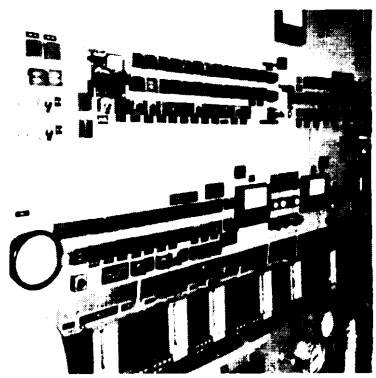
Protection of Proprietary Information

5

U.S. industry's primary concern about CWC inspections is the potential loss of ''confidential business information' (CBI), a general term covering trade secrets and other types of proprietary data. A trade secret is a commercially valuable plan, process, device, or formula, such as the chemical structure of a new pesticide or the recipe for Coca-Cola. CBI also applies to information on a company's costs, profits, suppliers, customers, manufacturing capacity, production schedules, and marketing plans. (See table 5-l.)

Protection of CBI is particularly critical in the chemical industry because U.S. chemical manufacturers face a highly competitive business environment both at home and abroad in which proprietary knowledge related to chemical products and processes is vital to a firm's success. Since basic synthesis methods have been published for most commodity chemicals, a company's competitive edge in the marketplace is often based on know-how or production techniques that provide small but significant margins of efficiency, yield, and cost, or result in a superior product that is purer, more attractive, or has a longer shelf-life. According to one analysis:

> In many cases, it is a small difference in expertise which gives one company the competitive edge over its competition—small differences which can ''make or break' a company's balance sheet. [1]



Because proprietary information is often the basis for a chemical company's competitive edge, both nationally and

[1] L. Zeftel, P. Weinberg and J. Schroy, ''Approaches to the Use of Instruments in Monitoring the Production of Chemical Weapons and Precursor Chemicals, '' in S. J. Lundin, cd., *Non-Production by Industry of Chemical-Warfare Agents: Technical Verification Under a Chemical Weapons Convention, SIPRI Chemical & Biological Warfare Studies No. 9 (New* York, NY: Oxford University Press, 1988), p. 147.

Table 5-I-Examples of Confidential Business Information

Manufacturing and process Information
• The formula of a new drug or specialty chemical
• A synthetic route that requires the fewest steps or the cheapest raw materials
• The form, source, composition, and purity of raw materials or solvents
• A new catalyst that improves the selectivity, efficiency, or yield of a reaction
• The precise order and timing with which chemicals are fed into a reactor
• Subtle changes in pressure or temperature at key steps in a process
• Isolation methods that give the highest yields consistent with good recycling of solvents and reagents
Business Information
• Expansion and marketing plans
. Raw materials and suppliers
• Manufacturing costs
• Prices and sales figures
. Names of technical personnel working on a particular project
• Customer lists

SOURCE: Office of Technology Assessment, 1993.

internationally, the theft of trade secrets can result in a major loss of revenue and investment—even for a large company. Industrial espionage can enable a competitor to obtain at minimal cost information that its originator acquired only through an enormous investment of time and money, thereby erasing the competitive advantage of that investment in R&D. For this reason, the theft of trade secrets ''can cripple even a giant company, and can be fatal to a smaller enterprise. ' This threat to proprietary information is probably greatest for U.S. chemical companies, which currently lead the world in many innovative processes. In contrast, chemical manufactureers in many other countries use older generations of chemical processes that are more widely known, so that there is less of value to "steal."

The value of proprietary information also depends on the industrial sector. Highly competitive, leading-edge industries such as speciality chemicals, biotechnology, and pharmaceuticals invest large amounts in research and development and must protect the resulting technical knowledge in order to recoup their investment and return a profit. Development and testing of a new pesticide takes an average of 10 years and $25 million.[3] Innovation in the pharmaceutical industry is even costlier. Each new drug that reached the market in the 1980s required an average of 12 years of research, development, and testing, and an after-tax investment (compounded to its value on the day of market approval) of roughly $194 million in 1990 dollars.[4] Yet although trade secrets are most critical to specialty-chemical producers, even commodity-chemical manufacturers using mature technologies can suffer serious economic losses from stolen trade secrets.[5]

The U.S. chemical industry has long been a major target of industrial espionage, which has been termed a serious threat to the nation's economic competitiveness.[6] For example, Rohm and Haas, a Philadelphia chemical manufacturer, spent more than 5 years investigating the theft of a secret formula for making latex paints. This search ultimately led to an Australian competitor, which was duplicating the Rohm and Haas product ''molecule for molecule, ' according to

[2] Kyle B. Olson, "The U.S. Chemical Industry Can Live With A chemical Weapons Convention%" *Arms Control Today*, vol. 19, No. 9, November 1989, p. 21.

[3] Tom Mauro, "When the Government Gives Away Companies' Trade Secrets, " *Nation's Business, Nov.* 1983, pp. 62-64.

[4] U.S. Congress, Office of Technology Assessment *Pharmaceutical R&D: Costs, Risks, and Rewards, OTA-H-522* (Washington DC: U.S. Government Printing Office, February 1993), p.1.

[5] J. Aroesty, K.A. Wolf, and E.C. River, *Domestic Implementation of a Chemical Weapons Treaty, report No.* R-3745-ACQ *(Santa* Monica, CA: RAND Corp., October 1989), p. *73.*

[6] William Carley, "As Cold War Fades, Some Nations' Spies Seek Industrial Secrets, *Wall Street Journal,* June 17, 1991, pp. Al, As.

[7] Orr Kelly, "Where There's a Profit, There's a Spy, " *U.S. News and World Report,* May 9, 1983, pp. 16-17.

company officials.[7] In addition to corporate spying, industrial espionage is reportedly conducted by the intelligence agencies of certain foreign governments, including U.S. political and military allies. With respect to the chemical industry, one analyst writes:

> U.S.-designed chemicals are counterfeited in large quantities abroad, cutting into three billion to six billion dollars in sales annually. German, French, South Korean, Japanese, Israeli, and Taiwanese chemical companies, at times in cooperation with their government, work hard to procure information on the American chernical industry and on each other. Free-lance consultants are paid hundreds of thousands of dollars a year to track technological developments in this U.S. industry. The methods of collecting information include both the complex and the mundane. A surprisingly common method is flying over chemical plants, particularly during their construction or renovatio.[8]

A nationwide survey of U.S. companies conducted in 1992 under the auspices of the American Society for Industrial Security's Standing Committee on Safeguarding Proprietary Information offers more detailed insights into the nature of the industrial espionage problem.[9] Out of a pool of 5,000 companies that were sent the questionnaire, 246 companies responded anonymously. These companies were from a wide variety of industries, including the chemical industry. Compared to an earlier survey conducted in 1985, the results of the 1992 survey showed a large rise in both the number of incidents involving the loss of proprietary information (an increase of 280 percent) and foreign involvement in these incidents (an increase of 360 percent).

