Chapter 1.
INTRODUCTION TO CLASSIFICATION

THE NEED FOR CLASSIFICATION

A government is responsible for the survival of the nation and its people. To ensure that survival, a government must sometimes stringently control certain information that (1) gives the nation a significant advantage over adversaries or (2) prevents adversaries from having an advantage that could significantly damage the nation. Governments protect that special information by classifying it; that is, by giving it a special designation, such as "Secret," and then restricting access to it (e.g., by need-to-know requirements and physical security measures).

This right of a government to keep certain information concerning national security (secrets) from most of the nation's citizens is nearly universally accepted. Since antiquity, governments have protected information that gave them an advantage over adversaries. In wartime, when a nation's survival is at stake, the reasons for secrecy are most apparent, the secrecy restrictions imposed by the government are most widespread,[*] and acceptance of those restrictions by the citizens is broadest.[†] In peacetime, there are fewer reasons for secrecy in government, generally the government classifies less information, and citizens are less willing to accept security restrictions on information.

MAJOR AREAS OF CLASSIFIED INFORMATION

The information that is classified by most democracies, whether in peacetime or wartime, is usually limited to information that concerns the nation's defense or its foreign relations—military and diplomatic information. Most of that information falls within five major areas: (1) military operations, (2) weapons technology, (3) diplomatic activities, (4) intelligence activities, and (5) cryptology. The latter two areas might be considered to be special parts of the first three areas. That is, intelligence and cryptology are "service" functions for the primary areas—military operations, weapons technology, and diplomatic activities. From a historical perspective, the classification of weapons technology became widespread only in the 20th century. Classification of information about military operations and diplomatic activities has been practiced for millennia.

---

[*] "When a nation is at war many things that might be said in time of peace are such a hindrance to its effort that their utterance will not be endured so long as men fight and that no Court could regard them as protected by any constitutional right" [*Schenck v. United States*, 249 U.S. 47, 52 (1919) (J. Holmes)].

[†] Since the September 11, 2001, terrorist attacks against the World Trade Center towers and the Pentagon, the United States considers itself to be in a war against terrorism. One consequence has been a significant shift in opinion, not only of the general public but also of some strong supporters of freedom-of-information matters, towards favoring more control of information that might aid terrorists. This increased control, especially pertaining to weapons of mass destruction, includes (1) establishing broader criteria for identifying information that is classified or "sensitive"; (2) permitting reclassification of declassified information, and (3) restricting further governmental distribution of documents already released to the public.

Military-Operations Information

Examples of military-operations information that is frequently classified include information concerning the strength and deployment of forces, troop movements, ship sailings, the location and timing of planned attacks, tactics and strategy, and supply logistics. Obviously, if an enemy learned the major details of an impending attack, that attack would be less successful than if it came as a surprise to the enemy.[*] Information possessed by a government about an adversary's military activities or capabilities must be protected to preserve the ability to predict those activities or to neutralize those capabilities. If the adversary knew that the government had this information, the adversary would change those plans or capabilities. Military-operations information is usually classified for only a limited time. After an operation is over, most of the important information is known to the enemy.

Weapons Technology

Weapons technology is classified to preserve the advantage of surprise in the first use of a new weapon,[†] to prevent an adversary from developing effective countermeasures against a new weapon,[‡] or to prevent an adversary from using that technology against its originator (by developing a similar weapon). A major factor in that latter reason for classifying weapons technology is "lead time." Classifying advanced weapons-technology information prevents an adversary from using that information to shorten the time required to produce similar weapons systems for its own use. Consequently, assuming continued advancements in a weapons technology by the initial developer of that technology, the adversary's weapons systems will not be as effective as those of the nation that initially developed that technology, and the adversary will be at a disadvantage.

