

UNCLASSIFIED

## Center for Cryptologic History Brochures

Use this [form](#) to order a copy of any of these publications.

[All brochures are unclassified]

### ***Solving the Enigma: History of the Cryptanalytic Bombe***

Traces the history of the development of the cryptanalytic Bombe during WWII. It discusses the history of the Bombe from the time the Poles solved the Enigma, through the British involvement in developing the machine, the Navy contract with National Cash Register Corp. to build an American version, and, finally, the Allied successes against German U-boats in the North Atlantic.

### ***The Start of the Digital Revolution: SIGSALY - Secure Digital Voice Communications in World War II***

A brief overview of the revolutionary effort to provide secure voice communications for high-level government officials.

### ***Army Security Agency Aerial Reconnaissance: Mission and Sacrifice.***

Describes the use of Army aircraft for D/F and ELINT collection, primarily during the Vietnam War.

### ***Sharing the Burden: Women in Cryptology during World War II.***

A brief look at the contributions and sacrifices made by women as civilian and military cryptologists during WWII.

### ***American Cryptology: Two Centuries of Tradition***

A synopsis of the role of cryptology in the American Revolution, Civil War, interwar period, and World Wars, and concluding with the establishment of the National Security Agency.

### ***The Cipher Disk***

Invented in Italy sometime before 1470, the cipher disk represented a breakthrough in ease of encipherment and decipherment. This basic invention survived to be used until several years after the First World War.

***The Cryptographic Mathematics of Enigma***

A first-time discussion of the derivation of the exact number of theoretical cryptographic key settings and machine configurations for the Enigma cipher machine. Also calculates the number of practical key settings Allied cryptanalysts were faced with daily during WWII. Shows the relative contribution each component of the Enigma added to the overall strength of the machine.

***Listening to the Rumrunners***

A brief history of the use of COMINT in tracking down the smugglers of illegal liquor during Prohibition.

***The National Cryptologic Museum***

A description of the CCH-sponsored museum, its history and highlights.

***Origins of NSA***

From the Army's Cipher Bureau to Herbert Yardley's Black Chamber to the Signal Intelligence Service through the various organizational maneuverings that led eventually to the formation of the National Security Agency.

***Pioneers in U.S. Cryptology***

The lives of Herbert O. Yardley, William F. Friedman, Captain Laurance F. Safford, Rear Admiral Joseph N. Wenger, Frank B. Rowlett, Elizebeth Smith Friedman, and Agnes Meyer Driscoll.

***Radio Intelligence on the Mexican Border, World War I: A Personal View***

In this interview, a member of the Radio Intelligence Service recalls his service on the U.S.-Mexican border from 1918 to 1919 monitoring the threat of a German-Mexican alliance.

### ***Rare Books in the National Cryptologic Museum***

This brochure looks at some of the most rare and interesting books ever published on cryptology publications dating from the 16th to the early 20th centuries and representing authors from all over Europe.

---

### ***The Venona Story***

Discusses the topics in the six public releases of Venona translations and related documents. These topics are:

1. Soviet atomic bomb espionage,
2. New York KGB messages of 1942 and 1943,
3. New York and Washington KGB messages of 1944 and 1945,
4. San Francisco and Mexico City KGB messages, GRU New York and Washington messages, and Washington Naval GRU messages,
5. KGB and GRU messages from Europe, South America, and Australia, and
6. Messages inadvertently left out of the previous five updates of the previously issued translations.

---

### Return to CCH Hardcopy Publications

Content Owner: [Feedback](#)  
Web POC: [Feedback](#)

Last Modified: Friday, February 28, 2003 08:39:44 by nsr  
Last Reviewed: February 28, 2003  
Next Review: 180 days

[REDACTED]

Approved for Release by NSA on 08-17-2006, FOIA Case # 42848



# Center for Cryptologic History Publications Sources In Cryptologic History

(b) (3) - P.L. 86-36

Use this form to order a copy of any of these publications.