Analysis of the data provided by the 11 respondents from the U.S. chemical industry yielded the following findings:[10]

- Eight of the 11 companies (73 percent) reported attempts to misappropriate proprietary business information, including technology and business plans, compared with 49 percent of all survey respondents.
- The 8 affected companies reported a total of 21 incidents, 6 of which cost the companies $86.25 million. (Costs were not provided for the other incidents, nor was the methodology by which the specified costs were calculated.)
- Customer lists, pricing data, and manufacturing process information were the types of proprietary information stolen most often.
- Current or former company employees were involved in 37 percent of the chemical-industry incidents, compared with 58 percent for the survey as a whole. Foreign firms or governments were involved in 35 percent of the chemical-industry incidents.
- The methods used to steal information from the chemical industry were varied and much more high-tech than the average industry. Approximately 24 percent of the incidents of communications intercept and electronic surveillance reported in the overall survey took place in the chemical industry.

The findings of this survey may be questioned on methodological grounds, since those companies affected by industrial espionage would arguably be more likely to return the questionnaire than others. Nevertheless, taken at face value, the data suggest that the chemical industry is one of the top five industries targeted by foreign companies and governments, and that the problem of industrial espionage is growing.

---

[8] Peter Schweizer, *Friendly Spies: How Americats Allies Are Using Economic Espionage To Steal Our Secrets (New* York, NY: Atlantic Monthly Press, 1993), p. 256.

[9] Richard J. Heffernan and Dan T. Swartwood, "Trends in Competitive Intelligence, " *Security Management,* January 1993, pp. 70-73.

[10] Dan T. Swartwood, President, Strategic Corporate Safeguarding, Inc. (Severna Park, MD), ' 'Proprietary and Trade Secret Theft in the U.S. Chemical Industry, " unpublished manuscript, May 1993.

PATENT AND TRADE-SECRET LAW

One way to safeguard proprietary technology is to file for patent protection. In exchange for a temporary monopoly that prevents others from producing, using, or selling an invention for a period of 17 years, the inventor makes a detailed description publicly available by filing it with the U.S. Patent and Trademark Office.[11] Much proprietary information in the chemical industry remains unpatented, however, for three reasons:

1. *Under U.S. law, a patent can be obtained only for a process, machine, product, or composition of matter that is novel, nonobvious, and useful,* Industrial know-how may be nonpatentable because it involves an improvement on a known process rather than a true innovation.
2. *Access to the information contained in a patent might help a rival firm to develop a similar but competing product or process. Since* patents require disclosures in applications and grants, companies may wish to protect sensitive information through secrecy instead.
3. *U.S. chemical companies often complain that enforcing a patent can be difficult or impossible because there are inadequate safeguards against patent infringement by unscrupulous foreign competitors.* Indeed, many countries either do not protect intellectual property rights or do not enforce the laws they do have.[12] As a result, many U.S. companies view published patents as ''a license to steal' and prefer to leave certain types of intellectual property unpatented and to protect them through secrecy.

U.S. State laws protect a company's trade secrets against unauthorized use or disclosure. According to the Uniform Trade Secrets Act, adopted by about half of the U.S. States, a trade secret may be any kind of information that requires at least some minimal investment or expense to generate and gives the holder an actual or potential commercial advantage because it is not widely known to competitors or to the public. Unlike a patent, ownership of a trade secret provides no legal protection against its independent discovery by others; the chief advantage is that a trade secret does not require any public disclosure of information. On the contrary, the law states that the holder of a trade secret must take concrete steps to preserve its confidentiality .13

Given the importance of proprietary business information for the U.S. chemical industry, company representatives are worried that intrusive declarations and inspections could allow trade secrets to fall into the hands of foreign competitors, adversely affecting the U.S. industry's competitiveness in both domestic and international markets. The most sensitive proprietary information concerns production process technologies and marketing data, such as customer and price lists. To recover damages in court for the theft of CBI, a company must prove that the information was stolen. Yet in many cases, the first indication that trade secrets have been compromised is when a foreign competitor starts selling a similar product

11 Patent protection applies to the idea underlying an invention, rather than any specific expression Of it. The patented invention may be licensed, publically disclosed, or distributed during the period of protection without altering its legal status. A patent also protects against independent discovery: in suing for patent infringement, it is not necessary to prove that a competitor deliberately copied the invention. See U.S. Congress, Office of Technology Assessment, *Finding* a *Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change, OTA-TCT-527* (Washington DC: U.S. Government Printing Office, May 1992), p. 12.

12 U.S. companies do have one recourse in such cases. Under the Omnibus Trade and Competitiveness Act of 1988, the U.S. Trade Representative (USTR) is authorized to identify, investigate, and retaliate against foreign countries that deny adequate and effective protection of intellectual property rights. Any interested party may file a petition with the USTR requesting that such an action be taken. This measure is known as ''Special' 301, since it is an expansion of section 301 of the Trade Act of 1974. Even so, there is no guarantee that such an action will be effective.

13 U.S. Congress, Office of Technology Assessment, *Finding a Balance,* op. cit., pp. 78-82.

at a lower price that does not reflect the costs of its own investment in research and development.

Perhaps the greatest threat of loss of proprietary data would be to small chemical companies that concentrate on particular markets or technology niches and whose business depends on the exclusive possession of highly specialized know-how. For example, some custom-chemical producers are expert in a single process (e.g., phosgenation, bromination, or sulfonation) while others have concentrated on serving a particular market (e.g., pharmaceuticals, pesticides, or photographic chemicals).[14] A specialty-chemical company whose economic survival depends on a cost or quality advantage in one type of reaction or product would be particularly vulnerable to industrial espionage carried out by a CWC inspector linked to a foreign company. Even visual inspection alone might reveal a unique process configuration that could be of great value to a competitor.

