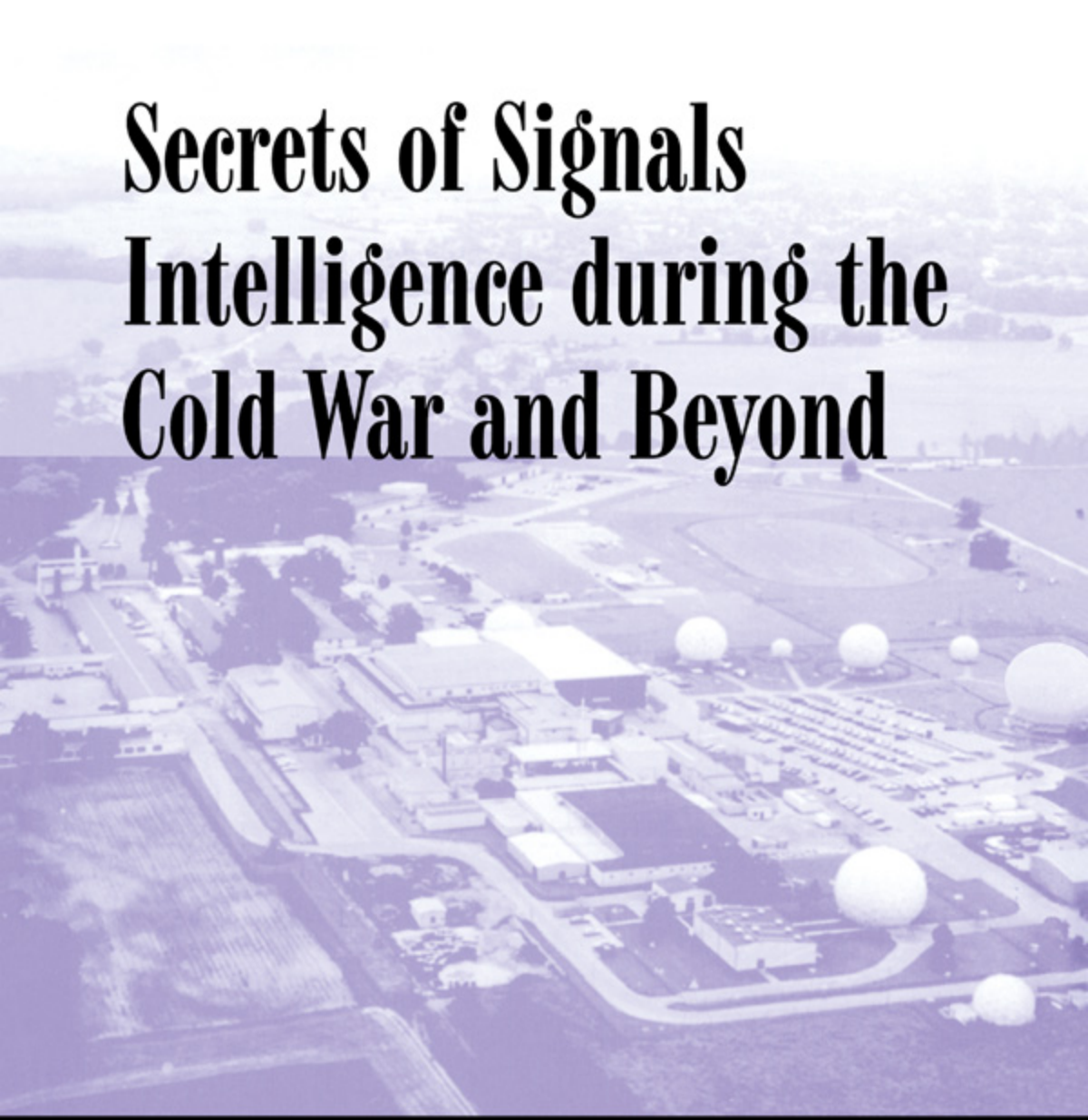
Secrets of Signals Intelligence during the Cold War and Beyond



Editors
MATTHEW M. AID AND CEES WIEBES
With a Foreword by CHRISTOPHER ANDREW

CASS SERIES: STUDIES IN INTELLIGENCE
(Series Editors: Christopher Andrew and Michael I. Handel;
Wesley K. Wark and Richard J. Aldrich)
ISSN 1368-9916

Secrets of Signals Intelligence during the Cold War and Beyond

Also in this series

American-British-Canadian Intelligence Relations, 1939–2000 edited by David Stafford and Rhodri Jeffreys-Jones

The Clandestine Cold War in Asia, 1945–65 edited by Richard J. Aldrich, Gary Rawnsley and Ming-Yeh Rawnsley

Allied and Axis Signals Intelligence in World War II edited by David Alvarez

The Norwegian Intelligence Service 1945–1970: Northern Vigil by Olav Riste

British Military Intelligence in the Crimean War, 1854–1856 by Stephen Harris

Intelligence and the Cuban Missile Crisis edited by James G. Blight and David A. Welch

Knowing Your Friends: Intelligence Inside Alliances and Coalitions from 1914 to the Cold War edited by Martin S. Alexander

Eternal Vigilance? 50 Years of the CIA edited by Rhodri Jeffreys-Jones and Christopher Andrew

Nothing Sacred: Nazi Espionage Against the Vatican, 1939–1945 by David Alvarez and Revd Robert A. Graham

Intelligence Analysis and Assessment edited by David Charters, A. Stuart Farson and Glenn P. Hastedt

Intelligence and Imperial Defence: British Intelligence and the Defence of the Indian Empire 1904–1924 by Richard J. Poppelwell

Espionage: Past, Present, Future? edited by Wesley K. Wark

Codebreaker in the Far East by Alan Stripp

Secrets of Signals Intelligence during the Cold War and Beyond

Editors

MATTHEW M. AID

Kroll Associates, Washington DC

CEES WIEBES

Netherlands Institute for War Documentation and University of Amsterdam

FRANK CASS

LONDON • PORTLAND, OR

First published 2001 in Great Britain by
FRANK CASS PUBLISHERS
2 Park Square, Milton Park,
Abingdon, Oxon, OX14 4RN

and in the United States of America by
FRANK CASS PUBLISHERS
270 Madison Ave,
New York NY 10016

Transferred to Digital Printing 2005

Website: www.frankcass.com

Copyright © 2001 Frank Cass & Co. Ltd.

British Library Cataloguing in Publication Data

Secrets of signals intelligence during the Cold War and beyond. – (Studies in intelligence)
1. Electronic surveillance – History – 20th century – Congresses 2. Cold War – Electronic intelligence – Congresses
1. Aid, Matthew M. II. Wiebes, Cees
327.1'2'09045

ISBN 0 7146 5176 1 (cloth)
ISBN 0 7146 8182 2 (paper)
ISSN 1368-9916

Library of Congress Cataloging-in-Publication Data

Secrets of signals intelligence during the Cold War and beyond / edited by Matthew M. Aid & Cees Wiebes.
p. cm. – (Cass series – studies in intelligence, ISSN 1368-9916)
Includes bibliographical references and index.
ISBN 0-7146-5176-1 – ISBN 0-7146-8182-2 (pbk.)
1. Electronic intelligence – Congresses. 2. Electronic surveillance–Congresses. 3. Cold War–Congresses. I. Aid, Matthew M., 1958– . II. Wiebes, Cees. III. Series.
UB255 .S43 2001
327.12--dc21 2001028241

Printed and bound by Antony Rowe Ltd, Eastbourne

This group of studies first appeared in a Special Issue on 'Secrets of Signals Intelligence during the Cold War and Beyond' of *Intelligence and National Security* 16/1 (Spring 2001) published by Frank Cass (ISSN 0268-4527).

All rights reserved. No part of this publication may be reproduced, stored in or introduced into a retrieval system or transmitted in any form, or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher of this book.

Jacket illustration: Aerial view of the US National Security Agency's Sigint station at Bad Aibling, Bavaria, Germany.
Us Army Intelligence and Security Command

Contents

Foreword

Signals intelligence (Sigint) was the best kept secret of the Cold War – so well preserved that most histories of that era do not even mention it. Though the Central Intelligence Agency (CIA) quickly became a household name, the National Security Agency (NSA), which runs American Sigint operations, remained almost invisible throughout the Cold War. The small circle of those in the know in Washington joked that NSA stood for 'No Such Agency'. NSA, however, has a far bigger budget than the CIA, employs far more people, and generates far more intelligence.

Since the end of the Cold War NSA has become a little less mysterious. One veteran of the era of total secrecy complained to me a few years ago that NSA now stood for 'Nothing Sacred Anymore'. It still, however, attracts far less public and scholarly interest than the CIA. Though Sigint is a basic fact of modern international relations, even the word remains largely unknown.

Part of the reason why most scholars ignore Sigint is the continued classification of most of the huge historical archive which it has generated. The main reason for its neglect, however, has been what psychologists call cognitive dissonance – the difficulty all of us have in grasping new concepts which disturb our existing view of the world. Sigint is just such a concept. Most scholars working on the international relations of the twentieth century have been unable to come to terms with it.

