Fall 1989

Cooperation on Export Control between the United States and Europe: A Cradle of Conflict in Technology Transfer

Robert van den Hoveen van Genderen

Follow this and additional works at: http://scholarship.law.unc.edu/ncilj

Part of the Commercial Law Commons, and the International Law Commons

Recommended Citation
Available at: http://scholarship.law.unc.edu/ncilj/vol14/iss3/3

This Article is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Journal of International Law and Commercial Regulation by an authorized editor of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.
Cooperation on Export Control Between the United States and Europe: A Cradle of Conflict in Technology Transfer?

Robert van den Hoven van Genderen*

A state has [legislative] jurisdiction if its contact with a given set of facts is so close, so substantial, so direct, so weighty, that legislation in respect of them is in harmony with international law and its various aspects (including the practice of states, the principle of non-interference and reciprocity of the demand of interdependence). A mere political, economic, commercial or social interest does not in itself constitute a sufficient connection. . . . 1

I. Introduction

Information2 and information technology3 are vital parts of economic, strategic, and administrative functions of the modern nation. Consequently, nations strive to control and to protect this information. One way in which nations safeguard information is through import and export laws. Although these laws may serve other important national objectives such as protecting economic independence and the privacy of citizens, their main thrust is preservation of national security and sovereign independence. Many nations that lack information technology must rely on international law to ensure the free flow of information across national borders.4 Other technology-rich nations support a national and international policy of with-

---

* Mr. van den Hoven van Genderen received a degree in International Law from the University of Amsterdam. He then worked in the department of technology policy in the Netherlands State Department of Economic Affairs. He is currently a member of the law faculty at the University of Utrecht in the Netherlands. Mr. van den Hoven van Genderen lectures on international institutional law, computer law, and telecommunications law.


2 The term “information” as used in this Article means any data, either alone or combined with other data and either before or after processing activities, that results in an addition to intelligence.

3 The term “information technology” as used in this Article means technology that generates, transports, accumulates, or processes information electronically, electromagnetically, or optically.

4 These nations base their demand on a variety of legal principles such as the liberalization of services in the General Agreement on Tariffs and Trade, opened for signature, Oct. 30, 1947, 61 Stat. A-11, T.I.A.S. No. 1700, 55 U.N.T.S. 194 (GATT), or the New International Economic Order, United Nations, Declaration on the Establishment of a New International Economic Order, General Assembly Resolution 3201 (S-VI), May 1, 1974, and United Nations
holding information and information technology from other nations. Some nations emphasize trade policies while others emphasize national security goals.

These different approaches make it difficult for nations with similar security interests to harmonize their export policies. In particular, these conflicting approaches have created problems for the Consultative Group and Coordinating Committee for Multilateral Export Controls (CoCom or the Committee), a group of Western nations who joined together after World War II to create a unified policy for the export of sensitive technology and information to non-Western nations. Because CoCom depends solely on the voluntary compliance of the participating nations, it is effective only if each member believes that CoCom's policies are in its own best interest. Each CoCom nation implements policy in different ways. Substantial differences often exist between the multilateral export policy of CoCom and the unilateral legal actions of the various CoCom members. Specifically, the U.S. export laws, as set forth in the Export Administration Act, are security oriented and are often applied extraterritorially, while the European laws are more oriented to economic concerns. This Article analyzes the current effectiveness of CoCom in light of the differing approaches taken by the United States and Europe.

II. Historical Background of Technology Export Control

After World War II the euphoric state of cooperation in East-West relations quickly gave way to a more restrained pragmatism. Because of the increasing tension between East and West, NATO countries developed a policy to withhold strategic goods from communist countries. As the Cold War expanded, the fear of both intended and unintended transfer of strategically sensitive knowledge and products increased. As early as 1947, the United States implemented a strategic embargo on East-West trade through the Foreign

NATIONS, Programme of Action on the Establishment of a New International Economic Order, General Assembly Resolution 3202 (S-VI), May 1, 1974.

5 The transfer of control over information from citizens to their government is another very sensitive issue. It is also a sensitive matter for a government to delegate these powers through an international agreement.

6 See infra notes 11-12 and accompanying text.


Assistance Act. This Act required countries receiving economic and military aid from the United States to follow the U.S. embargo policy. These countries accepted the U.S. embargo conditions mainly because the future Alliance depended on U.S. economic and military aid. Officially, most commercial shipments to Europe after March 1, 1948 needed export licenses, although the controls were not strictly enforced in the early post-war period.

The political atmosphere between East and West further deteriorated with the first Berlin crisis, the first Soviet nuclear explosion, and the Soviet-backed triumph of Mao-Tse Tung in China. The perceived military threat from Eastern European communism led to greater military and economic countermeasures by the Alliance. On November 22, 1949, the United States secretly initiated the formation of CoCom as one such countermeasure. CoCom was primarily the result of the establishment of a bipolar international political system. Even in 1949, CoCom members understood the strategic importance to NATO security of technology and information. These initial efforts at export control strongly influenced modern day laws and regulations governing the export of strategic information.

10 Berman & Garson, supra, note 8, at 796.
11 CoCom was formed in the same year that NATO was established. CoCom began operation on Jan. 1, 1950, when representatives of the United States, the United Kingdom, France, Italy, and the Benelux countries convened for the first time. Later that same year, Norway, Denmark, Canada, and West Germany became members; Portugal and Japan followed in 1952; Greece and Turkey in 1953; and Spain joined in 1958 after long hesitation. In Sept. 1952 a special committee for China, named ChinCom, was created. The activities of this committee were directed towards maintaining an embargo against China because of the Korean War. The members of this committee were the same as CoCom. ChinCom was abandoned in 1958. See generally G. Hufbauer & J. Schott, Economic Sanctions Reconsidered: History and Current Policy (1985).

The use of economic warfare is one important aspect of a general strategy and power policy designed to reach certain goals or to satisfy certain interests. The aforementioned events demanded both military and economic countermeasures. CoCom probably would not have been established without the parallel establishment of NATO or a comparable alliance.

13 This idea has been reaffirmed in recent years by the Defence Planning Committee (DPC). On May 22, 1986, the DPC endorsed an expanded role for conventional military forces through the continued and cost-effective exploitation of emerging technologies. Defence Planning Committee Communiqué, NATO Review, June 1986, at 30.
III. The Coordinating Committee for Multilateral Export Controls

CoCom does not exist as a formal entity but is nevertheless very influential. Its legal basis is simply a gentleman’s agreement.\textsuperscript{14} The purpose of CoCom is to coordinate a policy to restrict the export of products and information of strategic importance to the Soviet Union, Hungary, Bulgaria, Czechoslovakia, Poland, East Germany, Romania, Albania, North Korea, Mongolia, Vietnam, and the People’s Republic of China.\textsuperscript{15} CoCom consists of representatives from Japan and all NATO members except for Iceland.

A. Institutional Structure

Although CoCom has no formal structure, it resembles the structure of international intergovernmental organizations in general. The organization, located in an annex of the U.S. Embassy in Paris,\textsuperscript{16} consists of a permanent secretariat of thirty people and three policy layers. The lowest administrative layer is the regulating committee which is an almost permanent session of lower to middle ranking diplomats from different member nations. These diplomats perform everyday work such as drafting technology lists and coordinating technical problems. The middle layer, the Executive Committee, consists of higher level government representatives who convene twice each year. These officials decide on content-related issues, review and adjust the dual-purpose technology control list,\textsuperscript{17} and harmonize export regulations. In addition, the Executive Committee acts as an intermediary between CoCom, national politics, and technical interest groups.\textsuperscript{18} These two layers form the basic working component of CoCom. The highest layer, the supreme policy body, consists of high level government officials such as the Directors General on external economic relations.\textsuperscript{19} They meet once each year to translate political decisions on licensing rules into directives for the lower levels.

B. Function

Because CoCom is neither an official body within NATO nor an independent international organization recognizable under interna-
tional law, its decisions are not formally binding on members. In practice, however, members generally follow the unanimous decisions of the Committee by adjusting their applicable national export laws.\(^{20}\) In this sense, Committee policy determines national law in a very direct way. The decisions are essentially dictated by this informal policy-making committee without even a two-way flow of information.

The Committee prohibits the export of strategic goods and technology to embargoed destinations which are mostly the Warsaw Pact nations and China.\(^{21}\) Goods and technology that are considered strategic are placed on one of three lists: (1) the International Atomic Energy List, (2) the International Munitions List, or (3) the International List.\(^{22}\) The International List (IL) is the most important because it includes dual-purpose technologies which are technologies that have a strategic value only when applied in certain ways.

