our ability to conduct information operations will be one of our biggest challenges in the period ahead.[4]

However, while DOD sought to achieve the vision depicted in *JV2010* and operationalize the concept of information warfare by developing the doctrine and fielding units and organizations to specialize in this new type of warfare, security scholars were analyzing the evolving concept and warning of its inherent danger.

Raising the Alarm

As early as 1995 theorists and strategists argued that due to its relatively low cost, wide availability, and relatively high payoff, information warfare would have a destabilizing effect on international relations. The central point of the debate was the notion that potential adversaries did not need an industrial database nor were they required to invest a substantial portion of their GNP to achieve the effects that are usually associated with medium- to large-scale interstate warfare. As a result of these concerns, some called for international agreements to govern the use of information warfare. The first draft treaty for information warfare circulated on the internet in 1995 and simply stated, "The parties to this Convention agree not to engage in information warfare against each other"; however, it was not taken too seriously.[5] The first serious attempt came from Russia in 1998 and called on the First Committee of the United Nations to explore the need for an international agreement to address arms control for information

warfare weapons.[6] However, the United States did not officially express an interest in pursuing an information warfare arms control regime until 2004.

In July 2002, President Bush signed National Security Presidential Directive 16 (classified), which clarified circumstances under which the United States would be justified to launch computer network attacks against foreign adversary computer systems.[7] This development rekindled the discussions on the use of international agreements to regulate this potentially devastating weapon. More importantly, it may have motivated US policy makers to take action because the 19 July 2004 Congressional Research Service Report for Congress titled *Information Warfare and Cyberwar: Capabilities and Related Policy Issues* posits "possible effects of international arms control for cyberweapons" as a potential policy issue for Congress.[8] As with any other international agreement, an information warfare arms control agreement would present risks and costs for the United States. This report will explore these potential risks and costs.

Defining Terms

One of the first challenges to overcome in any discussion on information warfare is the definition, since "information warfare" means different things to different people. In addition, some have used the term interchangeably with "netwar," "cyberwar," and "infowar." To arrive at a definition for use in this paper, I started with the stated definition in the congressional report that questioned the need for an information warfare arms control regime, which is:

> Information itself is now a realm, a weapon, and a target. An information-based attack includes any unauthorized attempt to copy data, or directly alter data or instructions. Information warfare involves much more than computers and computer networks. It is comprised of operations directed against information in any form, transmitted over any media, including

> operations against information content, its supporting systems and software, the physical hardware device that stores the data or instructions, and also human practices and perceptions.[9]

However, for the purpose of this research, this definition is too broad. While certain information warfare capabilities primarily fall within the purview of state actors, such as deception and psychological operations, others, such as computer network attack, may also be executed by criminals and terrorists who will not abide by an arms control regime.[10] Therefore, for this paper, information warfare activities are limited only to those executed by state actors during interstate conflict or warfare.[11]

Organization

The paper consists of five parts. The first section will focus on how information warfare is securitized, since some have argued that although it is a concern, it is not a significant threat that warrants attention in the international arena. Section two briefly looks at the usefulness of arms control in the post-Cold War international environment. The concern is that arms control may have lost some of its luster since the end of the Cold War and may not be a viable institution to mitigate threats to the international order. Therefore, if information warfare is indeed a threat, it will be risky to rely on an outdated institution to provide for collective international security. Since an arms control regime is an international legal agreement, section three looks at the current international legal issues in information warfare and the implications they would have for an arms control regime. Section four explores the potential costs and will take a qualitative approach, since cost data are traditionally hard to generate and they are also hard to glean from previous arms control regimes. The fifth section explores the risk incurred by entering or not entering an agreement.

SECURITY

> The difference between normal challenges and threats to national security necessarily occurs on a spectrum of threats that ranges from trivial and routine, through serious but routine, to drastic and unprecedented. Quite where on this spectrum issues begin to get legitimately classified as national security problems is a matter of political choice rather than objective fact. Setting the security trigger too low on the scale risks paranoia, waste of resources, aggressive policies and serious distortions of domestic political life. Setting it too high risks failure to prepare for major assaults until too late.[12]

Is information warfare a threat to national security that warrants attention in the international arena? According to some experts, information warfare can be considered "war on the cheap" because one million dollars and twenty individuals, employing computer network attack, can "bring the US to its knees;"[13] $10, 000 and ten individuals can disrupt the defense information infrastructure (DII) for weeks;[14] and for $30 million, one hundred individuals could corrupt the national information infrastructure (NII) in such a manner that would take years to rectify.[15] Even if these experts were overly optimistic and the costs were actually 10 times what they asserted, it would still be significantly cheaper than many of the US major weapon systems during the same time frame, as shown in Table 1 below.

However, others have also looked at information warfare and concluded that while it is a concern it is not a serious threat to national or international security. In fact one author suggests that there is not a significant threat, and "hoaxes and myths about information warfare contaminate everything from official reports to newspaper stories."[16] He further adds, it is difficult to get the "ground truth" because "most of the people who are knowledgeable are on the government's payroll or in the business of selling computer security devices and in no position to serve as objective sources."[17] It would appear that the

Table 1: 1999 Program Acquisition Costs for Selected Weapon Systems

Weapon System	Program Acquisition Costs[18] ($M)	Quantity	Unit Costs ($M)
F/A-18E/F Hornet[19]	3178.2	30	105.9
C-17 Airlift Aircraft[20]	3192.2	13	245.6
E-8C Joint Stars[21]	663.2	2	331.6
Multiple Launch Rocket System (MLRS)[22]	152.1	24	6.3
Abrams (M1) Tank Upgrade Program[23]	702.2	120	5.9
LPD-17 Amphibious Transport Dock[24]	638.2	1	638.2

Source: Department of Defense, *Program Acquisition Costs by Weapon System: Department of Defense Budget for Fiscal Years 2000/2001*, (Washington, D.C.: 1999), on-line., Internet, 2 April 2005, available from http://www.defenselink.mil/ comptroller/ defbudget/fy2000/FY2000_weabook.pdf.

United Nations may subscribe to this latter view in light of the absence of information warfare from its latest assessment of current and future threats to international peace and security.

Following a speech to the UN General Assembly in September 2003, the Secretary General, Kofi Annan, convened a high-level panel that was charged with assessing the current threats to international peace and security, evaluating how existing policies and institutions have addressed those threats, and making recommendations to strengthening the United Nations in order to provide collective security for all in the twenty-first century.[25] In December 2004, the High-Level Panel reported its findings and defined "six clusters of threats with which the world must be concerned now and in the decades ahead" to include: economic and social threats; inter-state conflict; internal conflict; nuclear, radiological, chemical, and biological weapons; terrorism, and transnational organized crime."[26] In addition to

suggesting by exclusion that information warfare was not a serious threat to the international order, the inclusion of non-military threats also served to fuel a larger debate that has raged amongst security scholars for the past fifteen years. The significance of this ongoing debate is that outside the UN, both sides of the issue can agree that information warfare is a threat that warrants attention in the international arena.

Since the end of the Cold War, strategic studies scholars have questioned the primacy of the military element as the quintessential defining threat to national security.[27] Those who have raised this question have pointed to existing challenges from other sectors of society that should supplement the military sector in this defining role. As a result, within the field of strategic studies, there are primarily two views as to what constitutes a threat to national security: the military-centric traditionalist view, and the new one presented by the wideners.[28] While the traditionalists maintain a focus on the military and political sectors to define the threat, the wideners would also embrace environmental, economic, and other societal challenges as well., Although this debate has continued for the past 15 years without a resolution in sight, both traditionalist and wideners can agree that information warfare is a threat to national security, since it can threaten the military, economic, and political sectors both independently and simultaneously.

Within the discourse of security in the international arena, Barry Buzan states, "security is a self-referential practice in that the issue becomes a security issue not necessarily because an existential threat exists but because the issue is presented as such a threat."[29] A closer look at the deliberations on information warfare will show that those who are charged with securitizing issues for the state have securitized

information warfare within the military, political, and economic sectors, and in doing so have made information warfare a security issue within the international arena.

Military Sector

Within the military sector, the ruling elite generally define the security threats, and the state is the referent object that is being threatened. In addition, intergovernmental organizations and their responsible officials, such as the United Nations and its Secretary General, also have a limited ability to invoke abstract and collective principles as referent objects within this sector.[30] The following is a partial list of responsible actors who have securitized information warfare within the military sector over the last decade:

- 1994—Joint Security Commission: IW is "the major security challenge of this decade and possibly the next century"[31]
- 1996—John M. Deutch, DCI: Testimony Senate Select Committee on Intelligence[32]
- 1998—Presidential Decision Directive 63: Critical Infrastructure Protection Program[33]
- 1999—Chinese Army's Political Newspaper: Liberation Army Daily[34]
- 2000—Russian National Security Concept and Military Doctrine[35]
- 2002—SECDEF: Annual Report to the President and Congress[36]
- 2004—Director DIA: Testimony before the Senate Select Committee on Intelligence[37]

Economic Sector

While both the referent objects and the securitizing actors are relatively easy to identify in the military sector, the same does not hold true for the economic sector because there are "different views about whether states and societies or markets should have priority and

whether private economic actors have security claims of their own that must be weighed against the verdict of the market."[38] Moreover, while mercantilists and neomercantilists put politics first and would give the state primacy as the securitizing actor, liberal economic theorists would disagree, since in their view the market should operate freely; hence the market and not the state should decide what constitutes a threat to economic security.[39] These and a variety of other issues, to include the "nature of economic relations under liberalism," complicate any discussion on economic security.[40] However this debate also has larger implications in the post-Westphalian international order, where the state has a monopoly on the legitimate use of force.

Identifying an issue as a threat to national security implies that drastic measures, to include the use of force, might be required to negate the threat. Therefore, if a non-state actor or private authority has the responsibility to securitize an issue, this may imply that they may also have the authority to determine the legitimate use of force, which usurps the state's monopoly. To add clarity to the issue at hand, Buzan points out that most of what is assessed to constitute a threat in economic security is actually a byproduct or "overspill" of threats in the other sectors.[41] Moreover, although national economies have a greater claim to the right of survival, rarely will a threat to that survival (national bankruptcy or an ability to provide for the basic needs of the population) actually arise apart from wider security context, such as war or a large-scale natural disaster as seen in the recent tsunami in the Indian Ocean.[42] However, in regards to information warfare, the economic sector can be threatened without necessarily affecting the other sectors. Why?

Some strategic studies scholars and international relations theorists have argued that we have moved from an agrarian, to an industrial, and

now to an information age. This concept can be summarized as "markets are migrating from geographic space to cyberspace as electronic commerce grows in both the business-to-business and the business-to-consumer spheres. Finally, physical products are becoming digital services, data transmitted electronically over the internet."[43] This migration is depicted in the works of future-theorists Alvin Toffler who coined the concept of the "third wave."[44] Moreover, since the early 1990's, many authors have equated the image of the third wave with information technology, which is summarized in Figure 1.[45]

The Third Wave Summary

Descriptor	Agrarian	Industrial	Information
Physical Security provided by:	Warrior Class, Mercenaries, Militia	Professionals, Citizens	Information Knowledgeable Leaders
Dominant Society Pol/Econ force	Tribe, City, State, Family	Nation-State, Factories	Global Conglomerates
Economy Dominated by	Trade	Money	Symbols (financial databases)
War Characterized by	Representational Conflict	Mass Armies, High Casualties	Information Attacks, minimal casualties
Ultimate Destructive Capability	Gunpowder	Mass Destruction (NBC)	Critical Data Deletion
Leadership	Hierarchical	Top Down Orders	Flat Structure
Information Based Warfare	No	No	Yes
Information technology in War	No	No	Yes
Information War	No	No	Yes

Figure 1: The Third Wave[46]

In this context, the economy is not dominated by money or trade but by symbols. Various scholars have written on this subject and share this point of view. Peter Drucker writes, "The basic economic resource—'the means of production,' to use the economist's term—is

no longer capital, nor natural resources, nor labor. It is and will be knowledge."[47] Daniel Bell adds, "The crucial point about a post-industrial society is that knowledge and information become the strategic and transforming resources of the society, just as capital and labor have been the strategic and transforming resources of the industrial society."[48] And, "Finance no longer has anything to do with money, but with information."[49] Hence, within the economic sector, the referent object is the banking and finance system that utilizes symbols, or bytes of information, that represents intra- and interstate economic transactions. The following is a partial list of securitizing actors who have securitized information warfare within the economic sector:

