PUBLICATION

Interlocking Stakes in NATO Security: A Primer on Investment, Dual-Use Technologies, and Export Control for the Military Leader in NATO

Dean R. Clemons

October 2002

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Dean R. Clemons is a Lieutenant Colonel in the United States Air Force. His present assignment is to the Deputy Chief of Staff for Logistics, as the division chief for communications systems. Previous assignments have included tours at the Joint Chiefs of Staff, squadron command (Hurlburt Air Force Base, Florida., and Lowry Air Force Base, Colorado), and temporary duty to augment Bosnia-Herzegovinia. He prepared this report while a National Defense Fellow at Harvard in 2001–2002.

ISBN 1-879716-82-8 **P-02-5**

October 2002

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz Allen Hamilton
Center for Excellence in Education
Commission of the European Communities
Critical Path
CyraCom International
Ellacoya Networks, Inc.
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
John and Mary R. Markle Foundation
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp (Japan)
PDS Consulting
PetaData Holdings, Inc.
Samara Associates
Skadden, Arps, Slate, Meagher & Flom LLP
Sonexis
Strategy Assistance Services
TOR LLC
United States Government:
Department of Commerce
National Telecommunications and Information Administration
Department of Defense
National Defense University
Department of Health and Human Services
National Library of Medicine
Department of the Treasury
Office of the Comptroller of the Currency
Federal Communications Commission
National Security Agency
United States Postal Service
Upoc
Verizon

Executive Summary

War and human life have been coupled throughout human history. Ares, the Greek god of war, wielding fist and sword, battled with mortals and immortals alike. In more recent times, as economies and politics become increasingly interdependent—or, globalized—Janus, the Roman deity of doorways and passageways, who watched in two directions at once, has begun to take center stage, looking at both international stability and security.

This study examines international stability and security within the framework of globalization] from the perspectives of three interlocking stakes: international military and commercial investment; dual-use technologies; and export control. As a primer on these stakes for the rising military leader within the North Atlantic Treaty Organization (NATO), the study elucidates the issue of cooperation vs. competition intrinsic to NATO and the European Union (EU) as together they seek to increase transatlantic security. The enormous potential of dual-use technologies is examined, with a focus on the *angst* of military leaders about the military's increasing dependence on technologies that are widely commercially available to both friend and foe. Last, the competing demands of open markets and of international security involved in those two stakes lead to consideration of the third, the economic instrument of export control of technologies.

Globalization is irreversible. To be successful in future conflicts, the rising military leader will need to be fluent not solely in military affairs but also in the languages of economics and politics. Like globalization, coalition warfare is here to stay, and although, for that reason, interoperability of both systems and organizations remains desirable, competing demands of national economies pose significant challenges to achieving it. To meet such competing economic demands, the military leader of tomorrow will need to employ dual-use and science and technology programs to the advantage of both the U.S. military and the NATO alliance. By clearly articulating warfighting requirements and shortfalls and by understanding existing programs and processes, the military leader will be able to influence the export control process. Conflicts will undoubtedly occur in the twenty-first century, and the rising military leader will need to learn to leverage investment, dual-use technologies, and export control laws in order to mitigate actual bloodshed.

Acknowledgements

The author gratefully acknowledges the following people who reviewed and commented critically on the draft version of this report. Without their consideration, input, and encouragement, this study could not have been completed:

Kenneth W. Deutsch
Paul Fang
Thomas Flynn
Oswald H. Ganley
Robin Hamilton–Harding
David Hayes
John L. Hayes
Richard Levins
P. H. Longstaff
Raymond D. Lucas
Michael K. Molloy
Warren "Skip" Parish
Steven Spano
M. Dee Taylor
Marilyn Z. Wellons

These reviewers and the Program's Affiliates, however, are not responsible for or necessarily in agreement with the views expressed here, nor should they be blamed for any errors of fact or interpretation.

I would like to thank in particular my wife, Lisette, our sons Isaac and Aaron, and my friends in labor Margaret S. MacDonald, and Rohan Kariyawasam.

The views, opinions, and conclusions expressed in this paper are those of the author and should not be construed as an official position of the Department of Defense or any other government agency or department.

Contents

Illustrations

Figures

Tables

Chapter One

Introduction

Globalization and the information revolution bring enormous benefits to the transatlantic community, including its security structures, but they also increase its vulnerabilities. [1]

William S. Cohen,
Former Secretary of Defense

Since the terrorist attacks on the World Trade Center in New York City and the Pentagon on September 11, 2001, people "on the street" have repeatedly said that terrorism of this magnitude in the United States is new and different, and that nothing will ever be the same. In the words of President George Bush, "night fell on a different world."[2] In an immediate sense, yes. Within weeks, the United States and its allies in the North Atlantic Treaty Organization (NATO) were involved in a military effort in Afghanistan to root out Al Qaeda and to locate Osama bin Laden. Yet the primary issues of national security, international commerce, and international cooperation remain fundamentally unchanged, because, although difficult, complex, and even thorny, they are crucial to international stability and security.

War has always been with us, but the environment of war has changed.. Ares, the ancient Greeks' wild, ungovernable god of war, slashed about the countryside with his son Phobos (Fear), loving battle for its own sake, with no regard for the suffering it brought. Ares and son may still roam the global landscape, but sheer aggressiveness now comes up hard against the modern reality of globalization, which influences the actions of military and civilian leaders alike. Globalization may be defined as an interdependence of economies—free trade, workforce migration, and international competition—mixed with emerging threats and enlarging alliances and accompanied by the forging of strategic alliances on a scale perhaps never before seen. If the late twentieth-century is an indicator, a continued move toward globalization will characterize the economic, political, and social climate of the twenty-first century.

This work offers a primer for the military leader of tomorrow in the United States, as a member of NATO, who will need to understand this globalized environment and its nuances. Established in 1949, NATO in 2002 still undergirds world security, because since its inception member nations have agreed, according to Article V of the Treaty, that "an armed attack against one or more of them in Europe or North America shall be considered an attack against all of

---

[1]William S. Cohen, "Preface," *Strengthening Transatlantic Security: A U.S. Strategy for the 21st Century* (December 2000). Cohen was Secretary of Defense in the Clinton administration (1997-2001).

[2]President George Bush, Address to a Joint Session of Congress and the American People, 20 Sept. 2001, [On-line]. URL: http://www.whitehouse.gov/news/2001/09/20010920-8.html (Accessed on 21 Feb. 2002.)

them…and each of them will assist the Party or Parties so attacked."[3] As evidence of NATO's strength, Central and Eastern European nations clamor to be recognized as "partners for peace" or as full members.[4] Zbigniew Brzezinski postulated that a larger, more secure Europe will clearly be a central issue confronting world leaders in the twenty-first century.[5]

The focus in this primer is on three important stakes and their stakeholders: international military and commercial investment; dual-use technologies; and export control and administration—all viewed in relation to transatlantic security. The issues involved in the globalization of national security, international commerce, and international cooperation bring to mind another ancient deity, Janus, the Roman god of gates and passageways, because, confusingly, these issues often have more than one face and the faces look in opposite directions.

That there are critical links between global commerce and international security has long been recognized—since, for example, the Marshall Plan (1947–52) or the Maastricht Treaty (1991), establishing the European Union (EU). In the "cyber era," however, what is new are the increasing risk and challenge posed by information technology used by both business and military planners.[6] The deliberate use of export control protocols and the judicious use of dual-use technologies are fundamental to transatlantic security,[7] and a national economic advantage in export often yields to international security concerns. Yet corporations, national and international, want to achieve an advantage over their competition, and although Article II of the North Atlantic Treaty calls on member nations "to eliminate conflict in their international economic policies

---

[3]Article V, North Atlantic Treaty, Washington, D.C., 4 April 1949, [On-line]. URL: http://www.nato.int/docu/basictxt/treaty.htm (Accessed on 5 Oct. 2001.) The member nations of NATO are Belgium, Canada, the Czech Republic, Denmark, France, Germany, Greece, Hungary, Iceland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Spain, Turkey, the United Kingdom, and the United States.

[4]In 1999 the Czech Republic, Hungary, and Poland, previously partners for peace, became full-fledged members of NATO. Following the 1999 Washington summit, the countries supported for membership as partners for peace are Albania, Bulgaria, Estonia, Latvia, Lithuania, Macedonia, Romania, Slovakia, and Slovenia.

[5]Zbigniew Brzezinski, "America In the World Today," in *Complexity, Global Politics, and National Security* (Washington, D.C.: National Defense University, Institute for National Strategic Studies [INSS], 1999), 29-31. Brzezinski was an advisor to the Kennedy and Johnson administrations and national security advisor to President Jimmy Carter. See CNN Perspectives Series [On-line]. URL: http://www.cnn.com/SPECIALS/cold.war/kbank/profiles/brzezinski (Accessed on 16 Jan. 2002.)

[6]Peter H. Daly, The Roles of Business and Government in Cyber Era National Security [a study plan developed for the Program on Information Resources Policy] (1999). See Daly, *Soldiers, Constables, Bankers, and Merchants: Managing National Security Risks in the Cyber Era* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-00-3, June 2000), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?id=424 (Accessed on 21 Feb. 2002.)

[7]Military export controls have been an element of U.S. security since before World War II; see the Center for Strategic and International Studies (CSIS), Executive Summary, *Computer Exports and National Security: New Tools for a New Century* (Washington, D.C.: CSIS Press, A Panel Report of the CSIS Commission on Technology Security in the Twenty-First Century, June 2001), xiii–xxii, [On-line]. URL: http://www.csis.org/pubs/ (Accessed on 28 Feb. 2002.)

and…encourage economic collaboration between any or all of them," such competition exists and will continue.[8]

Interoperability of systems and organizational structures within U.S. forces and among the NATO allies remains elusive.[9] Military officers and many of their civilian counterparts already recognize that without it effectiveness in war is reduced,[10] but its criticality and urgency have not led to its implementation—nor has the connection between ensuring interoperability and the economic issue of competition vs. cooperation yet been clearly articulated.

The main domain examined here is transatlantic security as it was established and is still practiced by the members of NATO. This report accepts the premise that the military leader is the primary stakeholder, but insights into that premise can be useful also to the congressional stakeholder in the United States, the parliamentary stakeholder in the United Kingdom (U.K.), and the global commercial-sector stakeholder. Issues pertinent to the Russian Federation, China, and even "rogue states" also are included with respect to their relationship to NATO's defense and economic structures.

1.1 Structure

The next three chapters present perspectives on globalization, each related to the others and all together constituting the big picture. **Chapter Two** examines first the relationship between two organizations that are cornerstones of international security, NATO and the EU. Then the discussion moves to the need for interoperability of systems and organizations to support coalition warfare, which is the type of warfare most likely to occur in this century. One potential barrier to achieving interoperability is the inherent competitiveness of international markets; another is the declining level of international defense spending and investment, as shown by figures for defense spending as a percentage of the gross domestic product (GDP). The chapter concludes with a discussion of both the necessary reliance by all member states on the commercial sector to retain NATO's superiority in defense and the recognition of the need for the military to exert leadership in establishing requirements and defining standards.