The IL is further divided into three subcategories: (1) embargoed items (International List I), (2) quantitatively controlled items (International List II), and (3) exchange of information and surveillance items (International List III). Items on List I may not be exported to the East without a permit; items on List II may be exported but only in limited quantities; and items on List III may be exported but must be reported to CoCom and their end use specified.\(^{23}\) Most information technology items are on the International List I.

CoCom must rely on each member nation to adopt regulations enforcing these different lists. In addition to deciding which goods and technologies are placed on these lists, CoCom performs three other functions: (1) it monitors compliance with the lists by members; (2) it decides on exceptional requests for export of sensitive technologies;\(^{24}\) and (3) it tries to harmonize licenses and penalties among the members.\(^{25}\)


\(^{21}\) *Id.* at 1288. For a list of these countries, see *supra* note 15 and accompanying text.


\(^{23}\) Originally, the IL list consisted of three different subcategories: embargoed goods (International List I), export goods under quantitative restrictions (International List II), and supervised goods (International List III). These categories were abandoned in 1964 and replaced by the current categories. G. Bertsch, *East-West Strategic Trade, CoCom and the Atlantic Alliance* 33 (1983).

\(^{24}\) The Administrative Exception Notes (AEN) to the IL permit export to embargoed destinations in certain situations. Goods may be exported only when a member decides that the technical characteristics of the goods fall outside of the parameters of the AEN. The member must then notify CoCom; however, concurrence is not required. Hunt, *CoCom and Other International Cooperation in Export Control*, in *Coping with U.S. Export Controls*: 1989 67, 72 (1989).

CoCom members differ substantially in their views of CoCom regulations because of their different cultural, strategic, and economic backgrounds. Members have adhered to CoCom policy largely based on the conviction that it is in their own security interest to act in a unified manner. However, some members have used the security argument as an excuse to further certain national economic objectives. The conflict between economic and security interests is a significant and recurring problem for CoCom. In 1983, the European Community and Japan criticized the security emphasis within CoCom. Japan specifically objected to the expansion of the IL "beyond the scope of military materials." Japan argued that "if restrictions are expanded in order to prevent the Soviet Union's acquisition of foreign currencies, it may even lead to the denial of East-West trade as a whole in the end." Japan also argued that the development of East-West trade increased the Soviet economy's dependence on the West, thereby strengthening national security.

At a 1988 high level CoCom meeting, Japan and Europe again noted CoCom's restrictive policy on exports to the Warsaw Pact nations. They argued that the CoCom IL was outdated, too complicated, and certainly too long to be an effective control mechanism. They pointed to the INF Agreement and the increasingly liberal policies in the Soviet Union as evidence of a decreasing need for this kind of regulation. The United States, at least at the time of the meeting, was not convinced by these developments. During a visit to the Netherlands shortly after the 1988 Executive Committee meeting, Paul Freedenberg, the Undersecretary for Trade, declared that technological superiority in the Western military was necessary to counter the numerical supremacy of the East-Bloc military. Freedenberg's argument has been weakened somewhat by Mikhail Gorbachev's recent proposals to cut troops and armor and by the changes taking place in Eastern Europe.

Currently, a contradiction exists between the European/Japanese position and the U.S. position. The United States wants more severe regulations on the export of strategic goods instead of a shorter CoCom IL. Europe and Japan believe a shorter, more realistic list will strengthen intra-CoCom relations and will also prevent non-CoCom countries from taking over the trade market in the controlled goods. At the 1988 high level CoCom meeting, members

---

27 Id. (citing Nihon Keizai, Mar. 16, 1983, at 1).
28 Id.
30 Id.
31 As a result of U.S. industry complaints over the regulation of "simple" information
reached a tentative consensus on a shortening of the list with a concomitant strengthening of control. However, to achieve a lasting consensus, members must resolve the larger internal conflicts within CoCom that result from differing opinions over how much control should be exercised and when export licenses should be granted. These questions, in turn, are a function of both security interests and foreign policy interests. To better understand these conflicts, it is necessary first to examine the application of CoCom laws in the European Community and the United States.

A. European Viewpoint: Harmonization within the European Community?

The European Community is currently discussing the possibility of becoming a member of CoCom to force a harmonization of CoCom regulations within the Community. This move could lead to an unfortunate and dangerous mixing of European security and socioeconomic interests. Moreover, it is unclear whether CoCom-type regulations would be enforceable under the EEC Treaty. Although the general scope of the EEC Treaty does not extend to security issues, two Articles have formed the basis for a Community Council decision on a security issue and thus possibly could form a legal basis for the implementation of the CoCom IL to the European Community. Articles 223 and 224 of the Treaty give member states full sovereignty over regulations and other laws concerning military and semimilitary products. Anticompetitive economic activities within the Community may not be shielded, however.

On April 15, 1959, the EC Council established a list of products
over which member states retain sovereignty. This list differs from the CoCom IL in several ways. First, because the Council’s list has not been amended since it was first set out in 1959, it is technologically less up-to-date than the CoCom IL. Second, and more importantly, the contents of the Council’s list concern only products with specific military purposes. Third, the Council’s list is under the sovereignty of the individual member states and not a part of Community policy. This approach guarantees that member states will be free to fulfill obligations designed to maintain peace and international security. Consultation on these measures between member states is necessary only to ensure that the Common Market is not disturbed.

A recent EC Court of Justice ruling held that Article 224 was primarily a safeguard clause rather than a specific reservation of sovereignty. Thus it probably could not provide a legal basis for the individual policies of member states on this subject. The EEC Treaty is unclear on the extent to which member states have sovereignty over the CoCom IL, especially when it controls many nonmilitary technological products and information. It has been suggested that the Council should either update its list to comply with the CoCom IL, thereby giving the CoCom IL international legality, or it should issue a regulation, based on Article 113, concerning common commercial policy. Although the latter option is more realistic, the fact that Ireland would also be subject to the regulation makes this approach inappropriate. Therefore, updating the list with a Directive

---

35 This list was not published.
37 EEC Treaty, supra note 33, art. 223(1)(b).
38 See id., art. 224.
40 Kuyper, supra note 36, at 21. A similar approach was used in the early phases of the pipeline incidents. See infra text accompanying notes 86-88.
41 Ireland is the only EEC member who is not a member of NATO.
would be more appropriate. A Directive would also give individual member states the option of using legal instruments that are currently used for CoCom IL consensus. If these legal options were unavailable, member states would likely consider any restrictions on the transfer of CoCom-listed products among member states as detrimental to the Common Market. New and different export licenses would frustrate the guaranteed free flow of goods, services, capital, and persons in the Common Market.42

B. U.S. Viewpoint: The Export Administration Act

The Export Administration Act (EAA)43 is the legal instrument which protects U.S. security and foreign policy interests, and it is also the main source of conflict within CoCom. The EAA authorizes the President of the United States to “prohibit or curtail the exportation of any goods, technology, or other information subject to the jurisdiction of the United States or exported by any person subject to the jurisdiction of the United States.”44 Pursuant to Executive Order No. 12,525,45 the President delegated this authority to the Commerce Department which administers the Act through its Bureau of Export Administration (BXA).

The EAA is essentially a relic of World War II. Its original purpose was to prevent shortages of basic commodities necessary to support the war effort.46 Only after the war were export controls used for foreign policy and national security purposes and then mainly against the Soviet Union.47 The Export Control Act of 194948 became one of the primary instruments for controlling exports to Eastern Europe. Under the Export Control Act of 1949, the Department of Commerce reviewed prospective exports for their possible military significance.49 Congress has adhered to this same approach in the revised act, the Export Administration Act of

---

42 Article 3 provides:

For the purposes set out in the preceding Article, the activities of the Community shall include, under the conditions and with the timing provided for in this Treaty:

(a) the elimination, as between Member States, of customs duties and of quantitative restrictions in regard to the importation and exportation of goods, as well as of all other measures with equivalent effect;

(c) the abolition, as between Member States, of the obstacles to the free movement of persons, services, and capital;

EEC Treaty, supra note 33, art. 3(a),(c).


47 See Berman & Garson, supra note 8, at 795.


49 Leibman, supra note 46, at 367.
1969, its amended versions of 1979 and 1985, the recent amendments in the 1988 Omnibus Trade and Competitiveness Act (OTCA), and the Export Administration Regulations (EAR) promulgated under the EAA.

The stated policy behind the EAA is clear:

It is the policy of the United States to use export controls . . . (A) to restrict the export of goods and technology which would make a significant contribution to the military potential of any other country or combination of countries which would prove detrimental to the national security of the United States; (B) to restrict the export of goods and technology where necessary to further significantly the foreign policy of the United States or to fulfill its declared international obligations; and (C) to restrict the export of goods where necessary to protect the domestic economy from the excessive drain of scarce materials and to reduce the serious inflationary impact of foreign demand.