PROPRIETARY DATA AND REPORTING

Environmental laws that affect the chemical industry, such as the Toxic Substances Control Act (TSCA) and the Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA), include specific provisions to protect trade secrets and other proprietary data reported to regulatory authorities. For example, Section 10 of FIFRA permits a manufacturer to mark portions of submitted data as confidential and imposes criminal penalties on Federal employees who knowingly disclose such information.[15] In response to these laws, U.S. domestic regulatory agencies such as EPA and OSHA have developed complex and often legalistic procedures for preventing the disclosure of such information, and they generally do an effective job.[16]

Despite these controls, however, there appears to be a certain amount of "leakage" of proprietary information from U.S. regulatory agencies. Indeed, a recent study commissioned by the Chemical Manufacturers Association suggests that even if individual pieces of data do not warrant trade-secret protection, a trained engineer could combine them with other available information to "reverse-engineer' a company's technological secrets. The study also found that many chemical companies obtain their competitors' compliance reports under false pretenses by hiring consulting or law firms to serve as anonymous intermediaries.[17] Given this experience, the Chemical Manufacturers Association is concerned that proprietary information submitted to the U.S. Government for purposes of CWC verification might not be adequately protected from deliberate or inadvertent disclosure. To address this problem, the CMA seeks to minimize the quantity and sensitivity of information that must be included in treaty-mandated declarations and reports. For example, industry would prefer to declare production of scheduled chemicals in broad ranges rather than precise figures.

The chemical industry is also concerned that the Freedom of Information Act (FOIA), which allows individuals and companies to request the declassification and release of official U.S. Government documents, might be interpreted to provide broader access to proprietary information submitted to the National Authority under the CWC. Particularly worrisome to industry is the fact that foreigners have the same rights under the

---

14 Stephen C. Stinson, "Custom Chemicals, " *Chemical and Engineering News,* vol. 71, No. 6, Feb. 8, 1993, p. 35.

15 Edward A. Tanzman and Barry Kellman, "Legal Implications of the Multilateral chemical Weapons Convention: Integrating International Security With the Constitution " *International Law and Politics,* vol. *22,* 1990, pp. 515-516.

16 Kyle B. Olson, "Domestic Regulation of the U.S. Chemical Industry and Its Application to a Chemical Weapons Ban," in Thomas Stock and Ronald Sutherland, eds., *National Implementation of the Future Chemical Weapons Convention, SIPRI Chemical & Biological Warfare Studies No. 11* (Oxford, England: Oxford University Press, 1990), p. 106.

17 SRI International, *Analysis of Impact of U.S. Federal and State Reporting Requirements on Sensitive and proprietary Company Information: Final Report* (Menlo Park, CA: SRI International, Project 3307, July 1992), p. 4.

FOIA as do U.S. citizens. Some analysts allege that foreign corporations, often working through U.S. consulting and law firms, systematically file FOIA requests to gather information on U.S. corporate secrets.[18]

U.S. Federal courts have ruled that proprietary data qualifies for withholding under the FOIA if government disclosure would be likely to harm the competitive position of the person or corporation that submitted the information. Many agencies notify a submitter of business information that disclosure is being considered; the submitter then has an opportunity to convince the agency that the information qualifies for withholding. If the submitter and the government disagree on whether the information is confidential, the submitter may file a ''reverse' FOIA lawsuit to block disclosure under the law.[19] Nevertheless, the U.S. Court of Appeals for the District of Columbia has ruled that certain corporate information provided to the U.S. Government and designated confidential may not be withheld from disclosure under the FOIA if it does not meet the definition of a "trade secret. "[20] The chemical industry believes that this interpretation is too narrow and wants all information that companies consider confidential to be exempted from disclosure.[21]

To protect proprietary data submitted for CWC verification purposes, the implementing legislation might include strict rules against unauthorized disclosure. A useful model that already exists in U.S. law is the Chemical Diversion and Trafficking Act (CDTA) of 1988, which is designed to help combat the diversion of legitimate chemical shipments to illegal drug manufacturing.[22] The CDTA requires chemical manufacturers and distributors to file reports on transactions involving precursor chemicals and equipment used in the manufacture of illicit drugs, and gives the U.S. Drug Enforcement Administration (DEA) the authority to monitor potential diversions of chemical shipments. According to the statute, the Attorney General must take 'such action as maybe necessary' to prevent the unauthorized disclosure of information contained in the reports, and to "issue guidelines that limit, to the maximum extent feasible, the disclosure of proprietary business information. . . .' A company that suffers damages from the unauthorized disclosure of information may bring a civil action against the violator for appropriate relief, although not against DEA personnel.[23]

PROPRIETARY DATA AND INSPECTIONS

The U.S. chemical industry has been inspected for years, but only by domestic Federal and State agencies.[24] CWC inspections, in contrast, will be carried out by multinational teams under the auspices of an international organization that is

---

18 Schweizer, *Friendly Spies,* op. cit., p. 270.

19 U.S. House, Committee On Government Operations, *A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of Z974 to Request Government Records,* 103rd Congress, 1st Session, House Report 103-104 (Washington, DC: U.S. Government Printing Office, 1993), p. 13.

20 *National Parks and Conservation Association v. Rogers, 498* F.2d 765 (D.C. Cir. 1974), *and National Parks and Conservation Association v. Kleppe, 547* F.2d 673 (D.C. Cir. 1976).

21 Michael P. Walls, ' 'The private Sector and Chemical Disarmament,'' in Brad Roberts, cd., *The Chemical Weapons Convention: Implementation Issues, Significant Issues Series,* vol. XIV, No. 13 (Washington, DC: Center for Strategic and International Studies, 1992), p. 46.