From 1945 onwards, for example, almost all histories of the Second World War mentioned the American success in breaking the main Japanese diplomatic cipher over a year before the attack on Pearl Harbor. But, until the revelation of the Ultra Secret in 1973, it occurred to almost no historian (save for former intelligence officers who were forbidden to mention it) that there might have been major Sigint successes against Germany as well as Japan. Even after the disclosure of Ultra's important role in British and American wartime operations in the West, it took another 15 years before any historian raised the rather obvious question of whether there was a Russian Ultra on the Eastern Front as well.[1]

Many of the historians who now acknowledge the significance of Sigint in the Second World War still ignore it completely in their studies of the

Cold War. This sudden disappearance of Sigint from the historical landscape immediately after VJ Day has produced a series of eccentric anomalies even in some of the leading studies of policy-makers and international relations. Thus, for example, Sir Martin Gilbert's massive and mostly authoritative multi-volume official biography of Churchill acknowledges his passion for Sigint as war leader but includes not a single reference to his continuing interest in it as peacetime prime minister from 1951 to 1955. There is even less about Sigint in biographies of Stalin. Indeed, it is difficult to think of any history of the Soviet Union which devotes as much as a sentence to the enormous volume of Sigint generated by the KGB and GRU.[2] Studies of the presidency of George Bush (the first) invariably ignore his candid admission that Sigint was a 'prime factor' in his foreign policy – just as they neglect the use of Sigint by other post-war presidents.[3]

Hence the importance of this path-breaking collection edited by Matthew M. Aid and Cees Wiebes. They and the other contributors to this study have brought together a wider and more innovative range of material on the role of Sigint since the Second World War than has ever been published before. Sigint's importance, as they demonstrate, extended far beyond the Cold War superpowers. They are right to argue that intelligence studies need to become more 'internationalist' and take more account of intelligence in middle-ranking and minor powers, some of whom have highly significant liaison arrangements with the major players.

This volume confronts all historians of the Cold War and international relations specialists with a major challenge which most so far have ducked: either to seek to take account of the role of Sigint since the Second World War or to explain why they do not consider it necessary to do so.

CHRISTOPHER ANDREW
Cambridge, May 2001

NOTES

1. Geoff Jukes, 'The Soviets and "Ultra"', *Intelligence and National Security* 3/2 (April 1988) pp.233–47. Though Jukes's conclusions are debatable, his article remains a path-breaking study.
2. Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive: The KGB in Europe and the West* (London: Penguin 1999) Chapter 21.
3. Christopher Andrew, *For The President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush* (London: HarperCollins 1995) p.5 and Chapter 13.

Illustrations

This page intentionally left blank

Preface

The Cold War passed into history in 1989–91 with the dissolution of the Soviet Union and its allies bound together in the Warsaw Pact. The American, Canadian and European intelligence communities had to change their focus and attention shifted to different emerging threats like rogue states, money laundering, drug kingpins, organised crime and terrorists but also to environmental disasters and large-scale refugee problems. Partly because of this transformation in the world of intelligence more and more students of the Cold War begin to realise that the Western intelligence communities played an important role between 1945 and 1990. In recent years in particular the importance of Signals Intelligence (Sigint) has been emphasised and especially the capabilities and possibilities of reading and deciphering diplomatic, military, commercial and other communications of foreign nations.

This growing awareness of the importance of intelligence applies not only to the activities of the big services but also to those of the smaller nations like for example the Netherlands. For this exact reason a couple of years ago the Netherlands Intelligence Studies Association (NISA) was established in which academics and (former and still active) members of the Netherlands intelligence community work together in order to promote research into the history of Dutch intelligence communities. This growing interest had led in Holland to publications dealing with the history of the Dutch internal security service (1995), the Dutch Navy intelligence (1997) and the Netherlands foreign intelligence service (1998).

While the NISA hosts an international conference every two years it was this time decided to organise a congress dealing with 'The Importance of Sigint in Western Europe during the Cold War 1945–1999'. This conference took place on Saturday 27 November 1999 in Amsterdam. The speakers came from the United States, Norway, Germany, Great Britain, the Netherlands and altogether six papers were presented. This Sigint work is a spin-off of this conference, which was a great success with more than 100 participants from 11 different countries. The readers can not only find the expanded version of the papers presented at this Sigint conference but also additional contributions on the topic of Sigint in Canada and France. This

study also contains an introduction on the topic of the importance of Sigint and will end with conclusions regarding the eight different contributions.

Any questions regarding the activities of the NISA should be addressed to P.O. Box 18 210, 1001 ZC Amsterdam, the Netherlands. The editors of this work can be contacted at: Matthew M. Aid <mmaid@starpower.net> and Cees Wiebes <wiebes@pscw.uva.nl>.

1

Introduction: The Importance of Signals Intelligence in the Cold War

MATTHEW M. AID and CEES WIEBES

Today, our knowledge of about the role and importance of Signals Intelligence (Sigint) in the years after the end of World War II can only be described as an inventory of ignorance. The distinguished British historian Christopher Andrew has written that 'The biggest gap in our knowledge of United States intelligence collection during the Cold War concerns the role of Sigint. No history of the Second World War nowadays fails to mention the role of the Anglo-American codebreakers in hastening victory over Germany and Japan. By contrast, most histories of the Cold War make no reference to Sigint at all.'[1] By the same token, our lack of knowledge about role played by Sigint in countries outside the United States is deeper and even more profound.

Part of the problem stems from the heavy shroud of secrecy that has covered this immensely important subject for so long. Too many academics, researchers and journalists in the US, Europe and elsewhere still speak about the subject *sotto voce*, fearful of the strictures of the Official Secrets Act and similar laws that effectively bar public discussion of this subject. Another factor is that because of its technical nature, Sigint is an extremely difficult subject for the layman to understand, which has deterred academics and journalists from examining the subject in any depth, and what coverage there has been remains focused on the trials and tribulations of World War II.[2]

It is certainly true that Sigint lacks the glamour and sex appeal that surrounds the exploits and derring-do of secret agents, which have dominated the post-war literature on intelligence. One writer has put it thus: 'For many, Sigint conjures up images of grey men eavesdropping on conversations, cracking codes, and installing large-dish antennas. Compared with human intelligence, Sigint can seem rather boring and, frankly, a little grubby.'[3]

Moreover, partisans of the more traditional art of Human Intelligence (Humint), have been less than kind to Sigint in the past. For years the authors of this study have been told horror stories about the failings of Sigint from past or present practitioners of Humint. Former CIA officials, seeking to enhance the reputation of the CIA's clandestine service, have been particularly harsh in their public criticism of the National Security Agency (NSA) and other forms of technical intelligence gathering. In the best-selling novel *Tinker, Tailor, Solder, Spy*, George Smiley, John le Carré's master spy, voiced the widely-held opinion of many Humint professionals about their more technically-oriented counterparts in the intelligence services, saying: 'We all have our prejudices and radio men are mine. They're a thoroughly tiresome lot in my experience, bad fieldmen and overstrung, and disgracefully unreliable when it comes down to doing the job.'[4]

As a result, for more than 50 years Sigint professionals around the world have been forced to fight in complete secrecy an uphill battle arguing the value of radio intelligence. Oftentimes, the adherents of Sigint lost these bureaucratic battles against the numerous and usually more powerful partisans of Humint. A former senior Indian intelligence officer recalled that 'We dithered in creating an integrated set-up for signal interception... because of the pressures from our sprawling network of spies and human analysts, led by a technically illiterate bureaucracy.'[5]

And so, despite the latent prejudice and immense secrecy surrounding the subject, the question has been asked: why was Sigint so important during the Cold War? This contribution and the others that follow suggest that the history of post-World War II intelligence must be radically rewritten to take into account the important contributions made to the security of the United States and the nations of Western Europe by this arcane and difficult to understand intelligence discipline.

WHAT IS SIGNALS INTELLIGENCE?

An US Army publication defines Sigint as intelligence derived from the intercept, analysis, and parametric exploitation of foreign communications and non-communications radio-electronic emissions.[6] An US Marine Corps manual defines Signals Intelligence (Sigint) as 'intelligence gained by exploiting an adversary's use of the electromagnetic spectrum with the aim of gaining undetected firsthand intelligence on the adversary's intentions, dispositions, capabilities, and limitations'.[7]

Sigint is composed of three separate but interrelated intelligence collection techniques: communications intelligence (Comint), electronics intelligence (Elint), and foreign instrumentation signals intelligence

(Fisint).[8] Communications Intelligence (Comint) is intelligence information derived from the intercept and processing of voice, Morse code, radioteletype, facsimile, multichannel (or microwave radio relay), and video signals. Comint does *not* include the interception of unencrypted written communications (mail), the monitoring of foreign public media or propaganda broadcasts, the interception of communications obtained during counterintelligence investigations, or wartime censorship activities.[9]

For example, during the 1950s and 1960s NSA intercept operators around the world spent most of their time monitoring and transcribing radio traffic concerning the day-to-day routine activities at foreign military bases around the world, such as communications from airfield control towers or ground stations directing aircraft movements, the radio traffic of ground forces manoeuvring in the field, ship-to-ship and ship-to-shore naval radio traffic, foreign military and civilian weather broadcasts, and air-to-ground civilian airline communications.[10] During the Cold War, a typical American Comint target was the routine activity at Soviet airfields in East Germany and elsewhere. NSA voice intercept operators monitored the early morning radio checks from the air base, followed by radio traffic among the control tower, the firing range controller, the taxi strip monitor, the bombing range controller, the weather station, the aerial intercept controller, the ground safety crews, and the radar operators. The intercept operators then tracked the routine training flights of the base's combat aircraft as they practised aerial intercepts or bombing attacks at ranges near the airfield. This required listening to hours of mundane air-to-air and/or air-to-ground radio chatter, which in turn required further hours to transcribe and process every day.[11]