[Document classification is indicated after description]

**(U) A Collection of Writings on Traffic Analysis - Number 4, 1993.**

(U) (Vera R. Filby) Selected articles from NSA journals discussing developments in and concepts of traffic analysis as it has been viewed by different analysts over the past forty or more years. [TOP SECRET CODEWORD NOFORN NOCON]

**(U) The Friedman Legacy: A Tribute to William and Elizebeth Friedman - Number 3, 1992.**

(U) The classic six lectures by William F. Friedman, dean of American cryptologists. In Friedman's words, these lectures were designed to "create an awareness of the background, development and manner of employment of a science that is the basis of a vital military offensive and defensive weapon known as cryptology." Also includes articles on the Friedmans by Lambros Callimahos and James Chiles, as well as a posthumous tribute to Elizebeth. [UNCLASSIFIED]

**(U) A Reference Guide to Selected Historical Documents Relating to NSA/CSS, 1931-1985 - Number 2 [TOP SECRET CODEWORD]**

**(U) The Collected Writings of Brigadier John H. Tiltman - Number 1. 1981. (Edited by Henry F. Schorreck and William M. Nolte)**

(U) Views on codemaking and breaking from the British classical cryptologist whose sixty years' experience in the profession began in 1920s India and ended with his retirement from NSA in 1980. [SECRET CODEWORD]

Approved for Release by NSA on 08-17-2006, FOIA Case # 42848

Return to CCH Hardcopy Publications

Content Owner: [Feedback](#)  
Web POC: [Feedback](#)

Last Modified: Friday, February 28, 2003 08:44:40 by nsr  
Last Reviewed: February 28, 2003  
Next Review: 180 days

SECRET//COMINT//X1

(b) (1)  
(b) (3) - 50 USC 403  
(b) (3) - 18 USC 798  
(b) (3) - P.L. 86-36

# Center for Cryptologic History Special Series Crisis Collection

Use this form to order a copy of any of these publications.

[Document classification is indicated after description]

~~(S//SI)~~ [Redacted] : A Cryptologic History - 1993. Special Series Crisis Collection, Vol. 8. (Vera R. Filby)

(U) A case study of the SIGINT response to an unexpected and destabilizing Soviet military action. [TOP SECRET GAMMA B/TK NOFORN NOCON]

~~(S//SI)~~ The Capture of the USS Pueblo and Its Effect on SIGINT Operations - 1992. Special Series Crisis Collection, Vol. 7. (Robert E. Newton)

(U) Discussion of the events leading up to the capture of the SIGINT collector USS Pueblo, the actual capture, the extent of compromise of cryptographic information, and lessons learned. [TOP SECRET CODEWORD NOFORN NOCON]

(U) Supporting the Desert Warriors: The Role of the National Security Agency's Information Systems Security Organization in Operation DESERT SHIELD/DESERT STORM - 1992. Special/Crisis Series, Vol. 6. (Charles W. Baker)

(U) Documentation of the contributions, successes, and problems of NSA's ISSO during the Gulf War. [SECRET NOFORN]

(U) Shield and Storm: The Cryptologic Community in the Desert Operations - 1992. Special/Crisis Series, Vol. 5. (David A. Hatch)

(U) A review of the contributions of the U.S. SIGINT System during Operations DESERT SHIELD and DESERT STORM. [TOP SECRET CODEWORD NOFORN NOCON]



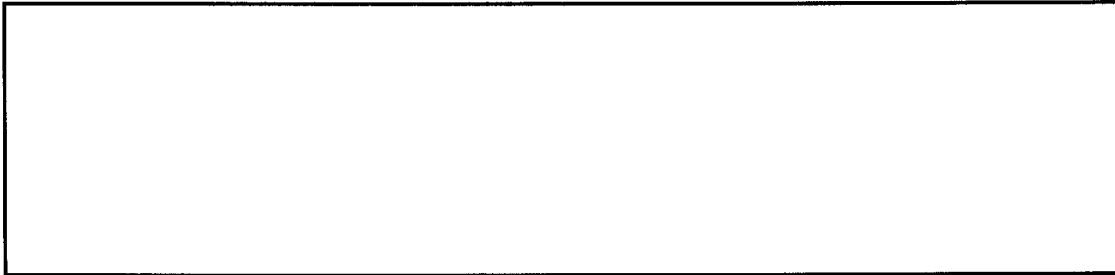
~~(S//SI)~~ **The National Security Agency and the EC-121 Shootdown - 1989.**  
Special/Crisis Series, Vol. 3. (Thomas P. Ziehm)

(U) The origin and purposes of the flight, NSA's response to the shootdown, the subsequent investigations, and the resulting changes in the U.S. aerial reconnaissance program, warning procedures, and the development of the National SIGINT Operations Center. [TOP SECRET CODEWORD]

(b) (1)  
(b) (3)-50  
USC 403  
(b) (3)-18  
USC 798  
(b) (3)-P.L.  
86-36

~~(S)~~ **The Suez Crisis: A Brief COMINT History - 1988.** Special/Crisis Series, Vol. 2.  
(Robyn G. Winder)