Parts (B) and (C) integrate both security and economic interests of the United States. The EAA has created problems because it does not clearly distinguish between national security controls and foreign policy controls.

The EAR generally prohibits the export of all commodities and technical data unless a license is obtained. The particular license needed for a given export depends on the type of commodity or technology being exported, the country where the shipment is destined, and the end use of the commodity. The EAR classifies countries into seven control groups depending on the strategic importance of each country. Countries that pose significant security risks are labelled controlled countries and further restricted. The EAR classifies commodities through the Commodity Control List (CCL) which divides commodities into ten general groups ac-

56 The EAR states: [T]he export from the United States of all commodities, and all technical data as defined in [§ 779.1], is hereby prohibited unless and until a general license authorizing such export shall have been established or a validated license or other authorization for such export shall have been granted by the Office of Export Licensing. . . .
15 C.F.R. § 770.3(a) (1989).
57 The technical requirements of obtaining a license are beyond the scope of this article. The EAR, which is over 500 pages long, provide detailed guidance on the licensing procedures. For a discussion see Hunt, The Export Licensing System, in COPING WITH U.S. EXPORT CONTROLS: 1989 11 (1989).
59 Controlled countries are defined as any countries described in the Foreign Assistance Act of 1961. 15 C.F.R. § 770.2 (1989).
cording to the type of good. The Defense Department, the Commerce Department, the State Department, and the Energy Department all participate in deciding which items are placed on the CCL. An exporter must consult the CCL to determine which license is needed.

The Commerce Department investigates and reviews not only license applicants but also their foreign subsidiaries, affiliates, joint venturers, and licensees. Foreign contract parties must submit documentation to the BXA stating the disposition abroad of the goods intended for export or re-export. In addition to regulating exports from the United States to certain foreign destinations, the EAA also regulates the re-export of U.S. goods from one foreign country to another. The re-export provisions have been extremely controversial because of their extraterritorial reach and because of the pipeline crisis. The EAA justifies the regulation of foreign companies based on its broad jurisdictional mandate over U.S. goods.

The extraterritorial application of the EAA has upset many European countries and companies. According to sources within the Dutch Government, U.S. officials informally agreed that there would be no such investigations of affiliates in the Netherlands. It is unclear

---

62 The BXA administers foreign policy related controls in consultation with the State Department, which acts principally through its Office of East-West Trade. The Customs Service and the Department of Commerce enforce the regulations.
63 The EAA authorizes a general license and a validated license. If an exporter qualifies for a general license, the exporter may ship the goods without submitting a license application which is required for validated licenses. Validated licenses are divided into four subcategories: a distribution license, a comprehensive operations license, a project license, and a service supply license. 50 U.S.C. app. § 2403(a)(2) (Supp. V 1987). The distribution license authorizes export of goods to approved distributors or users of the goods in countries other than controlled countries. Id. at § 2403(a)(2)(A). The Secretary of Commerce grants distribution licenses primarily on the basis of the reliability of the applicant and its foreign consignees not to divert goods to controlled countries. Id. See also Albenese, The Distribution License Program, in Coping With U.S. Export Controls: 1989 243 (1989).
64 "The applicant must disclose fully on the license application the names of all the parties who are concerned with or interested in the proposed export." 15 C.F.R. § 772.3(a)(2) (1989).
67 See supra notes 86-88 and accompanying text.
68 See supra note 55.
69 The author states that the source of the statement is confidential. —ED.
whether U.S. affiliates of Dutch companies are also immune.

In what appears to be a move towards liberalization, the United States has agreed to review the status of controlled countries each year rather than every third year. The criteria used for determining the status of a controlled country include:

(A) the extent to which the country's policies are adverse to the national security interests of the United States; (B) the country's Communist or non-Communist status; (C) the present and potential relationship of the country with the United States [and] with other countries friendly or hostile to the United States; ... and (F) other such factors as the President considers appropriate.

These guidelines permit a wide range of interpretation. In addition, a country not on the CCL is not necessarily free from restrictions because the United States may submit any country, including CoCom countries, to export controls if there is a question of U.S. security.

The EAA defines technology as:
the information and know-how (whether in tangible form, such as models, prototypes, drawings, sketches, diagrams, blueprints, or manuals, or in intangible form, such as training or technical services) that can be used to design, produce, manufacture, utilize, or reconstruct goods, including computer software, and technical data, but not the goods themselves.

Technology may be regulated under either security controls or foreign policy controls. The EAR generally states that when executing these regulations it is unimportant on which ground the regulation is based. European countries are unclear over how the security policy and foreign policy are applied to information technology.

V. The Effect of Economic Interests on CoCom

One key element to a mutually acceptable security-export policy is consensus among members over which technological products pose security risks. One problem in reaching such a consensus is the issue of economic interests in the different technological products. As previously mentioned, the clash between economic and security interests poses the greatest difficulty to the effectiveness of CoCom. This problem has been particularly troublesome for CoCom

---

71 Id.
72 Id. at § 2404(b)(1)(F).
73 Id. at § 2415(4).
74 The EAR provides:
No person may possess any commodities or technical data, controlled for national security or foreign policy reasons under section 5 or 6 of the Act: (1) With the intent to export such commodities or technical data in violation of the Export Administration Act or any regulation, order, license or other authorization under the Act, or (2) Knowing or having reason to believe that the commodities or technical data would be so exported.

throughout the 1980s, most notably in the pipeline crisis. The current state of disagreement between the United States and Europe over the role of CoCom may be understood only in light of the various failed attempts at resolving the tension between security and trade.

At the Ottawa Summit in July 1981, the NATO Alliance agreed to review export controls. The United States tried to convince its European allies to tighten their export controls to create a uniform Western policy. Because of a greater interest in trade than security, the West European partners refused to participate. They criticized the United States for exercising too much control. The United States classified some technologies as critical to national security while the Europeans thought these same technologies were not critical. In general, Western Europe considered the U.S. initiative an unnecessary intervention into European internal affairs and particularly unwise during a time of tension between Europe and the United States.

In several reports issued at this time, the U.S. Office of Technology Assessment (OTA) recognized this divergence of views. The OTA concluded:

1. Trade with the Soviet Union has been far more important for the economies of most of the United States' CoCom allies than for the United States itself.

2. There is a widespread skepticism in Europe and Japan over the utility of trade sanctions for achieving Western political objectives in the Soviet Union.

3. These nations, unlike the United States, consider trade with the Soviet Union a desirable part of their foreign and domestic economic policies, and they largely eschew the use of foreign policy for political purposes. These countries do not have national legislation comparable to EAA to provide a legal mechanism for such controls.

4. The United States and its allies had different expectations for detente and therefore saw the result differently. In general, Europeans have emphasized the gains in trading relations and the continuing dialogue with Moscow, both of which contribute to the maintenance of the European status quo. In the case of West Germany, detente has significantly improved relations with East Germany. Soviet activities in the Third World are seen by the Europeans as violations of a U.S.-defined code of conduct, but not necessarily a breach of the Soviet Union’s detente commitments in Europe.

---


76 Id. at 10, col. 3.

Given the constraints under which it operates, CoCom works well. It is an effective mechanism for implementing national security controls in areas where the members agree that such controls are necessary. CoCom does not function well where this consensus is lacking.

All CoCom partners agree that exports to the Soviet Union and technology with direct military relevance should be controlled for national security, but the United States tends to favor a much broader interpretation of "military relevance" than its allies use. Similarly, the European and Japanese definitions of "security" include an economic dimension which causes them to view trade with the Soviet Union as a positive factor in East-West relations.

Western Europe and Japan view with apparent equanimity the quantum rise in the level of East-West energy interdependence which will result from the West Siberian gas pipeline project.

West Germany, France, and Italy all consider importing Siberian gas as a desirable way to increase and diversify energy supplies while simultaneously stimulating equipment and technology exports. The latter consideration is also important to Japan.

Western importers of Soviet energy, particularly gas, are all mindful of the risks of energy dependence on the Soviet Union. These countries have developed contingency plans in case of a cutoff of Soviet gas. The plans may appear inadequate to U.S. observers; nevertheless, the nations involved believe that the potential benefits of importing Soviet gas outweigh the risks.

The OTA concluded that these developments could endanger the security of the Alliance. At the Ottawa Summit the European countries felt that the United States did not understand the extent to which history and geography influence European conceptions of national security. In particular, the European economies are export-dependent and in proximity to the Soviet Union. Most importantly, the European allies disliked the attempt by the United States to dictate what the Europeans view as matters of internal economic policy. The European countries also rejected the premise that the U.S. security policy is solely a foreign policy not affecting the domestic policies of the European allies.