Electronics Intelligence (Elint) is concerned with the interception and analysis of emissions from foreign electronic devices. The most common Elint targets are the wide variety of radar systems used around the world for early warning, missile detection, ground control intercept, missile targeting, fighter target vectoring, and altitude determination.[12] Through Elint, these radar systems can be identified by their function and type, their range and capabilities assessed, and their locations precisely fixed.[13] This intelligence information is principally of interest to the military because, as a recently declassified US Air Force document put it: 'By counting radars, specifying their precise location, determining their ranges, and evaluating their operational systems, analysts and engineers could develop countermeasures capable of jamming offensive surface-to-air missile radars and other defensive radars.[14] Other Elint targets include navigation aids and radio beacons which provide geographic position information to ships, aircraft and other vehicles; air-to-air and air-to-ground identification signals, such as Identification, Friend or Foe (IFF) transponders, repeaters and interrogators; emissions from countermeasures equipment and radio

jamming devices; radiation from missile guidance systems and artillery fuses; and emissions from meteorological devices, diathermy, radio heating, and research and development laboratories and field testing stations working on electronic devices.[15]

Fisint is defined as the collection and processing of emissions associated with the testing and operational deployment of aerospace, surface, and subsurface systems, which may have either military or civilian application. Fisint includes but is not limited to monitoring telemetry from ballistic missiles as well as manned and unmanned space vehicles, beaconry, electronic interrogators, tracking/fusing/arming/command systems, and video data links which relay data to a ground station concerning performance of space vehicles or weapons systems. As such, Fisint is the Sigint collection discipline primarily associated with the monitoring of foreign weapons research and development activities, including but not limited to ballistic missile testing.[16]

Finally, in the last decade Sigint has become deeply involved with a new kind of electronic communications medium: digital data communications signals, which refers to the transmission of vast amounts of digital data among and between computer systems and networks. A good example of the traffic passing along this medium is electronic bank transfer data. NSA and its English-speaking Sigint partners refer to data traffic by the covername 'Proforma'.[17]

THE IMPORTANCE OF SIGINT

Since the dawn of time, all governments have wanted to know what their friends and allies were doing. In justifying the continuing need for the huge Russian radio intercept station at Lourdes, Cuba, in December 2000 the Russian newspaper *Izvestia* wrote that 'Not a single state has yet been able to deny itself the temptation to learn more about other states (especially those it sees as rivals) than they would like to tell.'[18] And that the easiest way to do this is to listen to the secret communications of foreign governments. The former head of the US Navy Communications Intelligence Organisation, Captain (later Vice Admiral) Joseph N. Wenger, wrote that 'The ambition of every nation has been to develop unbreakable ciphers for its own use and to solve every cipher in use by its actual or potential enemies.'[19]

By its very nature, Sigint has certain intrinsic qualities, which make it a particularly effective intelligence-gathering tool.

The first is that Sigint is a passive intelligence collection technique that generally is conducted without the target's knowledge. Moreover, Sigint collects information against communications targets that are oftentimes thousands of miles away, thus negating the need for the intercept sites to be

near the targets being monitored. This means, generally speaking, that Sigint involves relatively little political or physical risk.[20] There was one exception to this rule, however. This was the peripheral aerial and maritime reconnaissance missions conducted by all sides during the Cold War, which resulted in a number of reconnaissance platforms either being destroyed or captured. A total of 146 NSA military and civilian personnel were killed in the line of duty during the Cold War, 60 of whom were killed in Vietnam. The single worst loss occurred during the Israeli attack on the NSA spy ship USS *Liberty* in June 1967, which resulted in the death of 34 Navy, Marine and NSA civilian cryptologists.[21]

By comparison, Humint collection during the Cold War was a particularly risky proposition. For example, the CIA, MI6, as well as the Norwegian, French, West German, and Turkish intelligence services lost more than 300 agents during attempts to infiltrate the Soviet Union between 1949 and 1955; plus several hundred more operatives who were lost trying to establish agent networks in Eastern Europe during the 1950s.[22] Between 1951 and 1953, 212 Chinese agents trained by the CIA were parachuted into northern China. According to declassified CIA documents, 101 of the agents were killed and 111 were captured.[23] Of the 49 CIA agents parachuted into Chinese-occupied Tibet between 1957 and 1960, only 12 survived. Of the remainder, 37 were killed or committed suicide, one surrendered, and one was captured by the Chinese.[24] Between 1958 and 1966, the CIA and Taiwanese lost 120 agents who were parachuted into mainland China as part of an operation called 'Grosbeak'.[25] Finally, according to a recent South Korean news report, between 1950 and 1972 a staggering 7,726 Korean agents working for American or South Korean intelligence were killed or disappeared while spying inside North Korea.[26]

Second, the objectivity and reliability of Sigint is great, but far from perfect. Former CIA Director Vice Admiral Stansfield Turner wrote in 1991 'electronic intercepts may be even more useful [than agents] in discerning intentions. For instance, if a foreign official writes about plans in a message and the United States intercepts it, if he discusses it and we record it with a listening device, those verbatim intercepts are likely to be more reliable than second-hand reports from an agent.'[27] A retired senior CIA officer opined that Humint can never be free from the biases and perceptions of its sources, that the information is oftentimes deemed tainted because it came from traitors motivated by greed or personal grievances, or that it was obtained by corrupting or seducing vulnerable human beings.[28] But in its raw form, Sigint reproduces exactly what it records in an unvarnished, unbiased and undistorted fashion. This historically has given Sigint tremendous credibility with intelligence consumers, particularly since paranoia on both sides of the Iron Curtain created an atmosphere that led analysts inherently

to question the credibility of every secret agent that came forward. A former CIA intelligence analyst was quoted as saying of Sigint's reliability that 'You know the origin and you know that this is genuine. It's not like a clandestine [Humint] report where you don't know if this is a good agent or a weak agent or a bad agent or a double agent.'[29] But another CIA officer was recently quoted as saying of Sigint that 'Electronic intercepts are great, but you don't know if you've got two idiots talking on the phone', suggesting that the reliability of a particular intercept is largely dependent on the seniority of the sender and receiver of the transmission.[30]

For example, some senior CIA intelligence analysts questioned the reliability of the information provided by Colonel Oleg Penkovskiy, in large part because the CIA's Clandestine Service would not tell them where the information came from.[31] A Top Secret 1976 study of CIA estimates on the Soviet military found that 'Because the Soviet Union remains a uniquely closed society, human contacts, traditionally the principal source of foreign intelligence, play a distinctly subordinate role in the preparation of these documents: not only is such information exceedingly scarce, but it is always suspect of being the product of a deliberate disinformation effort in which the Soviet government engages on a massive scale. Furthermore, information obtained from sensitive human sources often has such limited distribution that it does not play a significant part in the preparation of NIEs [National Intelligence Estimates].'[32]

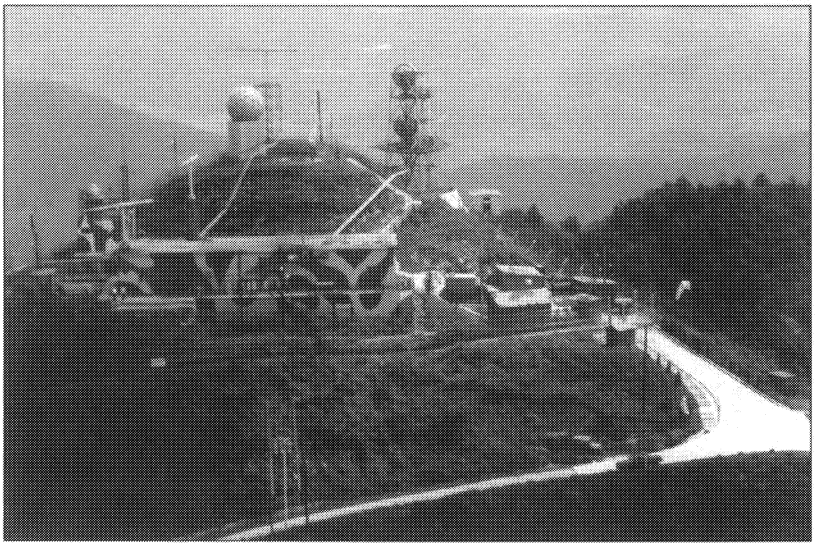
Third, unlike other sources, *some but certainly not all* Sigint intercepts can stand on their own without the need for analysis or correlation with other sources, although practitioners of the Sigint craft and 'all-source' intelligence analysts screech in dismay whenever this occurs. This led to the practice during the Cold War of the President of the United States and senior White House officials getting each morning a Top Secret intelligence summary from the CIA and an even more highly classified publication called the Black Book, containing the most important decrypts produced by NSA during the previous 24 hours, along with the Agency's commentary.[33] The same was true in the Soviet Union, where every day the KGB sent a selection of key intercepts in a bound volume called the Red Book to the top six members of the Politburo, although the KGB did not forward any materials contained in the decrypts which ran contrary to the prevailing political trends of the time within the Kremlin.[34] In Britain, the daily Sigint digest produced by GCHQ for the Prime Minister and senior Cabinet officials was called the Blue Book.[35] Individual Sigint reports produced by GCHQ were called Blue Jackets (BJs) because of the distinctive blue-coloured file folders that the reports came in.[36] The highly classified daily collection of diplomatic decrypts that was sent daily to the Dutch Cabinet was called the Green Edition. There were also special daily reports containing Sigint materials on

the Middle East (Red Edition), Latin America (Yellow Edition), and on economic intelligence matters (Blue Edition).[37]

Fourth, because of its reliability and the high-level attention that intelligence derived from Sigint received on both sides of the Iron Curtain, it proved to be (with apologies to U-2 and spy satellite aficionados) the premier source of information for national security officials and foreign policymakers during the Cold War. In 1966, Senator Milton Young of North Dakota stated that 'As far as foreign policy is concerned, I think the National Security Agency and the intelligence it develops has far more to do with foreign policy than does the intelligence developed by the CIA.'[38] In October 1998, John Millis, the late staff director of the House Permanent Select Committee on Intelligence, described Sigint as 'the INT of choice of the policy maker and the military commander'.[39] For example, Sigint has been used publicly by the US government in a number of instances, such as the Tonkin Gulf incidents (1964), the North Korean seizure of the USS *Pueblo* in 1968, and the C-130 (1958), EC-121 (1969), KAL 007 (1983) and Brothers to the Rescue (1996) shootdown incidents. President Ronald Reagan publicly justified the 1986 air strikes on Libya using NSA intercepts that reportedly linked Libya to the La Belle Disco bombing in West Berlin. By contrast, rare indeed have been the instances where major policy decisions have been significantly influenced or determined solely by information received from a human intelligence source.