- 1996—John Deutch, DCI: Testimony before the Intelligence Subcommittee[50]
- 1998—Presidential Decision Directive 63: Critical Infrastructure Protection Program[51]
- 2000—Russian President Putin: Russian Information Security Doctrine[52]
- 2001 George Tenet (DCI): Congressional Hearings on Worldwide Threats[53]
- 2004—Director DIA: Testimony before the Senate Select Committee on Intelligence[54]
- 2005—French Economic school for information warfare[55]

Political Sector

In the post-Westphalian international order, sovereignty is the central ordering principle; and in the political sector, it can be existentially threatened by anything that questions the recognition, legitimacy, or governing authority of the state.[56] Additionally, states establish international regimes to help provide for their collective security; and situations that undermine the rules, norms, and institutions that constitute these regimes can also threaten them

politically.[57] Therefore, the primary referent object within the political sector is sovereignty, and the securitizing actor is the government of the state. As in the military sector, the United Nations also has a role in this sector and is also a referent object "because of its central role as the repository of the basic principles of international society and international law."[58] The following list represents securitization of information warfare within the political sector:

- 1998—Russia tabled a resolution on IW in the UN's First Committee[59]
- 1999—UN passed Resolution 53/70[60]
- 2001 - Russian President adopted Russian Information Security Doctrine
- 2003/04—Director DIA: Testimony before Senate Select Committee on Intelligence[61]

Security Dilemma

Information warfare is a threat to national security not only because of the self-referential practice of security, but also because it exacerbates the security dilemma, a key aspect of the dominant theory in international relations; realism. Realists posit that the international order is anarchical and security is a self-help system, where each state is responsible for providing for its own security. In this self-help system, the security dilemma occurs because as one state tries to increase its security, its actions may decrease the security in others.[62] In this context, a 1996 National Security Agency report that indicated over 120 states either possessed or were actively developing information warfare technology could cause angst among their neighbors and motivate others to seek like capabilities, thereby heightening the threat.[63] In addition, statements such as China's declaration that it was "committed to becoming the world's foremost information warfare power" could lead to an information warfare arms

race.[64] Can the centerpiece of US national security policy during the Cold War mitigate the threat posed by information warfare? This question is the focus of the next section.

ARMS CONTROL

For strategic studies scholars, 1962 is a landmark year for two reasons. First, it brought the Cuban Missile Crisis, where the United States and the Soviet Union were closest to the brink of a nuclear exchange, and second, it marked the start of the modern theory of arms control as we know it today, which served as the centerpiece of US national security policy for over four decades.[65] However, since the end of the Cold War, security scholars have debated the ability of arms control to adequately address the diverse threats that we now face. This section will briefly look at the institution of arms control for two reasons. The first reason is to define arms control, and the second reason is to ascertain if arms control is still a viable institution to create and maintain stability in the post-Cold War, since it would be foolhardy to rely on an outdated concept to mitigate the burgeoning information warfare threat.

Although the United States primarily depended on deterrence and defense to provide for its national security, after World War II, it also turned to disarmament to help address the nuclear arms race and ever-present threat of a nuclear war with the Soviet Union.[66] However, by the mid 1950's the United States was getting increasingly disappointed with the slow pace of disarmament efforts and eventually turned to the modern concept of arms control as an "adjunct" to national security.[67] The three main objectives of this new arms control concept were to reduce the risk of war, reduce the cost of preparing for war, and reduce the damage should war occur.[68] However, due to the devastating effects that would result from a nuclear exchange, the first objective

received most of the focus and became the centerpiece of arms control negotiations for the remainder of the Cold War. This narrow focus is also one of the points of contention for those who question the viability of arms control in the post-Cold War era. They argue that since we now face formidable technological and other non-nuclear threats, and not the nuclear threat from a peer competitor, the second and third objectives should play a greater role in new arms control regimes.

Definitions

Although there is not a universally accepted definition of arms control, over the past two decades different types of international agreements have been developed and are often addressed under the rubric of "arms control," to include nonproliferation, disarmament, confidence-building measures, and laws of war.[69] Therefore, for this paper, the general concept of arms control is defined as an "agreement among states to regulate some aspect of their military capability or potential."[70] These different varieties are represented in Table 2 along with their potential to serve as an information warfare arms control regime.

There is a general agreement that arms control played a major part in addressing and successfully managing the proliferation and employment of nuclear weapons and other weapons of mass destruction during the Cold War. Moreover, arms control was also a great success in addressing the threats from conventional arms through such regimes as the Treaty of Conventional Forces in Europe, the Stockholm Vienna Confidence and Security Building regime and the Open Skies Treaty. However, there is no general agreement on the effectiveness of arms control in the post-Cold War era, due in part to the paucity of arms control agreements since the end of the Cold War.

Table 2: Arms Control Variants

Type	Definition	Applicable for IW[71]
Arms Control Convention	Agreements that are negotiated, signed, and ratified between sovereign states that possesses the weapon or capability in question on a basis of equality and reciprocity	High
Nonproliferation	Agreements that are signed to prevent the development of a capability or to prevent acquisition by new states	Low
Disarmament	Agreements that eliminate and further prohibit particular classes of weapons universally and without discrimination	Low
Confidence-Building Measures	Agreement that serve to make military activities and armaments in question more transparent in an attempt to ally the fears of neighbors and the international community	Medium
Laws of War	International laws that guide the use of weapons and techniques in armed conflict	High

Source: Allan S. Krass, *The United States and Arms Control: The Challenge of Leadership* (Westport, Conn.: Praeger Publishers, 1997), 5-7

Outlook

From 1986 to 1993, ten major arms control agreements were signed along with numerous confidence and transparency enhancing regimes. By contrast, in the four years after the signing of the CWC in 1993, there were only two significant achievements in arms control: the renewal and indefinite extension of the Nuclear Nonproliferation Treaty in 1995, and the Comprehensive Test Ban Treaty (CTBT) in 1996, which the US Congress failed to ratify in 1999. Although partisan politics played a significant role in preventing ratification of

the CTBT, for some this failure signaled a decline in the US commitment and reliance on arms control as a mechanism to maintain national security.[72] To put this into context, failure to ratify the CTBT was the first time that a security-related treaty was defeated in the US Senate since the Treaty of Versailles.[73]

The prospects for major arms control talks and agreements have not improved since the death of the CTBT in the US Congress. As one author stated "although [President] Bush professes deep concern about the spread of weapons of mass destruction in the wake of September 11, he shows little faith in the efficacy of treaty law as a means of thwarting it."[74] Other scholars of strategic studies also share this lack of confidence in arms control. One author wrote "the traditional arms-control process of negotiating legally binding treaties that both codify numerical parity and inexpensive verification measures has reached an impasse and outlived its utility."[75] Another has looked into the future and concluded that the bipolar nature of the Cold War and the clear and unmistakable threat of nuclear weapons provided the catalyst for the United States and the Soviet Union to forge meaningful arms control agreements. Therefore, since none of these facts remain true today, "arms control as it has traditionally been understood will be much less useful."[76]

Other scholars disagree and still see a viable role for arms control now and in the future. One author views arms control as part of a broad regime of security arrangements to improve global stability.[77] A second concedes that although arms control is not the centerpiece of US foreign policy like it was during the Cold War, its "decline in visibility should not be confused with a decline in importance."[78] And finally, a third stated, "The mere act of negotiating arms-control also may lead to

better communication, deepened understanding, and reduce hostility among adversaries."[79]

During the Cold War, the preeminent objective of arms control was to reduce the risk or war. This was primarily achieved through the use of the NPT, SALT, INF, START, and the ABM treaties that served to address the clearly defined threat presented by nuclear weapons and other weapons of mass destruction. In the case of information warfare, the threat still is not clearly defined. Therefore, there is a greater need for dialogue to understand how other states perceive information warfare, especially since the technology and vulnerabilities are rapidly changing. It would be unfortunate to inadvertently escalate an international crisis by executing information warfare actions that are deemed threatening to the sovereignty or survival of another state. As a case in point, it is reported that many senior Russian military officers view cyberwarfare as a trigger for nuclear war.

> From a military point of view, the use of Information Warfare against Russia or its armed forces will categorically not be considered a non-military phase of a conflict whether there were casualties or not ... considering the possible catastrophic use of strategic information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces.... **Russia retains the right to use nuclear weapons first against the means and forces of information warfare**, and then against the aggressor state itself.[80] [Emphasis Added]

Only by engaging in discussions to establish a clear understanding can we begin to advance towards a commonality of understanding of this still yet to be clearly defined concept of information warfare. In fulfilling this role, arms control can provide a legal framework that binds the signatories to continue or discontinue specific activities or standards of practice. However, information warfare presents unique

challenges to the existing international legal system, which must be fully understood and resolved before forging an arms control regime.

INTERNATIONAL LAW AND THE LAWS OF WAR

> If the international laws of war are to persist as meaningful constraints, they must be adapted when confronted with changes in technology or other external forces that would render them inefficient.[81]

The laws of war are comprised of two types of law: conventional law and customary law. Conventional laws are made by treaties or other explicit agreement among nations under the principle of *pacta sunt servanda*, or "agreements are to be observed," and customary laws are derived from case-by-case development in the same manner as American common law.[82] One of the touted successes of international law is its ability to address the many technical changes in warfare that have occurred over the centuries. Most often, applying existing laws or creating new ones to address the new weaponry helped to manage these changes. Unfortunately, the changes presented by information warfare challenge both approaches as well as other significant aspects of the international legal system. This section will discuss three of the most significant challenges because how they are resolved will present risks and greatly influence the realization of any information warfare arms control regime.

Intangible Damage

The introduction of Allied strategic bombing illustrates how existing laws can be interpreted to address a new technology. When the Allies first conducted strategic bombing against German and Japanese cities in World War II, the laws of war did not prevent the use of the airplane in this manner. On the contrary, due to the similarity in their effects, the existing laws of war for naval bombardment were used to justify strategic bombing. Specifically, the existing rules governing

naval bombardment "permitted the legal bombardment of workshops or plants useful to the enemy war effort, allowed the bombardment of defended locations, and even permitted the bombardment of undefended locations if the local authorities did not agree to remove all facilities of military usefulness."[83] Therefore, under this ruling the laws of war for naval bombardment were applicable to strategic bombing because the effects of both actions were deemed to be the same; unguided munitions raining down to destroy the enemy's war production facilities. One of the challenges presented by information warfare is this lack of similarity with other weapons that are currently addressed by arms control agreements. Specifically, since many of the intangible effects from information warfare do not have a commonality with weapons that operate outside of cyberspace, existing laws of war may prove difficult to adapt to address information warfare.

Challenge to Sovereignty

From the US perspective, information is a domain.[84] This is echoed in *Joint Vision 2020* which states "The label full spectrum dominance implies that US forces are able to conduct prompt, sustained, and synchronized operations with combinations of forces tailored to specific situations and with access to and freedom to operate in all domains—space, sea, land, air, and **information** [emphasis added]"[85] One of the more threatening characteristics of information warfare in this domain is its ability to propogate across international networks, or through the atmosphere, as electronic signals to achieve the desired effects, all while invisible to the naked eye. Moreover, these signals can inadvertently affect other states that are geographically seperated from the intended target. This capability undermines the concept of national territorial sovereignty, which holds that each nation has exclusive authority over events within its borders

and has been a fundamental principle of international law since the 1648 Treaty of Westphalia.[86] The challenge is how to apply the concept of sovereignty in the information realm. Fortunately, the international legal system has experience with this type of challenge because this is not the first time that technology has questioned the ordering principle of the international environment.