Despite these differences, the foreign ministers of NATO seemed to reach a much needed consensus a year later in the Versailles Summit of June 1982. They signed the Versailles Declaration in which they agreed to approach East-West economic relations "in a prudent and diversified manner consistent with our political and security interests." They further agreed to observe "commercial prudence" in granting export credits to the Communist world and to exchange information on "all aspects of our economic, commercial,

---

79 See Smith, supra note 75.
and financial relations with Warsaw Pact countries."

However, a week later French President Francois Mitterand declared that the Versailles Declaration would not affect France's credit policy with the Soviet Union. The United States believed this action destroyed the impression of a unified commercial policy. An OTA report concluded that the Versailles Declaration failed either because European nations only nominally agreed to the policies when they had no intention of carrying them out or because the United States failed to accept Europe's view of its own political and security interests. The latter interpretation is probably correct. The French declaration was likely only a public assertion of French sovereignty. Nonetheless, the United States reacted predictably, stating that it could not accept a European limitation on U.S. foreign policy interests even if the Europeans were acting only to protect their sovereignty. What should have been a showcase of Western unity proved to be the seed of disruption.

In response to the European refusal to adhere to the U.S. interpretation of the Versailles Declaration, President Reagan announced on June 18, 1982, that the United States would extend its foreign policy controls retroactively and extraterritorially to exports of oil and gas equipment to the Soviet Union. Previously, on December 30, 1981, the U.S. Department of Commerce issued EAR amendments designed to block the Soviet's building of the trans-Siberian pipeline. President Reagan wanted to apply political pressure on the Soviet Union after martial law was declared in Poland. The controversy became known as the "pipeline crisis." The purpose of the June 1982 EAR amendments was to cover completed contracts for equipment produced by subsidiaries and licensees of U.S.-based firms.

The European Community strongly objected to the June 1982 EAR amendments. Following its initial protest on the day the U.S. measures were made public, the EC Council of Ministers sent a de-

---


83 Id.

84 The historical sensitivity of the Germans to this kind of versailler diktat may also explain the failure of the Versailles Declaration.


tailed report (1982 EC Report) to the U.S. Department of State. The 1982 EC Report was followed by an "aide-memoire" on March 14, 1983. The affected individual EC member states also released ministerial declarations in which they condemned the U.S. action. The United Kingdom, France, Italy, West Germany, and, indirectly, the Netherlands ordered companies on their territory to disregard the U.S. order and to fulfill their contractual obligations in compliance with national laws. Notwithstanding the European reaction, the United States prohibited British, French, German, and Italian companies from importing any U.S.-origin goods or technical data relating to oil and gas exploration or to production, transmission, or refinement of the Soviet project.

In the 1982 EC Report, the European Community criticized the U.S. regulations:

The European Community believes that the U.S. regulations as amended contain sweeping extensions of U.S. jurisdiction which are unlawful under international law. Moreover, the new Regulations and the way which they affect contracts in course of performance seem to run counter to criteria of the Export Administration Act and also to certain principles of U.S. public law.

The report elaborated on these violations of international and U.S. law. First, it discussed the extension of U.S. jurisdiction to non-U.S. companies under international principles of territoriality and nationality. Second, it analyzed the new regulations under U.S. law and the existing framework of the EAA.

The European Community felt that neither the nationality principle nor the territoriality principle as applied under international

---

89 European Communities: Comments on the U.S. Regulations Concerning Trade with the U.S.S.R. (reprinted in 21 Int’l Legal Materials 891 (1982)).
90 EC Bulletin, March 1983 (reprinted in Lowe, Extraterritorial Jurisdiction 183-87 (1983)).
91 France, Italy, and the United Kingdom experienced the greatest effect from the regulations.
92 See Allies Justified in Attacks on Pipeline Policy, N.Y. Times, July 4, 1982, at F1, col. 5.
93 See e.g. United Kingdom: Statement and Order Concerning the American Export Embargo with Regard to the Soviet Gas Pipeline, (reprinted in 21 Int’l Legal Materials 851 (1982)). See also infra notes 176-81 and accompanying text.
94 These companies included AEG-Kanis and Mannesmann in West Germany; Creusot-Loire and Dresser France in France; John Browne Engineering in the United Kingdom; and Nuovo Pignone in Italy. Office of Technology Assessment, Technology and East-West Trade: An Update 66 (1979).
96 21 Int’l Legal Materials at 891.
97 The report noted: The principle that each state—and mutatis mutandis the Community insofar as powers have been transferred to it—has the right freely to organize and develop its social and economic system has been confirmed many times in international fora. The American measures clearly infringe the principle of territoriality, since they purport to regulate the activities of companies in the E.C., not under the territorial competence of the U.S.

Id. at 893.
law could justify the 1982 amendments. The territoriality principle could not justify regulating companies “not under the territorial competence of the U.S.” The nationality principle could not justify regulating companies not incorporated in the United States. In Barcelona Traction, the International Court of Justice reaffirmed that the nationality of a company should be determined by the place of incorporation and the place of registration of the office of the company. Although this case actually decided an issue relating to the doctrine of diplomatic protection, it illustrates the EC’s interpretation of the nationality principle.

The 1982 EC Report also rejected the U.S. idea that nationality could be extended to goods or technology. The EAA asserted jurisdiction over persons owning or even handling those goods or technology. Furthermore, the 1982 EAR amendments would, in some instances, require non-U.S. corporations to obtain special permission from U.S. authorities to export goods that were based on EC technology and were produced in the European Community. The European Community strongly condemned the statutory encouragement of voluntary submission to U.S. public policy in trade matters. The European Community considered the use of these “submission clauses” an abuse of the freedom to contract because they circumvent the limits imposed on national jurisdiction by international law. As one commentator stated: “The fact that submission clauses are

98 Id. The territoriality principle limits a state’s jurisdiction to persons and goods within its territory. See RESTATEMENT (SECOND) OF THE FOREIGN RELATIONS LAWS OF THE UNITED STATES § 17 (1965).
99 The nationality principle allows each state to regulate its nationals wherever they are located. Id. at § 30.
100 1970 I.C.J. 5, 43.
101 See 21 INT’L LEGAL MATERIALS at 894.
102 The report noted:
Goods and technology do not have any nationality and there are no known rules under international law for using goods or technology situated abroad as a basis of establishing jurisdiction over the persons controlling them. Several Court cases confirm that U.S. jurisdiction does not follow U.S. origin goods once they have been discharged in the territory of another country.
21 INT’L LEGAL MATERIALS at 894 n.2 (citing American President Lines v. China Mutual Trading Co., 1953 A.M.C. 1510, 1526 (Hong Kong Sup. Ct.); Moens v. Ahlers North German Lloyd, 30 R.W. 360 (Antwerp Tribunal of Commerce 1966)).
103 The report noted:
The public policy (‘ordre public’) of the European Community and of its Member States is thus purportedly replaced by U.S. public policy which European companies are forced to carry out within the E.C., if they are not to lose export privileges in the U.S. or to face other sanctions. This is an unacceptable interference in the affairs of the community.
21 INT’L LEGAL MATERIALS at 896.

This effect is similar to that of the Semiconductor Chip Protection Act of 1984, 17 U.S.C. §§ 901-914 (Supp V 1987). Under the Act, the European Community was required to follow U.S. controls because of the possibility of being excluded from the U.S. semiconductor market. The European Community followed the U.S. Act but also issued a Directive that resulted in a number of European versions of the U.S. Act.
couched in the language of contract cannot disguise the fact that they deal with matters of public and not private law, and are to be judged according to the standards of public international law."

The European Community also rejected two other U.S. bases for jurisdiction: the protective principle and the effects doctrine. The protective principle allows a nation jurisdiction to proscribe acts done outside its territory when they threaten its security. The protective principle could not justify the EAR amendments because they were passed pursuant to foreign policy controls rather than national security controls. The effects doctrine was inapplicable because there were no direct, foreseeable, or substantial effects within the United States. In addition, the retroactive application of the EAR to existing contractual obligations was a significant point of contention. Even members of Congress and industry considered this retroactive effect contrary to U.S. public policy.

Finally, the report criticized the failure of the United States to apply the "balancing of interests" approach which had been applied by several U.S. courts. This test, which is used in the Restatement (Second) of Foreign Relations Law, requires that a country exercise its enforcement jurisdiction so as to minimize potential conflicts. The report cited several of the Restatement (Second) factors used to balance the interests of conflicting jurisdictions:

a) vital national interests of each of the states;

b) the extent and the nature of the hardship that inconsistent enforcement actions would impose upon the person;

c) the extent to which the required conduct is to take place in the territory of the other state; and

d) the nationality of the person on whom the law is to be enforced.