22 Title VI, Subtitle A, Public Law No. 100690, *Anti-Drug Abuse Amendments Act of 1988,* 21 U.S.C. para 830 *et seq.*

23 P.L.100-690, Sec. 6052, in *Laws of 100th Congress—2nd Sess.,* p. 102 STAT.4314.

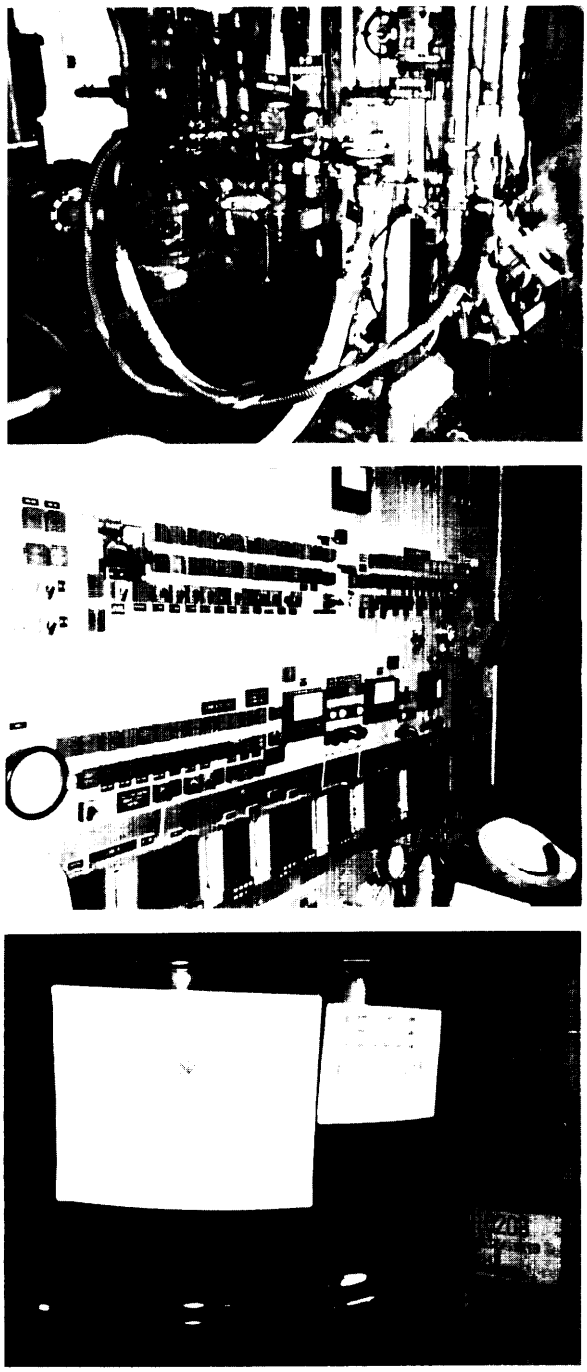
24 The one exception t. this rule Concerns a few U.S. pharmaceutical companies that produce sterile drugs for injection or ophthalmic use for sale in the United Kingdom. These companies must register with the British Medicines Control Agency, which periodically inspects the U.S. plants. The inspected facilities are given a notice of between 1 and 2 months, and must bear the costs of the inspection. In order to protect proprietary data, the Medicines Control Agency must obtain the U.S. company's permission before releasing any information.

not accountable to U.S. law, raising concerns about the potential loss of trade secrets. According to industry analysts, proprietary data might be compromised during an onsite inspection of a chemical plant in the following ways:

- manifests and container labels could disclose the nature and purity of feedstock materials ,and the identity of key suppliers;
- instrument panels might reveal the precise temperature and pressure conditions for a specific production process;
- chemical analysis of residues taken from a valve or seal on the production line could disclose proprietary information about other products made with the same equipment;
- access to piping and instrumentation diagrams, combined with visual information, could enable a trained chemical engineer to deduce certain flow and process parameters; and
- audits of plant records, ranging from cus - tomer lists to process documentation, could reveal a variety of sensitive information,

How serious is the threat of industrial espionage under the cover of a CWC onsite inspection? Although the innards of a chemical plant are bewildering to a neophyte, a skilled chemical engineer might be able to deduce a fair amount of valuable information from the configuration of the plant. According to an industrial-security expert, ‘ ‘There’s a lot that can be learned about a plant from an onsite inspection, provided that you know exactly what you’re looking for. "[25] This expert claims that an international inspector intent on spying would come equipped with extensive knowledge of the target facility and a laundry-list of specific questions to be answered.

The third U.S. National Trial Inspection, held at Monsanto Agricultural Co. Luling, LA plant, tried to assess the potential for industrial espionage during a CWC inspection. The team that carried out the trial inspection included a Mon-



SIGMUND R. ECKHAUS

Potential sources of proprietary information that might be divulged during onsite ins piping configurations (top), instrument panels (middle), and container labels (bottom).

[25] Telephone interview with Henry Clements, vice president, Technology Strategic Planning, Inc. (Stuart, FL), May 2 6, 1993.

santo chemical engineer, unfamiliar with the operation of the Louisiana plant, who was asked to determine how much useful proprietary data he could collect during the course of the inspection. By visually examining the plant and auditing plant records, he was able to deduce enough information about the production process to save a potential competitor signficant development time and money. This finding maybe a worst-case assessment, however, since the Monsanto engineer was allowed to concentrate on his "spying' assignment for two and a half days, did not perform regular inspection duties, and was not as closely supervised as the other team members.[26]

In practice, it would not be easy for a company or a foreign government to infiltrate a CWC inspection team for purposes of industrial espionage. To steal trade secrets from a particular plant, an unethical inspector with links to a foreign company or government would have to be assigned to the team that visited the facility of interest. He would also have to know precisely what type of information to look for and where in the plant to find it. Moreover, his access to the plant site would be governed by the agreed parameters of the inspection. Given the technical difficulties and political risks involved in suborning an international inspector, companies or foreign governments would probably favor less risky methods of gaining access to trade secrets. Hiring, bribing, or blackmailing a current or former company employee would almost certainly be easier and more cost-effective.

Another industrial espionage scenario would be for an individual CWC inspector to come across valuable proprietary information in the course of an inspection that he might then be tempted to sell to his own former employer or some other interested company. Industry officials also worry that even if the international inspectors have no intention of disclosing trade secrets, they might do so inadvertently. The inspectors will inevitably have access to highly sensitive proprietary information in the course of their work, which they will tend to discuss informally among themselves. This exchange of information---even if innocent in itself-could result in inadvertent leaks.

It seems likely that the extent to which CWC inspections could result in significant losses of proprietary information will depend on a number of situational factors, including:

1. how frequently a site is inspected (the treaty permits a maximum of two routine inspections per year of commercial plants);
2. the amount of access provided to the site and to related documentation;
3. the inspectors' prior knowledge, experience, and intent to engage in industrial espionage;
4. the existence of a private company or foreign government willing to pay handsomely for misappropriated information; and
5. the relative cost of obtaining information from a CWC inspection compared with alternate means, such as bribing a current or former employee.

6. any event, one should keep the U.S. chemical industry's concerns over proprietary information in perspective. Given that the chemical industry has long been targeted for industrial espionage, it is likely that the CWC's reporting and inspection requirements will only marginally increase the industry's exposure to foreign spying. By improving routine security practices, chemical manufacturers should be able to reduce losses of proprietary information from *all sources*, only a fraction of which will be directly attributable to CWC implementation.

PREPARING FOR INSPECTIONS

Although the threat of industrial espionage will exist during CWC inspections, it can be managed

[26] Conference on Disarmament, ''Report on the Third United States Trial Inspection Exercise, " document No. CD/1 100, Aug. 14, 1991, p. 20.

through advance preparation and planning. An respected facility can limit the ability of inspectors to collect proprietary data through a good understanding of potential collection techniques, effective assessment procedures. and well-trained personnel and escorts.