Until the advent of satellites, a state's sovereignty extended to the airspace over its borders. However, when the question of sovereignty was raised in respect to space travel, the international community did not extend the traditional understanding of sovereignty despite the request of several nations.[87] The 1963 UN resolution on this issue stated "Outer space and celestial bodies are not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means."[88] This statement was also incorporated as Article II in the *Treaty On Principles Governing The Activities Of States In The Exploration And Use Of Outer Space, Including The Moon And Other Celestial Bodies,* commonly referred to as the Outer Space Treaty. The substance of this arms control provision is contained in Article IV in which signatories state that they will not place "in orbit around the Earth, install on the moon or any other celestial body, or otherwise station in outer space, nuclear or any other weapons of mass destruction."[89] In addition, it also limits "the use of the moon and other celestial bodies exclusively to peaceful purposes and expressly prohibits their use for establishing military bases, installation, or fortifications; testing weapons of any kind; or conducting military maneuvers."[90]

Without a doubt, the ruling on space sovereignty significantly influenced the Outer Space Treaty and paved the way for the prohibition inclusion of these activities. Similarly, a ruling on

sovereignty in the information realm will significantly influence the type of activities that are prohibited under an information warfare arms control regime; therefore, this issue must be resolved beforehand.

Ambiguous Definition in Existing International Law

One of the key legal documents that govern the use of force in the international system is the UN Charter. However, its ability to address information warfare is limited due to a lack of specificity of key terminology that forms the basis for the legitimate use of force by an individual nation state, or the international community at large. The problem largely stems from the ability of information warfare to achieve its intended effects without the "traditional" use of force. One of the most egregious examples is contained in Article 51, which recognizes a state's right to use force in self-defense against an "armed attack," and where "armed attack" is not defined.[91] Other key omissions include "aggression," "force," and "intervention." Without a clear understanding of how these basic elements of international law apply to information warfare, any attempt to establish an arms control regime will be fruitless and frustrating.

Prospects for a Regime

Despite these legal issues, the outlook is not all grim for developing an information warfare arms control regime. This discussion indicates that there are several hurdles that must be conquered before proceeding with developing a regime. In response to Russia's request in 1998, the UN General Assembly adopted resolution A/RES/53/70, which "invited members to exchange views on information security issues and ways to fight information terrorism and crime."[92] In 1999 the United States concluded that it was premature to undergo negotiations for an international agreement on information warfare.[93] Based on the unsettled legal challenges discussed in this

section, this assessment may still be true today. Nevertheless, in light of the actions taken by President Bush and the response by the US Congress, a current review of the risks and costs of an information warfare arms control regime is a prudent course of action.

COSTS FOR INFORMATION WARFARE ARMS CONTROL

One of the factors that contributed to the high-water mark of arms control was the "quantitative and qualitative leap forward in verification," and the keynote accomplishment there was the Chemical Warfare Convention (CWC) that was signed in 1993.[94] The CWC "broke the arms control mold" by establishing intrusive multilateral verification provisions that had an aggressive international inspectorate and required cooperation among governments and private industry.[95] President Reagan promoted this new standard of verification by insisting that verification must be "effective" and not just "adequate," which had been the standard during the Nixon, Ford, and Carter administrations.[96] However, the "effective" standard was soon replaced by the new standard of "cost-effectiveness," which was not surprising in light of the ongoing debate regarding the viability of arms control agreements in the post-Cold War, as previously discussed in section two. What is surprising is the speed with which the concern over cost became a major factor in arms control negotiations.

Although the 1993 CWC did not have any language to address the cost issue, by 1994 "financial implications" was one of the explicit criteria for evaluating Biological Weapons Convention (BWC) verification measures.[97] Further evidence of the concern over cost and budgetary constraints in the arms control arena is seen in the 1995 Arms Control and Disarmament Agency's Inspector General Report that stated:

> The United States will not be able to meet the funding obligations implicit in all arms control agreements currently contemplated…. Budgetary constraints, including the political momentum to achieve a balanced budget early in the next century, require persuasive evidence that expenditures to implement current and proposed international understandings serve priority U.S. interests.[98]

The effects of current budgetary pressures are seen in the level of funding for the Nunn-Lugar Cooperative Threat Reduction (CTR) program, which was lauded as "the Marshall Plan of nuclear nonproliferation," by the National Defense University's (NDU) Center for Technology and National Security Policy.[99] The significance of this program is that it allows the US Department of Defense to assist the former Soviet Union with "safe and secure transportation, storage, and dismantlement of nuclear, chemical and other weapons in order to prevent these weapons from falling into the hands of the wrong parties."[100] Although President Bush expressed a strong level of support for these programs during a 2004 address on nonproliferation, the 2005 funding request for the Defense Department and the Energy Department portions of the program were reduced by nine percent and one percent respectively compared to the FY 2004 appropriated funding levels.[101] Therefore, given the existing level of fiscal support for long recognized and already agreed on threats to our national security and the focus on cost of verification provisions over the last decade, an information warfare arms control regime must be fiscal responsible in order to successfully compete for funding from an already stressed arms control budget. This section will explore the types of cost that would be expected to support an information warfare arms control regime.

Generic Costs

The evolution of costs for a generic arms control agreement is depicted in Figure 2 and is based on data for nuclear and conventional treaties, represented by the top solid line.[102] A slight modification was made to better represent the projected cost for the CWC since it is expected to maintain a high implementation cost well beyond the point where the cost for the nuclear and conventional treaties traditionally start to decline.[103]

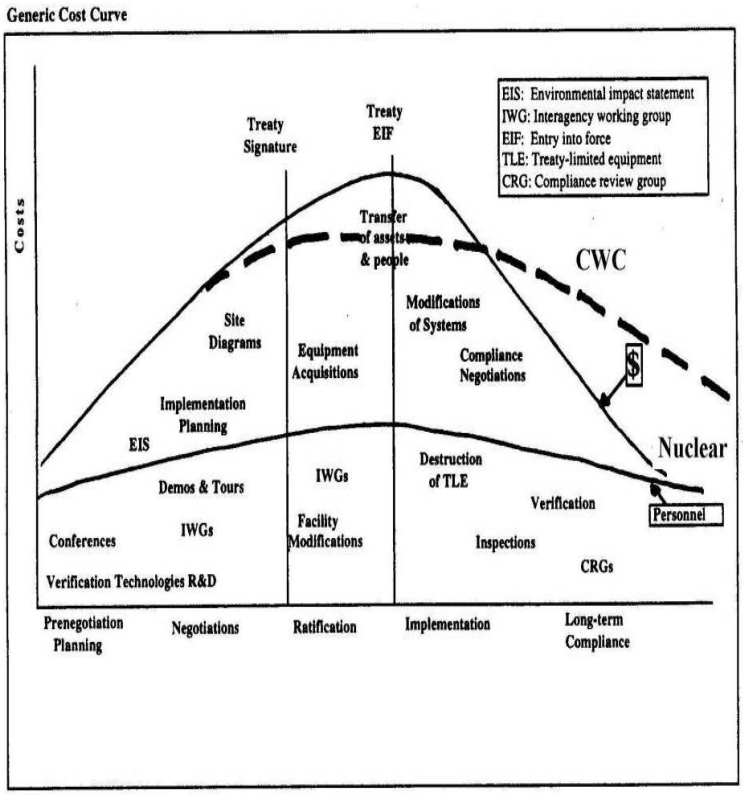

Figure 2: Generic Costs Curve[104]

One of the significant factors influencing this shift, and the resultant higher CWC cost, is the dual-use characteristic of chemical weapons technology that required very intrusive verification provisions

to ensure compliance. The cost for this aggressive intrusive verification provision is substantial and is the primary reason that the BWC does not have any such verification provisions. As one expert stated:

> Weight-for weight, BTW [biological and toxin weapon] agents are hundreds of times more potent than the most lethal chemical warfare agents, making them true weapons of mass destruction with a potential for mayhem that can exceed that of nuclear weapons. This makes their elimination by an international treaty with effective verification highly desirable. But "effective verification" of such a treaty is at best problematic and at worst an oxymoron. Because of the small scale of the facilities required and the widespread availability of necessary materials and technology, the monitoring and inspection effort required would be enormous, intrusive, and expensive. In addition…even if activities involving BW agents were discovered, there would usually be no way to tell if they were offensive (prohibited) or defensive (permitted).[105]

Since information warfare shares many of these same factors that mandated the CWC's expensive verification provisions, such as dual-use technology and small-scale production facilities, the cost curve for an information warfare arms control regime should approximate the CWC costs curve. Nevertheless, even with the best available data from previous agreements, accurate costs data for a new arms control agreement are still difficult to project. This point is emphasized by the CWC where over the past decade the projected cost to destroy weapons prohibited by the convention have increased almost 200 percent; see Table 3.

Types of Costs

Although Figure 2 depicts five phases in the evolution of a generic arms control agreement, for this paper these phases will be addressed by three types of costs that include pre-signature costs (pre-negotiation and negotiation phases), ratification costs, and post entry into force (EIF) costs (implementation and long-term compliance phases).

Table 3: Cost Estimates for Weapons Destruction under the CWC

Year of Projection	Agency	Projected Completion Cost ($B)	Projected Year of Completion
1994	DOD	8.6	2007
1998	DOD	14.6	2007
2000	GAO	14.9	2007
2001	DOD	23.7	2012
2004	GAO	> 25.0	2012

Source: General Accounting Office, "Arms Control: Status of US-Russian Agreements and the Chemical Weapons Convention" (Washington, D.C.: 15 March 1994), n.p., on-line, Internet, 17 November 2004, available from 222.fas.org/spp/starwars/gao/nsi94136.htm, 10-14; and Michael Mguyen, "GAO: US May Miss Chemical Destruction Deadline," *Arms Control Today* (May 2004), n.p., on-line, Internet, 7 Feb 2005, available from http://www.armscontrol.org/act/2004_05/GAO.asp.

Pre-Signature Costs

One of the key aspects of any arms control regime is a precise definition of what material or activity is prohibited under the agreement in question. In the case of the CWC, key terms such as chemical weapons," "toxic chemicals," and "precursor" are defined.[106] For the Ottawa Landmine Treaty terms such as "antipersonnel mine," "mine," and "anti shaking" are clearly defined.[107] And finally for the Missile Technology Control Regime (MTCR) terminology such as "development," "production," as well as the parameters of systems that are restricted for transfer, for example "…unmanned air vehicle systems (including cruise missile systems, target drones and reconnaissance drones) capable of delivering at least a 500 kg payload to a range of at least 300 km" as well as the specially designed "production facilities for these systems" are specified.[108] This requirement for specificity is critical because it helps to ensure signatories meet both the intent and the spirit of the agreement, thereby making breakout more difficult. Moreover, it helps to ensure only the

necessary activities and facilities are included in a verification provision, and the BWC illustrates this point.

In contrast to the CWC, MTCR, and Ottawa Landmine Treaty, the BWC does not define its key terminology. As a result, the lack of clearly defined terminology in the BWC, such as "microbial," "other biological agents," or "toxins" would result in the inspection of facilities such as breweries, yogurt manufactures, and agricultural ethanol plants if a verification provision was adopted.[109] Since there would be more facilities to inspect, this could significant increase the cost, decrease the probability to detect cheating, and eventually undermine the verification provision. Similarly, as already discussed in section three, key definitions that are required for an information warfare arms control regime are lacking and must be resolved during the pre-signature phase to avoid the aforementioned consequences that may result from ambiguity. This might not be an easy undertaking given that over the past decade, neither security scholars nor state actors have been able to propagate a common understanding of information warfare. Therefore, an inordinate amount of time might be required to arrive at a specific concept of information warfare for an arms control regime, which will be costly.

Another key cost in the pre-signature phase is due to research and development (R&D) of verification technologies that would help to ensure compliance with the regime in question. In the case of an information warfare arms control regime, the initial cost should be less than nuclear, biological, or chemical (NBC) agreements due to investments in this technology by the private sector. While NBC weapons were primarily developed for military use, many of the current information warfare tools were developed in the private sector for peaceful purposes, which were subsequently modified to conduct

malicious activities. Therefore, given the significance of information technology (IT) in fueling our economy and social behavior, private companies have invested in defensive technologies to counter these destructive or disruptive capabilities.

If verifications provisions are required in an information warfare arms control regime, some of these defensive capabilities can be readily applied to verify compliance. Nevertheless, the cost can still be significant due to the sheer abundance of network configurations and operating systems that must be addressed. Additionally, implementation may also require the destruction of existing arsenals, such as in the CWC and BWC, and R&D is often conducted to determine how to accomplish this in a safe and cost-effective manner. In regard to information warfare, this cost should be minimal due to the non-physical nature of most information warfare weapons.