The European Community expected that the balancing test would be applied in the rule making stage as well as the enforcement

---

104 Lowe, supra note 90, at 525.
106 21 Int'l Legal Materials at 897.
107 Under the effects doctrine, a state may also proscribe conduct occurring outside its territory that causes direct, foreseeable, and substantial effects which constitute elements of a crime or tort within the territory. Restatement (Second) of the Foreign Relations Laws of the United States § 18 (1965). See 21 Int'l Legal Materials at 897.
111 21 Int'l Legal Materials at 899 (citing Restatement (Second) of the Foreign Relations Laws of the United States § 40 (1965)).
stage. Because EAR amendments do not receive substantive judicial review, a clash of enforcement jurisdictions could occur before U.S. courts would have an opportunity to apply the balancing test. The EAA authorizes the use of a balancing test. The European Community complained that President Reagan did not follow these provisions, and thus failed to take into account several important factors:

(1) the supra-national status of the European Community on trade issues;
(2) the fact that the conduct solely affected E.C.- territories;
(3) the nationality ties and other links subject to the June 22, 1982 amendments primarily affected E.C. companies, not U.S. companies;
(4) there were justified expectations by E.C. companies, which were hurt by the U.S. measures.

The problems created by the 1982 EAR amendments were evident in *Dresser Indus. Inc. v. Baldridge.* The 1982 EAR amendments prohibited both the export of strategic technology to the Soviet Union from the United States and the re-export from any other nation. The new regulations applied to foreign firms controlled by U.S. companies, foreign companies using U.S. technology under a licensing agreement with a U.S. company, and foreign companies using U.S.-originated technology as a part of its product. Prior to the promulgation of these regulations Dresser-France, a wholly-owned subsidiary of Dresser Industries, Inc. (Dresser-USA), entered into contracts to deliver gas pipeline compressors to the Soviet Union. These compressors were manufactured by Dresser-France under a license granted by Dresser-USA. Before the 1982 EAR amendments, the EAR did not cover products manufactured by foreign subsidiaries of U.S. companies or by companies using U.S. tech-

---

113 "[T]he President shall consider: (c) the reaction of other countries to the imposition . . . or expansion of . . . export controls by the United States . . . ." 50 U.S.C. § 2405(b)(1)(C) (Supp. V 1987). "[T]he President shall determine that reasonable efforts have been made to achieve the purposes of the controls through negotiations or other alternative means." ld. at § 2405(e). "[T]he President shall take all feasible steps to initiate and conclude negotiations with appropriate foreign governments for the purpose of securing the cooperation of such foreign governments in controlling the export to countries and consignees to which the United States export controls apply of any goods or technology comparable to goods or technology controlled under this section." ld. at § 2405(b)(1).
114 21 INT'L LEGAL MATERIALS at 901.
116 15 C.F.R. § 785.2 (1989). Re-export is defined as the “re-export, transshipment, or diversion of commodities or technical data from one foreign destination to another.” 15 C.F.R. § 770.2 (1989).
The new regulations applied regardless of when the information was exported to the subsidiaries or licensees, and also provided for civil, administrative, and criminal sanctions.\textsuperscript{119}

Attempting to comply with the regulations, Dresser-USA ordered Dresser-France to cease manufacture of the compressors and suspend shipments to the Soviet Union. The French Government then ordered Dresser-France to fulfill its contractual obligations or face sanctions under French law. Dresser-USA and Dresser-France were thus subject to conflicting regulations of U.S. and French law. Dresser-USA and Dresser-France brought suit in federal court seeking a declaratory judgment and injunctive relief from the U.S. regulations.\textsuperscript{120} They argued that the EAA did not authorize jurisdiction over Dresser-France, that enforcement would violate international law, and that they were denied due process of law because they were unable to seek judicial review of the regulations.\textsuperscript{121} The court held that injunctive relief was inappropriate in light of the public interest in the enforcement of the regulations at issue and in the essential purpose of the regulations to aid U.S. foreign policy.\textsuperscript{122} However, strong protests from the French Government and the European Community eventually forced the U.S. Government to withdraw the regulations in October of 1982.\textsuperscript{123}

As one commentator observed, neither of the traditional principles of jurisdiction—territoriality and nationality—justified the extension of U.S. export regulations to a company that fell completely within French jurisdiction.\textsuperscript{124} Although it was owned by a U.S.-based parent company, Dresser-France had no operations in the United States nor was it a U.S. national. Under recognized legal principles, Dresser-France was a French national because it was incorporated in France.\textsuperscript{125} The U.S. Government asserted that shipments to the Soviet Union by Dresser-France would have a "direct and substantial" effect on U.S. foreign policy.\textsuperscript{126} The United States runs the risk of

\begin{flushleft}
\textsuperscript{118} 15 C.F.R. § 779.8(a)(1)-(3) (1989) (as amended by 47 Fed. Reg. 27,250 (1982)).
\textsuperscript{119} 15 C.F.R. §§ 768.4(b), 787.1, 788.1, 790.2(a) (1989).
\textsuperscript{120} \textit{Dresser}, 549 F. Supp. at 108.
\textsuperscript{121} See Leigh, \textit{ supra} note 87 at 627.
\textsuperscript{122} \textit{Dresser}, 549 F. Supp. at 110.
\textsuperscript{123} The Department of Commerce suspended the regulations in Oct. 1982. 15 C.F.R. §§ 779.4(f)(1)(i)(P), 785.2(a)(5), 785.2(c), 790.8, 799.1 Supp. 1 and 799.2 Supp. 1 (1989) (removed, revised, or amended by 47 Fed. Reg. 51,850 (1982)). In March 1983, the French Government nonetheless sent an aide-memoire in protest even though the EAA was due to expire on Oct. 1, 1983. France wanted to influence the new revisions to the EAA that would be enacted.
\textsuperscript{124} Leigh, \textit{ supra} note 87 at 627.
\textsuperscript{125} \textit{Id.} (citing The Convention of Establishment Between the United States of America and France, Dec. 21, 1960, art. XIV, para. 5, 11 U.S.T. 2398, T.I.A.S. No. 4625, which states that "companies constituted under the applicable laws and regulations of either High Contracting Party shall be deemed companies thereof.").
\textsuperscript{126} \textit{Dresser}, 549 F. Supp. at 110. The "direct and substantial" effect test is required by
\end{flushleft}
severely damaging relations with other nations by such excessive assertions of foreign policy and security interests.

Strangely enough, the U.S. Supreme Court has held that in the opposite situation, where the situs of a foreign subsidiary is the United States, the U.S. Government has exclusive jurisdiction. In *Sumitomo Shoji America, Inc. v. Avogliano*, \(^{127}\) a New York subsidiary of a Japanese trading company argued that it did not have to comply with U.S. employment and civil rights laws because of a bilateral treaty between the United States and Japan. The Court denied the protection of the treaty observing that “Sumitomo is a company of the United States, not a company of Japan.” \(^{128}\) Although limited to the interpretation of the treaty, the ruling may have broader implications. The Court stated:

> Determining the nationality of a company by its place of incorporation is consistent with prior U.S. treaty practice. The place-of-incorporation rule also has the advantage of making determination of nationality a simple matter. On the other hand, application of a control test could certainly make nationality a subject of dispute. \(^{129}\)

Also, in *Wisconsin v. Pelican Insurance Co.*, \(^{130}\) as noted in the 1982 E.C. report, a U.S. federal court held that it did not have jurisdiction to enforce foreign penal statutes. \(^{131}\) If a foreign government asserted that a U.S. licensee of a foreign company violated that foreign government’s export restrictions, a U.S. federal court would decline jurisdiction because U.S. courts will not enforce foreign penal statutes. \(^{132}\)

The extraterritorial effect of U.S. laws has increasingly annoyed several nations. These nations consider the application of U.S. law in a foreign jurisdiction an infringement of sovereignty. The United States justifies this policy under the “effects doctrine.” According to the argument, the internal security effects within the United States of some activities abroad justify U.S. enforcement of its laws in other jurisdictions. Two commentators noted the problem with the U.S. view:

> If foreign subsidiaries, chartered under the laws of a foreign sovereign, are nationals of the nation of a parent enterprise, from the fact of being controlled by that parent, the opportunities for sovereign conflict are substantially increased. While in part a problem of international complexity, two states seeking to regulate conduct partially within and partially without their territories, it should also be viewed

---

\(^{127}\) 457 U.S. 176 (1982).

\(^{128}\) *Id.* at 182.

\(^{129}\) *Id.* at 185 n.11 (citation omitted).

\(^{130}\) 127 U.S. 265 (1888).