Fifth, Sigint was usually the fastest source of current intelligence information available to consumers. A congressional intelligence committee official said of Sigint that 'it's there quickly when needed'.[40] Lieutenant General Daniel O. Graham, the former Director of the Defense Intelligence Agency (DIA), was quoted as saying 'Most collection agencies give us history. The NSA is giving us the present.'[41] During the Cold War, NSA emphasised the speedy delivery of finished Sigint to its customers because of the perishable nature of the product. Today, thanks to improvements in communications and data processing technologies, NSA can get the results of its Sigint collection efforts to its consumers in the field in near real-time.[42] NSA had its own dedicated communications system just for transmitting intercepts to Fort Meade, and another special distribution network called the SSO system for getting the finished product from NSA headquarters to its consumers. Between 1962 and 1965, NSA placed into operation the Critical Intelligence Communications (CRITICOMM), which allowed each of NSA's 150 Sigint collection and processing units around the world to bypass normal communications channels and transmit especially important intelligence information to Washington DC within 15 minutes.[43] NSA even had its own direct communications link with the White House, which was established shortly after the Cuban Missile Crisis, to feed the

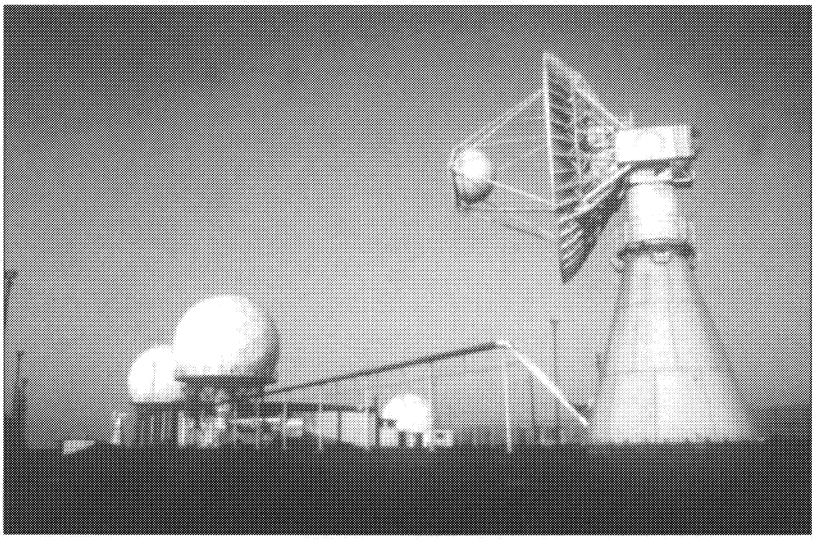
FIGURE 1.1



US Army 'Adventurer' border intercept site in South Korea.

US Army Intelligence and Security Command

FIGURE 1.2



US Army 'Hippodrome' space collection facility at Sinop, Turkey.

US Army Intelligence and Security Command

President of the United States and the National Security Council with key decrypts, thus bypassing the analysts at the CIA and DIA.[44]

As a result, Sigint intercepts usually found their way to consumers in far less time than imagery interpretation reports from satellites, and usually arrived weeks before Humint reports found their way to the hands of intelligence analysts.[45] For example, during the Cuban Missile Crisis in 1962, most CIA agent reporting from inside Cuba was accomplished by secret writing, which took a week or more to get to the CIA analysts from inside Cuba. Information derived from refugee interrogations was oftentimes months old by the time the Cubans were questioned by the CIA at Opa Locka, Florida.[46]

The Soviet experience was also the same. During the war in Afghanistan during the 1980s, the Russian Army depended on radio intercepts as their primary means of locating major units of Afghan guerrillas. The principal reason for the dependence on Sigint was that Russian field commanders found that the Humint reports that they received from the Afghan secret service – the Khad – almost always arrived to late to be of any tactical value.[47] This has meant that one of Sigint's most important functions was to provide forewarning of an enemy attack, something which slower intelligence sources, especially Humint, could not provide.

Sixth, Sigint produces more intelligence information on a broader range of subjects than any other intelligence source. In 1964 alone, NSA sent out approximately 150,000 finished intelligence reports and translations to its consumers in Washington, or more than 400 Sigint reports a day. By the end of the 1960s, this figure more than doubled to almost 400,000 finished intelligence reports being produced annually, which is the equivalent of more than 1,000 Sigint reports going to NSA's consumers every day.[48] By comparison, in 1960 the KGB deciphered 209,000 diplomatic cables sent by 51 countries, or the equivalent of 572 decrypts a day going to consumers.[49] In 1967, the KGB deciphered 188,400 diplomatic messages sent by 72 countries, or 516 decrypts a day.[50]

Seventh, Sigint never sleeps. Agents and their handlers must sleep (we are after all only human!), and darkness or adverse weather could shut down imagery collection systems for weeks at a time. But Sigint collects and produces intelligence 24 hours a day, 365 days a year, regardless of the weather or other environmental conditions.[51]

Eighth, Sigint is flexible and more responsive to consumer tasking than most other intelligence sources. A 1998 congressional report stated that 'much of NSA's past strength has come from its localised creativity and quick-reaction capability'.[52] You can quickly retarget Sigint, assuming that you possess the appropriate collection platforms and the manpower with the requisite skills to perform the mission. This made Sigint the source of

choice during fast moving world crises during the Cold War. For example, NSA was able to react to a series of Cold War crises faster than the rest of the US intelligence community, such as the Korean War, the Cuban Missile Crisis, and the Vietnam conflict.[53] You cannot, however, quickly change the tasking of agents nor build a new agent network overnight (unless of course you are a reporter for CNN); and the cost of retasking a spy satellite (and thus shortening its orbital life) was prohibitively expensive.

Ninth, intelligence insiders argue that Sigint's potential as an intelligence source is greater than all other intelligence collection disciplines. One successful solution of a major foreign cryptographic system can generate more intelligence information in a day than all other sources combined. A former American defence and intelligence official has written that a 'break' is the 'equivalent not of one but of a thousand spies, all ideally placed, all secure, and all reporting instantaneously'.[54] Even such a stalwart believer in Humint as the late Allen W. Dulles, the Director of the CIA from 1953 to 1961, opined that Sigint was 'the best and "hottest" intelligence that one government can gather about another'.[55]

And tenth, relative to all other intelligence disciplines, many intelligence 'insiders' consider Sigint to be one of the most cost effective means of gathering intelligence. American intelligence observers believe, for example, that despite NSA's huge workforce and budget, it produces on a dollar-for-dollar basis more 'bang for the buck' than any other intelligence source, with perhaps the exception of the National Reconnaissance Office's spy satellites.[56] This has been an extremely contentious issue within the US intelligence community for decades because of NSA's huge budget. The authors estimate that NSA and its predecessors have spent about $100 billion since 1945, 75 per cent of which was spent on Sigint and the rest on communications security.[57] More importantly, throughout the Cold War the US government spent four to five times as much money on Sigint than they did on Humint collection.[58]

There are no hard figures available for how much the Soviet Union and its allies spent on Sigint, but according to a former KGB official, by the late 1980s, Sigint collection was eating up 25 per cent of the KGB's annual budget.[59] But what is now clear is that by the early 1980s, the Soviet intelligence community, in particular the GRU, had come to depend to a greater degree on Comint because it proved to be a more productive source for strategic intelligence than the more traditional Humint sources.[60] According to a 1993 statement by Cuban Defence Minister Raul Castro, Russia got about 75 per cent of its strategic military intelligence information from the huge listening post at Lourdes, Cuba.[61]

The East German Sigint organisation, Hauptverwaltung III, was particularly successful during the Cold War. Throughout the 1970s and

1980s, the East German Sigint service eavesdropped on the telephone conversations of almost every important West German politician, including the sensitive conversations of former West German chancellor Helmut Kohl. The former head of the East German Sigint organisation, Major General Horst Männchen, told an interviewer that during the early 1980s, his service was intercepting approximately 40,000 West German telephone conversations per year, including those of the most senior members of the West German government.[62]

The result is that, as will be demonstrated throughout this work, Sigint was arguably the most important intelligence source for the US and its European allies during the Cold War. And since the demise of the Soviet Union, one can argue that the relative importance of Sigint has only increased. In the late 1950s, Sigint and U-2 imagery were producing about 75 per cent of the hard information available to the US intelligence community about the Soviet military.[63]