Chapter Three concentrates on dual-use technology and the diffusion of technology in relation to globalization. A definition of dual-use technology is offered with the suggestion that,

---

[8]Article II, final sentence, North Atlantic Treaty, [On-line]. URL: http://www.nato.int/docu/basictxt/treaty.htm (Accessed on 5 Oct. 2001.)

[9]Anthony W. Faughn, *Interoperability: Is It Achievable?* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, September 2001), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=555; and William F. Maher, Jr., *Legal Aspects of State and Federal Regulatory Jurisdiction Over the Telephone Industry: A Survey* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-85-3, March 1985), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=44

[10]See, for example, *Kosovo/Allied Force After-Action Report*, Report to Congress, Dept. of Defense, 31 Jan. 2000, [On-line]. URL: http://www.defenselink.mil/pubs/kaar02072000.pdf (Accessed 12 Feb. 2002.)

given NATO's growing reliance on commercial industry to retain security dominance, the expansion of dual-use technologies is probable. The prospect of over-reliance on technologies in the hands not only of allies but also of adversaries and the potential for both legal and illegal global diffusion are suggested as the cause of the *angst* at the heart of this issue. The Internet is used here as an example to highlight difficulties in controlling technology that adversaries of NATO and of the United States might use in their own military applications.

Chapter Four examines the history of the use of export control and the waning applicability of such control in a globalized world. The relationship between export control and dual-use technologies is discussed, particularly the importance of focussed controls, noting points of failure in the current (2002) export control regime. The intention here is to shed light on U.S. congressional and U.K. parliamentary debates on export control. International efforts to control technology also are discussed, with an emphasis on the need to bolster current programs without creating an insurmountable obstacle for legitimate enterprise.

Chapter Five consolidates the three perspectives delineated in those three chapters, draws rudimentary conclusions as to the look and feel of globalization, and offers suggestions meant to be open-ended, consistent with the method of the Program on Information Resources Policy, which is to say, not prescriptive by design. These conclusions and suggestions are intended to provoke additional thought and discussion in the ongoing dialogue about the globalization of economies and the accompanying security issues.

In the multipolar, post-cold war environment, civilian leaders in the United States and elsewhere will want to be able to count on the informed counsel of the military leadership as, from their different perspectives, they strive together to defend nations and alliances. Rogue states, transnational migration, and terrorism will continue to pose real threats, and like successful military officers in the past (Washington, Eisenhower, and Marshall, for example),[11] the military leader of tomorrow will need to be aware of all the instruments of national and international power.

[11]But unlike, for example, Ulysses S. Grant.

Chapter Two

Transatlantic Security, Interoperability, and Investment

It is logical that the United States should do whatever it is able to do to assist in the return of normal economic health in the world, without which there can be no political stability and no assured peace.[1]

General George C. Marshall

2.1 The North Atlantic Treaty and the EU: Cornerstones of International Security

In April of 1949, the United States and several of its European allies, recognizing a mutual interest in collective security, signed the North Atlantic Treaty. By staying committed to its articles, the North Atlantic Treaty Organization, the resultant organization of states, became one of two cornerstones of Atlantic security and, arguably, of global security. Most military officers and civilian leaders are familiar with Article V of the Treaty, quoted in **Chapter One**, which states that an attack against one member nation constitutes an attack against all and allows a collective military response.

The United States as well as its European allies have a vital interest in preserving peace and stability in Europe: "the presence of significant and highly capable U.S. forces in Europe will remain, for the foreseeable future, a critical linchpin," according to William S. Cohen.[2] The resolve to support expansion of the Area of Responsibility (AOR) was evident as recently as 1999, when military forces were employed in Kosovo in operation Allied Force. The next administration underscored this commitment when Donald Rumsfeld as secretary of defense invoked Article V within a day of the attacks of September 11, thus providing powerful testimony to NATO's overall approach to collective security.

In day-to-day interactions in the globalized environment, as opposed to crises, however, Article II of the North Atlantic Treaty is primary, because it is likely to provide the stability and security that leaders seek. For this reason, this article is worth looking at in some detail. In part it states:

---

[1]From a commencement address by George C. Marshall, Secretary of State, "On June 5, 1947,…at Harvard University, [when he] first called for American assistance in restoring the economic infrastructure of Europe. Western Europe responded favorably, and the Truman administration proposed legislation. The resulting Economic Cooperation Act of 1948 restored European agricultural and industrial productivity. Credited with preventing famine and political chaos, the plan later earned General Marshall a Nobel Peace Prize. The Economic Cooperation Act of 1948, April 3, 1948, page 1, General Records of the United States Government, National Archives and Records Administration [S.2202, 80th Congress, 2nd Session, Public Law 472, Chapter 169]." National Archives and Records Administration, [On-line]. URL: http://www.nara.gov/exhall/featured-document/marshall/marshall.html (Accessed on 22 Jan. 2002.)

[2]William S. Cohen, *Strengthening Transatlantic Security: A U.S. Strategy for the 21st Century* (Washington, D.C.: Dept. of Defense, December 2000), v.

> The parties will contribute toward the further development of peaceful and friendly international relations by strengthening their free institutions… and by promoting conditions of stability and well-being. They will seek to eliminate conflict in their international economic policies and will encourage economic collaboration between any or all of them.

The U.S. military establishment will need to recognize that in times of peace the United States and its allies will need to ensure and further Article II, and that, should such support fail, failure may be paid for with blood. The United States and its NATO allies increasingly need to complement warfighting tools with economic tools that cross oceans in a continuing effort to provide security by design, not by happenstance.

NATO is one of twin security cornerstones, the other being the EU. Because these Gemini provide the foundation of stability for international security—as one is bloodied so will its twin be—they are best studied in parallel. Globalization has come to mean that Europe and the United States are tightly linked in the economic instrument of national security and power. The EU is cousin to the Marshall Plan but with a greatly expanded international economic symbiosis. Many believe (as did the author), erroneously, that in the aftermath of World War II the United States was wholly charitable in its financial support of both allies and the former Axis partners, but the United States and its economy also benefited.[3] U.S. aid was economic—until 1953 (during the Korean conflict), that is, it did not include military aid.[4] The merging of economic and military aid with a global reach was an important harbinger of the relationship of the EU and NATO in the present and likely future.

The EU is the United States's largest trading partner and likely to remain so in the twenty-first century. The United States has invested nearly $4.5 trillion in Europe, and Europe has invested a similar amount in the U.S. economy. In 1999, the two-way trade between the United States and Europe was $507 billion. In the 1990s, it accounted for 14 million jobs. The economies of the member nations of the EU combined may soon surpass the U.S. economy as the largest in the world.[5] Strengthening the link between NATO and the EU may also improve the economic performance of the member states. The benefits of such cooperation might increase resources

---

[3]The money was used to buy goods from the United States, which had to be shipped across the Atlantic on U.S. merchant vessels. But it worked. By 1953, the United States had pumped in $13 billion into Europe, and Europe was standing on its own feet again.

[4]For further reading, see John Gimbel, *The Origins of the Marshall Plan* (Stanford, Calif.: Stanford University Press, 1976); Imanuel Wexler, *The Marshall Plan Revisited: The European Recovery Program in Economic Perspective* (Westport, Conn.: Contributions in Economics and Economic History, 1983); and Michael J. Hogan, *The Marshall Plan: America, Britain, and the Reconstruction of Western Europe, 1947–1952* (Cambridge, Eng.; New York: Cambridge University Press, 1987).

[5]*Strengthening Transatlantic Security: A U.S. Strategy for the 21st Century,* 7.

available to improve national defense capabilities of the U.S. and European member nations of both organizations.[6]

2.2 Interoperability: Critical to NATO's Coalition Operations

In military operations, interoperability is not free, but without it NATO would be less effective than it needs to be and will continue to need to be. Since passage of the Goldwater–Nichols Act in 1986,[7] the U.S. military has been in the process of transformation from a platform-based responding force into a "network-centric" fighting force,[8] a change that requires the United States and its allies to improve "sensor-to-shooter" capabilities. An effective network and network-centric capabilities emphasize the need for interoperability. NATO's operation Allied Force (in Kosovo in March–June 1999)[9] underscored the need for interoperable forces and, according to Admiral William Owens, confirmed a "significant gap" between the military capabilities of the United States and its allies. Owens pointed to precision-guided munitions, satellite reconnaissance communications, and other modern technologies as areas of the disparity.

The path to network-centric warfare will need to include interoperability, but interoperability is complex and the path to it has many forks. Again according to Admiral Owens, serious problems lie ahead in military operations that will involve NATO partners, because "a root premise of coalition warfare is that the partners be able to work together and that their military components…be coordinated seamlessly."[10] A recent (2002) review of coalition operations has shown that the political and economic dimensions of interoperability may be manifest at strategic, operational, tactical, and technological levels,[11] and to fight effectively in the future, as Lieutenant

---

[6]In some areas, such as agricultural policy and trade, members of the EU pool their sovereign powers, which allows the EU to negotiate directly with the United States and other countries. In other areas, including international defense and security, members retain individual sovereignty.

[7]"The Goldwater–Nichols Department of Defense Reorganization Act of 1986, sponsored by Sen. Barry Goldwater [Rep.-Ariz.] and Rep. Bill Nichols [Dem.-Ala.], caused a major defense reorganization, the most significant since the National Security Act of 1947." See URL: http://www.ndu.edu/library/goldnich/goldnich.html (Accessed on 28 Feb. 2002.) See also Gordon N. Lederman, *Reorganizing the Joint Chiefs of Staff: The Goldwater–Nichols Act of 1986* (Westport, Conn.: Greenwood Press, 1999).

[8]David S. Alberts et al., *Network Centric Warfare: Developing and Leveraging Information Superiority,* 2nd ed., rev. (Washington, D.C.: Command, Control, Communications, Computers, Intelligence Surveillance, Reconnaissance [C^{4}ISR] Cooperative Research Program [CCRP], August 1999).

[9]See Operation Allied Force, [On-line]. URL: http://www.defenselink.mil/specials/kosovo/ (Accessed on 23 Jan. 2002.)

[10]Admiral William A. Owens, with Edward Offley, *Lifting the Fog of War* (New York: Farrar, Straus, and Giroux, 2000), 190-191.

[11]Myron Hura, et al., *Interoperability: A Continuing Challenge in Coalition Air Operations* (Santa Monica, Calif.: RAND Corp., 2000), 177.

General Joseph Kellogg of the Joint Chiefs of Staff has emphasized, the intent of architectures will need to be "a seamless, end-to-end system of fully networked capabilities."[12]

Given that the United States and its NATO allies all share a vision of interoperable systems, it would seem that they would work together toward that end. The policy of the Department of Defense (DOD) on interoperability is broad and sounds inclusive of NATO allies and potential coalition partners as well as the U.S. Services:

> Interoperability within and among United States forces and U.S. coalition partners is a key goal that must be addressed satisfactorily for all Defense systems so that the Department of Defense has the ability to conduct joint and combined operations successfully.[13]

The DOD's acquisition policy appears to recognize the link between defense and economic stability:

> In order to foster interoperability with its allies and coalition partners, consideration shall be given to procurement or modification of Allied systems or equipment, or cooperative development opportunities with one or more Allied nations to meet user needs.[14]

Thus, the problem with interoperability policy is not the policy but, as with much policy, with implementation and enforcement.[15] In technologies such as cryptography and high-performance computing, NATO has shown a lag in interoperability, yet these technologies are available through export or diffusion. Thus, ensuring interoperability with NATO allies runs smack into the huge issue of competition vs. cooperation, that is, the relationship between the issues of national vs. international defense and of the security vs. commercial endeavor. To this point the background given here has emphasized the cooperative nature of NATO and the EU, but the competitive nature of the globalized world also has ramifications for international security.