One final cost to consider in this phase is derived from an equivalent to the environmental impact statement that is an integral part of previous NBC agreements. Although an environmental impact study

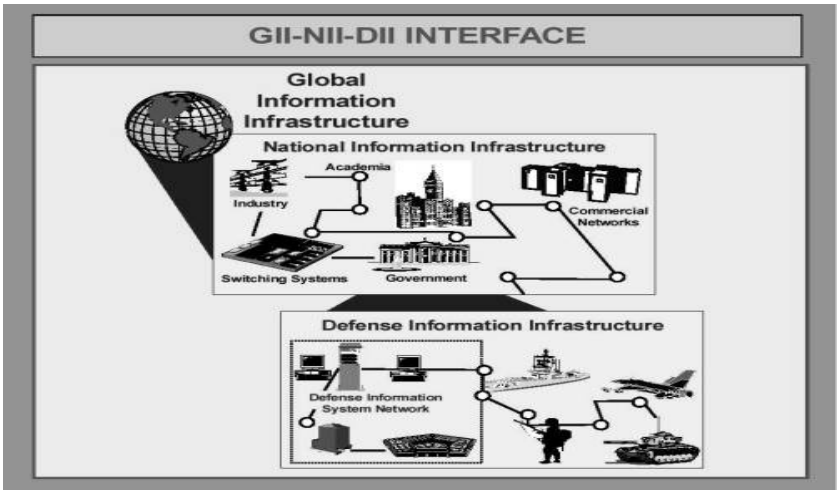

Figure 3: GII, NII and DII Relationship[110]

may not be required, a comparable study or analysis might be required for the National Information Infrastructure (NII) or the Global Information Infrastructure (GII) if intrusive verification provisions or constant monitoring of the Defense Information Infrastructure (DII) is adopted. This might be a requirement because "The DII is embedded within and deeply integrated into the NII." Their seamless relationship makes distinguishing between them difficult; see Figure 3.[111]

Ratification Costs

Once an agreement is signed, it may still be some time before it is ratified and enter into force, which can significantly increase the cost of ratification for an information warfare arms control regime; see Table 4. Moreover, the potential for significant cost increases will be greater the longer it takes for entry into force due to the rapid changes in the technology that has fueled the proliferation of information warfare weapons, the microchip.

Table 4 Entry into Force

Treaty	Signed	Entered into Force
Outer Space	Jan 1967	Oct 1967
BWC	Apr 1972	Mar 1975
Conventional Forces Europe	1990	1992
Open Skies	Mar 1992	Jan 2002
CWC	Jan 1993	Apr 1997

Source: "Treaties," *Arms Control Today*, n.p. on-line, Internet, 15 January 2005, available from http://www.armscontrol.org/treaties/.

During the late 1990's, microchip technology changed rapidly; where processor power and chip density doubled every 24 months, memory size tripled every 18 months, and the resulting cost for this new technology was halved every 18 months.[112] However, within the past few years this has changed in that processor power and chip density now double every six months, memory size triples every 6

months, and cost is now halved every 12 months.[113] This trend is further evidenced by the changes in US export controls for high performance computers (HPC).

In July 1999, the Clinton Administration announced that the policy for the export of high performance computers (HPC) would be reviewed and updated every six months in order to reflect rapid advancements in computer hardware.[114] Moreover, in October 2000, the upper limit for export HPC composite theoretical performance (CTP), measured in millions of theoretical operations per second (MTOPS), was changed for Computer Tier 3 countries, such as Afghanistan, Lebanon, and Vietnam, from 20,000 to 28,000 MTOPS. This was subsequently changed to 85,000 MTOPS in March 2001 and later to 190,000 MTOPS in December 2001.[115] The overall impact is that these faster and more powerful microprocessors can create new vulnerabilities or can lead to new information warfare capabilities or weapons.

Previous treaties have addressed this issue by including statements that prohibit all aspects of technological advancements. The ABM Treaty adopted this approach and stated

> Further, to decrease the pressures of technological change and its unsettling impact on the strategic balance, both sides agree to prohibit development, testing, or deployment of sea-based, air-based, or space-based ABM systems and their components, along with mobile land-based ABM systems. Should future technology bring forth new ABM systems "based on other physical principles" than those employed in current systems, it was agreed that limiting such systems would be discussed, in accordance with the Treaty's provisions for consultation and amendment.[116]

This approach may not work for an information warfare arms control regime for two reasons. First, since many of these new capabilities are developed in the private sector for peaceful purposes

are then modified by those who want to inflict harm, it may be difficult for an arms control agreement to inhibit these malicious activities. Second, given the rapid change in technology and with it new capabilities, there is a potential that the new capabilities may exceed the scope of the signed agreement since "no one can ban what is not yet discovered.… It is impossible to put the unknown into chains."[117] In most cases treaties and conventions automatically enter into force only after they are ratified by a predetermined number of signatories. If technology creates new security concerns that are outside the scope of the signed, but not yet ratified, arms control regime, signatories might be hesitant to ratify it and may call for more negotiations to address the impact of these changes, resulting in higher costs for the regime.

Post-EIF Costs

The cost for the implementation and compliance of an information warfare arms control regime can vary significantly and will depend on the verification provisions. The significant difference in costs between the CWC and the BWC illustrates this point. If verification provisions similar to the CWC are selected, this might entail the inspection of small IT firms and could be just as overwhelming as the inspection of breweries, yogurt manufactures, and agricultural ethanol plants would be for the BWC.[118] However, a significant portion of these costs are hard to quantify; therefore, they will be discussed in the next section as risks. Other costs in this phase include administrative costs, industry costs, and hidden or overhead costs. Although they are presented as post-EIF costs, in reality they occur throughout the evolution of an arms control regime. Nevertheless, they are presented in this section since this is where they are most costly.

Administrative Costs

One of the often overlooked costs for an arms control regime is the cost for the agency that is created to implement the verification provision, such as the Organization for the Prevention of Chemical Weapons (OPCW), for the CWC, and the International Atomic Energy Agency (IAEA) for treaties that address nuclear weapons. Although not all regimes require such an agency, if one is needed, its costs must be considered since it is funded by the parties to the agreement. In most cases, it is underfunded. A case in point is the IAEA, which only received in 2003 its first significant funding increase since 1988, despite the dramatic increase in the number of facilities and materials that require safeguarding. Upon receiving this funding, the Director General, Mohamed El Baradei, said most of the increase would to go toward the IAEA's verification program because it "has been experiencing the greatest demand for additional resources and has for years been the most chronically underfunded."[119]

The level of funding for these organizations is roughly based on the same proportion of the state's contribution to the United Nation's operations, which for the United States would be approximately 25 percent. However, the actual cost could be significantly higher based on non payment by other parties to the regime. The OPCW faced this situation before the CWC entry into force in 1997, and it has continued through 2001. In this time period a significant number of member states did not pay their assessed contributions to the budget.[120] A significant portion of the projected and approved inspections could not be carried out; this was as high as 60 percent in 2001.[121] And 20 percent of the CWC state parties lost their right to vote in the OPCW due to non payment.[122]

In response to this financial crisis the OPCW Director-General, José Bustani, warned that continued underfunding would result in a reduction in verification activities at weapon destruction facilities in the United States, India, and South Korea, and a reduction of over 80 percent of industry inspections as compared to the previous year.[123] In 2004 the IAEA faced another financial crisis when the United States and Europe threatened to cut their funding if the Non-Aligned Movement (NAM) maintained its stance to respect Iran's right to develop nuclear technology in accordance with the 1970 Nuclear Non-Proliferation Treaty.[124]

Regardless of the cause, the lack of funding can undermine the verification provision and the other states must often make contributions well beyond their fair share to maintain the sanctity of the arms control regime. Given the funding experiences of the OPCW and the IAEA, a similar agency for an information warfare arms control regime may not fare much better.

Industry Costs

As previously noted, the CWC was the keynote agreement that was signed during the high-water mark of arms control. The significant feature was the intrusive verification provisions that included the inspection of private companies in the chemical industry. Although only a portion of the inspection costs are borne by the industry, if these cost become excessive, industry and special interest groups may lobby government officials for relief or ask for rejection of the treaty. The Department of Commerce direct cost associated with these inspections was estimated at $1M annualized and consisted of the cost for personnel to process the data and fulfill the reporting requirements stipulated in the CWC.[125] As of May 2004 the, United States Department of Commerce, Bureau of Industry and Security (BIS)

reported the costs for Schedule 1 and Schedule 2 inspections under the CWC averaged $41,000 and the cost for schedule 3 and "unscheduled discrete organic chemicals" (UDOC) inspections averaged $24,000.[126] Similar costs for an information warfare arms control regime could cripple an already stressed United States IT industry that is facing stiff competition from offshore competitors such as China, Taiwan, and South Korea.

Hidden or Overhead Costs

Although these costs are not truly hidden, in most cases they are hard to obtain, estimate, or categorize. Nevertheless, they represent additional costs that must be considered to get a true estimation of how "cost-effective" an information warfare arms control regime is. This would include the salaries of military personnel serving in on-site inspection activities, FBI counterintelligence activities, temporary duty personnel from other agencies that accompany on-site inspections, personnel costs for the interagency committees and consultative bodies that analyze compliance and engage in negotiations.[127] One author summarized the significance of these cost by stating:

> The lack of detailed accounting for many of these costs is not surprising; they are often difficult to apportion accurately to different agreements, and in some cases it would not be worth the extra effort and cost to keep track of them. Such hidden costs are an unavoidable aspect of the implementation of any arms control agreement. They constitute a kind of "overhead" that will typically add a few percent to estimates of explicit costs.[128]

Summary

The intent of this section was not to conduct a cost-benefit analysis of an information warfare arms control regime. The purpose was to clearly develop what types of costs should be expected in the process of forging such a regime. Although cost-effectiveness is an important criterion it is not always the final arbiter in deciding issues of national

security. The lesson from these pages for those involved in negotiating information warfare arms control is an awareness of the costs that are involved in the evolution of such a regime.

RISKS FOR INFORMATION WARFARE ARMS CONTROL

In addition to the fiscal cost explored in section four, arms control agreements incur costs that cannot be expressed in budgetary terms. As one author stated, "No purely quantitative cost-benefit analysis of arms control is possible because benefits and risk are qualitative and depend on subjective values and assumptions."[129] This section will look at these non-quantifiable costs and risks that can be expected from an information warfare arms control regime.

International Legal System

Although information warfare is securitized and often referred to as an "electronic Pearl Harbor" threat, this characterization is not based on empirical data from an information warfare exchange in the context of interstate warfare.[130] On the contrary, most of the data was derived from simulations and wargames, such as Eligible Receiver.[131] This lack of empirical data is a challenge for the international legal system because as Oliver Wendel Holmes, a former Chief Justice of the US Supreme Court, stated, "The life of the law has not been logic; it has been experience."[132] Within US domestic law, this means that the courts seldom foresee a problem, then legislate laws, and put a legislative solution in place before the problem actually occurs. Instead, legislators create laws after the problem develops.

This also holds true for international law in that the international community does not normally negotiate treaties to deal with a problem until the results of that problem manifest themselves.[133] Therefore, until an interstate information warfare event occurs that is clearly evident to the international community at large, there is a risk in relying

on the international legal system to provide a timely "stamp of approval" to respond to an information warfare attack. Based on Article 51 of the UN Charter, a state can take action to respond in self-defense to a perceived threat or attack. However, a response might be limited to unilateral actions since other states may want to wait for a UN resolution, or another internationally sanctioned response, before supporting efforts that might be deemed illegal or classified as war crimes.

In obtaining a resolution, the threatened party may have to show an attack is imminent or the adversary is demonstrating hostile intent. With large conventional forces, high-resolution imagery can be used to convince the UN Security Council and the General Assembly that a threat does exist. This approach was used by the United States in 1990 to show Saudi Arabia the presence of Iraqi forces along the Saudi Arabian border, which resulted in access to Saudi Arabian bases and airspace for the impending military conflict with Saddam Hussein. Since the direct effects from many information warfare weapons are short-lived and may not leave behind any physical evidence to serve as the "smoking gun," it might be difficult to garner international support for a response to an attack. Moreover, given the level of skepticism from the international community over the photo imagery evidence presented by the United States to justify offensive actions against Iraq 2003, it is doubtful that a picture of a network diagram or high-energy radio frequency (HERF) detonation will galvanize support for a resolution. Even if cyber forensics can provide the smoking gun, this presents an additional risk in that it may reveal sensitive information and provide insight into one's capabilities, which will be discussed later in this section.