Dependence on Sigint by many Western European nations was even greater. For example, during the 1980s the vast majority (80–90 per cent) of the raw intelligence information reaching the British Joint Intelligence Committee in London every day came from Sigint.[64] In May 1999, British Foreign Secretary Robin Cook stated that 'GCHQ's work is vital in supporting our foreign and defence policies.'[65] The 2000 Annual Report of the British Parliament's Intelligence and Security Committee revealed that 'The quality of the intelligence gathered [by GCHQ] clearly reflects the value of the close co-ordination under the UKUSA agreement.'[66]

Sigint also accounted for the majority of the intelligence information generated by the Canadian intelligence community.[67] One informed observer has written that Canada's national Sigint organisation, the Communications Security Establishment (CSE), is that country's premier intelligence producer, adding that CSE was Canada's 'single-most important contributor to allied intelligence sharing agreements'.[68]

A 1952 French report stated that 'The study of enemy radio is by far our best source of intelligence.'[69] A 1973 memorandum to the Dutch Prime Minister described that nation's Sigint organisation as '[T]he most valuable asset we have to collect an intelligence product that is valuable to all interested parties.'[70]

PROBLEMS AND LIMITATIONS OF SIGINT

The following is a short summary of some of the basic weaknesses and limitations of Sigint, some of which apply to many of the other intelligence disciplines as well:

Secrecy of Sigint: Historically, because of the need to protect sensitive sources, Sigint intercepts were given extremely limited distribution with the highest levels of government and the military, and even then, only on a need-to-know basis.[71] A declassified 1952 US Army memorandum states: 'It is fully realised that enemy communications are probably the most sensitive of all intelligence sources, and that every precaution must be taken to protect the security of our efforts to exploit them.'[72] Each Comint report coming out of NSA during the 1950s and 1960s stated on its cover that 'This document is to be distributed and read by only those persons who are officially indoctrinated in accordance with communications intelligence security regulations and who need the information in order to perform their duties.'

There are numerous examples of the negative ramifications stemming from the decision to keep Sigint under wraps. The first was that few government officials ever came to fully appreciate Sigint. For example, a former senior NSA official has written that this high degree of secrecy 'preserved the anonymity (but also limited the appreciation) of the source' within the US intelligence community.[73] This also meant that, in many instances, government officials and military commanders who needed the information were denied access to Sigint because someone had determined that they did not have the 'need-to-know'.

A 1951 report concerning Comint support to the US Army during the Korean War found that the effectiveness of this crucial intelligence source was limited, in large part because the high security classification level of the intercepts prevented all but a few senior Army officers in Korea from seeing them. In addition, Army intelligence officers in Korea were barred by Comint security regulations from merging Comint with other forms of intelligence (such as Photint or Humint) into an 'all-source' intelligence product; and the sensitivity of the source oftentimes prevented Army field commanders from using the Comint information, leading some senior Army commanders in Korea to refer to Comint as a 'wasting asset'.[74] A 1951 report by a US Air Force inspection team found that Comint intercepts being generated by listening posts in Japan were so highly classified that they could not be distributed to most USAF intelligence consumers in Korea.[75] US Navy commanders in the Far East were also complaining that few combat commanders ever saw either tactical or strategic Comint during the Korean War because they did not possess the requisite security clearances.[76]

During the Vietnam War, NSA's Sigint coverage of North Vietnamese MiG flight activity was excruciatingly detailed and accurate, but because of security concerns NSA refused to give this highly perishable intelligence to the American pilots flying combat missions over North Vietnam. When

senior US Air Force and Navy commanders in Southeast Asia found out that NSA was collecting intelligence that could save the lives of American pilots, but was not distributing the intelligence because of security concerns, they were understandably furious.[77] Voicing the opinion of many soldiers in Southeast Asia, Command Sergeant Major John Martin, who served with the US Army Special Forces in Vietnam, recalled 'Because they [the US Army Sigint units and personnel] were so "special" you could never get them to work for you; you could only hope they would share something if it could save your ass. Other than those unusual situations, their info was just "too special" for us average boonie rats.'[78]

In the mid-1980s, American officials frequently hinted that they had 'indisputable evidence' [i.e. Sigint] demonstrating Nicaraguan and Cuban support for guerrilla forces operating in El Salvador. Despite calls for the evidence to be made public, the Reagan administration refused to release the materials because it would jeopardise sensitive intelligence sources and methods. This led a former CIA intelligence analyst to remark that 'Radio intercepts are not so novel, or so critical. They won't jeopardise anything... I can't believe that in the past years they wouldn't have been produced – so critical is this matter to US policy.' The analyst added that 'You don't save these expensive intelligence sources for the junior prom.'[79]

The United States was not the only country that applied these stringent security measures to protect their Sigint product. In the Soviet Union, Sigint intercepts were deemed so sensitive that they were delivered directly to a very small number of specially cleared consumers in the Politburo, the KGB and the GRU, thus bypassing regular intelligence analysis channels. Sigint sharing with the Soviet Union's allies in Eastern Europe was also specifically forbidden.[80]

In the British Foreign Office, a special messenger from the FO's Permanent Under Secretary's Department would periodically deliver copies of the Top Secret Blue Jacket reports from GCHQ to those few officials cleared to see them. After reading the reports, the GCHQ material was given back to the messenger, who returned them to the Permanent Under Secretary's office for storage. The rule was that there was never to be any mention of decrypts in official Foreign Office papers.[81]

In October 1975, senior officials of the Australian Sigint organisation, now known as the Defence Signals Directorate (DSD), apparently decided not to send to the Australian Prime Minister a sensitive intercept which revealed that the Indonesian military intended to kill five Australian journalists in East Timor covering the Indonesian invasion of that country. The DSD officials feared that Prime Minister Gough Whitlam would act on the information, thus revealing DSD's ability to read sensitive Indonesian

communications traffic. All five of the journalists were murdered by Indonesian special forces troops, and their bodies burned.[82]

Diminished Utility: The ability of consumers to use Sigint was strictly limited because of pervasive security considerations.[83] For example, during the Korean War, American Top Secret intelligence reports derived from Comint carried the following caveat emptor: 'Certain restrictions prohibit the further dissemination of this information either direct or paraphrased. Pertinent order of battle information included herein, that is not confirmed by other sources will be passed to divisions on a "need to know basis" only and will not be included in any routine intelligence reports or summaries.'[84]

During the 1950s and 1960s, every NSA Comint report carried the following edict on its cover: 'No action is to be taken on information herein reported, regardless of temporary advantage, if such action might have the effect of revealing the existence and nature of the source.'[85] Because of these limitations, US government officials and military commanders oftentimes found themselves severely circumscribed in how they could act on the Sigint that they received, which naturally diminished the utility of the intelligence to its consumers.[86]

Failure to believe Sigint: Cold War history is replete with many examples of government officials, military commanders, and intelligence analysts who chose not to believe the Sigint they received. In part, this was because the reader did not understand the information they received, or trust the reliability of the Sigint source. More often then not, the Sigint was misused or ignored because it did not fit some preconceived notion already held by the reader. Field-Marshal Lord Montgomery and General Douglas MacArthur, for example, were two commanders who did not particularly trust Sigint unless it confirmed their own personal assessments.[87]

During the Chinese Civil War, American intelligence analysts failed to heed information contained in decrypted Soviet clandestine radio traffic between Moscow and Mao Tse-tung's headquarters in Yenan, China, which revealed that as of October 1945, Mao's People's Liberation Army consisted of almost 1.1 million men under arms. A year later, in mid-1946, the US Army G-2 still was estimating that Mao's forces consisted of only 600,000 men, despite the fact that the PLA had by that time probably grown to almost two million men under arms.[88] During the war in Indochina in the early 1950s, some senior French commanders chose not to believe the information contained in decrypts of high-level Viet Minh military radio traffic because it did not match their assessments of the strength and capabilities of Ho Chi Minh's forces.[89]

Over-Reliance on Sigint. There are numerous examples of intelligence officials and military commanders placing undue reliance on Sigint to the exclusion of other sources of intelligence information. For instance, by the

late 1950s the US intelligence community was relying almost exclusively on Comint to provide warning of a Soviet military attack. Former senior CIA official Lyman Kirkpatrick stated that 'If the Soviets ever decided to go for broke, they wouldn't put anything on electronic communications or do anything visible by satellite. All the orders would go by officer couriers, which was what Hitler did at the Battle of the Bulge and caught us totally unprepared. We were relying too heavily on communications intelligence.'[90]

By the late 1970s, the US intelligence community had become so dependent on Sigint that in 1978, President Jimmy Carter said 'Recently... I have been concerned that the trend that was established about 15 years ago to get intelligence from electronic means might have been over-emphasised.'[91] A declassified 1976 CIA intelligence assessment confirmed that the Soviets also largely depended on Sigint as their primary source for strategic warning of a nuclear or conventional attack.[92]

The results of over-reliance on Sigint can be disturbing. The system backfired in November 1983, when Soviet Sigint stations in East Germany and Czechoslovakia detected the sudden cessation of radio traffic coming from American nuclear weapons units in West Germany, particularly among the units of the US Army's 56th Artillery Brigade, which was armed with Pershing nuclear missiles. This was followed by a change of ciphers and radio frequencies throughout the US Seventh Army. The Soviets interpreted these moves as indicative of an imminent nuclear attack by the US. In fact, it was only a nuclear release exercise, called 'Able Archer 83'.[93] Nevertheless, the Soviets were so alarmed that they placed many of their forces in Eastern Europe on alert. Between 2 and 11 November 1983, American and British Sigint stations in West Germany detected Soviet ground forces in East Germany and the Baltic Military District going to a heightened readiness status; Soviet air units in East Germany and Poland were placed on alert and routine training flights suddenly stopped; Soviet nuclear-capable fighter bombers were placed on runway alert on airfields in East Germany; and the Soviets suddenly ceased broadcasting weather reports throughout the Soviet Union and Eastern Europe.[94]