2.3 Economic Cooperation and Competition: Toward Achieving Interoperability

Through fifty-plus years the relationship of the United States and the its nineteen allies in NATO and its fifteen EU partners[16] has proved abiding, based as it is on a shared need for

---

[12]Interview by JoAnn Sperber, "Q&A: Interoperability Enforcer, Lt. Gen. Joseph K. Kellogg, Jr.," *Military Information Technology* **5**, 5 (2001), 19, [On-line]. URL: http://www.mit-kmi.com/archives/5_5_mit/5_5_index.cfm (Accessed on 12 Feb. 2002.)

[13]Dept. of Defense Directive 5000.1, 23 Oct. 2000, 2-3.

[14]Ibid.

[15]This observation is based on the author's experience in a tour at the Pentagon, where he found that the dedicated people who write policy almost always have good intentions and are reasonable at practicing compromise.

[16]The members nations of the European Union are Austria, Belgium, Denmark, Finland, France, Germany, Greece,

stability. All these nations possess some degree of nationalist fervor and have individual economies to foster. As each assesses the military threat to itself, it routinely reassesses its commitment of resources to defense in an effort to balance that commitment and other national objectives. No nation has infinite resources or sees zero threat to itself. The reassessment of resources by independent nations gives rise to stakes of economic cooperation and competition that put interoperability and "seamless" coalition operations in jeopardy. The situation is complex, as in Kosovo, where both sides of the Atlantic partnership fought together as a coalition, not as independent nations. Only a few years later, the multinational military response in Afghanistan to the terrorist attacks on the United States in September of 2001 again indicated that coalition warfare is likely in the twenty-first century.[17] While, on the one hand, dependence on coalition warfare brings a need for interoperable systems, support for specifically national defense may, on the other, override concern for collective security. Opportunities for cooperation bring with them serious hurdles for interoperability within national economies.

With the two-way trading bloc of the United States and the EU measured in trillions and with the known shared security concerns that burden all nations, the benefits of cooperation would seem self-evident. Yet relationships may "sour." For example, this occurred between the EU and the United States over U.S. defense mergers, mainly because, beginning in the early 1990s, defense-related industries in Europe have taken a serious economic hit. In the decade since then, owing to international competition, the United States's staunchest allies—Britain, France, and Germany—lost at least 100,000 high-paying, high-tech defense jobs, resulting in a lopsided transatlantic defense trade that favored the United States.[18]

Given shrinkages in the U.S. marketplace in the 1990s, however, a U.S. military-industrial-complex-centric reader might protest the Europeans' sour taste. Those defense mergers in the United States, which led to a loss in jobs, was driven primarily by a shrinking of the defense procurement budget by 70 percent.[19] The U.S. domestic market has shrunk from a high of 120,000 defense firms in 1990 to a low of 30,000 defense firms in 2000. The surviving firms managed, however, to grab 40 percent of the global market, whereas ten years earlier they had held only 25 percent. Current (2001) procurement budgets for all EU nations cannot ensure the long-term survival of even a third of European defense firms; thus the sour taste in European mouths.[20]

Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom

[17]Personal communication to the author from Mark Mills, Captain, USN, within the Theodore Roosevelt Battlegroup, 2001-2002.

[18]John L. Less, *The Souring of the Defense Industry: U.S.-European Competition*, [On-line]. URL: http://www.sais-jhu.edu/studorgs/foreignobserver//1197/defense.html (Accessed on 13 Dec. 2001.)

[19]See Jacques S. Gansler, *Military and Industrial Cooperation in a Transformed, NATO-wide Competition*, [On-line]. URL: http://www.csdr.org/98Book/gansler98.htm (Accessed on 13 Dec. 2001.)

[20]Less, 1.

Free trade among nations would appear to be the answer for interoperability. It would allow acquisition of equipment and systems at reasonable prices and ensure interoperability by excluding noncompetitive manufacturers. In 1998, Jacques S. Gansler, U.S. under secretary for defense for acquisition, noted that cooperation in the geopolitical, military, and industrial arenas and removal of inefficiencies could "improve transatlantic industrial ties" and, incidentally, improve goods and services, while recognizing the political realities of providing countries a fair return on their investments.[21] International interoperability requires that national leaders set standards and define requirements for emerging technologies. Competitiveness need not mean capitulation. For example, even though the manufacture of personal computer video graphic cards is highly competitive, the products are interoperable owing to the shared desire to build toward a common standard.[22]]

Its allies have economic reasons for not exporting to or importing exclusively from the United States. The computer industry, for example, is ripe for competition among the NATO allies (see **Table 2-1**). Simply put, the allies have indigenous manufacturing, assembly, and research capabilities of their own in this industry which directly compete with the United States,

Table 2-1

Manufacturing, Assembly, and Research Capabilities of Allied and Non-Allied Countries

Country	Computers	Components	Software	Research
Belgium	—	I	I	I
France	I	—	I	I
Germany	I	—	I	I
Italy	I	—	I	I
Netherlands	I	—	I	I
United Kingdom	I	I	I	I
China	I	I	I	I
Russia	F	I	I	I

Source: U.S. Department of Commerce; Merrill Lynch; Gartner Group. Data adapted from Table 2.1 in "Computer Exports and National Security" in *New Tools for a New Century* (Washington, D.C.: Center for Strategic and International Studies [CSIS], June 2001), 7.

I = indigenous capability F = capability from foreign subsidiary

[21]Gansler, 2.

[22]Personal communication to the author from Captain Michael D. Molloy, USAF (Ret.), on an earlier version of this report, 10 June 2002.

and their desire to further their own marketshare and economic advantage does not always synchronize with international security concerns.

The computer industry is not alone in the globally competitive environment. Military arms sales and "high technology" mirror a similar international competitiveness. As manufacturing becomes global, more and more countries enter this economic fray for their own economic gain, with little thought of aiding or abetting the United States's economic advantage. The United States's silver crown as "king of the global high-tech market" is rapidly being tarnished as adversaries and allies alike rush to build their own organic capability.[23] The National Science Foundation (NSF) has estimated that although the United States may retain the largest share of the high-tech market, the dimension of its share has dropped from roughly 25 percent in 1991 to 18 percent in 2001as other countries continue to enter their technologies into the market.[24]

2.4 International Investment in Defense: Driver of Economic Cooperation or Competition

The United States remains the single superpower, with military commitments throughout the globe, and in some quarters that is "good news": "The good news today is that American military power is still vastly superior to all likely competitors, in most categories, and barring any sudden technological breakthroughs, U.S. supremacy for a decade to come is assured."[25] The United States also spends more than any other nation on its military (see **Figure 2-1**). That in itself, however, is less remarkable than the huge disparity between what the United States spends and what its allies in NATO and the EU spend: the United States spends more than two times what all its allies combined spend. It spends a whopping $343.2 billion, compared with $147.219 billion for all other nations in the alliance combined.[26] It spends ten times more than its closest ally, the U.K., which spends only $34.5 billion. Only four (France, Germany, Italy, and the U.K.) of the other nations comprising both NATO and the EU spend more than $10 billion. Eight member nations of the NATO and EU spend less than $3 billion—the approximate cost of only nine U.S. B-1B bombers. Iceland, which can be said to function as a stationary platform—an aircraft carrier—for the alliance, contributes only $19 million, that is, less than the cost of a single military supercomputer.

The United States, one may argue, also spends an inordinate amount compared with its likely adversaries. It spends twenty-three times more than the $14.4 billion spent by all "rogue"

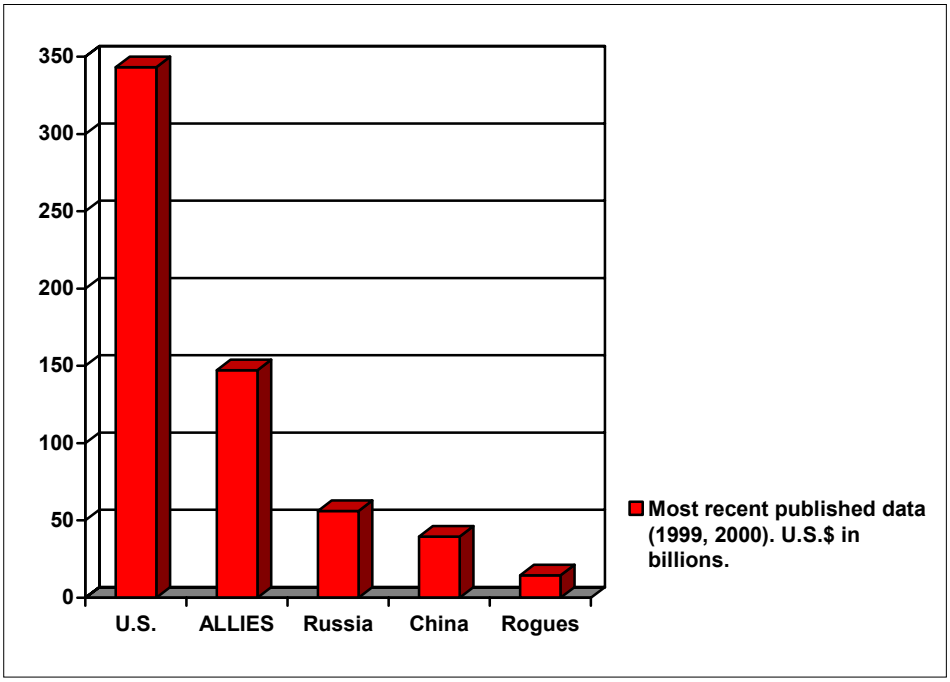
---

[23]An industry indigenous to a country or particular organization and not dependent on other sources for products or services is said to be "organic."

[24]CSIS, *Computer Exports and National Security: New Tools for a New Century* (Washington, D.C.: CSIS Press, A Panel Report, June 2001), 7, [On-line]. URL: http://www.csis.org/pubs/; citing NSF, *Science and Engineering Indicators 2000* (Washington, D.C.: NSF, 2000).

[25]Gordon R. Sullivan, editorial, "Increased Global Engagement Makes Greater Investment in Military Vital," *Tacoma News Tribune*, 18 Aug. 1998.

[26]All figures here and throughout the study are given in U.S. dollars.



Note: Allies include all NATO countries excluding the United States and Rogues, which include the United States's most likely adversaries in the view of the Pentagon: Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.

Sources: International Institute for Strategic Studies, U.S. Department of Defense; *The Defense Monitor* **XXX**, 7 (August 2001).

Figure 2-1

U.S. Military Spending vs. World Spending

nations combined, as these are identified by the Pentagon (Figure 2-1). It spends six times more than Russia, which spends $56 billion, and eight times the military budget of China, which is $39.5 billion.