\(^{131}\) *Id.* at 290.

as a direct challenge to the sovereignty of the nation which charters the subsidiary.\textsuperscript{133}

The pipeline crisis and the 1982 EAR amendments point out the problems that arise when the United States and Europe do not agree on common objectives.

VI. Other Conflicts Created By the Extraterritorial Application of U.S. Export Policy

The extraterritorial application of the EAA has created several other problems in addition to those associated with the pipeline crisis and the 1982 EAR amendments. In 1981, the U.S. Government attempted to strengthen its control over technology exports through "Operation Exodus," which was an enforcement program by the U.S. Customs Service designed to discover and interdict illegal technology exports.\textsuperscript{134} By 1983 this program led to the arrest of 276 persons in the United States for illegal export of strategic goods and weaponry to the East Bloc.\textsuperscript{135} Under "Operation Exodus" technology transfers were investigated more closely, and posters in the tradition of "Loose Lips Sink Ships" requested U.S. companies to inform the U.S. Customs Service of any suspicious activity.\textsuperscript{136} U.S. industry eventually resisted the operation because of the considerable loss of trade profits and the resulting trade imbalance.\textsuperscript{137} As a result, since 1985, national export restrictions have been relaxed somewhat.

\textsuperscript{134} Operation Exodus was begun in 1981. See generally Weyhrauch, Operation Exodus: The United States Government's Program To Intercept Illegal Exports Of High Technology, 7 Computer L.J. 203 (1986).
\textsuperscript{135} Netherlands Department of Economic Affairs.
\textsuperscript{136} One poster read:

\begin{quote}
Special Agents of the U.S. Customs Office are responsible for investigating criminal violations regarding illegal high technology and munitions transfers.

If you or your company has been the recipient of any suspicious inquiries regarding your high technology or munitions products or if you have any information or suspicions regarding high technology or munitions transfers, please call exodus coordinator.
\end{quote}

\textsuperscript{137} A DOC spokesman estimated that the United States lost $300 to $600 million in exports to the Soviet Union as a result of the Dec. 1981 export controls on oil and gas equipment and technology. Economic Relations with the Soviet Union: Hearings Before the Senate Subcomm. on International Economic Policy and the Senate Comm. on Foreign Relations, 97th Cong., 2d Sess. 11 (1982) (statement of Lionel H. Olmer, Undersec'y for Int'l Trade, Dep't Of Commerce).

There has been discussion in the United States over the cost to U.S. industry from the stringent requirements of the EAA. One area that was criticized was the failure of the EAA to focus on whether similar products are available from sources outside the United States (sometimes referred to as the foreign availability problem) instead of on the potential military usefulness of the technology. As one commentator observed: "[T]here is no sense in penalizing United States companies with a substantial loss of sales, . . . if the purpose of the controls is not accomplished and the results are merely symbolic." 138

The U.S. Congress incorporated this foreign availability provision into the 1979 and 1985 revisions to the EAA:

[T]he President shall not impose export controls for foreign policy or national security purposes on the export from the United States of goods or technology which he determines are available without restriction from sources outside the United States in sufficient quantities and comparable in quality to those produced in the United States so as to render the controls ineffective in achieving their purposes, unless the President determines that adequate evidence has been presented to him demonstrating that the absence of such controls would prove detrimental to the foreign policy or national security of the United States. 139

In 1975, Control Data Corporation contracted to sell an "old" Cyber-76 computer to the Soviet Union for research and weather forecasting. 140 After two years of research on the question, the Commerce Department denied permission to export the computer. 141 Stanley J. Marcuss, Deputy Assistant Secretary for Domestic Commerce, explained the decision: "as is the case with almost any advanced computer, the Cyber-76 has potentially military as well as peaceful uses." 142

As the Control Data situation illustrates, the U.S. Government is often slow in making determinations on the foreign availability of comparable goods and technology. Two commentators have proposed solutions to solve this problem. Professor Homer Blair suggests the United States could better protect its security interests by a self-policing export control system under which the exporting company submitted an affidavit describing in detail where the goods are available. 143 He proposes that the affidavit would accompany the export license application and would be signed by three people in the

140 Computer Exports To The Soviet Union: Hearing Before the Subcomm. on International Economic Policy and Trade of the House Comm. on Intern'l Relations, 95th Cong., 1st Sess. 7 (1977) (statement of Stanley J. Marcuss, Dep'ty Ass't Sec'y for Domestic Commerce, Dep't of Commerce).
141 Id. at 10-13.
142 Id. at 7.
143 Blair, supra note 138, at 371-72.
company. The company would be held responsible for the correctness of the information by criminal prosecution. Harold Levine argues that Professor Blair's solution is not strict enough although it does recognize the foreign availability problem. Mr. Levine distinguishes between technologies that are useful and those that are critical because they would provide the Soviet Union with a revolutionary increase in its technology. He advocates that Congress establish a critical technology list.

Certainly such a list could serve any policy or interest. It is just a question of interpretation of the terms used. The control list, like the EAA provisions, would prove to be highly discretionary. No method can guarantee that technology export regulations will be applied in a rational way. For example, U.S. authorities might regard as a security risk the export of information or advanced technology to an East Bloc country from a European country. Yet, the export of a comparable product from the United States to the same recipient would not be considered detrimental to the foreign policy or security of the United States. The recent 1988 OTCA amendments appear to adopt much of the approach advocated by Professor Blair.

In addition to creating problems for industry, the EAA unnecessarily restricts scientific research. Placing restrictions on scientific information undercuts the liberalizing tendency of the EAA. Exchange of information is crucial for commercial and scientific advances, and harsh export controls hamper the free flow of such exchanges. The Declaration of Policy to the EAA recognizes this fact:

It is the policy of the United States to sustain vigorous scientific enterprise. To do so involves sustaining the ability of scientists and other scholars freely to communicate research findings, in accordance with applicable provisions of law, by means of publication, teaching, conferences and other form of scholarly exchange.

Despite this stated policy, the 1985 amendments to the EAA continued to prohibit the export of scientific information without a license when such information has a negative effect on U.S. security or for-

---

144 Professor Blair advocates that a corporate officer, the corporate lawyer, and the person who researched the foreign availability sign the affidavit. Id. at 372.
145 Id.
147 A new section provides:

The Secretary shall make a foreign availability determination . . . on the Secretary's own initiative or upon receipt of an allegation from an export license applicant that such availability exists. In making any such determination, the Secretary shall accept the representations of applicants made in writing and supported by reasonable evidence, unless such representations are contradicted by reliable evidence, including scientific or physical examination, expert opinion based upon adequate factual information, or intelligence information.

The Commerce Department may also classify information as sensitive, although not "classified" information in the traditional sense, and on that ground withhold the information from publication, dissemination, or use. In a policy statement in 1986, former National Security Adviser John Poindexter emphasized the strategic importance of information and information systems. The statement implemented an earlier National Security Directive which provided the "initial objective, policies and organizational structure to guide the conduct of national activities toward safeguarding systems which process or communicate sensitive information from hostile exploitation." The 1986 statement explained this policy:

Federal Departments and agencies shall ensure that telecommunications and automated information systems handling sensitive but unclassified information will protect such information to the level of risk and the magnitude of loss or harm that could result from disclosure, loss, misuse, alteration or destruction.

The crucial issues for the implementation of this policy are how sensitive information is defined and who determines it.

The text describes what is "sensitive information":

Sensitive but unclassified information is information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other federal government interests. National security interests are those unclassified matters that relate to the national defense or to foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens.

The policy applies to all government entities and related contractors. The Director of the Central Intelligence Agency is responsible for identifying the sensitive but unclassified information. The execution of controls, protective regulations, and other protective measures are the responsibility of the head of each agency or department. Thus the NSC Directive further controls information possibly beyond the EAA.

European countries do not even accept "pure" security regulations with extraterritorial effects. They doubt the claim of a security interest in the economic aspects of trade in information technology.

---

149 Id. § 2402(a)(1).
152 See id. at 7.
153 Id.
and other advanced technology. However, if a nation cannot protect its sovereignty through export control regulations it will find alternate means. Because U.S. leadership in information technology is decreasing, it is understandable from a security as well as an economic perspective that the United States would attempt to enforce extraterritorial export control regulations on her allies. The question is whether extraterritorial export control regulations with a clear economic purpose are a breach of the sovereignty of the countries affected by those regulations. Regulations that protect national security within a nation's borders are clearly acceptable because a nation has a sovereign right to protect its natural resources. But it is questionable whether this sovereign right also allows a nation to enact laws, such as the EAA re-export provisions, which operate within another nation's borders.  