With respect to lead time, when weapons systems can be significantly improved, then information on "obsolete" weapons is much less sensitive than information on newer weapons. Thus, information on muzzle-loading rifle technology was not as sensitive as that on breech-loading rifle technology, which was not as sensitive as information on lever-action rifle technology, . . . semiautomatic rifle . . . automatic rifle . . . machine gun. However, with respect to nuclear weapons, a "rogue" nation or terrorist group can probably achieve its objectives just as easily with "crude" kiloton nuclear weapons that might require a ship or truck to transport as with sophisticated megaton nuclear weapons that might fit into a (large) suitcase. Thus, "obsolete" nuclear-weapons technology should be continue to be protected, especially with respect to technologies concerning production of highly enriched uranium or other nuclear-weapon materials.

---

[*]However, during the Greek and Roman eras in the Mediterranean, when the infantry was paramount and both sides were approximately equally equipped with respect to weapons, many battles were fought without attempts to maintain secrecy of troop movements or with respect to surprise attacks (B. and F. M. Brodie, *From Crossbow to H-Bomb*, Indiana University Press, Bloomington, Ind., 1973, p. 17).

[†]"Secret" weapons have proven decisive in warfare. One example of the decisive impact of a new weapon was at the battle of Crecy in 1346. At this battle, the English used their "secret" weapon, the longbow, to defeat the French decisively. Although the French had a two-to-one superiority in numbers (about 40,000 to 20,000), the French lost about 11,500 men, while the English lost only about 100 men (W. S. Churchill, *A History of the English-Speaking Peoples*, Vol. 1, Dodd, Mead and Co., New York, 1961, pp. 332-351; B. and F. M. Brodie, *From Crossbow to H-Bomb*, Indiana University Press, Bloomington, Ind., 1973, pp. 37-40).

[‡]In World War II, the Germans developed an acoustic torpedo designed to home in on a ship's propellers. However, the Allies obtained advance information about this torpedo so that when it was first used by the Germans, countermeasures were already in place (B. and F. M. Brodie, *From Crossbows to H-Bombs*, Indiana University Press, Bloomington, Ind., 1973, p. 222).

Weapons technology includes scientific and technical information related to that technology. World War I marked the start of the "modern" period when science and technology affected the development of weapons systems to a greater degree than any time previously.[1] That interrelationship became even more pronounced in World War II, with notable scientific and technological successes: the atomic bomb, radar, and the proximity fuse. World War II, particularly with respect to the atomic bomb, marked the first time that the progress of military technology was significantly influenced by scientists, as contrasted to advances by engineers or by scientists working as engineers.[2]

With respect to classification, the more that applied scientific or technical information is uniquely applicable to weapons, the more likely that this information will be classified. Generally, basic research is not classified unless it represents a major breakthrough leading to a completely new weapons system. An example of that circumstance was the rigid classification during World War II, and for several years thereafter, of much basic scientific research related to atomic energy (nuclear weapons).

Diplomatic Activities

The need for secrecy in diplomatic negotiations and relations has long been recognized. A nation's ability to obtain favorable terms in negotiations with other countries would be diminished if its negotiating strategy and goals were known in advance to the other countries.[*] The effectiveness of military-assistance agreements between nations would be impaired if an adversary knew of them and could plan to neutralize them. In *New York Times v. United States*, the "Pentagon Papers" case, U.S. Supreme Court Justice Stewart recognized the importance of secrecy in foreign policy and national defense matters:

> It is elementary that the successful conduct of international diplomacy and the maintenance of an effective national defense requires both confidentiality and secrecy. Other nations can hardly deal with this Nation in an atmosphere of mutual trust unless they know that their confidences will be kept . . . . In the area of basic national defense the frequent need for absolute secrecy is, of course, self evident.[3]

During the term of the first U.S. president, it was established that some need for secrecy in diplomatic matters would remain even after negotiations were completed. President Washington, in 1796, refused a request by the House of Representatives for documents prepared for treaty negotiations with England and gave the following as one reason for refusal:

> The nature of foreign negotiations requires caution, and their success must often depend on secrecy; and even when brought to a conclusion a full disclosure of all the measures, demands, or eventual concessions which may have been proposed or contemplated would be extremely impolitic; for this might have a pernicious influence on future negotiations, or produce immediate inconvenience, perhaps danger and mischief, in relation to other powers.[4]

---

[*] In 1921, the United States, Britain, France, Italy, and Japan held a conference to limit their naval armaments. The United States had broken Japan's diplomatic code and thereby knew the lowest naval armaments that Japan would accept. Therefore, U.S. negotiators had merely to wait out Japan's negotiators to reach terms favorable to the United States (J. Bamford, *The Puzzle Palace*, Houghton, Mifflin Co., Boston, 1982, pp. 9-10).