As the sole superpower, the United States spends so much on defense because its goal is to "preserve an American technological edge," on the premise that in a globalized world it must always be able "to maintain superior status in a technologically stratified international system."[27] But beyond merely preserving that edge, it spends these sums to have that edge in order to prevent military operations against itself. Should such operations prove unavoidable, then what has been spent will afford the United States the advantages offered by technology to defeat its adversaries. Significantly, even though the dollar amount appears enormous in relation to what allies of the United States spend, historical trends of the military percentage of the U.S. GDP tell a different story, one with potentially catastrophic implications for modernization and for retention of a technological edge.

---

[27]Janne E. Nolan, "Cooperative Security in the United States" in *America's Strategic Choices*, edited by Michael Brown (London, Eng.; Cambridge, Mass.: The MIT Press, rev. ed., 2000), 214.

In 2001 the amount of money the United States spent on defense, as a percentage of the GDP, was at the lowest it has been since 1940. From more than 6 percent of the GDP in 1989, in 2001 it hovered at around 3 percent of the GDP.[28] Several current and former prominent members of the U.S. military have publicly denounced as insufficient the current budget of 2.9 percent of GDP, saying that the U.S. military is heading for a "train wreck" because of its inability to recapitalize the force or to sustain current readiness on that budget.[29] They have said that the changing world environment, and the need to sustain readiness, recapitalize, modernize, and transform the U.S. military, mandate that the military budget rise to at least a "four-percent solution."[30]

To make matters worse, the United States's power on the world stage may slip when it is recognized that, although "modernization" is 30 percent of the DOD's budget for fiscal year (FY) 2002 and the DOD's goal is 3 percent of the Total Obligation Authority (TOA), the current (2002) Presidential Budget was only 2.7 percent of the TOA. The Services, too, are struggling. In 2001 funding for Science and Technology, for example, was only 2.1 percent of the Air Force TOA.[31]

2.5 Growing Reliance on Commercial Technology: Harbinger of the Future?

The problem of disparate military and commercial spending on research and development (R&D) is compounded by the growing awareness that the U.S. military neither leads in innovation nor drives technological advances. The commercial sector, as is widely accepted, leads in advanced technology integrated into modern information-intensive systems, especially the software and the consumer microelectronics sectors,[32] and the U.S. military more and more relies on commercial technologies, many of them available on the open market for consumption by friend or foe. In the globalized marketplace the commercial sectors, in the United States and elsewhere, pay little attention to national boundaries.

---

[28]Briefing by Major General Rodney P. Kelly, Deputy Chief of Staff, Plans and Programs, distributed to Senior Service School Air Force Fellows 2001–2002 on 6 Aug. 2001, at Analytic Services, Inc. (ANSER), "a public-service institute, an independent, not-for-profit corporation chartered in California with the assistance of the RAND Corporation in 1958." See URL: http://www.answr.org/ (Accessed on 15 Jan. 2002.)

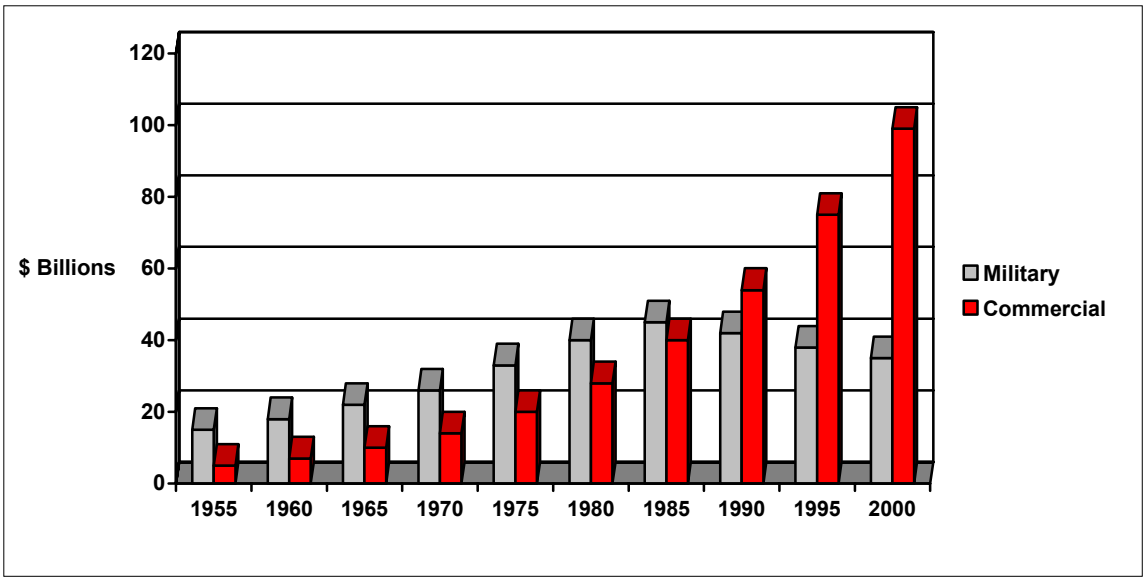
[29]For example, briefing by Major Gen. Kelly, 6 Aug. 2001.

[30]The following are recommended reading on the "Four Percent Solution": Frank J. Gaffney Jr., "The 'Four Percent Solution' for Military Readiness," *San Diego Union Tribune*, 13 Aug. 2000; Hunter Keeter, "Marine Commandant Calls for Defense Spending Increase," *Defense Daily*, 16 Aug. 2000, 6; Tom Stuckey (Associated Press), "Fleet Strength at Risk, Retiring Admiral Says," *Washington Times*, 23 July 2000, C-13; and Gordon R. Sullivan, editorial, "Increased Global Engagement Makes Greater Investment in Military Vital," *Tacoma News Tribune*, 18 Aug. 1998.

[31]Briefing by Brigadier General Faykes, *AF Budget Update*, distributed to Senior Service School Air Force Fellows 2001–2002, 2 Aug. 2001.

[32]Office of the Under Secretary of Defense for Acquisition and Technology, *Final Report of the Defense Science Board Task Force on Globalization and Security* (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, December 1999), [On-line]. URL: http://www.acq.osd.mil/dsb/globalization.pdf (Accessed on 27 Nov. 2001.)

The erosion of the DOD's dominance in technological advance is not new, nor is its need to look to the commercial industry for such advances. **Figure 2-2** indicates the demise of the U.S. military's prominence in technological advancement between 1955 and 2000. Although the DOD's initial investment in R&D in 1955 was $15 billion, that sustained only a 4 percent increase until the mid-1980s and achieved a maximum of $45 billion in 1985–86. After that, the accepted decline in R&D spending has led to only $35 billion in 2000. Commercial high-tech industry began in 1955 with only a $5 billion investment in R&D but has sustained an annual growth rate of 7 percent since then, and around 1985 it surpassed the DOD's spending in this area.



Source: *Naval Research Advisory Committee Report*: *Science and Technology* (June 2000), 15, [On-line]. URL: http://nrac.onr.navy.mil/ (Accessed on 15 Jan. 2002.)

Figure 2-2

U.S. Military vs. Commercial Spending on R&D

According to commercial forecasts, industry will continue the 7 percent commitment for the foreseeable future, and the trend toward military reliance on commercial technology will grow.[33] The implication for the military is a mandate to incorporate commercial technologies that may or may not be exclusive to the U.S. military or its allies. Another implication, for both the United States and its allies, is that military leaders will need to become familiar with cooperative economic strategies for both the military and the commercial sectors, for example, to break down the barriers of "fortress defense" and "fortress industry," and will need also to be able to articulate the military's technological requirements. With respect to its EU partners, the United States's

[33]*Naval Research Advisory Committee Report*: *Science and Technology* (June 2000), 15, [On-line]. URL: http://nrac.onr.navy.mil/ (Accessed on 15 Jan. 2002.)

long-term (five to ten years) technological development will need to be conducted in collaboration with competitors in the EU.

Thus, the DOD, for reasons of interoperability, performance, and cost, will need to take advantage of commercial technology and participate in framing the requirements for industry.[34] And as the U.S. military increasingly relies on information superiority[35] to enable new operational concepts of dominant maneuver, precision engagement, focussed logistics, full-dimensional protection, and, through their synergy, full-spectrum dominance,[36] it also becomes increasingly dependent on a commercial sector that pays scant attention to national boundaries.

2.6 Investment in Niches to Achieve Technological Advantage in Military Operations

The U.S. government, though limited and shrinking in relation to the previous year's GDP, remains an important weapon in the security arsenal. For the United States and its NATO defense partners to remain dominant in international security, they will need to look at technological niches (such as cryptography, defense satellites, nuclear technology) where the commercial sector does not often participate.

The DOD's Science and Technology Program was organized to support the missions described in the National Security Strategy (1995), in particular to respond to the strategy's goals and objectives, among them, preservation during a conflict of an information advantage over the adversary.[37] This program—actually, a cluster of subprograms that explore many scientific and technological areas—can be applied to security at home and abroad. As an instrument, the science and technology investment is critical to implementing Article II of the North Atlantic Treaty.[38] Further, by clearly articulating their requirements to the national science and technology community, warfighters can make that community sensitive to the opportunities that the military niche presents for international security.

---

[34]Ibid., 37.

[35]Information superiority may be said to exist when one competitor can establish a relative information advantage over another, usually an adversary.

[36]Arthur Money, *Information Superiority: Making the Joint Vision Happen* (Washington, D.C.: U.S. Dept. of Defense, U.S. Gov't Printing Office, [2000]).

[37]Ibid.

[38]Maintaining Military Advantage Through Science and Technology Investment (1995), [On-line]. URL: http://clinton4.nara.gov/WH/EOP/OSTP/nssts/html/chapt2.html (Accessed on 5 Feb. 2002.) The Science and Technology Program is heir to and expands the Advanced Research Projects Agency (ARPA), which, in the late 1960s, built ARPAnet, forerunner of the Internet. Article II of the North Atlantic Treaty empowers the United States to counter military threats and expands policymakers' options to include those other than war to promote stability and prevent conflict.

2.7 Summary

The United States and its NATO allies remain committed to the articles and principles of NATO. In a post-cold war environment, the military leadership on both of sides of the Atlantic needs to familiarize itself with the means to implement Article II of the Treaty, and, should efforts to maintain stability fail, to conduct operations as a coalition. Although recent experience in Kosovo and Afghanistan has shown that doing so requires extensive interoperability of systems and structures, the disparity between U.S. systems and those of its allies is growing, which is damaging to the prospects of achieving interoperability.

A partial explanation of this failure to achieve interoperability can be found in an examination of the globalized environment and of the allied commitment of resources to military and R&D budgets. Nation states act in their own interests, and the business of defense and its spinoffs is lucrative for individual nations, which therefore are not always compelled to act to improve the collective security of all NATO partners. Although the U.S. investment outweighs those of even its allies by far, it has been shrinking as a percentage of the GDP, with the result that its ability to fund advances in technology has begun to wane. This situation has led to a growing reliance on commercial technological sectors to implement the U.S. network-centric model of warfighting.

With this environment as a backdrop, proponents of Articles II and V of the North Atlantic Treaty look for cheaper yet dependable alternatives in order to achieve international security. The movement to and employment of dual-use technologies and export control to retain international security have been growing in prominence, but there are many ramifications of these trends, both in the stakes and for the stakeholders in these domains. The next two chapters address these stakes in detail and highlight the potentialities and the pitfalls.