(U) A study of the 1956 crisis from an intelligence perspective, focusing on how SIGINT is conducted during a "brushfire" situation when set in a unique intelligence dilemma in which two U.S. allies (Britain and France) opposed American policy objectives. [TOP SECRET CODEWORD NOFORM]



~~(S//SI)~~ **Attack on a SIGINT Collector, the USS Liberty - 1981.** Special/Crisis Series, Vol. 1. (William D. Gerhard and Henry W. Millington)

(U) The technical rationale for the Liberty mission, the particulars of the Israeli miscalculation, the details of U.S. communications failures, a narrative of the attack and of attempts to minimize the compromise of cryptologic materials, and the lessons learned. Also addressed, how U.S. SIGINT agencies organized their response to requirements brought on by this crisis. [TOP SECRET CODEWORD NOFORM]

Return to CCH Hardcopy Publications

Content Owner: Feedback  
Web POC: Feedback

Last Modified: Friday, February 28, 2003 08:45:35 by nsr  
Last Reviewed: February 28, 2003  
Next Review: 180 days

~~SECRET//COMINT//SI~~

DERIVED FROM: NSA/CSS MANUAL 123-2  
DATED: 24 FEB 1998  
DECLASSIFY ON: X1

SECRET//COMINT//X1

## Center for Cryptologic History Regular Series Histories

Use this [form](#) to order a copy of any of these publications.

[Document classification is indicated after description]

**(U) Pullin' Ponyals: A History of Russian Voice Transcription at the National Security Agency and Its Predecessors, 1949-1970.** 2002, Series VI, Vol. 8. (James Y. Blanchard)

~~(C//SI)~~ Discusses the origins of Russian voice exploitation in the military services and the early days of Russian voice transcription at the Armed Forces Security Agency and the National Security Agency. [TOP SECRET//COMINT//X1]

**(U) Spartans in Darkness: American SIGINT and the Indochina War, 1945-1975.** 2002, Series VI, Vol. 7. (Robert J. Hanyok)

~~(S//SI)~~ Relates the story of the involvement of the U.S. SIGINT system in the Vietnam conflict from the end of World War II to the conclusion of U.S. participation in the mid-1970s. Includes discussions of the critical role of SIGINT during the Gulf of Tonkin crisis and how it influenced America's entry into the war; the controversy over whether the intelligence community predicted the Tet Offensive in 1968; how Hanoi "won" the cryptologic battle; how the course of the pivotal battle of Dien Bien Phu in 1954 was monitored by the COMINT agencies of France, the United States, and the Viet Minh; the air war, the Ho Chi Minh Trail, Saigon's COMINT service, and the fall of Saigon. [TOP SECRET//COMINT//X1]

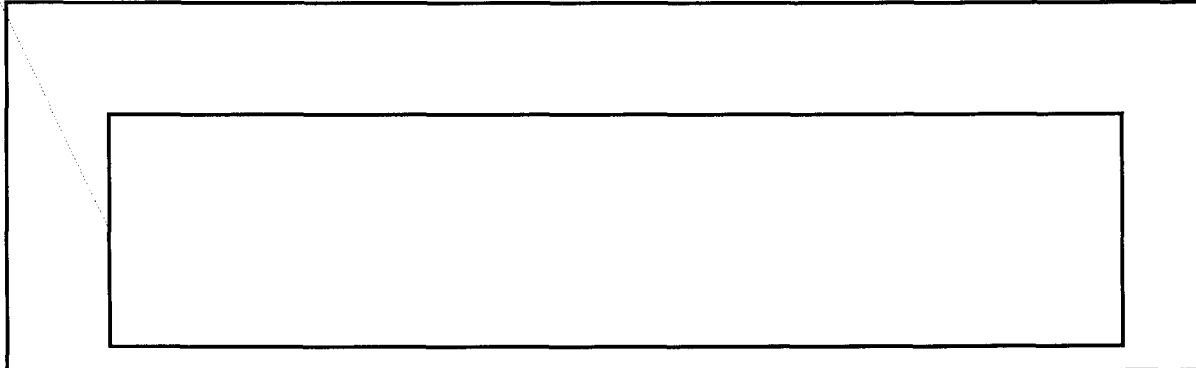
**(U) The Invisible Cryptologists: African-Americans, WWII to 1956.** 2001. Series V, Vol. 5 (Jeannette Williams)