The international legal system also presents another risk in that it may expose citizens to crimes that are not illegal in their own state. This type of risk is highlighted in the wording of the Council of Europe's Cybercrime treaty which banned "hate speech" from the internet. While this type of prohibition is common in European nations, it can violate the First Amendment of the US Constitution, the right to free speech.[134]

Sovereignty in the Information Realm

As discussed in section three, a ruling on sovereignty in the information realm must be decided before forging an information warfare arms control regime. However, if the Westphalian concept of sovereignty is upheld, US public diplomacy programs, a polite term for what many would regard as propaganda, that fall under the purview of the Broadcasting Board of Governors (BBG) will be put at risk.[135]

The BBG was formed under the 1998 Foreign Affairs Reform and Restructuring Act and is an independent autonomous entity that is responsible for all US government and government sponsored, non-military, international broadcasting.[136] Additionally, the BBG supervises the International Broadcasting Bureau (IBB) which provides the administrative and engineering support for the broadcast operations that include Radio Free Asia (RFA); Radio Free Europe/Radio Liberty (RFE/RL), Radio Sawa, and Radio and TV Martí.

> **Radio Free Asia** – RFA is the principal BBG-sponsored broadcaster in Asia. It broadcasts news and information in nine languages to its Asian audience, where accurate and complete news might be otherwise unavailable.[137] In addition, it also broadcasts works of literature and nonfiction that have been banned in its target countries that include China, Tibet, Burma, Vietnam, Laos, Cambodia, and North Korea.[138]
>
> **Radio Free Europe/Radio Liberty (RFE/RL)** – The mission of RFE/RL is to promote democratic values and institutions by disseminating factual information and ideas to its audience that is

located in Central, Southeastern, and Eastern Europe; the Caucasus; and Central and Southwestern Asia.[139] RFE/RL reportedly played a role in the downfall of communism.[140]

Radio Sawa – Radio Sawa seeks to provide timely mews, information, and entertainment to the youthful population of Arabic-speakers in the Middle East. It began broadcasting in 2002, and originates its broadcasts from various locations, to include Washington DC.[141]

Radio and TV Marti – The Office of Cuba Broadcasting directs the operations of Radio and TV Marti. The purpose of the broadcast is to provide commentary and information about events in Cuba and elsewhere to promote the free flow of ideas in Cuba and to foster democracy.[142]

The information content of these broadcasts is viewed as a political threat by several of the target countries because in their estimation, it undermines their political system and their rule of law. As a result, some target countries are actively conducting jamming operations to prevent their populations from receiving these broadcasts. These countries include China, Cuba, North Korea, and Vietnam.[143] Therefore, if an information warfare arms control regime affirmed a state's sovereignty in the information realm, these states could claim they have the exclusive right and absolute power to determine what type of information is received by their citizens, thereby making a legitimate claim that these types of US public diplomacy programs are a violation of international law. Although this might ordinarily be difficult to enforce, because radio waves do not recognize territorial borders, if a state is overtly broadcasting information to deliberately challenge and undermine the lawful government of another state, the new ruling on sovereignty may help to cancel these broadcasts.

Verification and Compliance Risks

The CWC is often viewed as a success in arms control because of the depth and breadth of its verification provisions, which include national declarations, routine on-site inspections, consultation and

clarification mechanisms, challenge inspections, and close scrutiny of dual-use facilities in the private sector.[144] While establishing these intrusive verification provisions, the drafters of the convention realized that they also presented risks to include loss of proprietary information, release of non-treaty-related trade secrets, industrial espionage, and a higher risk of proliferation.[145] If similar verification provisions are adopted for an information warfare arms control regime, these risks may also be applicable to the IT industry along with the risk of undetected cheating and intelligence losses. This section will examine risks to the CWC to provide an understanding of how they may be applicable to the IT industry.

Undetected Cheating

To help counter the risks to the chemical industry, the drafters of the CWC developed an annex to the CWC titled "*Annex on the Protection of Confidential Information.*" This aspect of the verification provision was often referred to as "managed access," and its overall purpose was to prevent inspectors from seeing or sampling anything that the inspected party did not deem relevant to the convention.[146] However, in practice, managed access has also served to undermine the sanctity of the verification provisions and promotes undetected cheating.

While the purpose of managed access was to strike a balance between a state's genuine concern to protect proprietary or national security information and the OPCW inspector's ability to access plant sites and facility records to fulfill the inspection mandate, state-parties have overly emphasized the former concerns which have led to the ineffectiveness of the latter. In addition,

> CWC members have approved procedures giving host governments the right to confiscate and retain any piece of recording equipment that host officials claim has not been

> satisfactorily cleared of data unrelated to treaty compliance. Even more egregious, OPCW inspectors are currently required to allow host officials to copy all of the information in their notebooks, laptop computers, electronic cameras, and video recorders before they depart from an inspected industry site.[147]

This practice may also provide the inspected countries with access to new tools and techniques that can detect cheating, thereby allowing them to exploit weaknesses to further mask any prohibited activity or capability. Overall these actions by state-parties negate the provisions of the CWC that guarantees "the inviolability of inspection records so that the inspectors can perform their duties without undue interference from hostile government officials or plant managers." [148] Even without these duplicitous practices, the verification provision presents other risks such as intelligence losses.

Intelligence Losses

In December 1995, US satellites obtained photographic images that clearly showed that India was preparing to conduct a nuclear test at the Pokharan Test Site. The US ambassador to India, Frank Wisner Jr, showed the photographs to the appropriate Indian officials and succeeded in persuading India not to conduct the test.[149] The photographs revealed how the United States obtained the information and more importantly, what indicators it used to determine that a test was pending. The key indicator was the presence of cables and wires running into the shaft where the test was to be conducted.[150] Consequently, when India conducted its first nuclear test on 11 May 1998, US intelligence was caught off guard because the reliable indicator was not present as before. The revelation of US methods and capabilities had provided India with all the required information to defeat the US intelligence system. In preparing for the 1998 test, they simply buried the cables and wires that were previously exposed and served as the tipoff for the pending testing activity.[151] An information

warfare arms control regime might also present similar intelligence losses since a suspected violator of the regime may want proof that its activities were indeed discovered.

This example also illustrates a dilemma in verification provisions, especially those that rely heavily on national technical means or advanced scientific methods to detect violations. In exposing the violation they also risk revealing sensitive sources and methods, which may negate their usefulness in the future. However, there is also a risk of proliferation of the prohibited activity or capability, if the knowledge of the prohibited activity is not revealed in order to protect these sources and methods.

Proliferation Risks

Although an arms control regime might be established to help stem the proliferation of destabilizing information warfare capabilities, there is also a risk that the process of negotiating this regime might result in proliferation due to the declarations that might be required in similar fashion to the declarations in the CWC. Article III of the CWC, Declarations, required each State Party to declare and specify, among other things, the location, aggregate quantity, and detailed inventory of chemical weapons it owns or possesses; any chemical production facility it has or has had under its ownership or possession; and the precise location, nature and general scope of activities of any facility or establishment under its ownership or possession, to include laboratories and test and evaluation sites.[152] The risk is that in fulfilling this declaration, the identity of advanced weapons and their associated facilities must be revealed, which otherwise might have remained undiscovered, Moreover, this revelation could motivate others to seek to obtain parity in this capability before the regime is ratified and entered into force. Proliferation is also a risk during inspections since

inspectors could get to see the insides of advanced technology facilities and return to their home state with this knowledge.[153]

False Sense of Security

One of the purposes of verification provisions is to allow for the timely detection of prohibited activities to warn if breakout is about to occur, and intrusive verification provisions can help to further minimize this risk. However, despite the adaptation of intrusive verification provisions in an information warfare arms control regime, breakout can still occur due to two factors: the dual-use nature of information technology and its rapid changes. Consequently, an information warfare arms control regime may only provide a false sense of security.

As discussed in section four, the rapid changes in IT produce faster and more powerful microprocessors, which can create new vulnerabilities or lead to new information warfare capabilities that are beyond the scope of an established arms control regime. Even if these technological advances are prohibited by a treaty or convention in the same manner the ABM Treaty addressed new technologies for missile defense, it is unlikely that an arms control regime can prohibit the development of similar advances to fight cybercrime in the private sector. Once developed, these new technologies can be adopted for military use, which can then lead to a breakout, as witnessed in one of the earliest arms control agreements, the Washington Naval Treaty.

The 1922 Washington Naval Treaty limited battleships (the major naval weapon of World War I), aircraft carriers (the future major naval weapon system), and the number and size of guns each could carry.[154] At the time the treaty was signed, naval aviation consisted of wooden aircrafts that were relegated for use as scout vehicles. Therefore, the treaty did not address the airplane, which in reality was the weapon that

made aircraft carriers especially dangerous. Within the private sector, the all-metal airplane was developed for mail and passenger service. This technology was then adopted by the military to develop the torpedo and dive bombers, which subsequently allowed the aircraft carrier to vastly exceed the limits on offensive power imposed by the treaty.[155] The rapid changes in IT and its dual-use nature can also produce similar results for an information warfare arms control regime.

Defensive Risk

The CWC is hailed as a landmark in arms control because it banned an entire class of weapons. However, from a defensive point of view it is permissive since it did not prohibit activities "directly related to protection against toxic chemicals and to protection against chemical weapons."[156] In contrast, the ABM Treaty was restrictive for defense since it was all encompassing and purposefully set out to prohibited the deployment of antiballistic missiles (ABM), to include the testing and development of systems based on current technology, future technology, and the use of non-ABM systems in an ABM role.[157] These two examples illustrate the two extremes of how the defensive aspects of an information warfare arms control regime can be addressed. However, either of these approaches presents risk since they can both undermine the viability of an agreement.

The drafters of the ABM purposefully set out to prohibit the development of any defensive capabilities against nuclear missiles in order to deny any advantage that could be gained by conducting a first strike. The thinking was that if a potential aggressor was not able to defend against retaliation, it would be unlikely to initiate a nuclear exchange in the first place. This line of reasoning formed the basis of the mutual assured destruction (MAD) nuclear strategy. However, on 13 December 2001, President Bush announced his intention to

withdraw from the ABM Treaty because he concluded that the "ABM treaty hinders our government's ability to develop ways to protect our people from future terrorist or rogue state missile attacks."[158]

The US withdrawal from the ABM Treaty is a stark reminder that although treaties and other arms control regimes can help solve the security dilemma, a state is unlikely to remain bounded by an arms control regime if the regime cannot evolve to address new threats. Therefore, an information warfare arms control regime must contain provisions that allow state-parties to develop new defensive capabilities to counter an evolving threat or risk abandonment. However, granting these defensive provisions can also undermine the viability of the regime since defensive information warfare weapons can be used offensively and vice versa.

In September 9 1998, a group of hackers, Electronic Disruption Theater, coordinated attempts to launch an attack against DOD's primary public information Internet site, Defenselink.[159] This was a denial of service attack that used a mini-application, called Floodnet, to direct participant's computers to dial and redial the Defenselink site.[160] The purpose of the attack was to flood the Defenselink server with request to cause it to shut down or go offline. However, the Pentagon had advanced warning of the impending attack and placed its own mini-application, named Hostile Applet on the Defenselink site.[161] Consequently, when the attack was launched and Hostile Applet detected the presence of Floodnet on a new connection to Defenselink, it directed the shutdown of the browser for the new connection; thereby preventing the redial and saturation of the server.[162] Although some have called the Pentagon's actions an "active defense" and questioned its legality, this example shows how a cyber weapon, the mini-application, can be use for offensive and defensive purposes

simultaneously. Therefore, an information warfare arms control regime must strike a balance between a restrictive and permissive approach to defensive concerns since either can undermine the viability of the regime. In addition, the actions by the Pentagon highlight one of the advantages of information warfare that might be put at risk by an information warfare arms control regime.

Increased Kinetic Targeting

Based on the reported destabilizing aspects of information warfare, there is a strong possibility that an information warfare arms control regime will restrict the employment of information warfare against certain classes of targets such as critical infrastructure, restrict specific types of activities such as psychological operations, or restrict specific weapons such as computer network attack. However, for any of these outcomes there is a risk that future interstate conflicts might be more destructive due to a reliance on traditional kinetic weapons that could otherwise be replaced by less lethal non-kinetic information warfare assets.