Chapter Three

Dual-Use Technology and the Diffusion of Technology

This diffusion of explicitly military technology goes together with the problem of so-called "dual-use" technologies. If you can make semiconductors, you can put your chips in PCs, or in cruise missiles….[1]

Cosma R. Shalizi

National security concerns have traditionally motivated the policies, of both the United States and its allies, that support the development and implementation of advanced technologies. During World War II and in the war's immediate aftermath defense programs dominated U.S. R&D, and the payoffs were impressive as well as necessary and appropriate to recovery. Over the next half-century, however, defense needs changed, probably irreversibly. The age of dead-reckoning for success with military technology has passed. Historically, international conflicts and military operations have occurred where there are national borders. In the future, however, another likely battleground will be cyberspace, where "in a single second, a single strand of fiber-optic cable can transmit the data contained in 11,000 encyclopedia volumes."[2] In this environment of both bordered and borderless battlescapes, dual-use technology will become pivotal if military equipment is to be kept current to deal with these battlescapes, and its source will almost undoubtedly be the commercial sector.

The definition of dual-use technologies given here is technologies and goods developed for commercial use but which can be used either as military components or for the development or production of military systems. This chapter examines how the DOD has embraced technologies thus defined, such as the Internet—as have adversaries and pirates in the globalized world.

3.1 Dual-Use Technologies: Source of Answer or *Angst*?

Several industrialized nations, including the United States and many of its NATO allies, reserve the right to promote the proliferation of technology and thus, intentionally or not, may support the development or production, or both, of military systems abroad.[3] Globalization affects the DOD not only by altering the supporting industrial base but also by reshaping the military-

---

[1]Cosma R. Shalizi, in a review of William W. Keller, *Arm in Arm: The Political Economy of the Global Arms Trade* (New York: Basic Books, 1995), in *The Bactra Review* (15 Feb. 1996), 1, [On-line]. URL: http://www.santafe.edu/~shalizi/reviews/arm-in-arm/ (Accessed on 20 Feb. 2002.)

[2]Linda D. Kozaryn, "Fast-Paced, High-Tech Advances Provide Winning Edge," *American Forces Press Service,* 14 (Nov. 2000), [On-line]. URL: http://www.defenselink.mil/news/Nov2000/n11142000_200011141.html (Accessed on 16 Jan. 2002.)

[3]Janne E. Nolan, "Cooperative Security in the United States," in *America's Strategic Choices*, edited by Michael Brown (London, Eng.; Cambridge, Mass.: The MIT Press, rev. ed., 2000), 208.

technology environment.[4] As discussed in section **2.4**, the federal government now provides only 2 percent of the money that goes toward R&D, whereas in the 1950s it provided around 44 percent. Because globalization has forced the security elements of NATO to rely on dual-use technologies developed and initially produced in the commercial sector, achieving information superiority, implementing the Global Information Grid,[5] and, ultimately, conducting military operations successfully in a network-centric manner will require an understanding of these technologies and of how to employ them.

As all joint vision documents state, how well the United States and its allies will fight in the future will depend on the ability to field superior technology. The most important factor for achieving information superiority, according to John J. Garstka, may be a relative information advantage across the spectrum of conflict.[6] The basis for achieving supremacy on the battlefields of tomorrow will be dual-use technologies, such as high-performance computing, communication and networking services, and information dissemination management tools.[7] Toward such aims, the United States, and its NATO allies, may need to pursue objectives such as those of the formal Dual-Use Science and Technology Program, established only in 1997, which links the Services' researchers and developers to the commercial sector. These objectives are partnering with industry and jointly funding the development of dual-use technologies. According to Delores M. Etter, deputy under secretary of defense for science and technology, "the joint military and industry mission is to be sure that [the United States is] developing affordable and superior technology for the warfighter."[8] For industry to continue to bring revolutionary warfighting tools to the security establishments, those establishments will need to support its products by purchasing and applying them, that is, with commitments and funding.

---

[4]Final Report of the Defense Science Board Task Force on Globalization and Security (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, December 1999), [On-line]. URL: http://www.acq.osd.mil/dsb/globalization.pdf (Accessed on 27 Nov. 2001.)

[5]The Global Information Grid is the DOD's vision for implementing policy, process, and capabilities to ensure sensor-to-shooter integration.

[6]According to Garstka, "Relative Information Advantage is achieved when one competitor outperforms its competitors in the information domain and performance in the information domain is relative to what information one needs." See John J. Garstka, "Information Superiority for the Warfighter," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2000* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-1, October 2001), 4 [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?id=557 *Joint Vision 2010* (1996) defines information superiority as "The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." See URL: http://www.dtic.mil/jv2010/jvpub.htm (Accessed on 16 Jan. 2002.)

[7]A discussion of these individual areas is beyond the scope of this report.

[8]Jude E. Franklin, vice president and chief technology officer, Litton PRC, in an address to a conference on "Commercial Technology for the Warfighter" held by the DOD, McLean, Va., 8 Nov. 2000.

3.2 Military Dual-Use Programs: Fertile or Feeble?

Imagine that all stakeholders are delighted with dual-use technologies and with the way in which the United States and its allies employ them to further international security. Imagine that the militaries get "revolutionary" equipment that gives them both information and technical advantages through dual use. Imagine that the militaries are infused with low-cost, fast-paced high technologies to improve systems already fielded. And imagine, too, that at the same time the industrial base is alive and the commercial sector is both viable and delighted.

If a technology comes to be listed as dual-use in the military sense—technologies and goods developed for commercial use that can be used either as military components or for the development or production of military systems (see section **3.1**)—then the technology will come under the processing rules for export control of the Department of State (DOS) (see **Chapter Four**). From the viewpoint of commercial industry, these rules slow trade far too much and have often been criticized for protecting or even prohibiting commercial sale of technologies already available globally. "No commercial firm doing international business wants [its technology] to [be under auspices of the DOS's licensing process]," according to Jack Nunn, who for fifteen years (until 2001) headed the staff of the Dual-Use Science and Technology Program for independent assessment.[9]

Few commercial companies want to risk the security of their own country by providing an enemy nation with a technology that could offer or increase that enemy's information advantage. More important than blanket control, however—and more enforceable—is deciding which technologies to control [MSM, but may be redundant: and then enforcing the controls. More important than blanket control, however is the need to focus on which technologies to control and, then—more difficult—enforcing the controls. Many potential military applications of commercial technologies can neither be understood by the military generally or by civilians nor policed by them. Complete control of every conceivable commercial product that might be used in a military manner appears impossible. The terrorists of September 11th used ordinary technologies: commercial airliners, commercial telephones, on-line travel agencies, and the Internet.

Not all commercial companies want to do business with defense establishments around the world. Several have been "second sourced"—that is, an anticipated contract is given instead to a competitor that had not needed to pay for R&D or an engineering section. According to Jack Nunn, the U.S. commercial sector has complained of both excessive delays in payment and excessive oversight.[10]

---

[9]Personal communication to the author by Jack Nunn, 31 Dec. 2001.

[10]Ibid.

Both industry and the military and security establishments will need to emphasize the benefits of dual-use technologies. In considering whether to participate in the Dual-Use Program, the military leadership will need to point out the benefits to industry, and industry will need to recognize that it can indeed benefit—from cost-sharing among the commercial sector, the Office of Secretary of Defense, and the Services. For instance, a minimum requirement of the current Dual-Use Program is that the DOD fund 50 percent of the cost of the technology. Through this program a firm can develop and foster long-term partnerships with other firms and with defense labs and universities. Cost sharing can improve the potential for the transition of a technology into defense systems, which can then lead to increased markets globally. What needs to be fostered is a win-win philosophy that is to the benefit of both the military and commercial industry.[11]

The military and security establishments will have a role to play in encouraging continued support not only for what the Dual-Use Program does but also for the Program itself. That role, in addition to employing the Program, will be to praise it to congressional liaisons and constituents—and, if the appropriated dollars continue to decline, to request additional funding. As shown in **Table 3-1**, fiscal support for the program has slipped from a high of $68 million in FY 1998 to a steady state of only $30 million since 1999. Program dollars are revisited every year and are subject to congressional appropriation.

Table 3-1

Funding for the Dual-Use Science and Technology Program

Fiscal Year	**Support** (millions)
1997	$65
1998	68
1999	30
2000	30
2001	30

Source: URL: http://www.dtic.mil/dust/faq.htm

The DOD has come a long way in acquisition reform and in employment of dual-use strategies to capitalize on synergies between global commercial sectors and their companion defense establishments. Since the Clinton Administration announced the "21st-Century Defense Technology Strategy" (22 February 1998), which called for an increasing focus in R&D on dual-use technologies and emphasized reaching out globally for international cooperation, there has

[11]For a "Dual-Use Fact Sheet," see URL: http://www.dtic.mil/dust/faq.htm (Accessed on 4 Dec. 2001.)

been significant progress.[12] As a result, considerable advances have been made in critical technologies are being advanced in information technology, manufacturing, materials, and advanced simulation.[13]

In a globalized world, economic and technological imperatives for the DOD's increased reliance on the commercial sector have required rethinking of how and where warfare will be conducted. The diffusion of technologies not even regarded as candidates for the Dual-Use Program has been remarkable. Such technologies have been neither monitored nor licensed by either the DOS or the Department of Commerce (DOC). After only a few years following reengineering, nearly all DOD business operations, and many critical military functions (e.g., logistics), will be conducted over the Internet. For the United States and its allies, as also for their adversaries, the explosion of the use of the Internet within the U.S. Transportation Command (USTRANSCOM) has been a harbinger of its expanded use to conduct military business.[14] The Internet, like the Global Positioning System (GPS) has become a necessary tool for conducting warfare in the NATO scenario, and offers a model of a dual-use technology that is nearly impossible to control.

3.3 The Internet and Its Diffusion Friends: Models for Limiting the Effectiveness of the DOD's Dual-Use Program

Like the United States, many countries have determined that in a knowledge-based economy it is essential to upgrade and privatize communications infrastructures and to make computers and access to the Internet widely available and affordable. Simply put, to remain competitive in this environment, access to and use of the Internet are mandatory. Today's Internet is not the ARPAnet of old.[15] Whereas ARPAnet and the early Internet were accessible mainly by government and university researchers (primarily defense-related), today's Internet is accessible by anyone with a computer and a telephone connection, and such wide access is here to stay. A doorway that appears to look toward collaboration among allies in peace, looked through from a different direction, with Janus presiding, lies open to nefarious purposes.

---

[12]The three pillars are: reform the current DOD acquisition process, biased against the use of commercial processes and products within defense systems; focus more R&D within DOD on dual-use products and processes, emphasizing the need to achieve advances in high-tech defense systems that are affordable; and reach out globally to our allies, to benefit from international cooperation on a technology-by-technology basis. See URL: http://www.ibiblio.org/darlene/tech/report7.html (Accessed on 4 March 2002.)

[13]*Defense Technology: The Payoffs for Economic and Military Security*, [On-line]. URL: http://www.ibiblio.org/darlene/tech/report7.html (Accessed on 3 Dec. 2001.)