(U) This history tells the story of African-Americans employed by NSA and its predecessors from 1939 to the mid-1950s. It is the story of the movement of African-Americans from a segregated society and a segregated workplace to their joining the mainstream. The story is both infuriating and inspiring. [UNCLASSIFIED]

**(U) So Power Can Be Brought into Play: SIGINT and the Pusan Perimeter.** 2000. Series V, Vol. 4 (Jill E. Frahm)

(U) An unclassified study of how the Armed Forces Security Agency - NSA's immediate predecessor - and the service cryptologic agencies supported the U.S. 8th Army during a critical period of the Korean conflict. [UNCLASSIFIED]

(b) (3)-P.L.  
86-36



(U) **The Korean War: The SIGINT Background.** 2000. Series V, Vol. 3 (David A. Hatch with Robert Louis Benson)

An unclassified general overview of the Korean conflict from a cryptologic perspective. Provides some initial answers to some of the more important questions about intelligence support. [UNCLASSIFIED]

(U) **A History of U.S Communications Intelligence during World War II: Policy and Administration (U) 1997. Series IV, Vol. 8.** (Robert Louis Benson)

(U) A discussion of how Army and Navy COMINT activities were run as well as how COMINT was structured in the Coast Guard, FBI, and FCC. The Military Intelligence Service and Office of Naval Intelligence are also discussed at length. Chronicles the growth of U.S. cooperation with the United Kingdom in COMINT activities. [UNCLASSIFIED]

(U) **The Quiet Heroes of the Southwest Pacific Theater: An Oral History of the Men and Women of CBB and FRUMEL - 1997. Series IV, Vol. 7.** (Sharon A. Maneki)

(U) A collection of reminiscences of men and women who served at Central Bureau Brisbane and Fleet Radio Unit Melbourne during World War II. The COMINT produced by these organizations was often a major factor in decision making by General MacArthur and other leaders in their efforts to resist Japanese advances in the Pacific and to retake captured territory. [UNCLASSIFIED]

(U//FOUO) **American Cryptology during the Cold War, 1945-1989, Books I-IV - 1995-1999. Series VI, Vol. 5.** (Thomas R. Johnson)



(U) A four-part history of the U.S. cryptologic system in the post-World War II period. Details the responses of the SIGINT system to the challenges of that era, analyzes how events and personalities affected the development of cryptology institutionally and professionally, and discusses the success or failure of cryptologic operations in the various crises that have challenged the SIGINT system. [TOP SECRET CODEWORD TK]

[REDACTED]

(U) A study of the development of the Soviet problem following World War II. [TOP SECRET CODEWORD]

~~(S//SI)~~ NSA's Involvement in U.S. Foreign SIGINT Relationships through 1993 - 1995. Series VI, Vol. 4. [REDACTED]

(U) A review of NSA's Second and Third Party relationships and the evolving factors leading to the present NSA national responsibilities for management, funding, control, and liaison responsibilities for them. [TOP SECRET CODEWORD NOFORN]

(b) (3) - P.L. 86-36

[REDACTED]

(U) A study of the events leading to the establishment of an important Third Party relationship. [TOP SECRET CODEWORD NOFORN]

(U) Essential Matters: A History of the Cryptographic Branch of the People's Army of Viet-Nam, 1945-1975 - 1994. Special Series, No. 5. (David W. Gaddy)

(U) A translation of a 1990 Vietnamese publication, including a supplement on cryptography in the Border Guard from 1959-1989. [UNCLASSIFIED]

(U) Pearl Harbor Revisited: United States Navy Communications Intelligence, 1924-1941 - 1994. Series IV, Vol. 6. (Frederick D. Parker)

(U) The results of research into Japanese Navy messages which remained untranslated until 1945 and undiscovered until now. These messages revealed the Japanese Navy's plans for war with the U.S., Britain, and the Netherlands and the preliminary exercises which occurred in the months before the attack on Pearl Harbor. [UNCLASSIFIED]

**(U) PURPLE DRAGON: The Origin and Development of the United States OPSEC Program - 1993. Series VI, Vol. 2. (Stephen J. Kelley)**

(U) Discusses the genesis of Operations Security during the Vietnam War. Describes the initial problems in air operations which prompted a high-level investigation, explains the weaknesses in U.S. practices which the investigation identified, shows how Operations Security principles were developed, and tells how Operations Security became institutionalized. [TOP SECRET CODEWORD NOFORN]

**(U) Masked Dispatches: Cryptograms and Cryptology in American History, 1775-1900 - 1993. Series I, Vol. 1. (Ralph E. Weber)**