It has been said that President Nixon initially was not going to attempt to stop the New York Times and other newspapers from publishing the "Pentagon Papers." However, the executive branch was then in secret diplomatic negotiations with China, and Henry Kissinger "is said to have persuaded the president that the Chinese wouldn't continue their secret parleys if they saw that Washington couldn't keep *its* secrets."[5]

Intelligence Activities

Intelligence information includes information gathering and covert operations. Collecting military and diplomatic information about other nations involves the use of photoreconnaissance airplanes and satellites, communication intercepts, the review of documents obtained openly, and other overt methods. However, information gathering also includes the use of undercover agents, confidential sources, and other covert methods. For those covert activities, secrecy is usually imposed on the identity of agents or sources, on information about intelligence methods and capabilities, and on much of the information received from the covert sources. Few clandestine agents could be recruited (or, in some instances, would live long) if their identity were not a closely guarded secret. Information provided by a clandestine agent must frequently be classified because, if a government knew that some of its information was compromised, it might be able to determine the identity of the person (agent) who provided the information to its adversary. Successful intelligence-gathering methods must be protected so that the adversary does not know the degree of their success and is not stimulated to develop countermeasures to stop the flow of information. Intelligence information from friendly nations is generally classified by the recipient country. Allies would be less willing to share intelligence information if they knew that it would not be protected against disclosure.

Cryptology

Cryptology encompasses methods to code and transmit secret messages and methods to intercept and decode messages. Writing messages in code, or cryptography,[*] has been practiced for thousands of years. One of the earliest preserved texts of a coded message is an inscription carved on an Egyptian tomb in about 1900 B.C.[6] The earliest known pottery glaze formula was written in code on a Mesopotamian cuneiform tablet in about 1500 B.C.[7] The Spartans established a system of military cryptography by the 5th century B.C.[8] Persia later used cryptography for political purposes.[9] Cryptography began its steady development in western civilization starting about the 13th century, primarily in Italy.[10] By the early 16th century, Venice's ruling Council of Ten had an elaborate organization for enciphering and deciphering messages.[11]

Restrictions on cryptologic information are necessary to protect U.S. communications. Diplomatic negotiations could not successfully be conducted at locations other than the seat of government if safe communications could not be established. Cryptologic information must also be protected to prevent an adversary from learning of a nation's capabilities to intercept and decode messages. If an adversary learns that its communications are not secure, it will use another method, which will require additional time and effort to defeat.[*] The Allies' World War II success in breaking

[*] The breaking of codes is termed cryptanalysis.

[*] Even "friendly" nations get upset if they know that one of their codes has been broken. As noted earlier in this chapter, the United

the German codes contributed to shortening that war.[12] That success was kept secret until 1974, about 34 years after the German code had been broken and about 29 years after World War II had ended. The U.S. Army's success in breaking a World War II U.S.S.R. code (the Venona project, which began in 1943 and continued until 1980) was not made public until about 1995. That was about 50 years after the first such message had been deciphered (and about 45 years after the U.S.S.R. had learned through espionage of the Army's success).

BASIS FOR CLASSIFICATION IN THE UNITED STATES

The need for governmental secrecy was directly recognized in the U.S. Constitution. Article I, Sect. 5, of the Constitution explicitly authorizes secrecy in government by stating that "Each House shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as in their Judgment require Secrecy." Also included in the Constitution, in Article I, Sect. 9, is a statement that "a regular Statement and Account of the Receipts and Expenditures of all public Money shall be published from time to time." A U.S. Court of Appeals has determined that the phrase "from time to time" was intended to authorize expenditures for certain military or foreign relations matters that were intended to be kept secret for a time.[13]

The Constitution does not explicitly provide for secrecy by the Executive Branch of the U.S. Government. However, the authority of that Executive Branch to keep certain information secret from most U.S. citizens is implicit in its executive responsibilities, which include the national defense and foreign relations.[14] This presidential authority has been upheld by the Supreme Court in a number of cases.[15] Judicial decisions have also relied on a common-law privilege for a government to withhold information concerning national defense and foreign relations.[16] Congress, by two statutes, the Freedom of Information Act and the Internal Security Act of 1950, has implicitly recognized the president's authority to classify information (see Chapter 3).