[14]Tasked with global transportation responsibilities in peace and war, USTRANSCOM uses the World Wide Web extensively to track passengers and cargo moving through commercial and military pipelines.

[15]ARPAnet, the foundation of the Internet, was the DOD's Advanced Research Projects network, built in 1968. See Martin C. Libicki, *Information Technology Standards: Quest for the Common Byte* (Boston: Butterworth–Heinemann, Digital Press, 1995), 251, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/libicki/libicki_quest/libicki_quest.html (Accessed on 29 Jan. 2002.)

The explosion of information technologies such as the Internet has serious implications for military and national security concerning the diffusion of technology. Loss of operational security, technological superiority, and knowledge of the enemy—issues paramount to winning and all as old as Sun Tzu[16]—all result from diffusion over the Internet. But in 1998, during a U.S. military exercise, the computers and linkages that allowed the United States to communicate large amounts of information to allies in war were found, again as with Janus, to have another aspect:

> it only requires a modest capability that is easily available to seriously disrupt vital services like electric power distribution and telecommunications systems. A small handful of capable computer specialists—a capability well within the reach of even moderately developed countries—using off the shelf, existing tools and techniques can wage war on the largest nations in the world.[17]

The diffusion of technologies such as computers and the Internet has become common. Some advocates of technological warfare talk of a time when war by bayonet will be replaced by war with computer viruses, logic bombs, and data manipulation. NATO's allies and adversaries see the adoption of new technology as essential to their own economic growth and not as belonging exclusively to adversaries of U.S. Recent studies of technology diffusion have shown that the capacity to purchase and the ability to learn new technologies are more important than geographic boundaries.[18] Studies of the integration of computers into society have found that the source and type of trade with other countries are important determinants of technology diffusion, whereas the English-speaking share of the population has no significant effect.[19]

Diffusion and the use of computers and the Internet, which lie beyond the auspices of international dual-use programs (and export control laws), pose serious questions for the military and political leadership. On the Internet, what constitutes sovereignty? What are the limits of the right to self-defense when the United States can be attacked from a computer in one country over a telephone line that passes through two others? Should the use of cyberspace for military purposes be limited because the same cyberspace has become the backbone of the global economy? What kind of arrangements, procedures, or treaties are needed that would simultaneously protect national security, promote electronic commerce (e-commerce), and

---

[16]Sun Tzu, *The Art of War: The Oldest Military Treatise in the World*, edited by Lionel Giles (Harrisburg, Penna.: Military Service Pub. Co., 1944), 51.

[17]Remarks by John Hamre at "Confronting the Security Challenges of the New NATO," the 15th NATO Workshop on political-military decisionmaking, Vienna, Austria, 22 June 1998. See news briefing, Office of the Assistant Secretary of State, Public Affairs, URL: http://www.defenselink.mil/news/Jul1998/t07081998_t0622nat.html (Accessed on 3 Dec. 2001.)

[18]Francesco Caselli and Wilbur J. Coleman II, "Cross-Country Technology Diffusion: The Case of Computers," *National Bureau of Economic Research Digest* (July 2001), 1.

[19]Ibid.

communications, and preserve personal privacy? As is true of outer space, the management of cyberspace will require new regimes and approaches.[20]

Globalization has forever changed the military and political landscape. Increased use of the commercial sector to modernize existing military systems or to provide new ones has become standard and essential. Transatlantic partnerships, which could yield returns in interoperability and maintainability, are ripe to strengthen the underpinnings of the defense industrial base and promote greater NATO cohesion.[21]

The establishment of a clearly articulated dual-use strategy *that will be followed* will be critical to success on the battlefields of the twenty-first century, whether those contested fields are on the ground, in the air, or in cyberspace. Shrinking dollars, mandatory extension of military systems, urgent interoperability concerns, and international competitive practices all drive the need for such a strategy. Unfortunately, international dual-use programs are accompanied by export controls and administration, which are the subject of **Chapter Four**.

---

[20]See Rachel Bronson and Daniel Goure, "Diplomatic Consequences of the Coming RMA: When the U.S. Is Unrivaled Militarily, What Happens to Our Alliances?" *Foreign Service Journal* (September 1998), ¶95, 2-4.

[21]Office of the Under Secretary of Defense for Acquisition and Technology, *Final Report of the Defense Science Board Task Force on Globalization and Security* (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, December 1999), [On-line]. URL: http://www.acq.osd.mil/dsb/globalization.pdf (Accessed on 27 Nov. 2001.)

Chapter Four

Export Control and International Positions

Existing international and national controls over the export of nuclear materials and technologies…have demonstrated their low level of effectiveness.[1]

General (Ret.) Remir F. Stepanov, USSR, Head of Dept., International Fund for Social and Economic Reform, Former Director of Export Control (1992)

4.1 Export Control, International Security, and Interoperability

Dual-use technologies fall under federal oversight, and the control mechanism is export control law. Current export controls were developed when manufacturing was local and only government-unique components were used.[2] Given the expanding international development of technologies, the United States and other governments have increased their review of export control law. As this is occurring, for the sake of international security, U.S. military leaders will need to watch the process carefully and contribute to the discussion. Were the defense establishment mute on changes in export control law, economic considerations might come to override security concerns.[3] As shown in **Figure 2-2**, in the mid 1980s commercial investment in technology surpassed the DOD's, leaving defense security concerns and interoperability to play second fiddle to the industry. Technology transfer from commercial enterprise has become a competition among allied peers, but if security voices are not heard finance might lead the way.

For NATO operations, the primary concern is the tie between export control and inter-operability. As allied nations build an indigenous capability, seek the lowest cost options for components (which often are external to NATO), and try to reduce the cycles for components, U.S. export laws drive them to look elsewhere for technology solutions, with potentially disastrous effects. According to a recent report by the Center for Strategic and International

---

[1]Remir F. Stepanov, "Basic Trends in the Development of Mechanisms for Controlling the Export of Dual-Use Products," in *Dual-Use Technologies and Export Administration in the Post-Cold War Era* (Washington, D.C.: National Academy Press [Documents from a joint program of the National Academy of Sciences and the Russian Academy of Sciences/Office of International Affairs, National Research Council], 1994), 139.

[2]CSIS, Executive Summary, *Technology and Security in the Twenty-First Century: U.S. Military Export Control Reform* (Washington, D.C.: CSIS Press, A Panel Report, May 2001), 6, [On-line]. URL: http://www.csis.org/export/execsum.htm (Accessed on 16 Jan. 2002.)

[3]The need for military leaders to contribute to the discussion on export control is illustrated by the discussion that was almost not held on the sale of the frequency spectrum, in which economic considerations nearly outweighed security concerns about interoperability.

Studies (CSIS) on U.S. Military Export Control Reform, security procedures and export controls that were designed to protect U.S. security have increasingly become "the cause of security problems and may contribute to the worsening of interoperability problems within NATO seen during the air war in the Balkans."[4]

The United States has what may be called an international perception problem that undercuts its stated desire to achieve interoperability in military operations. Both its export control practices and its wariness of including into its own defense establishment technologies developed in other NATO nations have been perceived abroad as "economic colonialism." From the European perspective, the United States is the 800-pound gorilla on the international economic stage. It may speak of "international cooperation," but its practice is often protectionist. The Bush Administration's intervention in 2002 to protect U.S. steel producers provides one example. In another, the United States has often sought allies' agreement to buy and use U.S. technologies, but, after the investment has been made, then either abandoned the technology or moved on to the next generation, leaving allies skeptical of U.S. overtures of international cooperation—and obligated to buy the next U.S. technologies just to keep up. Compounding this perception of the United States's intentions, allies have been asked to cooperate with the United States in becoming international "gun runners" when U.S. arms are sold directly to potential adversaries or are diffused to them through secondary buyers. At the same time, the United States appears neither to have acknowledged or, perhaps, appreciated its allies' contributions to earlier military operations in which the United States has been involved, such as operation Joint Endeavor (Bosnia-Herzegovina), nor the ways in which its allies' national histories and political environments shaped those countries' tasks and contributions to international stability.[5]

4.2 Dual-Use Technologies and Export Control: A Necessary but Not Ideal Marriage

The security environment of the post-cold war world, unlike that of the bipolar world, will increasingly require interdependence of the instruments of national power. For the United States to continue its leadership in international security, the economic instrument will need to be used liberally and expertly. This may require modification of export control laws from the cold war construct still current in 2002 in order to reflect transnational partnership in certain areas: entire end-items or their components; globalization of the Internet; diffusion of technology; and increased reliance on commercial solutions for military capability. In this post-cold war world, most nations are also experiencing a waning domestic defense capability.

---

[4]CSIS, Executive Summary, *Technology and Security in the Twenty-First Century: U.S. Military Export Control Reform* (Washington, D.C.: CSIS Press, A Panel Report, May 2001), 3 [On-line]. URL: http://www.csis.org/export/execsum.htm (Accessed on 16 Jan. 2002.)

[5]The author owes this perception of the reasons for the United States's difficulty in achieving international economic cooperation to discussion and correspondence with Robin Hamilton Harding, retired chief financial officer, Canadian Bell, who commented on an earlier version of this paper in May 2002.

Military technologies, in many respects, have been caught up with and often surpassed by civilian technologies. The U.S. military may no longer have a preponderance of or preeminence in certain technologies, yet to maintain information superiority—perhaps even at the expense of interoperability—the United States cannot afford to surrender primacy in information technologies. The sale or export of dual-use technologies interoperability can enhance military systems in three ways: (1) exports enhance U.S. security by ensuring that allies have the same or similar equipment; (2) exports defray the costs of development and maintain a viable manufacturing capability for future sales and, presumably, for greater stability; and (3) exports that support the economies of allies allow the United States to "profit" through its allies' good will. But there are challenges to export control laws throughout the NATO alliance.

4.3 Recognition of Weaknesses in Export Control

The commercial sector does not welcome federal oversight of the technologies it develops and produces, but for a technology to be licensed for government use it must be processed either by the DOC or the DOS (see section **3.1**). This system has been choking on the volume of applications for routine technology being exported to friendly countries. To remedy this situation, the Cox Commission called on the United States to build "higher fences" around a smaller set of critical components while attempting to control fewer goods.[6]

The volume of applications has led to a situation in which most of the U.S. military licenses granted each year have been approved or denied with little scrutiny or debate. The military leader has had and will continue to have a role in articulating the need to control sensitive or unique technologies and in helping to establish measured, disciplined, enforceable processes based not on economics but on security and stability. Processes built on political compromise may not always have national or international security interests at heart. Of approximately 55,000 applications for licenses or for agreements processed annually through the DOS, for example, most will be decided by the DOC, less than 20 percent will be referred to other agencies for review, and less than 1 percent will be referred to Congress for resolution.[7] Military leaders will need to fight against bureaucratic export control solutions—increasingly common in the absence of unanimity on U.S. objectives.[8]

---

[6]Ibid., 7. "In the 105th Congress, Rep. [Christopher] Cox [Re.-Calif.] served as chairman of the [bipartisan] Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China… created…June 18, 1998, [which] unanimously approved its report December 30, 1998, prompting major legislative and administrative action. The unclassified version of the report was issued in three volumes in May 1999." According to the Select Committee, the PRC had been stealing from the U.S. National Laboratories, as early as the 1970s and as recently as the mid-1990s. See URL: http://www.house.gov/coxreport/ (Accessed on 21 Feb. 2002.)