The CWC states that '' [i]n conducting verification activities, the Technical Secretariat shall avoid undue intrusion into the State Party's chemical activities for purposes not prohibited under this Convention. ''[27] Clearly, inspectors will not need to know the details of a proprietary process to determine that it is not involved in the production of chemical weapons. The treaty also entitles companies to take active measures to minimize any loss of proprietary information associated with CWC inspections. Special provisions for this purpose were built into the treaty at industry's request. For example, the inspected facility may request that all sample analyses be carried out onsite and limited to determining the presence or absence of treaty-controlled chemicals.

In preparing for inspections, it is essential to assess which items need to be protected and to follow up this assessment with a concrete plan of action. A chemical plant preparing for a CWC inspection might undertake some or all of the following measures:

1. inventory plant equipment and processes and identify which activities are particularly sensitive and vulnerable to observation;
2. determine which aspects of a critical process or item of equipment must be protected, such as its size, shape, or very existence;
3. prepare an inspection route through the facility to keep inspectors out of areas containing activities unrelated to the treaty;
4. train a core group of senior plant managers to escort the inspectors;
5. inform plant personnel about which parts of the facility will be subject to inspection, how to make their work areas secure, and how to interact with the inspectors to prevent them from damaging the facility and to answer their questions without revealing sensitive information;
6. shield proprietary equipment by installing shrouds, boxes, or screens (although shrouding control panels and other equipment could interfere with production to some extent);
7. turn off computers, cover up labels and manifests, and remove sensitive documents; and
8. in those few cases where proprietary information cannot be protected by covering or shrouding, limit the inspectors' access to highly sensitive areas of the facility—provided the plant officials can satisfy the inspectors' compliance concerns by other means,

Auditing Records

Since giving inspectors access to production records arguably creates the greatest risk for loss of proprietary data, companies will need to draw the line at that information essential to verifying treaty compliance.[28] Facility agreements and established guidelines will determine the types of records that can be examined. For example, CWC inspectors may request access to production records to determine the relative amounts of raw materials consumed and to verify the production figures stated in the declaration. The inspectors may also wish to calculate a rough materials balance for the plant by comparing records on the consumption of raw materials with those on the production and shipping of finished product.

To the greatest extent possible, however, companies will be allowed to screen records for proprietary information. Plant officials should not have to open up their most sensitive files,

[27] Article IV, paragraph 10, in Conference on Disarmament, *Draft Corn) ention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction,* extracted from CD/l 173, Sept. 3, 1993, p. 23.

[28] Michael P. Walls, Chemical Manufacturers Association, personal communication.

including data on process variables (temperature, pressure, catalysts, and reaction times), production yields, product mix, or supplier and customer lists. CWC inspectors, for their part, will be expected to retiain from engaging in "fishing expeditions and to use auditing only to answer specific compliance questions that arise during an inspection.

Companies subject to CWC inspections can also take measures to protect sensitive production records. Multiuse plants often keep records on feedstock materials used to manufacture both treaty-controlled and uncontrolled chemicals at the same site. Since all production records relating to scheduled chemicals are potentially subject to audit, however, chemical companies may find it desirable to segregate these records to protect proprietary data not directly relevant to treaty compliance.[29] Although setting up a separate accounting system for scheduled chemicals would entail a significant upfront investment, it would make it easier for companies to generate and update reports and would probably save money in the long run.

Inspected companies can also make arrangements with the OPCW Technical Secretariat to protect proprietary information that does not need to be removed from the facility. During the second U. S. National Trial Inspection, for example, the host company installed a locked container at the site for storing sensitive documents and drawings that would be needed by the inspection team for reference on subsequent visits. Although the inspectors took away some calculations and sketches to write their report, no confidential facility drawings, piping and instrumentation diagrams, documents, or descriptions of operating procedures were removed from the site.[30]

In sum, concerns about loss of proprietary information can generally be minimized through adequate preparation. Since preparing for inspections costs money, however, companies will generally undertake the bare minimum needed to protect their legitimate trade secrets. The extent to which commercial chemical plants (including certain defense contractors) will need to prepare for inspections depends on the sensitivity of the work being done there. Ideally, the vulnerability-assessment process should identify the most cost-effective approach for shielding proprietary or national security information. Without careful planning, companies may tend to overprotect their proprietary assets, resulting in unnecessary preparation costs. For example, instead of preparing a costly shroud, it may be sufficient to cover a label or gauge with a piece of tape, move an object to another room, or turn it around.

The U.S. Government could support the chemical industry by providing guidance on how companies can best prepare for inspections so as to protect their trade secrets. Measures the government could take to facilitate industrial preparation include:

- providing special vulnerability-assessment and training programs,
- encouraging companies to pool their resources,
- providing tax breaks and material aid such as shrouds,
- carrying out additional National Trial Inspections of commercial plants as a useful training mechanism for both government and industry personnel, and
- encouraging chemical plants to prepare facility agreements for Schedule 3 plants, even though they are not mandated by the CWC. Since facility agreements specify which parts of a plant are subject to inspecticm,

29 It is possible, however, that Some inspection teams may insist on seeing all production records on chemicals manufactured in a given plant to make sure that the segregated information on treaty-controlled chemicals is accurate.

30 Conference on Disarmament, Ad Hoc Committee on Chemical Weapons, "Report on the Second United States Trial Inspection Exercise," document No. CD/CW/WP.301, June 27, 1990, p. 5.

what records may be reviewed, and where samples may be taken, drawing them up could help companies prepare for routine inspections.

The U.S. Department of Defense has created an interagency program known as the Defense Treaty Inspection Readiness program (DTIRP), which is administered by the On-Site Inspection Agency (OSIA). This program is designed to help defense contractors and government-owned facilities prepare for foreign arms-control inspections such as those mandated by the INF, START, and Open Skies treaties and the CWC.[31] In advance of CWC implementation, the OSIA has already undertaken vulnerability assessments of certain government facilities and is prepared to conduct similar assessments of defense contractors; the agency is also working with the Department of Commerce to provide advice and assistance for private industry .32 Non-defense chemical manufacturers could benefit from a civilian version of DTIRP.

In conclusion, CWC implementation involves an unavoidable tradeoff between the need to protect U.S. trade secrets and to establish a treaty verification regime with enough teeth to deter violators and build international confidence in the regime. The CWC as written, however, provides ample flexibility to balance these two desirable objectives.