At this time in the United States, information is classified either by presidential authority, currently Executive Order 12958, or by statute, the Atomic Energy Act of 1954, as amended (Atomic Energy Act). Classification under Executive Orders and under the Atomic Energy Act is extensively discussed in Chapters 3 and 4, respectively.

CLASSIFICATION AND SECURITY

States deciphered Japan's diplomatic code in 1921. Herbert O. Yardley, who was principally responsible for breaking this code, wrote a book, *The American Black Chamber*, published in 1931, which included information on this matter. Yardley's book did not contribute to developing friendly United States-Japanese relations. A consequence of this revelation was enactment of a U.S. statute that made it a crime for anyone who, by virtue of his employment by the United States, obtained access to a diplomatic code or a message in such code and published or furnished to another such code or message, "or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States" (48 Stat. 122, June 10, 1933, codified at 18 U.S.C. Sect. 952.)

Classification has been variously described as the "cornerstone" of national security, the "mother" of security, and the "kingpin" of an information security system.[17,18,19,20] Classification *identifies* the information that must be protected against unauthorized disclosure. Security determines *how to protect* information after it is classified.[21] Security includes both personnel security and physical security.

The initial classification determination, establishing what should not be disclosed to adversaries and the level of protection required, is probably the most important single factor in the security of all classified projects and programs.[22,23] None of the expensive personnel-clearance and information-control provisions (physical security aspects) of an information security system comes into effect until information has been classified; classification is the pivot on which the whole subsequent security system turns (excluding security for other reasons, such as to prevent theft of materials). [19] Therefore, it is important to classify only information that truly warrants protection in the interest of national security.[24]

Since the mid 1970s, several classification experts have remarked on the increasing emphasis by some government agencies on physical-security matters, which has been accompanied by a decreased emphasis on the classification function. One of the founders (and the first chairman) of the National Classification Management Society (NCMS), who was also an Atomic Energy Commission Contractor Classification Officer, has expressed concern about the tendency to emphasize the word "security" at the expense of the word "classification" with respect to security classification of information.[17] In the mid 1980s another charter member of the NCMS pointed out that, although the status of classification still remained high in the Department of Energy (DOE), the situation had changed within the Department of Defense, where Classification Management had been organizationally placed under Security.[25] Even the NCMS, founded as a classification organization, appears to be changing to become increasingly oriented towards security matters rather than classification matters.[26] It is noteworthy that the marked emphasis by the U.S. Government in recent years on physical-security measures has not been accompanied by any significant increased emphasis on classification matters.

The previous paragraph was written in 1989, and the trend described in that paragraph has continued. The classification function at DOE headquarters is now a part of the security organization as is the classification function at many DOE operations offices and DOE-contractor organizations. That function generally used to be part of a technical or other non-security organization. The NCMS has also continued to become more security-oriented.

With respect to classification as a profession (or lack of recognition thereof), it is interesting to note some comments and a recommendation in the *Report of the Commission on Protecting and Reducing Government Secrecy*.[27] In this 1997 report, that Commission noted the "all-important initial decision of whether to classify at all,"[28] and that "this first step of the classification management process . . . tends to be the weakest link in the process of identifying, marking, and then protecting the information."[29] The Commission further stated that "the importance of the initial decision to classify cannot be overstated."[30] However, the Commission then stated that "classification and declassification policy and oversight . . . should be viewed primarily as information management issues which require personnel with subject matter and records management expertise."[31] Although recommending that "The Federal Government . . . [should]

create, support, and promote an information systems security career field within the Government,"[32] the Commission made no similar recommendation for security classification of information as a profession or career. *Res ipsa loquitur*.