(U) A collection of essays on specific episodes in U.S. history in which cryptology played a key role. [UNCLASSIFIED]

**(U) A Priceless Advantage: U.S. Navy Communications Intelligence and the Battles of Coral Sea, Midway, and the Aleutians - 1993. Series IV, Vol. 5. (Frederick D. Parker)**

(U) A discussion of the use to which communications intelligence was put in these significant battles of World War II. [UNCLASSIFIED]

**(U) The Origins of the National Security Agency - 1990. Series V, Vol. 1. (Thomas L. Burns)**

(U) The story of the struggle to control a unique resource - a competition that the author contends continues to the present day. [TOP SECRET CCO]

**~~(S//SI)~~ The Cryptology of the German Intelligence Services - 1989. Series IV, Vol. 4. (David P. Mowry)**

(U) Detailed descriptions of the cryptographic systems used by German intelligence organizations and their agents in Latin America as well as systems used on a number of agent circuits in Europe. [TOP SECRET CODEWORD]

**~~(S)~~ German Clandestine Activities in South America in World War II - 1989. Series IV, Vol. 3. (David P. Mowry)**

(U) First of a two-part history of German clandestine activities in South America. A thorough account of the German intelligence agencies engaged in clandestine work in South America that addresses the



(U) Tracing the birth, growth, and final demise of a successful experiment - [REDACTED]

~~(C)~~ **Technical Research Ships, 1956-1969 - Special Series, Vol. 2. (George F. Howe)**

(U) A record of these seaborne SIGINT platforms' unique and valuable contributions, the unusual management and control problems they posed, and the tragic international incidents that hastened their demise. [TOP SECRET CODEWORD NOFORN]

~~(S//SI)~~ **Space Surveillance SIGINT Program - Special Series, No. 3.**

(U) A study of the program developed by NSA during 1960-61 in an effort to provide an adequate U.S. collection capability to meet high priority SIGINT requirements related to Soviet space activities. [SECRET CCO]

~~(S//SI)~~ **Focus on Cambodia, Parts One and Two. 1974. Cryptologic History Series (SEA)** [REDACTED]

(U) An account of the SIGINT support rendered to U.S. forces during the Cambodia cross-border operations of May and June 1970. [TOP SECRET CODEWORD]

~~(U)~~ **SIGINT Applications in U.S. Air Operations - 1972. Cryptologic History Series (SEA)** [REDACTED] William Gerhard).

(U) A discussion of SIGINT operations and the use made of SIGINT by the Air Force and Navy in Southeast Asia during the 1960s. [TOP SECRET CODEWORD]

~~(U)~~ **Working against the Tide Parts One and Two. 1970. Cryptologic History Series (SEA)** [REDACTED]

(U) The story of the attempts of U.S. COMSEC monitors and analysts to bring security to the voluminous wartime communications during the Vietnam War. [TOP SECRET CODEWORD NOFORN]

~~(S//SI)~~ **Focus on Khe Sanh - 1969. Cryptologic History Series (SEA). (Theodore Lukacs).**

(U) Recounts SIGINT assistance to the U.S. forces, particularly the

26th Marines, during the North Vietnamese attempt to take the Khe Sanh Combat Base in early 1968. [TOP SECRET CODEWORD]

~~(S//SI)~~ **In the Shadow of War (To the Gulf of Tonkin) - 1969.** Cryptologic History Series (SEA). (William Gerhard).

(U) Documents the joint NSA-SCA involvement in Southeast Asia in the years between the end of World War II and the Gulf of Tonkin incident of August 1964. [TOP SECRET CODEWORD NOFORM]

**(U) It Wasn't All Magic: The Early Struggle to Automate Cryptanalysis, 1930s-1960s.** 2002, Special Series, Vol. 6. [REDACTED]

(U) Follows and links the development of automatic data processing from the critical conceptual work of the 1930s through the practical experiments born of national necessity in WWII to the postwar development and the previously untold story of NSA's postwar computer development. [TOP SECRET//COMINT//X1]

(b) (3) - P.L. 86-36

Return to CCH Hardcopy Publications

Content Owner: [Feedback](#)  
Web POC: [Feedback](#)

Last Modified: Tuesday, May 27, 2003 10:48:06 by nsr  
Last Reviewed: May 27, 2003  
Next Review: 180 days

~~SECRET//COMINT//X1~~

DERIVED FROM: NSA/CSS MANUAL 123-2  
DATED: 24 FEB 1998  
DECLASSIFY ON: X1

SECRET//COMINT

# Center for Cryptologic History Histories by Subject

Use this form to order a copy of any of these publications.