INSPECTOR RELIABILITY

Because of the technical complexity of CWC verification, the international inspectors will need to be highly trained specialists who possess a detailed knowledge of chemical engineering, industrial processes, or analytical chemistry techniques. Although some individuals currently employed by local or national regulatory authorities might have the necessary qualifications, many inspectors will probably come from the chemical industry. Unfortunately, the recruitment of inspectors from industry could give rise to real or perceived conflicts between the role of an international civil servant and residual identification with national or corporate interests. Individuals who maintain strong ties to their fomer employers—particularly those who plan eventually to return to their previous jobs—may be tempted to engage in industrial espionage. Furthermore, in those countries where the government owns, controls, or is closely aligned with the national chemical industry, an inspector linked to a government entity or a nationalized company may be tempted to funnel sensitive data from reports and inspections to the state-run industry. In sum, as one analyst has pointed out, "The dilemma is that the very people who would be best qualified for inspection duties because of their industrial experience could also be most capable of violating confidentiality while performing those duties. "[33]

This dilemma might be addressed in a number of ways. First, within 30 days after the treaty enters into force, the OPCW Technical Secretariat will publish a list of inspectors for review by the participating countries, and States Parties to the CWC will have the right to prohibit individuals whom they consider untrustworthy from conducting inspections on their territory. This ability to vet inspectors will enable countries to screen out those considered most likely to engage in abuses. Although participating countries can reject inspectors at any time, each request will only become effective after 30 days to prevent coun-

31 U.S. Senate, Select Committee on Intelligence, *Intelligence and Security Implications of the Treaty on Open Skies*, 103rd Congress, 1 st Session, report No, 103-44 (Washington, DC: U.S. Government Printing Office, 1993), p. 16.

32 Interview with Michael H. McMillan, Chief, Security Office, On-Site Inspection Agency, June 3, 1993.

33 Julian P. Perry Robinson, cd,, *The Chemical Industry and the Projected Chemical Weapons Convention: Volume II, SIPRI Chemical and Biological Warfare Studies No.5 (New* York, NY: Oxford University Press, 1986), p. 29.

tries from rejecting inspectors as a means of delaying an inspection.

Second, the OPCW should seek the highest standards of inspector reliability and impartiality, backed up with an active internal-security program and stringent disciplinary measures. Although the CWC empowers the Director General to strip inspectors of their diplomatic immunity if they are found guilty of a serious breach of confidentiality, it will take political courage to implement this provision. Some analysts contend that CWC inspectors should not be allowed to return to employment in private industry for at least 5 years. Others go further, arguing that it would be preferable not to draw inspectors from industry at all but to train them from the ground up so that their first loyalty is to the international organization. [34]

Finally, because of the economic insecurity associated with short-term appointments, one way to reduce the temptation for inspectors to engage in spying would be to give them greater job security by creating a professional corps and a career track for them within the agency .35 The availability of permanent positions would also make it easier to attract the most qualified individuals. Given the inherently stressful nature of field inspection work, which tends to cause ''burn out" after a few years, inspectors might be rotated at regular intervals to desk jobs within the Technical Secretariat, where they could analyze data obtained from other onsite visits. Unfortunately, the financial constraints on OPCW funding may severely limit the number of career-track positions open to inspectors.

SAFEGUARDING REPORTED DATA

Protecting the proprietary information contained in the declarations and inspection reports submitted under the CWC from unauthorized disclosure will require special safeguards, both during the collection of data from industry by the U.S. National Authority and the subsequent transfer of this information to the OPCW Technical Secretariat. Both the National Authority and the Technical Secretariat plan to establish secure databanks to store confidential information provided by companies.[36]

In response to suggestions from the world chemical industry, the CWC also contains a special ''Annex on the Protection of Confidential Information, ' which is designed to safeguard proprietary business information disclosed in required declarations, reports, and inspections.[37] This annex includes the following provisions:

- In administering the treaty, the OPCW will demand 'only the minimum amount of information and data necessary for the timely and efficient carrying out of its responsibilities.
- Data designated by industry as confidential will be subject to a system of formal classification, secure storage, and other security measures to protect against unauthorized disclosure.
- Staff members of the Technical Secretariat must enter into individual secrecy agreements covering their period of employment and 5 years thereafter.
- Dissemination of confidential business information within the OPCW will be on a strict ''need-to-know' basis.
- Officials will handle as much information as possible in a form that precludes direct identification of the facilities concerned.
- Inspectors will not be allowed to participate in challenge inspections of chemical plants in their native countries.

---

34 Barbara Hatch Rosenberg, State University of New York at Purchase, personal communication, May 28, 1993.

35 Aroesty et al., Domestic *Implementation, Op.* cit., p. *54.*

36 *E* P. Yesodharan, ''The Chemical Weapons Convention: A Point of View from Industry, ' *UNIDIR Newsletter, No. 20,* December 1992, p. 29.

37 *Draft Chemical Weapons Convention,* op. cit., pp. *169-174.*

- The OPCW plans to establish a ‘ ‘Commission for the Settlement of Disputes Related to Confidentiality, ’ which will consider breaches of confidentiality involving members of the Technical Secretariat.
- The Director General of the OPCW will develop ‘ ‘appropriate punitive and disciplinary measures’ for the wrongful disclosure of confidential information. He will have the power to waive immunity from prosecution for individual inspectors accused of “serious breaches of confidentiality.

If the monetary rewards of industrial espionage are sufficiently high, however, they could blunt the deterrent effect of the threatened punishment. The Director General’s power to waive the diplomatic immunity of an inspector will also have little practical effect unless the accused individual is in the custody of a government with both the power and the political will to prosecute.[38] One possible solution would be to require all parties to the CWC to either prosecute or extradite inspectors found guilty of violating the confidentiality guidelines. There is a trade-off, however, between the need to maintain industry’s confidence in the integrity of the OPCW and the possibility that aggressive measures to enforce the security regulations could undermine the morale and effectiveness of the inspectors. Indeed, CWC violators might even use false allegations of espionage to intimidate honest inspectors from carrying out their tasks. The reason international civil servants enjoy immunity from prosecution is so that they can perform their work free from threats and harassment; exceptions to this important principle of international law are warranted only if there is clear evidence of abuses.