Psychological Operations

During the 2003 Gulf War, Iraqi soldiers experienced less attrition on the battlefield due to increased desertion rates by the enlisted and officer corps, where in some cases units experienced desertion rates as high as 90 percent.[163] Based on interviews with Iraqi military personnel, one of the significant factors that led to their desertion was the US psychological warfare efforts that consisted primarily of radio broadcasts and leaflet drops.[164] In addition, the psychological warfare campaign included "sending thousands of e-mail messages to commanders, promising protection for those who comply with the order to not use weapons of mass destruction against allied forces."[165] The coalition psychological warfare campaign, specifically leaflets,

was also credited with saving the Iraqi oil fields from destruction. Although many of the oil wells were booby-trapped with explosives, the valves were switched off to minimize damage to the oil fields because as one Iraqi oil official explained, "We read your leaflets. We heard your broadcasts. We understand that keeping the oil infrastructure was important for our future. And so while we complied for our own protection with the regime, we ensured that true damage to the oil fields would not occur."[166] As these examples show, information warfare, specifically psychological operations, had a significant impact on the conduct and outcome of this interstate conflict. Without the use of information warfare there could have been a greater attrition of Iraqi forces and an ecological disaster if the oil officials carried out Saddam Hussein's orders to destroy the oil fields. However, the salient point is that these psychological operations efforts began well before the start of armed conflict and could be made illegal by an information warfare arms control regime. In fact, coalition

Figure 4 Operation IRAQI FREEDOM Leaflet (IZD-070)

aircraft scattered the first of 43 million leaflets well before the shooting war started on 20 March. The leaflet that the Iraqi oil official referred to, IZD-070, was first dropped on 10 March, (see Figure 4).

Infrastructure

During the 1991 Persian Gulf War, coalition Tomahawk missiles dispensed ribbons of carbon fiber over Iraqi electrical power switching systems to shut down the significant portions of the Iraqi power system."[167] In addition, an F-117 Stealth fighter directed precision-guided munitions through the air-conditioning shaft of the Iraqi telephone system in downtown Baghdad, taking out the entire underground coaxial cable system, which tied the Iraqi high command to their subordinates in the field.[168] These attacks on the power and telecommunications infrastructures played a critical role in rendering a significant portion of the Iraqi integrated air defense system (IADS) both deaf and blind; thereby denying their ability to engage coalition air assets who were then able to achieve air superiority with relative ease and set the conditions for the ground war.

However, besides achieving their military objectives, these attacks also affected a significant segment of the Iraqi population, who were without electrical power and telephone service through the end of the conflict. Similar kinetic attacks on the infrastructure also served as scapegoats for the dismal conditions in Iraq for many years after the end of Desert Storm in March 1991. In contrast to these destructive attacks, there is a report that the United States was able to achieve similar results on other aspects of the IADS through the use of less destructive information warfare weapons.

According to news reports, several weeks before the start of the 1991 Gulf War, US intelligence agents replaced a microchip in a printer that was destined for Iraq as part of its air defense system. This

new microchip contained a virus, which infected the air defense network once it was connected, and caused information on the computer screens to vanish, thereby rendering the network ineffective.[169] More importantly, the effects of the virus can be reversed by replacing the affected components in the network, which should take considerably less time than rebuilding a power and telecommunication system for the country. As this vignette illustrates, information warfare can help to minimize collateral damage; therefore, if an information warfare arms control regime categorically restricts certain targets, such as infrastructure, or specific weapons there is a risk of increased destruction due to the preponderance of targeting by kinetic weapons.

Political Risks

Coalitions and alliances play an important part in providing for US security because they can help to deter aggression, set conditions for success in combat if deterrence fails, enhance our expeditionary capabilities by providing access to local resources, and provide access to regional intelligence to allow for the precise application of military power.[170] In addition, the 2002 *National Security Strategy* for the United States clearly stated that "There is little of lasting consequence that the United States can accomplish in the world without the sustained cooperation of its allies and friends in Canada and Europe."[171] However, if the United States does not sign and ratify an information warfare arms control regime, this can negatively impact our ability to form coalitions and result in non support for US information warfare activities during coalition operations. In this context, an information warfare arms control regime can become a political risk that is reminiscent of the Ottawa Landmine Treaty.

The 1997 Ottawa Landmine Treaty requires each state party to discontinue the use of antipersonnel mines; not develop, produce, otherwise acquire, stockpile, retain or transfer to anyone, directly or indirectly, anti personnel mines; and not to assist, encourage or induce, in any way, anyone to engage in any activity prohibited to a State Party under this Convention. Within NATO, all countries are party to the treaty except the United States and Turkey. During Operation Allied Force (OAF), 24 March to 10 June 1999, the United States reportedly did not conduct any mining missions against Yugoslavia. However, if it did, it would have put its NATO allies at legal risk and further complicated an already complex operation, since in accordance to the treaty our NATO allies could not provide any assistance to any facet of the mining missions. Although the US and NATO were not faced with this situation in OAF, its potential for complicating coalition operations is real and was voiced by Robert Bell, special assistant to the president for national security and counselor to the assistant to the president for national security affairs, in 1998.

He was asked the question "Given the fact that most US allies have signed the Ottawa landmine treaty, what effect will that have on the ability of the United States to conduct coalition operations using landmines?[172] His reply was

> What we're discovering is that our allies, particularly in NATO but also in Asia, in most cases had simply not thought this through. You had a case where the negotiating position was being driven principally out of foreign affairs ministries, and the defense ministries had not cranked in analytically and in terms of their own view on this. So, we're in a situation now where these countries have signed the treaty and are clearly going to ratify, at least eventually, and their own defense ministries are saying, "What does this mean for coalition operations?"[173]

However, if the United States did attempt to conduct mining missions during OAF, the NATO allies could have protested by "playing the red card."[174]

In the game of soccer, the official holds up the red card to tell a player he/she is out of the game. In multinational operations such as OAF, a NATO ally could "play the red card" to tell the other coalition members to accept that nation's objection to a mining mission or that nation will withdraw from the game or the coalition. For air operations, coalition members can express their objections in many ways to include limiting the use of their aircraft to certain missions (airlift, air defense, etc.), preventing certain types of aircraft from operating in their sovereign territory, and not approving objectionable weapons or targets on a target nomination list. For OAF, "playing the red card" could also entail denying support from the NATO E-3 Airborne Warning and Control System (AWACS).

Therefore, if an information warfare arms control regime contains similar language that prohibits a party to the regime to aid in any aspect of an information warfare mission that is prohibited, the United States may face political risk if it is not a party to the agreement and must request support from a country that has played the red card. This risk is further heightened if the adversary is using the computer or telecommunication resources of a coalition member to attack US interests that are outside the geographic area of the coalition's operations.

CONCLUSIONS

Although the scholarly debate is far from over, traditionalists, who only see threats in the military sector as the quintessential defining threat to national security, and wideners, who also see threats in the others sectors as worthy contenders, can both agree that information

warfare is a threat to national security. However, this agreement does not extend to a common definition of information warfare or what aspects should be addressed in international agreements to solve the security dilemma. In this regard arms control can play a decisive role because it "is about establishing norms agreed by the international community at large to attain co-operative international security and states that do not adhere to such norms are rogue to the consensus of the international community."[175]

When faced with the first efforts to negotiate an information warfare arms control agreement in 1999, the United States assessed that it was premature to do so at the time. Since many of the factors that influenced this decision are still unresolved, this assessment might still be true today. The most consequential of these factors are the legal issues of sovereignty in the information realm and the clear definitions of key terminology within the current laws of war. Besides their legal implications, these are also important because the manner in which they are resolved will greatly impact the risk and cost of any ensuing arms control regime that must now be cost-effective in the post-Cold War environment.

Although cost has become a prime concern in arms control over the past decade, the lack of available data made it difficult to determine the expected cost with any degree of fidelity. However, previous nuclear, biological, and chemical weapons agreements did shed some light on the types of cost to be incurred during the evolution of a generic arms control regime, and that comparison was adopted for this research effort, with slight modifications to account for the unique challenges presented by information warfare. One of most significant factors for costs and risk will be the type of verification provision that is adopted to ensure compliance.

An intrusive verification provision like the CWC would provide a degree of transparency to ensure compliance, but would also introduce additional costs to industry and risks of proliferation, intelligence loss, and cheating. In addition, the cost to conduct inspections under these verification provisions may lead to the absence of verification provisions as in the BWC, which minimizes costs but significantly increases the risk.

In examining the risk for an arms control regime, I also discovered several factors that should be considered while forging an agreement. First, it may be impossible to prevent vertical proliferation due to the dual-use nature of the technology and the realization that the driving force behind IT innovation is the private sector and not the military. Moreover, given that the DII is inextricably linked to the NII, threats to the private sector will migrate to the military sector along with the solutions to these new threats. This leads to the second factor; an arms control regime must allow for the adaptation of new defenses to face evolving offensive threats. To do otherwise may lead to the same results recently experienced with the CTBT and ABM Treaty. Despite US unpreparedness to sign and ratify an information warfare arms control agreement, the United States must stay engaged and participate in the process to help guide the discourse in the international community. In the end we may not become a party to the agreement; however, by staying engaged during deliberations we would help to define the norms for information warfare within the international community.

Final Thoughts

Although the purpose of this research was to examine the costs and risk of an information warfare arms control regime, and not a cost-benefit analysis or a feasibility assessment, these latter topics are

important and must be accomplished before undertaking negotiations for a regime. However, in working through these issues it is important to keep in mind one of the tenets of traditional arms control, which states "arms control and military strategy should work together to promote national security."[176] Therefore, if one of the principles of our current national security strategy is to rely on coalitions and allies to counter threats to our security, it would be prudent to keep this in mind while deciding on issues, such as an information warfare arms control regime. If we do otherwise, we may find ourselves isolated and unable to garner the required support from others during times of conflict.

NOTES

[1] According to the Office of Net Assessment in the Office of the Secretary of Defense, a Revolution in Military Affairs is a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operations and organizational concepts, fundamentally alters the character and conduct of military operations.

[2] Previous RMAs included the railway, telegraph, steam powered ships, the machine gun, the submarine, armored fighting vehicles, radio, and radar. See Sharjeel Rizwan, "Revolution in Military Affairs," *Defence Journal* (September 2000), n.p., on-line. Internet. Available from http.www.defencejournal.com/2000/sept/military.htm.

[3] Steven Metz and James Kievit, *Strategy and the Revolution in Military Affairs: From Theory to Policy* (Carlisle Barracks, PA: Army War College, 1995), iii.

[4] Department of Defense, *Joint Vision 2010* (Washington DC: Joint Chiefs of Staff), 16.

[5] Department of Defense, *An Assessment of International Legal Issues in Information Operations* (Washington, DC: Office of General Counsel, 1999), 47.

[6] Department of Defense, Assessment of Legal Issues, 48 and UN General Assembly Resolution A/RES/53/70, "Developments in the Field of Information and Telecommunications in the Context of International Security," 4 December 1998.

[7] Clay Wilson, *Information Warfare and Cyberwar: Capabilities and Related Policy Issues* (Washington, DC: Congressional Research Service, 2004), CRS-10.

[8] Ibid, CRS-10.

[9] Ibid, CRS-2.

[10] These malicious activities consist of "cyberterror," "cybercrime," and "cyberactivism." See Gregory Rattray, "Security in Cyberspace." In *Arms Control: Cooperative Security in a Changing Environment*, ed. Jeffrey Larsen (Boulder, CO: Lynne Rienner Publishers, 2002), 312-313.

[11] This definition is intentionally restrictive to limit the discussion to address only those activities that may fall under the purview of the Department of Defense, the State Department, or their equivalent in other states. Under normal circumstances neither the Armed Forces nor the State Department will be called to remove a crowd that was preventing customers from entering a bookstore. Similarly, they should not be expected to respond to computer hackers that were conducting denial of service attacks against e-commerce websites. In both cases, these activities are the responsibility of local law enforcement officials, such as campus police or the FBI.

[12] Barry Buzan, *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era* (Boulder, CO: Lynne Rienner Publishers, 1991), 115.