More recently, on 11 May 1998, the government of India tested three nuclear devices at the Pokhran nuclear test site in western India. Not surprisingly, the Indian nuclear tests dramatically heightened the state of tension between India and neighbouring Pakistan. Two weeks later, on 27 May 1998, the Signals Intelligence Directorate of the Indian Army intercepted and decrypted a message from the Pakistani Foreign Ministry in Islamabad to the Pakistani High Commission in New Delhi, which reported that Pakistan had 'credible information' that India was ready to mount a pre-emptive strike against Pakistani nuclear installations. The following day, 28 May 1998, Pakistan conducted its own series of nuclear tests. India publicly

denied that it had any intention of attacking Pakistani military installations, but the military forces of the two countries remained on hair-trigger alert for many weeks afterwards.[95]

Sigint Snobbery. As the importance of Sigint grew during the years after World War II, followed by the introduction of spy satellites in the 1960s, the value of Humint was rapidly marginalised within the American and British intelligence communities.[96] This led to a pervasive sense of snobbery and self-infatuation by the denizens of the Sigint community in the West. Intelligence insiders referred to this elitism as the 'Green Door' syndrome. This led Humint partisans to complain that greater credence was almost always given to Sigint over Humint.[97] A recently declassified NSA history noted that during the 1950s, many high-level intelligence reports referred to Humint and other collateral intelligence as 'unconfirmed information'. Only Sigint was deemed reliable enough to be described as 'a usually reliable source'.[98]

Talking about his experiences with the US Army Sigint organisation, the Army Security Agency (ASA), during the Vietnam War, one US Army officer wrote:[99]

> ASA came very close to total alienation from the [US Army] combat arms. This seemed to result partly from the avid devotion [by ASA] to the strategic [Comint] mission and its highly classified and controlled product, as well as a self-imposed snobbery and self-infactuation. Every combat arms officer from the Vietnam War I've met has his own story of the 'green door' syndrome and hyper-classification of signal intelligence from ASA. While ASA served the combat troops better than they realised during the conflict, the superior and separatist attitude of even tactical ASA units has left a bad taste in the mouths of many commanders even to this day. Those who don't dread our attachment to their commands in the future look forward to 'straightening us out' and making 'real' soldiers of us.

The Fragmentary Nature of Sigint: Sigint usually will provide hundreds if not thousands of pieces of a complex puzzle, but rarely will it yield the entire puzzle. Much of the information obtained by Sigint is fragmentary and indirect, requiring that analysts patiently sift through hundreds or thousands of intercepts in order to piece together the pieces of a puzzle. Even then, the puzzle more often than not remains largely incomplete, as in the case of the much-touted Venona decrypts. The fragmentary nature of most decrypts make them extremely difficult to understand, much less use.[100] A senior American intelligence official was quoted as saying that 'You rarely get a Sigint smoking gun. It's usually very fragmentary... Very often you don't even know who you're listening to.'[101] Voicing a feeling

often heard from intelligence consumers around the world trying to understand Sigint, in 1976 the Dutch Prime Minister complained that the Sigint that he was receiving was raw, unfinished materials that were sometimes unbalanced or fragmentary.[102]

Sigint Does Not Provide All the Answers. Generally, Sigint cannot measure a nation's political will or morale, or detail the innermost workings of foreign governments. Even Ultra and Magic during World War II failed to yield this kind of information, but it should be pointed out that the much vaunted Humint effort during the war did not either. Current and former senior intelligence officials in the US, Canada and Europe interviewed by the authors have all emphasised that Sigint is only useful when it is combined with intelligence obtained from other sources into an 'all-source' product.[103]

Lack of Timeliness: Although Sigint insiders pride themselves on being fast, sometimes they are not fast enough because of the time and effort required to process, analyse and report to consumers the results of Sigint collection.[104] For example, an intelligence community post-mortem of 1968 Czechoslovakian Crisis found that Sigint did not find its way to consumers in Washington until days after it had been intercepted. A small consolation for NSA was the fact that the CIA's Humint and Imint reporting was much slower.[105]

Too Much Information: Experience during the Cold War showed that NSA often did drown intelligence analysts in a sea of paper, such as during the 1968 Czech crisis and before the 1973 Middle East War. After the 1973 Mid-East War, the CIA blamed NSA in part for the failure to predict the war, claiming that CIA intelligence analysts were swamped by hundreds of Comint summaries every week pertaining to Egyptian and Syrian military activities. A post-mortem study done after the war concluded, however, that the overworked CIA and DIA intelligence analysts responsible for the Middle East were not trained to understand or effectively evaluate the information contained in the NSA Comint summaries.[106]

When Sigint satellites were placed in orbit, the vast amount of information that they generated swamped the available analytic resources. For instance, the intercept tapes generated by the US Navy's first Grab Elint satellite, which was launched from Cape Canaveral, Florida on 22 June 1960, so thoroughly saturated NSA's analysts that it took months to process a few weeks of intercepts.[107]

Smaller nations, such as India, are also suffering from an information glut from their Sigint collection operations. A former Indian Cabinet official recently wrote that 'We are in the throes of a similar crisis in our technical collection capability as we are also not able to utilise a major portion of intercepted traffic.'[108]

Lack of Sigint: In some instances during the Cold War, good operational and communications security by the Soviet Union and its allies 'blacked out' Sigint, although these instances were fewer than previously believed. For example, in 1959 the Algerian National Liberation Front (FLN), which was fighting for the independence of Algeria from France, changed all of its codes, making them impossible for the French Comint service to decrypt.[109]

Deniability: Access to Sigint data can be denied by the use of encryption and other secure forms of communications, such as landline telephone and telegraph circuits, or more recently fibre-optic cables.[110] For example, NSA lost much of its access to high-level Soviet communications traffic in the late 1940s and early 1950s when the Russian military shifted much of its high-level communications traffic to landlines.[111] Recently introduced complex communications technologies, such as frequency hopping radio systems, have made the job of the Sigint intercept operator far more difficult then in the past.[112] In recent years, Pakistani-backed guerrillas operating in the Indian state of Kashmir, calling themselves the Hizbul Mujahideen, have begun using frequency-hopping radios, burst transmission technology, citizen-band radios, satellite telephones, even sophisticated encryption technology, which has made it increasingly difficult for the Indian government's Sigint services to monitor their communications traffic.[113]

Fragility of the Source: Because it is dependent on extremely fragile and sensitive sources and methods, Sigint is particularly vulnerable to damage caused by treason, defections, news leaks, or poorly considered public statements by government officials.[114] A KGB operative named William Wolfe Weisband, who worked inside the US Army Sigint organisation, the Army Security Agency (ASA), during the late 1940s single handedly destroyed three years of successful work against Soviet cipher systems. After Weisband told the KGB about ASA's successes against Soviet systems, on 29 October 1948, known within NSA as 'Black Friday', the Russians executed a massive change of all of their cryptographic systems and communications operating procedures, shifting all of their mainline systems to unbreakable one-time pads. It would take six years before NSA could solve another high-level Soviet cipher system.[115]

The June 1960 defection of two NSA civilian employees, William H. Martin and Bernon F. Mitchell, caused immense damage to NSA's Sigint effort against the Soviet Union. According to one source, Martin and Mitchell's defection resulted in a 'partial dimout of United States communications intelligence', requiring that NSA work in double shifts for months trying to fix the damage done to the US Sigint effort.[116]

In 1969, President Richard M. Nixon revealed at a press conference that the US had the ability to read Soviet and North Korean communications. After making this statement, the Soviets, Chinese and North Koreans

changed many of their cryptographic systems. It took NSA months to repair the damage caused by Nixon's off-the-cuff remarks.[117]

In the 1970s, the East German Secret Service, the STASI, was able to infiltrate the French listening post in West Berlin. This led the East Germans to change their communications procedures and manipulate their radio traffic so as to deceive the French.[118]

In 1989, the transcript of an intercepted telephone conversation involving Colombian drug lord Pablo Escobar was leaked to Bogotá newspapers, which revealed to the members of the Medellin Cartel that the US was eavesdropping on their telephone calls.[119]

Communications Deception: Sigint is vulnerable to communications deception, although this is a very difficult and dangerous game to play.[120] For example, the KGB decided not to play communications deception games with the Berlin Tunnel in order to protect their source inside MI6, George Blake.