1 The IAEA Experience

Useful lessons about the ability of large international organizations to keep secrets can be drawn from the experience of the International Atomic Energy Agency (IAEA), the multilateral organization charged with administering the provisions of the Nuclear Non-Proliferation Treaty. Similarities between the nuclear and chemical nonproliferation regimes include extensive reliance on private-sector declarations, reports, and onsite inspections, although the scope of IAEA activities is much narrower.[39] The founding Statute of the IAEA forbids the disclosure of proprietary data, as do the individual safeguards agreements negotiated between the agency and signatory countries. According to the Statute, IAEA staff

> We shall not disclose any industrial secret or other confidential information coming to their knowledge by reason of their official duties for the Agency. Each member undertakes to respect the international character of the responsibilities of the Director General and the staff and shall not seek to influence them in the discharge of their duties.[40]

The IAEA has also established staff rules and regulations for implementing these principles, and the Director General may impose disciplinary measures or summarily dismiss a staff member for serious misconduct.[41] For example, the confidentiality of safeguards-related information is ensured by access on a ‘‘need-to-know’ basis

38 Burrus M. arnahan, “Chemical Arms Control, Trade Secrets, and the Constitution: Facing the Unresolved Issues, ” *The International Lawyer*, vol. 25, No. 1, spring 1991, p. 174.

39 Although the IAEA has always had, in theory, the power to conduct ‘‘ special’’ or challenge inspections, until recently all its inspectors have focused only on declared nuclear facilities intended for peaceful uses and have relied primarily on record checks and mass balances of a few fissionable materials.

40 Article VII.F, ‘ ‘Staff, in *Statute of the International Atomic Energy Agency As Amended Up to 2.9 December 1989* (Vienna: IAEA, June 1990), p. 18.

41 A. von Baeckmann, ‘ ‘The Chemical Weapons Convention and Some IAEA Experiences, ‘‘ in S. J. Lundin, cd., *Non-Production by Industry of Chemical-Warfare Agents: Technical Verification Under a Chemical Weapons Convention, SIPRI Chemical & Biological Warfare Studies No. 9 (New* York, NY: Oxford University Press, 1988), pp. 183-184.

only by those individuals charged with inspecting a particular facility.

Although the best rules cannot rule out the unauthorized disclosure of confidential information through theft, accidents, or misconduct of individual staff members, the IAEA does not appear to have had serious problems with the leakage of information, When the agency was established, protecting proprietary data was a matter of deep concern to Western Europe and Japan, yet no member-country or operator has ever lodged a complaint against the IAEA alleging that trade secrets have been compromised.[42] In view of this experience, the Chemical Manufacturers Association believes that there is "a reasonable likelihood" that the OPCW will be able to safeguard the confidential business information in its possession.[43] Even so, given the difficulty of limiting access to data within a multinational organization, the most effective means of protecting proprietary information may be to store and handle it in a form that has limited utility for industrial espionage—for example, by not identifying specific facilities by name.

Like the IAEA, the OPCW will face conflicting demands in its handling of data related to monitoring activities. Whereas the IAEA observes strict limits on the release of such information both internally and in public statements, it must also make enough data publicly available to maintain the credibility of its assurances.[44] In recent years, the IAEA has come under increasing pressure to provide more detailed information on safeguards implementation to the agency's Board of Governors and, through its annual report, to the public. While such greater openness might allow countries to exploit sensitive information for political or commercial purposes, the advantages appear to outweigh the disadvantages. As Lawrence Scheinman has pointed out:

> There is a tension between interest in *confidentiality* of information on the one hand, and demand for. . . providing more and more detailed information on safeguards implementation in the name of increasing *credibility,* on the other. Optimizing between these two values is a problem of political choice that may be even more significant in a Chemical Weapons Convention due to the even more intense degree of competition in the world chemical market than in the nuclear market and the resulting likely higher sensitivity regarding proprietary information.[45]

COMPENSATION FOR LOSS OF PROPRIETARY INFORMATION

The CWC gives industry no mechanism for financial compensation if inspections result in the loss of valuable proprietary information through inadvertence or industrial espionage. U.S. companies have generally been willing to absorb the incidental expenses associated with treaty compliance as a cost of doing business, but some firms contend that they should be able to sue for economic damages resulting from the theft or inadvertent disclosure of proprietary information by members of the U.S. National Authority or the OPCW Technical Secretariat. Although it has not yet been decided whether such a compensation mechanism is justified or how such claims would be adjudicated, various legal approaches to this issue are discussed below.

---

42 Lawrence Scheinman, Cornell University, personal communication.

43 Michael P. Walls, CMA, response to OTA questionnaire.

44 James F, Keeley, *International Atomic Energy Agency Safeguards: Observations on Lessons for Verifying a Chemical Weapons Convention, Arms Control Verification Occasional Papers No. 1* (Ottawa, Canada: Dept. of External Affairs, Arms Control and Disarmament Division, September 1988), p. 31.

45 Lawrence Scheinman,' 'Operational Considerations, '' in H. Bruno Schiefer and James F. Keeley, *International Atomic Energy Agency Safeguards as a Model for Verification of a Chemical Weapons Convention, Arms Control Verification Occasional Papers No. 3* (Ottawa, Canada. Dept. of External Affairs, Arms Control and Disarmament Division, October 1988), p. 57.

I Claims Against the OPCW

Under certain circumstances, American companies can sue a foreign government or an international organization in U.S. Federal court for damage or loss to property in the United States resulting from actions committed by foreign or international civil servants in their official capacity. The CWC, however, specifically rules out this legal avenue for compensation by granting the OPCW legal immunity and thus shielding it from law suits. By ratifying the treaty, the U.S. Government would accept this stipulation.

I Claims Against an Inspector

The Director General of the OPCW has the power to waive the immunity of an individual inspector suspected of stealing trade secrets. To win a civil suit against the inspector, the damaged company would only need to present a preponderance of evidence; proof beyond a reasonable doubt would not be necessary. Even so, there are obvious problems of proof when the only evidence for theft of trade secrets is that several months after a U.S. company is inspected, a foreign plant starts shipping a product believed to have been made according to a secret process developed by the U.S.firm. It would be extremely difficult to prove that the theft had occurred, much less identify the guilty party in a multinational inspection team or trace his connection to the benefited company. Even in the unlikely event it were possible to catch and convict an inspector for divulging trade secrets, the harmed company could not obtain compensation if the guilty individual were unable to pay damages. A more appropriate target for a damage suit would be the foreign company that benefitted from the stolen information, but here again, it would be hard to prove that a theft of trade secrets had occurred.

| Claims Against the US. Government

The Fifth Amendment provides that if private property is seized by the U.S. Government, the affected individual or corporation is entitled to due process of law and compensation for the fair market value of the loss. Such government expropriation can result either from a‘ ‘taking’ of private property in the public interest (e.g., by ‘‘eminent domain’ or from a ‘‘tort’ such as the theft or breakage of property by a U.S. official. In *Ruckelhaus v. Monsanto Co., the* Supreme Court ruled that trade secrets are a form of property and are thus protected by the Fifth Amendment from government expropriation.[46] Even if U.S. officials reveal trade secrets, however, such disclosure is only considered an unjust ‘‘taking’ if it results in tangible economic damage to the affected company. In such cases, American firms may have grounds to sue the U.S. Government for fair compensation.[47]

Whether the U.S. Government would be liable for the loss of proprietary data resulting from CWC inspections under the Fifth Amendment ‘ ‘takings’ ‘ clause is a matter of legal debate. Under the ‘‘state action’ doctrine, the court must examine whether ‘‘a sufficiently close nexus exists between the state and a challenged action, so that the action may fairly be treated as that of the state itself. ” [48] According to one view, the U.S. Government cannot be accused of ‘taking’ private property simply by complying with the CWC verification regime, since it bears no direct responsibility for the theft of corporate trade secrets by international inspectors operating outside their mandate.