## Cold War

- (U) American Cryptology during the Cold War (1945-1989)
- (U) The Korean War: The SIGINT Background
- [Redacted]
- ~~(S//SI)~~ Operation REGAL: The Berlin Tunnel
- ~~(S//SI)~~ The Capture of the USS Pueblo and Its Effect on SIGINT Operations
- [Redacted]
- (U) So Power Can Be Brought into Play: SIGINT and the Pusan Perimeter

## Famous Personalities

- ~~(S)~~ The Collected Writings of Brigadier John H. Tiltman
- (U) The Friedman Legacy: A Tribute to William and Elizebeth Friedman

## Middle East

- ~~(S//SI)~~ Attack on a SIGINT Collector, the USS Liberty
- (U) Shield and Storm: The Cryptologic Community in the Desert Operations
- (U) Supporting the Desert Warriors: The Role of the National Security Agency's Information Systems Security Organization in Operation DESERT SHIELD/ DESERT STORM
- ~~(S)~~ The Suez Crisis: A Brief COMINT History

## NSA

- ~~(U//FOUO)~~ American Cryptology during the Cold War (1945-1989)
- (U) The Origins of the National Security Agency
- (U) The Invisible Cryptologists: African-Americans, WWII to 1956.

## Second and Third Party Relationships

- [Redacted]
- ~~(S//SI)~~ NSA's Involvement in U.S. Foreign SIGINT Relationships through 1993

## Vietnam

- (U) Essential Matters: A History of the Cryptographic Branch of the People's Army of Viet-Nam, 1945-1975

- (U) PURPLE DRAGON: The Origin and Development of the United States OPSEC Program
- (U) Focus on Cambodia, Parts One and Two.
- ~~(S//SI)~~ Focus on Khe Sanh
- ~~(S//SI)~~ In the Shadow of War (To the Gulf of Tonkin)
- (U) SIGINT Application in U.S. Air Operations
- (U) Working against the Tide, Parts One and Two.
- (U) Spartans in Darkness: American SIGINT and the Indochina War, 1945-1975

## World War II

- (U) A History of U.S. Communications Intelligence during World War II: Policy and Administration
- (U) The Quiet Heroes of the Southwest Pacific Theater: An Oral History of the Men and Women of CBB and FRUMEL
- (U) Pearl Harbor Revisited: United States Navy Communications Intelligence, 1924-1941
- (U) A Priceless Advantage: U.S. Navy Communications Intelligence and the Battles of Coral Sea, Midway, and the Aleutians
- ~~(S//SI)~~ The Cryptology of the German Intelligence Services
- ~~(C)~~ German Clandestine Activities in South America in World War II
- ~~(C)~~ A New View to Pearl Harbor: United States Navy Communications Intelligence
- ~~(S//SI)~~ American Signals Intelligence in Northwest Africa and Western Europe

---

### Return to CCH Hardcopy Publications

Content Owner: [Feedback](#)  
Web POC: [Feedback](#)

Last Modified: Friday, February 28, 2003 08:42:06 by nsr  
Last Reviewed: February 28, 2003  
Next Review: 180 days

~~SECRET//COMINT//X1~~

DERIVED FROM: NSA/CSS MANUAL 123-2  
DATED: 24 FEB 1998  
DECLASSIFY ON: X1

[REDACTED]

(b) (3) - P.L. 86-36

## Center for Cryptologic History Other Publications

Use this [form](#) to order a copy of any of these publications.

[Document classification is indicated after description]

### **(U) *The Voynich Manuscript: An Elegant Enigma - 1978* (Mary D'Imperio)**

(U) A study of what has been called the "most mysterious manuscript in the world." The actual Voynich Manuscript is a small quarto volume without covers composed in the fifteenth or sixteenth century by an unknown author, written on vellum by an unknown scribe in an unknown script, and containing colored drawings of unidentified botanical, astronomical, and astrological objects and human figures.

[UNCLASSIFIED]

---

### Return to CCH Hardcopy Publications

Content Owner: [Feedback](#)  
Web POC: [Feedback](#)

Last Modified: Friday, February 28, 2003 08:43:58 by nsr  
Last Reviewed: February 28, 2003  
Next Review: 180 days

[REDACTED]

Approved for Release by NSA on 08-17-2006, FOIA Case # 42848