VII. Current View of the European Community: Is the 1982 EC Report Still Up To Date?

Several EC member states considered the export controls applied by the United States in the early 1980s a "rude jolt." It has colored their view of all subsequent export control efforts. The restrictions have had the positive effect of stimulating the search for non-U.S. sources of information and information technology. Both EC Commissioner Willy de Clerq and the European Parliament sharply criticized the application of the EAA, particularly the regulations on the re-export of assembled information technology, information, or knowledge. They viewed these measures as going far beyond CoCom regulations.

Europeans continue to believe that security and foreign policy regulations should not be applied extraterritorially. In April 1987, Mr. de Clerq expressed this feeling in a general discussion on trade barriers:

If the United States Congress is considering a series of bills [sic] aimed at restricting trade still further, it should wake up to the fact that "unfair trade" is not, as Congress seems to imagine, something practiced exclusively by America's trading partners. The United States is not innocent of these practices.  

Although the EAA defines national security, it does not define foreign policy, making U.S. export controls purely discretionary on the

154 For example, persons are prohibited from "export[ing] any technical data from the United States with the knowledge that it is to be reexported, directly or indirectly in whole or in part, from the authorized country(ies) of ultimate destination." 15 C.F.R. § 779.8(a)(2) (1989).
155 See infra text accompanying note 157.
part of the U.S. Government. Although the European Community generally shares the security interests of the United States, it views the extraterritorial application of U.S. laws within the jurisdiction of the European Community as unacceptable and contrary to the principles of international law.

In the 1988 OTCA amendments, the U.S. Congress made several changes in the EAA in an attempt to alleviate some of the problems discussed in this Article. The most significant change was the addition of a provision designed to address some of the problems relating to the re-export provision. A new subsection has been added: "No authority may be required . . . to reexport any goods . . . to any country which maintains export controls . . . pursuant to [CoCom]. . ."\(^{158}\) However, the OTCA expressly provides an exemption in four important areas,\(^{159}\) thereby undermining much of the force of the new subsection. Given the broad exception, this new subsection will not likely liberalize the EAA significantly. European countries remain skeptical despite these recent amendments to the EAA. In a 1989 report\(^ {160}\) the European Community continued to assert that the EAA applies extraterritorially in violation of international law although the European Community admitted that the 1988 OTCA relaxed national security controls somewhat.\(^ {161}\) Thus most of the criticisms of the 1982 EC Report remain valid.

VIII. The Netherlands Experience

The implementation of CoCom rules in the Netherlands illustrates some of the general problems associated with CoCom.\(^ {162}\) The Netherlands is a loyal follower of CoCom regulations, but it is often critical of regulations that go beyond those agreements. The Netherlands is quick to defend principles of international law, and the independence of states and national policies. For example, the Government of the Netherlands recommends that companies refuse to accept submission clauses. This attitude, however, can cause prac-


\(^{159}\) The four areas include:

(i) supercomputers;

(ii) goods or technology for sensitive nuclear uses . . . ;

(iii) devices for surreptitious interception of wire or oral communications; and

(iv) goods or technology intended for such end users as the Secretary may specify by regulation.

\(^{160}\) COMMISSION OF THE EUROPEAN COMMUNITIES, DIRECTORATE-GENERAL I, EXTERNAL RELATIONS, 1989 REPORT ON U.S. BARRIERS TO TRADE (May 1, 1989).

\(^{161}\) Id. at 34.

\(^{162}\) For a comparison of Netherlands law and U.S. law in this area, see Terporten, Vergunningen Voor De Export Van Computers En Computersoftware Uit De Verenigde Staten Van Amerika Naar Nederland, 1 COMPUTERRECHT 3-11 (1987).
tical problems for Dutch corporations who are active in the U.S. market.

As with other CoCom countries, the Netherlands has implemented the CoCom lists into its national regulations, namely the Export Decree on Strategic Goods (the Act). The Crown may take Import and Export Decrees only when it determines that the Decree is required in the interest of internal or external security; the international legal order; or a related international arrangement. Unlike the EAA, the Act does not mention foreign policy as a basis for control. Violation of the Act or the decrees based upon it constitutes a felony punishable on the basis of the Wet op de economische delicten. The Decree authorizes the Secretaries of Economic and Foreign Affairs to issue special regulations for goods of strategic importance. The measures may include prohibitions of import, export, or transit without license, and authorizations for the Minister responsible for imposing certain surcharges.

As in most other CoCom nations, “goods” described in the Decree include those designed or suitable for the transfer of information about the design, production, or use of technology. Exceptions are made for software (because it is a separate item on the list) and for publicly known technology. Similarly, computers and related goods, such as software embedded in the computers, are considered to be of strategic importance. In a recent case, several persons in the Netherlands were arrested with the help of U.S. authorities for exporting computer parts to Bulgaria.

Currently in the Netherlands the twelfth adjustment to the 1963 Decree is in force, plus an adaption in force as of January 1, 1988. The listed strategic goods, lijst strategische goederen, and related technology, including books, papers, and other information, are subjected to a licensing system directed by the Department of Economic Affairs. The list contains computer software and manuals, computer hardware and related technology, and semiconductor...
Currently, the list directly corresponds to the CoCom IL. Export of these goods without a permit is prohibited not only to East Bloc countries, but to all countries except Belgium and Luxembourg where the dangers of a “three-corner trade” or diversion are present. Exports to China are subject to a more liberal system of licensing as with CoCom.

The list is not as strict as it may appear. For example, it is possible to apply for an exception to the embargo with the Centrale Dienst voor In-en Uitvoer. Due to the recent discussions within CoCom, the Netherlands, in coordination with other CoCom states, has decided to include more computer technology in the liberal process used for China. Permission, however, is particularly dependent on the risk of diversion and on the prevailing political situation.171

A. Penal Law (Wetboek van Strafrecht)

Generally, the Netherlands Penal Code makes it risky to transport any information to another country if the information endangers a vital interest of the originating state. The publication of data originating from government sources or restricted areas could be classified as such. In Articles 92 through 107 of the Second Book (Felonies), there are several activities which, under Netherlands criminal law, endanger state security. Article 98 states that a person may not supply any data or goods that clearly represent a security risk to a person who is not entitled to this information. Violations of this article may result in a maximum of six years in prison or a maximum fine of Dfl. 100,000. The same penalty applies to anyone who discloses data from a restricted area that is of vital importance to the security of the state or her allies. If this information is made public or communicated to a foreign power, the person responsible can be punished even more severely.172

Furthermore, it is a criminal of-

---

170 Item 1564 on the list.
171 The government typically denies these factors. See also Netherlands Sanction Act of 1977. This act was not especially enacted for the protection of strategic interests, but it certainly has an effect. For instance, the Sanction Decree on Licenses to South Africa of 1982, which is based on this Act, forbids the export of technology and accompanying information for the construction or maintenance of weapons and related systems in South Africa.
172 The sentence could be 15 years imprisonment. Second Book (Felonies), art. 98(a). If the activity takes place during a time of war or is done in the service of another power, the punishment is even greater—20 years or life imprisonment. Id., art. 98(a)(2). A person may be imprisoned for six years for making preparations for the aforementioned felony. Id., art. 98(a)(3). If state secrets are revealed by a person’s culpable behavior, he may be imprisoned for one year. Id., art. 98(b). A civil servant who reveals information that he should have known to be a state secret may also receive a one year term. Id., art. 272.1.

In addition, there are other regulations for civil servants in the General Regulations for Civil Servants. Algemene Rijks Ambtenaren Reglement. Article 55 states that civil servants may not divulge anything heard in the line of duty. Article 59 establishes a general obligation of secrecy. These articles cover not solely strategic information but also all information about state affairs that are considered "sensitive."
fense to hold this information illegally to oneself or to attempt to obtain this information illegally, intentionally, or by false means.\footnote{Id., art. 98(c).}

The law does not describe the kind of information that is considered vital for state security. It may be safely assumed that the prohibition covers information ranging from confidential information (vertrouwelijk) to secret information (zeer geheim). It does not matter whether the information is embodied in letters, books, telecommunication signals, semiconductor chips, micro dots, or the human voice. The act of communicating the information as such constitutes the criminal act. Under the Dutch Constitution, Freedom of Information is restricted by the individual responsibility as prescribed by law.\footnote{Constitution of the Netherlands, art. 7, para. 3.}

B. Examples of Economic and Security Conflicts

The following cases illustrate the spectrum of results that arise from intermingling economic and security interests in a single policy.