The counterargument is that the U.S. Government, in pursuing the security benefits of participation in the CWC, is deliberately putting private U.S. companies in a position where they will be vulnerable to losses of proprietary information.

---

46 *Ruckelhaus* v. *Monsanto Co.*, 467 U.S. 986, 1001-04 (1984).

47 Such a suit could be filed under the Tucker Act, 28 U.S.C. 1491.

48 *Black's Law Dictionary*, 6th ed. (St. Paul, MN: West Publishing Co.,1990), p.1407.

This argument is strengthened by the fact that industry's participation in the veification regime is involuntary and may even be enforced by government officials through administrative or criminal search warrants. It is therefore possible to argue under the "state action' doctrine that any economic harm to private companies arising from the inspections is the result of a deliberate decision by the United States to sign and ratify the CWC and to implement the verification regime.[49]

Yet even if the courts establish that the theft of trade secrets by international inspectors is indeed a "state action,' the U.S. Government would not be financially liable for the resulting damages unless it took an affmative step to accept this liability. The reason is that the doctrine of ''sovereign immunity' allows the Federal Government to deny recovery of damages resulting from the acts of Federal employees or foreign inspectors. Although the Federal Tort Claims Act (FICA) provides a limited waiver of this immunity by permitting suits against the United States for official misconduct, in recent years the right to sue the U.S. Government for damages under the FTCA has been limited by several exceptions, which have been broadly applied to matters affecting national security.[50] Thus, if Congress wishes to enable companies harmed by CWC inspections to recover monetary damages from the U.S. Government, it will need to waive sovereign immunity under the FTCA. Such a waiver might be included in the implementing legislation.

Administrative Claims Procedure

In all of the legal remedies discussed above, the costs and risks of litigation (either against an individual inspector or the U.S. Government) would give the chemical industry little assurance that it could recover damages resulting from CWC verification. As an alternative to litigation, some analysts want Congress to establish a ''nonburdensome administrative process' for the arbitration and payment of just claims.[51] This process would have the effect of placing on the U.S. Government the financial liability created by the misconduct of international civil servants, unless and until fair compensation can be obtained from some other source. Given the size of the U.S. Federal deficit, however, any additional fmancia1 burden of this type would be undesirable.

Complex legal questions would also attend the establishment of a nonburdensome administrative claims procedure, including what criteria a complainant would have to meet to justify payment of claims arising from CWC implementation, and how the value of lost proprietary data would be quantified. Should Congress decide to set up a compensation mechanism, the implementing legislation might establish guidelines for assigning the ''burden of proof" to a company's claim that a CWC inspection resulted in the loss of a valuable trade secret. If the burden of proof is set too high (e.g., the requirement for an exact causal link), this test could probably not be met and companies would never be compensated for their losses. Yet if the burden of proof is set too low, the U.S. Government would effectively become an insurer of last resort for any loss of trade secrets, even those unrelated to CWC inspections. A reasonable balance between these alternatives might be to expect a firm to provide a ' 'preponderance of evidence" that a trade secret was lost as a direct result of treaty compliance and not through some other form of industrial espionage. Companies making claims might also be required

---

[49] Tanzman and Kellman, ''Legal Implications of the Multilateral Chemical Weapons Convention' op. cit., pp. 510-511.

[50] The ''discretionary function'' exemption, for example, provides that an administration official who exercises discretion within his delegated regulatory function cannot be held liable for the consequences of that decision.

[51] Edward A. Tanzman and Barry Kellman, *Harmonizing the Chemical Weapons Convention With the United States Constitution*, technical report No, DNA-TR-91-216 (Alexandria, VA: Defense Nuclear Agency, April 1992), p. 67.

to demonstrate that trade secrets were lost despite concerted efforts to protect them.[52]

International Trust Fund

The OPCW might establish its own administrative procedure for compensating companies or individuals for losses suffered as a result of CWC verification activities. In this case, the government of the inspected state would adjudicate or settle damage claims arising out of onsite inspections and would be reimbursed by the OPCW for somewhat less than 100 percent of the loss. All of the other States Parties would cover the reimbursement by paying into an international trust fund set up for this purpose. Since the United States will contribute about a quarter of the OPCW's budget, it would end up providing a substantial share of any trust fund set up to compensate industry, no matter who was at fault for the loss of trade secrets and without retaining any direct influence over the procedures established to adjudicate claims. Nevertheless, requiring all States Parties to the CWC to share in the costs of industrial espionage committed by members of the Technical Secretariat would give the participating states a stake in ensuring that the rules on handling confidential information are enforced to the maximum extent possible.[53] The proposal to create such an international trust fund may eventually be addressed by the PrepCom.

Industry Self-Insurance Scheme

The U.S. chemical industry might set up its own self-insurance fund, which would not have to be specified in the implementing legislation. Under such a scheme, chemical companies would contribute to the fund an amount proportional to their yearly profits or market share, and would be insured for the loss or theft of proprietary information during CWC implementation. All participating firms would then be able to submit damage claims to an adjudication process. U.S. industry is unlikely to support such a self-insurance scheme, however, on the grounds that companies should not be held responsible for any damages arising from treaty-mandated inspections. As a politically more viable alternative, a hybrid scheme might be established in which the U.S. Government provides some of the funding or assumes responsibility for the task of examining and adjudicating claims.

In sum, the drafters of the implementing legislation will need to decide whether to establish a mechanism for compensating firms for losses of proprietary information and, if so, the best way to go about it.

---

52 Prof. Barry Kellman, presentation on 'Implementing Legislation for the Chemical Weapons Convention, ' sponsored by The Committee for National Security, Washington, DC, Apr. 16, 1993,

53 Carnahan, ''chemic~ Arms Control, Trade Secrets, and the Constitution, ' op. cit., pp. 178-179.