[7]Janne E. Nolan, "Cooperative Security in the United States," in *America's Strategic Choices*, edited by Michael Brown (London, Eng.; Cambridge, Mass.: The MIT Press, rev. ed., 2000), 211.

[8]Ibid.

An important nuance of export control has been the "blanket prohibition" of technologies. Many governments place such prohibitions on technologies with commercial applications, such as space-launch vehicles. These prohibitions might be acceptable, except that often lobbyists apply political pressure and are granted waivers. As a result, the technology soon diffuses to secondary and tertiary customers and the blanket prohibition becomes unenforceable. This situation represents the worst-case scenario: "unenforceable export controls with no ability to monitor either the destination or uses of transferred technologies."[9]

Globalization of dual-use technologies combined with ineffective export controls threaten transatlantic security. Determining whether a commercial product has a military application can be more art than science. Although commercial airliners may be used as military airliners, before September 11th few people would have imagined that one military application for them could be missile functionality. In information technology, the line between commercial and military applications is fuzzy at best. According to William Keller, if you can make semiconductors, you can make personal computers for organizing food recipes or chips for cruise missiles.[10]

A staunch export conservative may find it alarming that an adversary possesses the power of a 486 microprocessor and thereby "more computing power than United States scientists had when they developed the first atomic bomb."[11] But military applications do not require high MTOPS (millions of theoretical operations per second) computing power. For example, the air superiority fighter for the twenty-first century, the F-22, "was designed with a 958 MTOPS Cray supercomputer, roughly one-quarter the power now found in mass-produced Pentium chips."[12] Diffusion of explicitly military technology is inevitable as the line between military and civilian dual use blurs. Information technologies may be the most difficult to control, owing to their lucrative and legitimate nature.

4.4 Export Control Policy: Boiling Debate

Before 1996, national and international export control systems were primarily the domain and responsibility of individual nations acting in their own best security and economic interests. Many countries, however, following the lead of the United States and Russia, recognized that to ensure international security "the emergence of transnational business and industrial partnerships

---

[9]Ibid., 212.

[10]Cosma R. Shalizi, in a review of William W. Keller, *Arm in Arm: The Political Economy of the Global Arms Trade*.

[11]Philip Heerman, computer scientist, Sandia National Laboratories, quoted by Jeremy Hay, in "Fun and War Games," *Wired* (April 2001), [On-line]. URL: http://www.wired.com/wired/archive/9.04/mustread.html?pg=11 (Accessed on 21 Feb. 2002.)

[12]Seymour E. Goodman, Peter Wolcott, and Patrick Homer, *High-Performance Computing, National Security Applications, and Export Control Policy at the Close of the 20th Century (*Washington, D.C.: U.S. Dept. of Commerce, Bureau of Export Administration, 1998), 15.

requires a new model of government oversight,"[13] and toward that end in July of 1996 the United States and thirty-two other countries, including all members of NATO with the exception of Iceland, signed the Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. To be admitted to the WA, a country must be a producer or an exporter, or both, of arms or sensitive industrial equipment.

Participating nations agree to report on certain categories of export approvals of licenses or transfers and denials of licenses to nonmembers. The objective of the WA is to encourage "transparency, consultation, and, where appropriate, national policies of restraint to foster greater responsibility and accountability in transfers of arms and dual-use goods and technologies."[14] The urgency of establishing international export control oversight in the post-cold-war security environment would seem obvious, yet debate and then agreement on the WA by the thirty-three nations took three years. The U.S. ambassador to the WA, David T. Johnson, although "reasonably impressed" with progress thus far (as of early 2002), has pointed out that the United States can ill afford to be complacent about the Arrangement.[15] The items that fall under its auspices are legal and lucrative, and in an economically competitive global environment the challenge is to muster the political will and exercise the national discipline to control such technologies. For example, electronics, computers, telecommunications, and information security all are on the WA Dual-Use Control Lists of sensitive dual-use items, yet the United States and several of its allies export these items simply because they are so lucrative.[16]

Under the WA, participating states notify one another of denials of exports of sensitive dual-use items. They also inform all other participating nations that have approved a license for a transaction denied by another member within the last three years. To strengthen bilateral consultation before authorization of an export of a dual-use technology, the United States proposed adoption of a procedure for notification of denial that is similar to that used by other multilateral export control regimes. In the proposed procedure, before approving exports the participating states would consult with other participating states that deny the export of similar items to the same end-user. Adoption of "denial consultation" would be relatively painless for the

---

[13]CSIS, Executive Summary, *Technology and Security in the Twenty-First Century: U.S. Military Export Control*, 9.

[14]See The Wassenaar Arrangement, Questions and Answers, [On-line]. URL: http://www.usun-vienna.usia.co.at/wassenaar/WAQ&A.htm (Accessed on 9 Oct. 2001.)

[15]David T. Johnson, Opening Statement of the 12 Feb. 1999 Meeting, Wassenaar Arrangement Assessment, [On-line]. URL: http://www.usun-vienna.usia.co.at/wassenaar/johnson01.htm (Accessed on 9 Oct. 2001.)

[16]Participating states agree to control all items set forth in the list (and its two annexes) of sensitive items and a limited number of very sensitive items. The list is reviewed regularly to reflect technological developments critical to indigenous military capabilities. For the computer list, see URL: www.wassenaar.org/list/Cat%204%20-%2099.pdf (Accessed on 4 March 2002.)

participating states, given that "In the first two and half years of the [WA] there were only forty reported denials of Sensitive List and Very Sensitive List items."[17]

The Dual-Use Control Lists are extensive, and forty reported denials make for a relatively small proportion. The position of the United States has been to increase strategic security by reducing the opportunity for a potentially nefarious end-user to "shop around" for dual-use technologies that could aid or abet a military application. The United States and its NATO allies have seen the globalization of information technology as both an economic center of gravity and as a catalyst for control of exports and, for these reasons, have begun to review their own laws. For example, the United Kingdom has begun to revamp its much criticized Import, Export, and Customs Powers (Defence) Act, written in 1939. In 1998, its Department of Trade and Industry published a White Paper on the modernization of strategic control powers to accommodate modern means of trading, such as transferring information over the Internet and brokering deals that involve the transfer of goods between two countries.[18]

The U.K. and the United States share some concerns. Both countries remain committed to transatlantic security and to providing greater transparency of export items. But neither wants its own industry to sacrifice a competitive advantage in the global marketplace. The U.K. has been concerned that foreign governments that have been buying technologies will look elsewhere for their next purchase, that is, to a country with less transparent export laws. According to the 1998 White Paper, "any process involving publication of individual applications…would mean identifying companies and the nature of their planned or actual export business which would likely harm their competitive advantage."[19]

Key to the success of the WA, as has been true of other international trade and export agreements, will be communication within and among the United States and its allies. Bulgaria's effort to join NATO offers an example of communication on international trade that can lead to increasing security, but its effort to control exports of arms and dual-use technologies illustrates the problem: the siren of dollars woos even a nation desirous of collective security and stability. Seeking admission to NATO and the EU, Bulgaria, through the WA, has agreed to implement a "responsible" arms trade policy consistent with the EU's Code of Conduct on Arms Exports, which lists export criteria as a guide to decisions on whether to grant or refuse an application for

---

[17]For the United States's "Position on Strengthening Wassenaar's Dual-Use Procedures," see URL: http://www.usun-vienna.usia.co.at/wassenaar/position04.html (Accessed on 9 Oct. 2001.)

[18]For the White Paper, see the Department of Trade and Industry, Strategic Export Controls, Presented to Parliament by the President of the Board of Trade by Command of Her Majesty, July 1998, [On-line]. URL: http://www.dti.gov.uk/export.control/stratex/1sec.htm (Accessed on 9 Oct. 2001.)

[19]Ibid., Section 2, Accountability in Strategic Export Controls, 3, [On-line]. URL: http://www.dti.gov.uk/export.control/stratex/2sec.htm (Accessed on 9 Oct. 2001.)

an arms export license.[20] Therein lies the rub. Bulgaria hopes to improve its chances of gaining entry into NATO and the EU by demonstrating that it is a good world citizen, but "its domestic legislation has yet to incorporate international regulations to which the country has committed."[21] Bulgaria lags, in part because its regulatory enforcement remains weak while incentives to export are strong.

The importance of NATO, and its Treaty, as an enabling force for international security cannot be overestimated. Bulgaria and other former Warsaw Pact nations regard NATO as underpinning their national security, too. Thus, the United States has the opportunity to build on the structure of NATO and other international organizations to spread the message, and reality, of information technology interoperability consistent with transatlantic security.

Military leaders will need to become familiar with DOD Directives, in particular the 1985 DODD 2040 on International Transfers of Technology, Goods, and Services. In an effort to take responsibility for achieving security with the economic instrument of national power, DODD 2040 states that defense-related technology ought to be treated as a valuable, limited resource, to be husbanded and invested in in pursuit of national security. It also recognizes the importance of international trade to a strong U.S. defense industrial base and therefore directs the DOD to apply controls in a way that will interfere only minimally with legitimate trade and scientific endeavor.[22] Debate in the U.S. Senate on the Export Administration Act of 2001 suggests the interests, security and economic, that need to be weighed.[23] A week before the attack on September 11th, Senator Fred Thompson (Rep.-Tenn.) said that the Senate "[is] debating legislation that weakens our export control practices in order to enhance our commercial interests."[24]

4.5 The Internet and Export Control

Will the Internet promote a breakdown of all export control laws, and are the United States and its allies merely punishing firms that are trying to conduct business? Stakeholders in international security may delude themselves by believing they can limit the export of technologies critical to security but already in the public domain and possibly already being used for organized crime, espionage, and terrorism.

---

[20]The EU's Code of Conduct on Arms Exports seeks to create "high common standards" that are politically binding on members' arms export decisions and to increase transparency on arms exports among EU members.

[21]Annemarie van Berkel, "Bulgaria's Arms Trafficking: An Issue Yet to Be Resolved," *Weekly Defense Monitor* **3**, 46 (2 Dec. 1999), 1, [On-line]. URL: http://www.cdi.org/weekly/1999/issue46.html#2 (Accessed on 28 Feb. 2002.)

[22]DOD Directive 2040, 2, 17 Jan. 17, 1984; Administrative Reissuance Incorporating Change 1, July 5, 1985.

[23]U.S. Senate Committee on Banking, Housing, and Urban Affairs, Committee Documents Online—107th Congress, Summary: The Export Administration Act of 2001, 23 Jan. 2001, [On-line]. URL: http://banking.senate.gov/docs/eaa/summ01.htm (Accessed on 4 March 2002.)

[24]News release, Senator Fred Thompson (Rep.-Tenn.), Thompson Statement on Export Administration Act [S.149], *Congressional Record*, 4 Sept. 2001.