[13] Cited in Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," (United States Air Force Academy, CO: Institute of Information Technology Applications), June 1999, on-line, Internet, 2 April 2005, available from http://atlas.usafa.af.mil/iita/Documents/Schmitt1.pdf, 10.

[14] Ibid.

[15] Ibid.

[16] George Smith, "An Electronic Pearl Harbor? Not Likely." Issue in Science and Technology Online, Fall 1998, n.p., on-line, Internet, 11 March 2005, available from http://205.130.85.236/issues/15.1/smith.htm.

[17] Ibid.

[18] These figures only represent the cost of the weapon system during 1999 since many of the program costs are amortized over the life cycle of the weapon system. See Department of Defense, *Program Acquisition Costs by Weapon System.*

[19] The F/A-18E/F is a twin-engine, high-performance, multi-mission, tactical aircraft for deployment in Navy and Marine Corps fighter and attack squadrons. It can perform strike, interdiction, close air support, fighter escort, and fleet air defense missions. See Department of Defense, *Program Acquisition Costs by Weapon System.* 8.

[20] The C-17 is a wide body, four-engine, turbofan aircraft that meets the nation's strategic aircraft requirement for a new core to modernize the US strategic aircraft capability. The C-17 provides outsize intratheater airland/airdrop capability. See Department of Defense, *Program Acquisition Costs by Weapon System,* 12.

[21] The E-8C Joint Surveillance Target Attack Radar System is a Boeing 707 class aircraft that is modified to operate a target attack radar system to detect and track both moving and fixed enemy ground targets. JSTARS can provide battlefield surveillance, attack planning, and post attack damage assessments. See Department of Defense, *Program Acquisition Costs by Weapon System*, 14.

[22] The MLRS consists of a tracked, self-propelled launcher loader, disposable rocket pods, and fire control equipment firing 227 mm ballistic rockets loaded with anti-personnel/anti-material bomblets. The mission of MLRS is to neutralize or suppress enemy field artillery and air defense systems and supplement common artillery systems. See Department of Defense, *Program Acquisition Costs by Weapon System,* 26.

[23] The SAN ANTONIO Class Amphibious Transport Dock ships embark, transport, and land elements of Marine landing forces in an amphibious assault by helicopters, landing craft, and amphibious vehicles. See Department of Defense, *Program Acquisition Costs by Weapon System,* 40.

[24] The mission of the M1 Upgrade program is to provide a main battle tank with increased survivability, mobility, firepower, and lethality for US armor forces. See Department of Defense, *Program Acquisition Costs by Weapon System.* 42.

[25] UN General Assembly Document A59/565, Follow-up to the Outcome of the Millennium Summit, 2 December 2004, 3.

[26] Ibid, 25.

[27] Barry Buzan, Ole Weaver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner Publishers, 1998), 4.

[28] Ibid, 1.

[29] Ibid. 24.

[30] Ibid. 49-55.

[31] Douglas Waller, "Onward Cyber Soldiers," *TIME*, 1995, 39.

[32] Senate, *Worldwide Threat Assessment: Hearings before the Senate Select Committee on Intelligence*, 104th Cong., 2d sess., 1996.

[33] Presidential Decision Directive/NSC-63, "Critical Infrastructure Protection," 1998.

[34] Although a newspaper is not a securitizing actor, in this instance the *Liberation Army Daily* is the official newspaper for the Chinese Army and given the government control of information, the contents of the paper can be taken as the official government position. See US Embassy Beijing: PLA Colonels on "Unrestricted Warfare: Part 1," November 1999, n.p., on-line., Internet, 12 November 2004, available from http://http://www.fas.org/nuke/guide/china/doctrine/uresw1.htm.

[35] Stephen J. Main, "Russia's Military Doctrine." April 2000, n.p., on-line., Internet, 29 January 2004, available from http://www.da.mod.uk/CSRC/documents/Russian/OB77. Stated that one of the mail threats to military security included "hostile information (information-technical, information-psychological) operations that damage the military security of the Russian Federation and its allies."

[36] Department of Defense, Annual Report to the President and the Congress (Washington, DC: Office of the Secretary of Defense, 2002), 72.

[37] Senate, *Current and Projected National Security Threats to the United States: Hearings before the Senate Committee on Intelligence*, 108th Cong., 2d sess., 2004, 10-11.

[38] Buzan et al., 95.

[39] Ibid. 95-96.

[40] Ibid.

[41] Ibid.

[42] Ibid.

[43] Stephen J. Korbin, "Economic Governance in an Electronically Networked Global Economy," in *The Emergence of Private Authority in Global Governance*, ed. Rodney Hall and Thomas Biersteker (Cambridge: Cambridge University Press, 2002), 50.

[44] The Agricultural Revolution was the "first wave" and the Industrial Revolution was the "second wave."

[45] See Robert K.Elliott, "Information Technology: The Third Wave," *The CPA Journal*, November 1992, n.p., on-line, Internet, 11 March 2005, available from http://www.nysscpa.org/cpajournal/old/13856813.htm;

Michael J. Robbat, "Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework, and the Creation of a New Paradigm," *Journal of Science and Technology Law*, 1 June 2000, n.p., on-line, Internet, 13 October 2004. Available from http://jstl.law.miami.edu/vol6/Volume%206/6jstl10.pdf.

[46] "Information Warfare," 19 April 2004, n.p., on-line, Internet, 23 November 2004, available from http://www.nvcc.edu/home/joney/IST%20246%20Lecture%209%20-%20Information%20Warfare.ppt.

[47] Peter Drucker, *Post-Capitalist Society* (New York: Harper Business, 1993), 8.

[48] David Ronfeldt, "Cyberocracy is Coming," *The Information Society Journal 8*, no. 4 (1992): 243-296.

[49] Ibid.

[50] Senate, *Worldwide Threat Assessment, 1996.*

[51] Presidential Decision Directive/NSC-63, 1998.

[52] Main.

[53] Senate, *Worldwide Threat 2001: National Security in a Changing World: Hearings before the Senate Select Committee on Intelligence*, 107th Cong., 1st sess., 2001.

[54] Senate, *Current and Projected National Security Threats to the United States*, 2004.

[55] Steven A. Hildreth, *Cyberwarfare* (Washington, DC: Congressional Research Service, 2001), CRS-14.

[56] Buzan et al., 141-145.

[57] Ibid.

[58] Ibid. 148.

[59] Department of Defense, *An Assessment of International Legal Issues in Information Operations (*Washington, DC: Office of General Counsel, 1999), 48.

[60] UN General Assembly Resolution A/RES/53/70, "Developments in the Field of Information and Telecommunications in the Context of International Security," 4 December 1998; and William Church, "Information Warfare," *International Review of the Red Cross*, no. 837, 31 March 2000, on-line., Internet, 29 January 2005, available from http://www.icrc.org/web/eng/siteeng0.nsf/html/57JQCZ, 205-216; and Gregory Rattray, "Security in Cyberspace," in *Arms Control: Cooperative*

Security in a Changing Environment, ed. Jeffrey Larsen. (Boulder, CO: Lynne Rienner Publishers, 2002), 315.

[61] Senate, *Current and Projected National Security Threats, 2004, 10-11 and Senate, Current and Projected National Security Threats to the United States: Hearings before the Senate Committee on Intelligence*, 108th Cong., 1st sess., 2003, 15.

[62] Robert Jervis, "Cooperation Under the Security Dilemma," in *Conflict After the Cold War: Arguments on Causes of War and Peace*, ed. Richard Betts (New York: Pearson Longman, 2004), 382-384; and Buzan, 121.

[63] James T. McKenna, "Tighter Security Urged for Defense Computers," *Aviation Week & Space Technology*, 20 January 1997, 60.

[64] Michael J. Robbat, "Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework, and the Creation of a New Paradigm," *Journal of Science and Technology Law*, 1 June 2000, on-line. Internet, 13 October 2004, available from http://jstl.law.miami.edu/vol6/Volume%206/6jstl10.pdf.

[65] Michael Sheehan, *Arms Control: Theory and Practice* (New York: Basil Blackwell Inc., 1988), 22.

[66] Allan S. Krass, *The United States and Arms Control: The Challenge of Leadership* (Westport, Conn.: Praeger Publishers, 1997), 2.

[67] Jeffrey Larsen, in *Arms Control: Cooperative Security in a Changing Environment* (Boulder, CO: Lynne Rienner Publishers, 2002), 6.

[68] Larsen, 8; and Sheehan, 6.

[69] Krass, 5-7.

[70] Larsen, 1.

[71] This is an assessment that is based on the characteristics of information warfare. The two items are assessed as "low" due to the dual-use nature of information warfare and the realization that most of the advancements in IT are made in the private sector and not the military. Therefore, attempts to disarm or prevent proliferation might be difficult since there are legitimate requirements for the technology in the private sector.

[72] See Larsen; Terry L. Deibel, "The Death of a Treaty," *Foreign Affairs* 81, no. 5 (2002): 141-161; Daryl G. Kimball, "Trust but Don't Verify," *Arms Control Today*, September 2004, n.p. On-line, Internet, 7 Feb 2005, available from http://www.arms control.org/act/2004_09/Focus.asp; and Jonathan B. Tucker, "The Chemical Weapons Convention: Has It Enhanced US Security." *Arms Control Today*, April 2001, n.p. on-line.

Internet, 7 Feb 2005, available from http://www.armscontrol.org/act/2001 _04/ tuck er.asp.

[73] Center for Arms Control And Non-Proliferation, "Comprehensive Test Ban Treaty Fact Sheet." September 2002, an-line. Internet. 10 November 2004, available from http://www.clw.org/control/ctbt.pdf.

[74] Deibel, 141-161.

[75] Larsen, 1.

[76]John A. Nagl, "Arms Control in the year 2025," in *Arms Control: Cooperative Security in a Changing Environment*, ed. Jeffrey Larsen (Boulder, CO: Lynne Rienner Publishers, 2002), 335.

[77] Andrew H. Cordesman, "Concepts of Arms Control—IV: Shaping the Future," May 2000, on-line. Internet, 17 September 2004, available from http://www.csis.org/strat assessment/reports/armescontrol4.pdf.

[78] Krass, 3.

[79] Larsen, 3.

[80] Steven A. Hildreth, *Cyberwarfare*, (Washington, DC: Congressional Research Service, 2001), CRS-11.

[81] Gary M. Anderson and Adam Gifford, "Order Out of Anarchy: The International Law of War," 8 August 2004, n.p. on-line. Internet, 24 February 2005, available from http://www.cato.org/cgi-bin/scripts/ printtech.cgi/dailys/08-08-04-2.html.

[82] Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, "Information Warfare and International Law," n.p. on-line. Internet, available from http://www.au.af.mil/au/awc/awcgate/ndu/iwil/ iwilindex.htm.

[83] Anderson.

[84] A domain is a unique dimension in which to conduct military operations. Land, sea, air, and space are the pre-existing dimensions and information warfare is often referred to as the fifth dimension. See Maj Gen John P. Casciano, address, Air Force Association National Symposia, Los Angeles, Ca., 18 October 1996, n.p. on-line. Internet, 11 March 2005, available from http://www.aef.org/pub/la9.asp.

[85] Department of Defense, *Joint Vision 2020*, (Washington DC: Joint Chiefs of Staff, 2000), 6.

[86] Greenberg et al.

[87] Ibid.

[88] UN General Assembly Declaration 1962, "Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space," 13 December 1963.

[89] "Treaty On Principles Governing The Activities Of States In The Exploration And Use Of Outer Space, Including The Moon And Other Celestial Bodies." *Arms Control Today*, 10 October 1967, n.p. on-line. Internet, 25 January 2005, available from http://www.armscontrol.org/ documents/outerspace.asp.

[90] Ibid.

[91] Greenberg et al.

[92] UN General Assembly Resolution A/RES/53/70, "Developments in the Field of Information and Telecommunications in the Context of International Security," 4 December 1998.

[93] Department of Defense, *An Assessment of International Legal Issues in Information Operations, (*Washington, DC: Office of General Counsel, 1999), 48.

[94] Allan S. Krass, *The United States and Arms Control: The Challenge of Leadership* (Westport, Conn.: Praeger Publishers, 1997), 29.