Because of it is often compartmentalised away from all other intelligence sources, Sigint is particularly vulnerable to political manipulation by those senior government officials who control access to the intelligence reports. Henry Kissinger, President Richard Nixon's National Security Advisor, reportedly ordered that certain sensitive NSA intercepts not be shared with the Secretaries of State and Defense.[121] In 1986, NSA refused a request by Secretary of Defense Caspar Weinberger for access to NSA intercepts concerning the Iran-Contra affair, stating that the Pentagon had no 'need-to-know'. What Weinberger and Secretary of State Schultz did not know was that on orders from the White House, the State and Defense Departments had been specifically barred from access to these intercepts. Senior Pentagon officials were later outraged to learn that while they were not allowed to see the intercepts, NSA was providing copies of these reports to Richard Secord, who although a retired Air Force General, was not a government official and held no security clearance.[122]

Lack of a Co-ordinated Sigint Effort: Competing bureaucracies were the bane of the American and Soviet Sigint efforts during the Cold War, resulting in massive duplication of effort and wasted resources. Declassified documents clearly demonstrate that during the 1940s and 1950s, the intelligence components of the three US military services pursued independent intelligence collection and processing efforts that were 'conducted with a minimum of service co-ordination'.[123] For instance, by 1951 senior CIA officials had become so frustrated by the continuing internecine fighting between the three American military Comint organisations in the Far East, as well as the inability of NSA's predecessor organisation, the Armed Forces Security Agency (AFSA), to impose order over its quarrelling subordinates, that the CIA came to view AFSA as

unresponsive to civilian authority or national intelligence requirements. By mid-1951 CIA Director General Walter Bedell Smith was so unhappy with how the American Comint system was working that he threatened to stand on his right as the head of the US intelligence community and reorganise the entire American Comint system unless the State and Defense Departments stepped in and did something to fix the problems.[124]

During the manhunt for Colombian drug lord Pablo Escobar in 1992–93, US Army and CIA airborne Sigint units operated independently of each other in order to prove that their personnel, equipment and equipment were superior to their counterparts. US Army intelligence officers believed that the CIA station chief in Bogotá was taking credit for information that they had collected.[125]

In the Soviet Union there was also little cooperation or coordination of effort between the Sigint units of the KGB and the intelligence organisation of the Soviet military, the GRU, throughout the Cold War.[126]

But the superpowers were not the only ones who suffered from this affliction. During the Cold War the West Germans fielded five Sigint organisations, four military and one civilian unit run by the West German foreign intelligence services, the Bundesnachrichtendienst (BND) For almost 20 years, from 1970 until the end of Cold War in 1989, the West German military services and the BND fought a series of bitter internecine battles over mission and resource allocation, as well as control of the West German government's Sigint effort.[127]

During the 1950s there was no coordination of effort among the Dutch army, navy and air force Sigint units, resulting in tremendous duplication of effort. The Dutch Army Sigint unit, for example, did not even bother to tell the Dutch naval Sigint organisation, the TIVC, which targets it was copying or what results it was obtaining. A proposed merger of the three service Sigint organisations collapsed because each of the services feared that their requirements would not be met in a unified Sigint organisation. A former Dutch Sigint official later admitted that Sigint cooperation with foreign services was better than between the three Dutch Sigint organisations.[128]

Technical Issues: Sigint's ability to perform effectively is subject to the vagaries of atmospheric conditions and solar flare activities. For example, in the mid-1950s, the Canadian intercept site at Churchill in Manitoba was forced to shut down its operations for days at a time because atmospheric anomalies, which are common in the northern climes, prevented the station's operators from hearing any high-frequency signals.[129] Terrain is also a significant limiting factor. For example, Sigint intercept operators have historically experienced great difficulty copying radio signals emanating from urban areas, densely wooded terrain or in mountainous regions.[130]

Finally, radio interference coming from major urban areas or industrial activities in the vicinity of the listening post can wreak havoc with radio intercept operations.[131] For example, the Canadian listening post at Inuvik in northern Canada had to be closed in April 1970 because radio interference from nearby oil exploration activity significantly affected the station's ability to monitor HF radio signals coming from the Soviet Union.[132]

NOTES

1. Christopher Andrew, 'Conclusion: An Agenda for Future Research', *Intelligence and National Security* 12/1 (Jan. 1997) p.228.
2. A more detailed discussion of these matters is contained in Matthew M. Aid, 'Not So Anonymous: Parting the Veil of Secrecy About the National Security Agency', in Athan G. Theoharis (ed.) *A Culture of Secrecy: The Government Versus the People's Right to Know* (Lawrence: UP of Kansas 1998) pp.65–7.
3. William Rosenau, 'A Deafening Silence: US Policy and the Sigint Facility at Lourdes', *Intelligence and National Security* 9/4 (Oct. 1994) pp.730–1.
4. John le Carré, *Tinker Tailor Soldier Spy* [1974] (NY: Coronet Books 1994) p.206.
5. Maj. Gen. Yashwant Deva (Ret.), 'Of Tapes and Tapping: Technical Intelligence Scores Over Human Intelligence', 2 July 1999, located at http://www.ipcs.org/issues/articles/217-ip-deva.htm.
6. Department of the Army, Field Manual FM 34-2, *Collection Management*, Oct. 1990, pp.2–5.
7. US Marine Corps, Marine Corps Warfighting Publication (MCWP) 2-15.2, *Signals Intelligence*, June 1999, p.1-1.
8. US House of Representatives, Permanent Select Committee on Intelligence, *Annual Report by the Permanent Select Committee on Intelligence*, 95th Congress, 2nd Session, 1978, p.50.
9. US Senate, Report No. 94-755, *Final Report of the Select Committee to Study Governmental Operations With Respect to Intelligence Activities*, 94th Congress, 2nd Session, 1976, Book III, p.737; US House of Representatives, Permanent Select Committee on Intelligence, Report No. 95-1795, *Annual Report by the Permanent Select Committee on Intelligence*, 1978, pp.31, 58; Department of Defense Directive S-5100-20, *The National Security Agency and the Central Security Service*, 23 Dec. 1971, p.2, DoD FOIA; Air University Extension Career Institute, *Electronic Signals Intelligence Exploitation Craftsman Career development Course AFSC 1N571* (Goodfellow AFB, 17th Training Wing, 21 March 1995) Vol.II, pp.34–5, USAF FOIA; *Naval Cryptology in National Security*, 1985, p.30, COMNAVSECGRU FOIA; David L. Christianson, 'Signals Intelligence', in Gerald W. Hopple and Bruce W. Watson (eds.) *The Military Intelligence Community* (Boulder, CO: Westview Press 1986) p.41.
10. Patrick J. McGarvey, *CIA: The Myth and the Madness* (NY: Saturday Review Press 1972) pp.42–3.
11. Ibid., pp.74–6.
12. Headquarters Strategic Air Command History Division, *SAC Reconnaissance History: January 1968 – June 1971*, 7 Nov. 1973, p.72, via Dr Jeffrey T. Richelson.
13. Air University Extension Career Institute, *Electronic Signals Intelligence Exploitation Craftsman Career development Course AFSC 1N571* (Goodfellow AFB, 17th Training Wing, 21 March 1995) p.19, USAF FOIA.
14. Headquarters Strategic Air Command, History Division, *SAC Reconnaissance History* (note 12) p.3, via Dr Jeffrey T. Richelson.
15. US House of Representatives, *House Intelligence Committee 1978 Annual Report*, p.36; NSGTP 69304-B, *Naval Cryptology in National Security* (note 9) pp.30–1, COMNAVSECGRU FOIA; NSGTP 68322, *Cryptologic Operators Manual for Noncommunications Operations*, 1980,

pp.6–12, 40–4, COMNAVSECGRU FOIA; FM 34-2, *Collection Management*, Oct. 1990, pp.2–5; Charles A. Kroger Jr, 'ELINT: A Scientific Intelligence System', *Studies in Intelligence* (Winter 1958) p.72, RG-263, Entry 37, Box 1, Folder 6, US National Archives, College Park, Maryland (hereafter 'NA, CP'); Memo with attachment, Radford to Secretary of Defense, 20 July 1954, RG-330, Entry 200B OSD 1954, Box 47, 334 Joint Electronics Analysis Group, NA, CP.

16. FISINT was formerly known as Telemetry Intelligence (Telint). Christianson, 'Signals Intelligence' (note 9) p.40; *Naval Cryptology in National Security* (note 9) p.48.
17. National Air Intelligence Center, *Draft, Technical Requirements Document (TRD) for the Sigint System Integration Contract*, 24 July 2000, located at www.pixs.wpafb.af.mil/pixslibr/DATAEX/sigsoo_drft1.doc.
18. 'Paper Looks at Continuing Value of Russian Tracking Station Near Havana', *BBC Monitoring*, 18 Dec. 2000.
19. SRH-264, *A Lecture on Communications Intelligence by Captain J.N. Wenger, USN*, 14 Aug. 1946, p.8, RG-457, NA, CP.
20. US Marine Corps, MCWP 2-15.2, *Signals Intelligence*, June 1999, pp.1-4 – 1-5.
21. *NCVA Cryptolog*, Summer 1996, p.3.
22. Confidential interviews.
23. Evan Thomas, *The Very Best Men* (NY: Simon & Schuster 1995) pp.52–3, 360.
24. John Kenneth Knaus, *Orphans of the Cold War: America and the Tibetan Struggle for Survival* (NY: BBS Public Affairs 1999) p.233; William M. Leary, 'Secret Mission to Tibet', *Air & Space*, Jan. 1998, pp.62, 70.
25. Department of State, *Foreign Relations of the United States 1964–1968: Vol. XXX, China* (Washington DC: GPO 1998) pp.476–7, 495.
26. 'ROK Spies Who Died After Infiltrating NK Number 7,726', *Korea Times*, 27 July 1999.
27. Stansfield Turner, 'Intelligence for a New World Order', *Foreign Affairs*, Fall 1991, p.158.
28. Confidential interview.
29. Transcript, National Public Radio, Morning Edition, National Security Agency, 14–16 March 2000.
30. Bob Drogin, 'At CIA School, Data Outweigh Derring-do', *Los Angeles Times*, 27 Aug. 2000, p.A7.
31. John M. Maury, *Memorandum for the Record: Conversations With Messrs. Ed Proctor and Jack Smith Re Use of CHICKADEE Material for NIE 11-8-61*, 7 June 1961, CIA FOIA Page at www/odci.gov/. Another former CIA official stated that Penkovskiy gave 'little information of major importance that had any significant effect on our intelligence estimates. He was primarily useful in... confirming data from other sources, and adding confidence to existing assessments', for which see Herbert Scoville Jr, 'Is Espionage Necessary For Our Security', *Foreign Affairs*, April 1976, p.488.
32. *Intelligence Community Experiment in Competitive Analysis: Soviet Strategic Objectives: An Alternative View: Report of Team 'B'*, Dec. 1976, p.9, RG-263, NA, CP.
33. David Kahn, *The Codebreakers* (NY: Macmillan 1967) p.727.
34. Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story* (NY: HarperCollins 1990) p.455; Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (NY: Basic Books 1999) pp.352–3.
35. Mark Urban, *UK Eyes Alpha* (London: Faber 1996) p.8.
36. Aldrich contribution.
37. Wiebes contribution, p.254.
38. Harry Rowe Ransom, *The Intelligence Establishment* (Cambridge, MA: Harvard UP 1970) p.127.
39. 'Address at the CIRA Luncheon, 5 Oct. 1998; John Millis' Speech', *CIRA Newsletter*, Winter 1998/1999, p.6.
40. Ibid.
41. David Kahn, 'Big Ear or Big Brother?', *New York Times Magazine*, 16 May 1976, p.62.
42. US Marine Corps, MCWP 2-15.2, *Signals Intelligence*, June 1999, p.1-5; Penelope S. Horgan, *Signals Intelligence Support to US Military Commanders: Past and Present* (Carlisle Barracks, PA: US Army War College 1991) p.88.