Complicating the debate on export control of information technologies is one particular, apparently ubiquitous information technology: the Internet. The Internet has rendered debate on export controls of some dual-use technologies, such as encryption, meaningless. Encryption software has already gone into the public domain, spread there in the 1990s, in Debora L. Spar's phrase, by "pirates and well-wishers" who distributed key algorithms by using the Internet:[25]

> the advent of the Internet seemed to shift power away from the state. Pushed by technology that was evolving much faster than policy, national governments abandoned their restrictions on high-powered encryption or, as in the U.S. case, weakened them substantially.[26]

Diffusion of technologies such as the Internet along with the exchange of other information technologies or of data riding on the Internet may seriously jeopardize national security.

4.6 Export Control and Russia

The need to balance the conflicting demands of national security and economic growth and development is not unique to the United States and its NATO allies. Russia also has been struggling with the Janus faces of this dilemma and with how best to achieve a balance. Russia's technologies need to be controlled for security purposes. At the same time, however, Russia needs to unleash them to stimulate desperately needed economic growth.

The need for controls on trade between the United States and Russia of dual-use technologies relevant to the development and deployment of weapons will diminish as relations between these nations improve and greater trust is established, overcoming the cold-war legacy of mutual suspicion and fear of threat. Military leaders will need to understand that continuing improvement in political and economic relations and the growth of mutual trust, like that between NATO and Japan, are possible.[27] The terrorist attack of September 11th and the apparently warm relations between U.S. President George W. Bush and Russia's President Vladimir Putin seem to have improved relations also between NATO and Russia, as was evident later that month, when General Anatoly Kvashnin, Chief of the General Staff, told RIA-Novosti, the Russian Information Agency, that relations were moving from the theoretical plane toward practical cooperation in

---

[25]Debora L. Spar, *Ruling the Waves: Cycles of Discovery, Chaos, and Wealth from the Compass to the Internet* (New York, San Diego, London: Harcourt, 2001), 247.

[26]Ibid., 248.

[27]Office of International Affairs, National Research Council, *Dual-Use Technologies and Export Control in the Post-Cold War Era: Documents from a Joint Program of the National Academy of Sciences* (Washington, D.C.: National Academy Press, 1994).

international stability.[28] The Russian Federation is already a member of the WA and could prove a stabilizing force in export controls.

International debate on export controls and security will probably continue as the global environment of free trade, work force migration, and international competition, mixed with emerging threats and enlarging alliances, drive nations to reconsider both domestic and foreign interests.

[28]From Moscow RIA–Novosti, the Russian Information Agency, part of the state media holding company, and found in a daily press highlight for Air Force Fellows, 20 Nov. 2001 (in Russian).

Chapter Five

Conclusions and Suggestions

In the globalized world of the twenty-first century, the outlook of military leaders, as this would-be primer has suggested, may necessarily be broadened. Military leaders may not be able to expect to conduct strategic operations using only the military as an instrument of national power. Instead, they will need to be able to contribute to the debate involving several instruments of national power: political, economic, and informational. An examination of transatlantic security through the lens of the economic instrument suggests that this huge aspect of globalization remains to be explored.

Within the North Atlantic Treaty, military and commercial investment in technology, particularly dual-use technologies, and export control provide grounds for conclusions and suggestions that, especially for NATO military leaders, may prove useful. Along with a developing understanding of globalization, these may offer launch points for the discovery of other elements for later investigation.

- Globalization has mandated that the military leader learn the languages of economics and high technology and use them in support of international stability. The focus in this report has been primarily on transatlantic security, but, given that NATO essentially underpins world security, lessons learned in and around the Atlantic theater may be extrapolated to the global scene.

- NATO's invocation on September 12, 2001, of Article V of its Treaty, which enforces collective security and military response, demonstrated that this commitment remains important for global security. Beyond fulfilling the terms of Article V, military leaders will need to be able to contribute to stability by articulating their role in implementing Article II, which calls for ensuring stability through economic means.

- In the future, military operations will be conducted by coalitions, will rely on advanced technology, and will depend on interoperable systems and structures. Achieving interoperability will remain a worthwhile objective, but issues of national sovereignty and healthy economic competition may impede implementation of interoperability. In the era of cyberspace and cyberwar—that is, the borderless battle-scape—diffusion of technologies may overcome even well-intended export controls of military materiel, complicating the pursuit of interoperability. For NATO to maintain its military superiority it will need to adapt to, fund, and implement a balance of defense and economic priorities that will themselves then be balanced against international cooperation or overlap, as within the EU.

- The EU is the most viable instrument for achieving a lasting economic balance in transatlantic security. As the United States's largest trading partner—accounting for more than $500 billion in two-way annual trade—the EU is a blockbuster is and likely to grow even more important through the acceptance in most of Europe of a common currency. The

United States and Europe have approximately $4.5 trillion invested in each other's economies, and leaders on both sides of the Atlantic will need to leverage that investment for security purposes that support interoperability.

Although the two-way investment of $4.5 trillion may seem singularly impressive, it may, as suggested here, present an altogether different picture of international defense spending and investment. As of early 2002, all NATO members were suffering from declining defense budgets and competition among suppliers, which would have kept prices low. The opportunity for international cooperation exists, yet the watchword these days would seem to be competition. The United States has been spending nearly six times more than its next ally on national defense, and the NATO allies have shown no concerted effort to close that gap. Instead, their investment in defense has stayed largely flat over several years (see **Figure 2-3**). In deciding on requirements, U.S. military leaders will need to temper an appetite for goldplating systems.

- The shrinking international defense trade has led to a souring of relations between the EU and United States. In a global environment of decreasing defense spending, a decreasing defense industrial base, and a commensurate rise in the costs of military operations and maintenance, interoperable systems will be difficult to achieve. The opportunity for cooperation exists, but the globe remains plagued by nationalism. Because each and all of the NATO allies has its own indigenous manufacturing, assembly, and research capabilities in the defense and high-technology industries, controversy over how best to reach consensus on international trade will undoubtedly continue.

Given that the type of military operation most probable in the future is coalition warfare, and given that interoperable systems aid coalition warfare, there is a need to state the requirements of global warfare. Should a shortfall in technology exist in the NATO alliance, military leaders will need to state these requirements objectively, unbiased by national economic objectives.

- Defense spending as a percentage of the GDP has slipped to its lowest point since the end of World War II, yet the need to modernize weapons systems appears paramount for information superiority. Recognizing that, military leaders will need to push for increased defense spending as a percentage of the GDP. With that push comes the need to be able to delineate clearly any shortfall in the equipment needed for warfare as well as concrete plans to achieve fiscal responsibility.

- Military leaders will need to be familiar with the DOD's Science and Technology Program and be able to apply it to enhance security both at home and abroad. By providing technologies that aid evolutionary change, such a program may prove a valuable instrument for furthering warfare in a network-centric environment. It may also prove important to the military leader, because, with the decrease in defense spending for R&D, the DOD's ability to influence high-technology advancement has been marginalized. Military leaders will need to leverage this program in order to fill niches in technology where the commercial sector either is not the champion or is wanting. The United States's reliance on information superiority to enable dominance in operations and

logistics itself relies on technological niches that will need to be filled through recourse to this program.

• In an outgrowth of globalization, several nations have reserved their right to promote the proliferation of technology and to encourage their own commercial industries to export liberally. As a result, U.S. defense and security stakeholders, both military and economic, will need to rely on dual-use technologies that may have originated in the commercial sector, although such dependence may be troubling to the U.S. military officer. It will, however, most likely prove necessary: in the 1950s the federal government provided nearly 45 percent of the R&D dollars, whereas now (2001–02) it provides only 2 percent. Military leaders will therefore need to apply dual-use technologies to achieve information superiority, to implement the Global Information Grid, and, ultimately, to conduct network-centric war.

• Diffusion of technology that could be used for military purposes against members of the NATO alliance remains an increasing threat. Now nearly ubiquitous, computers and the Internet have been used for attacks on computer networks and for terrorism. The military leader will need to regard the Internet as a model of the military potential of technology diffusion and become educated about the means of diffusion available to pirates and criminals.

• Military leaders will need to be less naïve than at present about the military implications of global technologies and will need to work to minimize NATO's vulnerability to attack. Globalization has rendered the Eurocentric mindset of the past less appropriate now that geographic boundaries have become almost irrelevant and English-speaking nations have become simply part of the global herd—certainly no longer solely dominant in technology transfer. Questions of sovereignty, right of defense, and the limits of cyberspace have ascended in importance, and rigid defense structures have become passé.

• Export control of military systems and dual-use technologies that may be used in military applications has become critical to maintaining international security, along with acceptance of the increasing obsolescence of current export practices and processes. As a recent in-depth study has suggested, current U.S. export control practices may even contribute to interoperability problems in the NATO alliance.[1] Such problems arise, for example, when export control practices squeeze legitimate business exports or make processing so difficult that locating alternate sources of technologies becomes expeditious, which lead to an environment with disparate systems. By being neither obstructionist nor mute on export control of technologies that might promote interoperability, military leaders will ultimately aid international stability.

Exports clearly can enhance U.S. security by ensuring that allies have the same or similar equipment, defraying costs of development, and maintaining a viable

[1]CSIS, *Technology and Security in the Twenty-First Century: U.S. Military Export Control Reform* (Washington, D.C.: CSIS Press, A Panel Report, May 2001), [On-line]. URL: http://www.csis.org/export/ (Accessed on 16 Jan. 2002.)

manufacturing capability for future sales. By articulating the need for control of sensitive or unique technologies and by helping to establish measured, disciplined, enforceable processes, based on security and stability and not simply economics, military leaders will have an impact on and will be able to assist in building unanimity concerning NATO's defense objectives and the associated export controls and will be able to assist in building unanimity concerning NATO's defense objectives and the associated export controls. They would be well advised to do so.

- For reasons of transatlantic security, continued participation by NATO members in the Wassenaar Arrangement would seem mandatory. So would continued encouragement of full participation in the WA by the Russian Federation, particularly in regard to exports with a high probability of reaching unintended third parties. Full disclosure of previously denied exports would strengthen transatlantic security, and, to date, although such denials have been few, any denial of material with military applications will enhance security. Full participation in Wassenaar would help to reduce the number of potential adversaries that would "shop around" in order to exploit technology for nefarious purposes.

A premise of this study is that globalization appears irreversible. To remain relevant on the stage of international security, military leaders in NATO and the United States, rather than having a solely military perspective, will need a broader perspective on international stability. In effect, they will need to be part diplomat and part economist while retaining a military outlook.

.

Acronyms

AOR	Area of Responsibility
C^4ISR	Command, Control, Communications, Computers, Intelligence Surveillance, Reconnaissance CCRP
COCOM	Coordinating Committee for Multilateral Export Controls
CCRP	Cooperative Research Program
CSIS	Center for Strategic and International Studies
DOC	U.S. Department of Commerce
DOD	U.S. Department of Defense
DOS	U.S. Department of State
EU	European Union
FY	fiscal year
GPS	Global Positioning System
INSS	Institute for National Strategic Studies
MTOPS	millions of theoretical operations per second
NATO	North Atlantic Treaty Organization
O&S	Operations and Support
OSD	Office of the Secretary of Defense
TOA	Total Obligation Authority
U.K.	United Kingdom
USAF	United States Air Force
USSR	Union of Soviet Socialist Republics
USTRANSCOM	U.S. Transportation Command
WA	Wassenaar Arrangement
WWW	World Wide Web

ISBN 1-879716-82-8

PPClemons