REFERENCES

[1] B. and F. M. Brodie, *From Crossbow to H-Bomb*, Indiana University Press, Bloomington, Ind., 1973, p. 172. Hereafter this book is cited as "Brodie."

[2] Brodie, p. 233.

[3] *New York Times v. United States*, 403 U.S. 713, 728 (1971).

[4] J. D. Richardson, *A Compilation of Messages and Papers of the Presidents*. 1789-1897, U.S. Government Printing Office, Washington, D.C., Vol. I, at 194-195 (1896).

[5] Richard Gid Powers, "Introduction," in *Secrecy–The American Experience*, by Daniel Patrick Moynihan, Yale University Press, New Haven, Conn., 1998, p. 32.

[6] D. Kahn, *The Codebreakers*, MacMillan, Inc., New York, 1967, p. 71. Hereafter cited as "Kahn."

[7] Kahn, p. 75.

[8] Kahn, p. 82.

[9] Kahn, p. 86.

[10] Kahn, p. 106.

[11] Kahn, p. 109.

[12] See, for example, F. W. Winterbotham, *The Ultra Secret*, Harper & Row, New York, 1974.

[13] *Halperin v. CIA*, 629 F.2d 144, 154-162 (D.C. Cir., 1980).

[14] U.S. Constitution, Article II, §2.

[15] See, for example, *Totten v. United States*, 92 U.S. 105 (1875); *United States v. Reynolds*, 345 U.S. 1 (1952); *Weinberger v. Catholic Action of Hawaii*, 454 U.S. 139 (1981).

[16] F. E. Rourke, *Secrecy and Publicity: Dilemmas of Democracy*, Johns Hopkins Press, Baltimore, 1961, pp. 63-64.

[17] D. B. Woodbridge, "Footnotes," *J. Natl. Class. Mgmt. Soc.* **12** (2), 120-124 (1977), p.122.

[18] R. J. Boberg, "Panel–Classification Management Today," *J. Natl. Class. Mgmt. Soc.* **5** (2), 56-60 (1969), p. 57.

[19] E. J. Suto, "History of Classification," *J. Natl. Class. Mgmt. Soc.* **12** (1), 9-17 (1976), p.13.

[20] James J. Bagley, "NCMS - Now and the Future," *J. Natl. Class. Mgmt. Soc.* **25**, 20-29 (1989), p. 28.

[21] T. S. Church, "Panel–Science and Technology, and Classification Management," *J. Natl. Class. Mgmt. Soc.* **2**, 39-45 (1966), p. 40.

[22] W. N. Thompson, "Security Classification Management Coordination Between Industry and DOD," *J. Natl. Class. Mgmt. Soc.* **4** (2), 121-128 (1969), p. 121.

[23] W. N. Thompson, "User Agency Security Classification Management and Program Security," *J. Natl. Class. Mgmt. Soc.* **8**, 52-53 (1972), p. 52.

[24] *Department of Defense Handbook for Writing Security Classification Guidance*, DoD 5200.1-H, U.S. Department of Defense, Mar. 1986, p. 1-1.

[25] F. J. Daigle, "Woodbridge Award Acceptance Remarks," *J. Natl. Class. Mgmt. Soc.* **21**, 110-112 (1985), p. 111.

[26] D. C. Richardson, "Management or Enforcement," *J. Natl. Class. Mgmt. Soc.* **23**, 13-20 (1987).

[27] *Report of the Commission on Protecting and Reducing Government Secrecy*, S. Doc. 105-2, Daniel Patrick Moynihan, Chairman; Larry Combest, Vice Chairman, Commission on Protecting and Reducing

Government Secrecy, U.S. Government Printing Office, Washington, D.C., 1997. Hereafter cited as the "Moynihan Report."

[28] Moynihan Report, p. 19.

[29] Moynihan Report, p. 35.

[30] Ibid..

[31] Moynihan Report, p. 44.

[32] Moynihan Report, p. 111.