[95] Marie I. Chevrier, "Chemical and Biological Weapons," in *Arms Control: Cooperative Security in a Changing Environment*, ed. Jeffrey Larsen. (Boulder, CO: Lynne Rienner Publishers, 2002), 143.

[96] Krass, 101.

[97] Ibid. 102.

[98] Ibid. 102.

[99] Goodby, James, et al., "Cooperative Threat Reduction for a New Era," *Center for Technology and National Security Policy* (Washington, DC: National Defense University, September 2004), 1.

[100] John Spratt, "The Bush Administration's Nuclear Weapons Plans: A Critical Assessment," Arms *Control Today*, May 2004, n.p., on-line, Internet, 9 February 2005, available from http://www.armscontrol.org/ events/May_2004Press Conference.asp.

[101] Miles A. Pomper, "Bush Stresses Importance of Nunn-Lugar Programs but Cuts Funds in 2005 Budget Request," *Arms Control Today*, March 2004, n.p., on-line. Internet, 7 February 2005, available from http://www.armscontrol.org/act/2004_03/ NunnLugarFunding.asp.

[102] Krass, 105.

[103] Ibid, 105.

[104] Adapted and updated from Krass, 105.

[105] Ibid, 60.

[106] Department of State *Chemical Weapons Convention –Article II: Definitions and Criteria* (Washington, DC: Bureau of Industry and Security), n.p., on-line. Internet, 17 January 2005, available from http://www.cwc.gov/treaty/articles/art-02_html.

[107] "The Ottawa Landmine Treaty," *Arms Control Today*, September 1997, n.p., on-line. Internet, 25 January 2005, available from http://www.armscontrol.org/act/ 1997_09/apltreat.asp.

[108] "Missile Technology Control Regime," *Arms Control Today*, 7 January 1993, n.p., on-line. Internet, 25 January 2005, available from http://www.armscontrol.org/document s/mtcr.asp.

[109] "Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction." *Arms Control Today*, 26 March 1975, n.p., on-line. Internet, 25 January 2005, available from http://www.armscontrol. org/treaties/bwc.asp. and Krass, 60.

[110] Ibid.

[111] Department of Defense, *Joint Doctrine for Information Operations, JP3-13,* (Washington, DC: Chairman of the Joint Chiefs of Staff, 9 October 1998), available from http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf, I-14.

[112] Capt Jason Brooks, "Information Operations," (Maxwell AFB, AL: College of Aerospace Doctrine, Research, and Education, Visual Education, 2004), Slides, 7.

[113] Ibid.

[114] Department of Commerce, *Archive of HPC News Item*, (Washington, DC: Bureau of Industry and Security, 19 January 2001), n.p., on-line. Internet, 12 February 2005, available from http://www.bis.doc.gov/hpcs/ ArchivedNewsItems.html.

[115] Department of Commerce, *Archive of HPC News Item*, (Washington, DC: Bureau of Industry and Security, 2 January 2002), n.p., on-line. Internet, 12 February 2005, available from http://www.bis.doc.gov/hpcs/ ArchivedNewsItems.html; and Department of Commerce, *High Performance Computer Export Controls,* (Washington, DC: Bureau of Industry and Security, 10 December 2003), n.p., on-line. Internet, 12 February 2005, available from http://www.bis.doc.gov/hpcs/ default.htm.

[116] Department of State, "Treaty between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems," (Washington, DC: October 1972) n.p., on-line., Internet, 26 January 2005, available from http://www.state.gov/www/global/arms/treaties/abm/abm2.html.

[117] Michael Sheehan, *Arms Control: Theory and Practice* (New York: Basil Blackwell Inc., 1988), 60.

[118] Krass. 60.

[119] Staff Reporting, "International Response: IAEA Board Approves Budget Increase." *Global Security Newswire*, 21 July 2003. n.p., on-line. Internet, available from http://www.nti.org/d_newswire/issues/2003/7/21/7s.html.

[120] Chevrier, 150.

[121] Ibid.

[122] Ibid.

[123] Jonathan B. Tucker, "The Chemical Weapons Convention: Has It Enhanced US Security," *Arms Control Today*, April 2001, n.p. on-line. Internet, 7 Feb 2005, available from http:// www.armscontrol.org/act/2001_04/ tuck er.asp.

[124] "Western States Threaten to Cut IAEA Funding over Iran Row," 18 September 2004, n.p., on-line, Internet, 27 February 2005, available from http://www.globalsecurity. org/wmd/library/news/iran/2004/iran-040918-irna04.htm.

[125] Department of Commerce, *Assessments of the Costs and Benefits of BXA Regulation: Chemical Weapons Convention Regulations and Declarations Forms* (Washington, DC: Bureau of Industry and Security, 29 November 1999), n.p., on-line. Internet, 12 February 2005, available from http://www.cwc.gov/Regulations/cba/cost_benefit_analysis_html.

[126] Department of State, *Industry Issues* (Washington, DC: Bureau of Arms Control, 18 May 2004), n.p., on-line. Internet, 12 February 2005, available from http://www.cwc.gov/Industry_Outreach/Publications/004/cwc_intro_to_imp/industry _issues; see Jack L. Brock, *Arms Control - Experience of US Industry with Chemical Weapons Convention Inspections* (Washington DC: United States General Accounting Office, 2000).; Schedule 1 chemicals are toxic chemicals that have little or no commercial use and were primarily developed for military use. Schedule 2 chemicals can be used to produce chemical weapons, but have commercial uses and are not produced in large quantities. Schedule 3 chemicals can be used to make chemical weapons, but also have significant commercial uses.

[127] Krass. 109.

[128] Ibid.

[129] Allan S. Krass, *The United States and Arms Control: The Challenge of Leadership* (Westport, Conn.: Praeger Publishers, 1997), 103.

[130] "Electronic Pearl Harbor," was coined by Richard Clarke, President Clinton's national coordinator for security, infrastructure protection and counter-terrorism, to represent a surprise IW attack against the country's critical infrastructures, such as transportation, power, and telecommunications.

[131] Dorothy E. Denning, *Information Warfare and Security* (Reading, MA: Addison-Wesley, 1999), 75; and George Smith, "An Electronic Pearl Harbor? Not Likely," *Issues in Science and Technology Online*, Fall 1998, n.p., on-line, Internet, 11 March 2005, available from http://205.130.85.236/issues/15.1/smith.htm.

[132] Department of Defense, *An Assessment of International Legal Issues in Information Operations* (Washington, DC: Office of General Counsel, 1999), 1.

[133].Ibid. 1-2.

[134] Declan McCullagh, "Bush Pushes for Cybercrime Treaty," *CNET*, 18 November 2003, *news.com*, n.p., on-line, Internet, 24 September 2004, available from http://news.com.com /Bush+pushes+for+cybercrime +treaty/2100-1028_3-5108854.html.

[135] "About the BBG: An Organization of US International Broadcasters," *International Broadcasting Bureau,* n.p., on-line, Internet, 14 February 2005, available from http://www.bbg.gov/bbg_aboutus.cfm.

[136] Ibid.

[137] "RFE/RL Mission Statement," n.p., on-line, Internet, 14 February 2005, available from http://www.rferl.org/about/organization/mission-statement.asp.

[138] Ibid.

[139] Ibid.

[140] Ibid.

[141] "About Us," n.p., on-line, Internet, 14 February 2005, available from http://www.radiosawa.com/english.aspx.

[142] About the BBG.

[143] "No End to Jamming," *International Broadcasting Bureau Editorial*, 6 July 2002. n.p., on-line, Internet, 14 February 2005. Available from http://www.ibb.gov/editorials/ 09989.htm.

[144] Jonathan B. Tucker, "The Chemical Weapons Convention: Has It Enhanced US Security." *Arms Control Today*, April 2001, n.p. on-line. Internet, 7 Feb 2005, available from http:// www.armscontrol.org/act/2001 _04/ tuck er.asp.

[145] Krass, 127.

[146] Ibid, 57.

[147] Tucker, 3.

[148] Ibid.

[149] Thomas Evan, John Barry, and Melinda Liu, "Ground Zero: India's Blasts Dramatize the New Nuclear Age. How Did the CIA Miss Them? And What's to Do Now?" *Newsweek*, 25 May 1998, 29-32A.

[150] James Risen and Tim Weiner, "US May Have Helped India Hide Its Nuclear Activity," *New York Times*, 25 May 1998, A3

[151]Ibid.

[152] Department of State, *Chemical Weapons Convention –Article III: Declarations* (Washington, DC: Bureau of Industry and Security), n.p., on-line. Internet, 17 Janurary 2005, available from http://www.cwc.gov/ treaty/articles/art-03_html.

[153] Krass, 127.

[154] Charles H. Fairbanks, Jr. and Abram N. Schulsky, "Arms Control: The Historical Experience," in *Conflict After the Cold War: Arguments on Causes of War and Peace*, ed. Richard Betts (New York: Pearson Longman, 2004), 428-432.

[155] Hans Mark, transcript of interview by Harry Kreisler for *Technology, Universities, and the Changing International Environment*, 15 March 1998, n.p., on-line, Internet. 11 February 2005, available from http://globetrotter.berkeley.edu/conversations/Mark/mark-con6.html.

[156] Department of State *Chemical Weapons Convention –Article II: Definitions and Criteria* (Washington, DC: Bureau of Industry and Security), n.p., on-line. Internet, 17 January 2005, available from http://www.cwc.gov/treaty/articles/art-02_html.

[157] Jeffrey A. Larsen and Kurt J. Klingenberger, "Treaties, Agreements, and Organizations of Particular Interest," in *Arms Control: Cooperative*

Security in a Changing Environment ed. Jeffrey Larsen (Boulder, CO: Lynne Rienner Publishers, 2002), 372.

[158] George W. Bush, “President Discusses National Missile Defense" (Washington, D.C.: The White House, 2001), n.p., on-line, Internet. 20 January 2005, available from http://www.whitehouse.gov/news/releases/2001/12/print/30011213-4.html.

[159] George I. Seffers, "Hackers Take Offense at Pentagon Defense," *Defense News*, 1998; and William Jackson, “DOD fires back at hackers preying on its Web servers,” *GCN.com*, Vol. 17, no. 25, 21 September 1998, n.p., on-line, Internet, 24 January 2005, available from http://www.gcn.com/17_25/news/33020-1.html.

[160] Seffers.

[161] Ibid.

[162] Seffers and Jackson.

[163] Carl Conetta, "Catastrophic Interdiction: Air Power and the Collapse of the Iraqi Field Army in the 2003 War," 26 September 2003, on-line. Internet, 19 February 2005, available from http://www.comw.org/ pda/fulltext/0309bm30.pdf.

[164] Ibid.

[165] Matthew French, “DoD aims psy-ops at Iraqi officers,” *FCW.COM*, 24 March 2003. n.p., on-line, Internet, 19 February 2005, available from http://www.fcw.com/fcw/articles /2003/0317/web-psyops-03-21-03.asp.

[166] Kevin Coughlin, "War—It's Not Just Firing Guns," *The Star-Ledger*, 11 April 2003.

[167] Denning, 5.

[168] Ibid.

[169] “Iraq Computers Reportedly Got American Bug: NSA Virus Aimed at Air Defense," *The Washington Post*, 12 Jan 1992, 13. and Computer Virus Use Cited in Gulf War." *Boston Globe*, 12 Jan 1992, 12.

[170] Department of Defense, *National Military Strategy of the United States* (Washington, DC: Joint Chiefs of Staff. 2004), 22.

[171] The White House Office, *The National Security Strategy of the United States of America* (Washington, DC: Government Printing Office, 2002), 25.

[172] Robert Bell, "Strategic Agreements and the CTB Treaty: Striking the Right Balance," *Arms Control Today*, January/February 1998, n.p. On-line.

Internet, 18 February 2005. Available from http://www.armscontrol.org/act/1998_01-02/belljf.asp.

[173] Ibid.

[174] Notes, Command and Control Warfare Advanced Course, May 2002.

[175] Glen Segell, "Arms Control and Nuclear Proliferation," Paper presented at the 44th International Studies Association Conference. Portland Oregon, 25 February–1 March 2003.

[176] Jeffrey Larsen, in *Arms Control: Cooperative Security in a Changing Environment* (Boulder, CO: Lynne Rienner Publishers, 2002), 7.