Courts of other nations do not consider U.S. foreign policy principles when deciding a jurisdictional issue. In addition, other nations accept the effects doctrine only in limited circumstances. The Netherlands District Court at The Hague rejected the effects doctrine in Compagnie Europeene des Petroles S.A. v. Sensor Nederland B.V.\footnote{Reprinted in INT'L LEGAL MATERIALS 66, 73 (1983). For a discussion of the case, see Leigh, supra note 87, at 696-37.} Sensor Nederland (Sensor), a Dutch company wholly owned by a U.S. parent company, refused to fulfill a contractual obligation to deliver geophones to a French company because the equipment was ultimately destined for the Soviet Union. Sensor notified its French contractor that Sensor was unable to fulfill its contract because it was bound by the requirements of the EAA. The French contractor then requested the District Court of the Hague to order Sensor to deliver the disputed goods or face liquidated damages of Dfl. 10,000 per day. Sensor attempted to invoke a defense of force majeure by relying on "exonerating circumstances" under section 74 of the Uniform Act Governing the International Sale of Goods.

The court held that the contract was subject to Netherlands law and that, under general principles of international law, a nation may not exercise jurisdiction over acts performed outside its borders unless permitted by certain exceptions. According to the court, neither the nationality principle nor the protection principle applied in this case. The nationality principle did not apply because the U.S. regulatory criterion—"owned or controlled" by a U.S. parent company—
was not generally accepted in international law nor under Article XXIII of the Treaty of Friendship, Commerce and Navigation between the Netherlands and the United States.176

The protection principle did not apply because it only protects against consequences of acts performed outside the territory of the regulating country when such acts jeopardize the security or creditworthiness of that nation. Those interests do not include the "foreign policy interest that the U.S. seeks to protect."177 Most importantly, the court failed to see "how the export to Russia of goods not originating in the United States by a non-American exporter could have any direct and illicit effects within the United States."178 Therefore, "the jurisdiction rule cannot be brought into compatibility with international law."179

2. Grandia Project Service

Grandia Project Service180 illustrates the lucrative business of smuggling advanced information technology to the East. In December 1988, U.S. and Italian authorities arrested two Dutchmen and a Belgian and intercepted a Digital Equipment Corporation VAX 8800 computer, a highly advanced J-937 memory test system, and an M-218 Laser reperation system.181 The smugglers used as cover a company called Grandia Project Service which was headquartered in Amsterdam with a daughter company in Vienna. The smugglers used several other front and real companies to transfer the computers from the United States to Bulgaria or from Belgium to the U.S.S.R. Grandia is a clear criminal case and is very different from Dresser or Sensor. The legal principles are straightforward: the Dutchmen were properly arrested by the United States on U.S. territory for committing a criminal offense. The only questionable issue is whether the United States will extradite the smugglers to the Netherlands if they are convicted in the United States.

3. Kongsberg Vaapenfabrik/Toshiba

From 1982 to 1983, Toshiba, a subsidiary of a Japanese firm, sold precision machining technology to the Soviet Union. A Norwegian state-owned company, Kongsberg Vaapenfabrik (KV), supplied

176 Article XXIII provides that "companies constituted under the applicable laws and regulations within the territories of either party shall be deemed companies thereof and shall have their juridical status recognized within the territories of the other Party."

177 See also Leigh, supra note 87, at 636.

178 Id.

179 Id.


181 Id.
the software to run the equipment. It is believed this software helped the Soviet Union produce ship propellers that are substantially quieter than current Soviet propellers thereby making Soviet submarines harder to detect. The exported technology was on CoCom’s list but probably was not contained in Japan’s or Norway’s national regulations. Disturbed by this export, the U.S. Senate passed a resolution banning imports from KV and Toshiba for two to five years. This action had immediate economic consequences for Norway as KV lost a large order from the U.S. Navy leaving U.S. national suppliers to fill the gap.

Europeans felt that the U.S. action was a hypocritical attempt to take business from foreign suppliers and give it to U.S. suppliers. In Oslo it was noted that the strongest advocates of banning KV imports were congressmen from states where competitors of KV were located. Norway tried to reconcile the problem but did not succeed, leaving it bitterly disappointed. Toshiba, on the other hand, was barred from only U.S. Government contracts because a total ban would have affected too many U.S. companies which were dependent upon Toshiba products. The technology sent to the Soviets contained no U.S. components but only technology derived from U.S. sources.

IX. Conclusion

The foregoing cases as well as the political conflicts in the 1980s point out the major problems that affect CoCom. If CoCom is to function effectively, its members must resolve some of these substantial problems. First, the inconsistency between economic and security interests must be resolved. One way to alleviate this problem is to update the CoCom IL more often. One quarter of the CoCom IL is supposed to be updated each year, but in practice the list has become rapidly outdated. For example, home computers with 64 K-bytes of RAM, hardly products of strategic importance, were still on the Netherlands list in 1987.

Second, members must harmonize implementation of CoCom rules in the different legal systems of each member. The granting of export licenses varies greatly between CoCom members. For example, the likelihood of obtaining an export license under the Netherlands Export Decree on Strategic Goods of 1963 and under the EAA may vary substantially. In addition, some goods are considered

184 Export permits for home computers are easier to obtain than those for complete network applications.
to be of strategic value in certain situations even though in daily use they have none.\textsuperscript{186} This ambivalence creates uneven economic competition between CoCom members and can lead to a "lowest common denominator" kind of national security. Thus, not only must CoCom's list be updated, but it must be harmonized within each member's legal system.

Third, members must agree to some rules limiting unilateral acts which have an extraterritorial effect. Currently, unilateral extraterritorial actions are simply dividing CoCom members. Although these actions provide short-term security, they weaken the entire structure in the long term. These actions must be banned, and a consensus must be reached on limits on the extraterritorial application of national laws. Some CoCom members distrust the security motivation behind other members' export regulations and believe such regulations are simply intended to frustrate opposing economic interests. If members agreed to certain common policies and goals, then they would not intrude into the domestic affairs of other members because all members would have voluntarily placed this specific element of their sovereign powers into the hands of the Alliance as a whole.

Lately there has been a liberalizing trend in CoCom. Reviews have taken place more frequently to update the lists.\textsuperscript{187} During the late 1970s the CoCom IL was applied rather liberally, particularly by the European NATO partners. However, when the Soviets intervened in Poland and Afghanistan, the United States took a more restrictive approach to export control. Whether renewed arms control along with glasnost and perestroika will cause CoCom to liberalize its lists further is an open question. The substantial changes in Eastern Europe create further pressure for liberalization of CoCom con-

\textsuperscript{186} Technically, any item has potential military usefulness. A commonly cited example is the use of computer games to train gunners or military pilots. A more realistic example is an export embargo on certain civil trucks that could be useful in times of war. If this line of reasoning were taken to its logical extreme, cake could have a positive effect on military morale and therefore be regulated.

Many in the United States have adhered to the long-standing position that every article that could potentially enhance Soviet industrial power should be considered a strategic good. Western Europe would reserve that term for goods of military importance. Crawford & Lenway, Decision Modes and International Regime Change: Western Collaboration on East-West Trade, 37 WORLD POLITICS 375, 390 (1985).

The United States does not have a monopoly on restrictive thinking about strategic trade. "When ... Sweden restricted the import of footwear from the EEC contrary to its Free Trade Agreement with the Community it justified its action on public security grounds, claiming that maintaining a viable domestic footwear industry was a military necessity to ensure the supply of boots for the armed forces in the event of war." Although Sweden is not a CoCom member, it is interesting to note that "[b]oots are not on the CoCom list." Hunnings, Legal Aspects of Technology Transfer to Eastern Europe and the Soviet Union, in TECHNOLOGY TRANSFER AND EAST-WEST RELATIONS 146, 149 (1985).

\textsuperscript{187} More than 90,000 items remain on the Control List.
There are possible countervailing forces to this liberalizing trend. The expected increase in East-West trade may increase U.S. fear of losing its market share to Western Europe and Japan. The United States and other NATO members may also see the strengthening of export controls as a necessary replacement for the intermediate range ballistic missiles traded away by the INF Treaty. Currently, it is impossible to make a strong prediction. Whatever the result, CoCom must ultimately set a standard for free export.\footnote{189}

The greatest threat to CoCom's future is the character of information and information technology. The growing global information and communication network has diffused technology and information. Technology in non-CoCom states will continue to increase creating further confusion and mistrust among CoCom nations over how to apply restrictive export rules. The only solution is a liberalization of CoCom rules to a level which is acceptable to all CoCom countries and, to some extent, to the rest of the world. Unfortunately, this solution is essentially impossible and the effectiveness of export control regulations will continue to erode.

\footnote{188} Timmerman, \textit{It's Too Early to Relax Technology Curbs for East Bloc}, Wall St. J., Nov. 20, 1989, at A19, col. 3. ("The reformers within the Warsaw Pact don't need the type of technology COCOM controls; only the Warsaw Pact military has such needs.").

\footnote{189} This standard could either be the state-of-the-art in the Soviet Union or that in the West.