43. DOD Directive S-5100.19, *Implementation of National Security Council Intelligence Directive No. 7*, 19 March 1958, pp.1–4, DOD FOIA; JCS 2010/143, *Fulfillment of Proposed NSCID No. 7 and COMINT Communications Requirements*, 18 July 1958, RG-218, CCS 334 NSA, Section 22, NA, CP; NSA/CSS Manual No. 22-1, *National Security Agency Central Security Service Organization Manual*, 21 Jan. 1974, p.2, NSA FOIA; McGarvey, *CIA* (note 10) pp.45–6; Central Intelligence Agency, *A Consumer's Guide to Intelligence*, Sept. 1993, pp.5, 38; NWP-5, *Naval Cryptologic Operations*, p.3-2, ONI FOIA; NSGI C3211.1D, *CRITIC (Critical) Information*, 2 Aug. 1990, COMNAVSECGRU FOIA; ESCR 200-40, *The CRITIC Test and Evaluation Program*, 12 May 1987, AIA FOIA; Tad Szulc, 'The NSA-America's $10 Billion Frankenstein', *Penthouse*, Nov. 1975; 'US Electronic Espionage: A Memoir', *Ramparts*, Aug. 1972, p.43.
44. Paul Bracken, *The Command and Control of Nuclear Forces* (New Haven, CT: Yale UP 1983) p.26; Bruce D. Berkowitz and Allan E. Goodman, *Strategic Intelligence for American National Security* (Princeton UP 1989) p.35.
45. *CIA: The Pike Report* (London: Spokesman Books 1977) p.140; Roy Godson (ed.) *Intelligence Requirements for the 1980s: Clandestine Collection* (Washington DC: National Strategy Information Center 1982) p.119.
46. *Report to the President'as Foreign Intelligence Advisory Board on Intelligence Community Activities Relating to the Cuban Arms Build-Up: 14 April through 14 October 1962*, undated, p.24, National Security Files: Countries: Cuba, Box 61, Kennedy Library, Boston, Massachussetts.
47. Lester W. Grau, *Road Warriors of the Hindu Kush: The Battle for the Lines of Communication in the Soviet-Afghan War* (Ft Leavenworth, KS: Foreign Military Studies Office, Aug.1996) located at http://call.army.mil/call/fmso/fmsopubs/issues/roadwar/roadwar.htm.
48. *Annual Historical Report US Army Security Agency FY 1964*, p.72, INSCOM FOIA and Confidential interviews.
49. Vladislav M. Zubok, 'Spy vs. Spy: The KGB vs. the CIA, 1960-1962', *Cold War International History Project Bulletin*, No. 4, Fall 1994, pp.22–33.
50. Raymond Garthoff and Amy Knight, 'New Evidence on Soviet Intelligence: The KGB's 1967 Annual Report', *Cold War International History Project Bulletin*, No. 10, March 1998, p.214.
51. Department of the Army, DA Field Manual 34-40-12, *Morse Code Intercept Operations*, 26 Aug. 1991, p.2-4, INSCOM FOIA; US Marine Corps, MCWP 2-15.2, *Signals Intelligence*, June 1999, p.1-5; SSgt Regina Mason, 'Flight Commanders: Moral and Mission Are Key Responsibilities', *Spokesman*, Jan. 1991, p.9.
52. US House of Representatives, Permanent Select Committee on Intelligence, Report 105–508, *Intelligence Authorization Act for Fiscal Year 1999*, 105th Congress, 2nd Session, 5 May 1998, p.10.
53. See the case studies detailed in USAFSS Historical Office, *A Special Historical Study of USAFSS Response to World Crises, 1949–1969*, 22 April 1970, AIA FOIA.
54. Angello Codevilla, *Informing Statecraft: Intelligence for a New Century* (NY: The Free Press 1992) pp.14–15.
55. David Kahn, 'Cryptology', *The Encyclopedia Americana*, 1987, Vol.8, p.276.
56. David A. Fulghum, 'Sigint Aircraft May Face Obsolescence in Five Years', *Aviation Week & Space Technology*, 21 Oct. 1996, p.54.
57. A discussion of this contentious issue can be found in Godson, *Intelligence Requirements for the 1980s* (note 45) p.119.
58. 'Address at the CIRA Luncheon, 5 October 1998; John Millis' Speechs', *CIRA Newsletter*, Winter 1998/1999, p.6.
59. Rosenau, 'A Deafening Silence' (note 3) p.726.
60. Confidential information.
61. US Defense Intelligence Agency Testimony to US Senate Select Committee on Intelligence, 'Worldwide Threat to US National Security', Aug. 1996, located at www.securitymanagement.com/library/000255.html.

62. Peter Conradi, 'Stasi Phone Taps Sound Alarm in Kohl's Inner Circle', *Sunday Times*, 9 April 2000, p.26; Roger Boyes, 'Stasi's Spies Bugged 100 Kohl Phone Lines', *London Sunday Times*, 29 June 2000. On the East German Sigint service in general, see Ben B. Fischer, 'One of the Biggest Ears in the World: East German Sigint', *International Journal of Intelligence and Counterintelligence* 12/2 (Summer 1998) pp.142–53.
63. Gene Poteat, 'Stealth, Countermeasures, and ELINT, 1960–1975', *Studies in Intelligence*, 42/1 (1998) p.52, CIA FOIA.
64. Mark Urban, *UK Eyes Alpha* (London: Faber 1996) p.5.
65. Press Release, 'GCHQ Accomodation Project Site Announced', 7 May 1999, located at www.fco.gov.uk/news/newstext.asp?2391.
66. CM 4897, Intelligence and Security Committee, *Annual Report 1999–2000*, 2 Nov. 2000, www.official-documents.co.uk/document/cm48/4897/4897-02.htm.
67. Rudner contribution, p.103.
68. Stuart Farson, 'Accountable and Prepared? Reorganizing Canada's Intelligence Community for the 21st Century', *Canadian Foreign Policy* 1/3 (Fall 1993) p.49.
69. Alexander Zervoudakis, 'Nihil Mirare, Nihil Contemptare, Omni Intelligere: Franco-Vietnamese Intelligence in Indochina, 1950–1954', *Intelligence and National Security* 13/1 (Spring 1998) pp.203–25.
70. Wiebes contribution, p.243.
71. Horgan, *Signals Intelligence Support to US Military Commanders* (note 42) p.84.
72. Memo, Col. T.F. Van Natta, Assistant Chief of Staff, G2, Eighth US Army to Assistant Chief of Staff, G-2, Department of the Army, *Clearance for Access to Communications Intelligence*, 24 Oct. 1952, RG-338 Records of GHQ Far East Command, Entry 34015A AC of S, G-2 Executive (Coordination) Division, Box 70, File: 333.5, NA, CP.
73. Oliver Kirby, 'Louis Tordella Led by Example', *Cryptolog*, Spring 1996, p. 8.
74. *Agenda Prepared by Army Field Forces Observer Team No. 5*, August 1951, p. 167, MISC 333 AFF-FECOM, OCMH, Washington DC; Memo for the NSA/CSS Representative Defense, *NSA Transition Book for the Department of Defense*, 9 Dec. 1992, p.2. The author is grateful to Dr. Jeffrey T. Richelson for making a copy of this document available. Ed Evanhoe, *Dark Moon: Eighth Army Special Operations in the Korean War* (Annapolis MD: Naval Institute Press 1995) pp.86–7; Private information.
75. Eduard Mark, *Aerial Interdiction in Three Wars* (Washington DC: Center for Air Force History 1994) p.277.
76. US Naval Security Group, *US Naval Communications Supplementary Activities in the Korean War: June 1950–August 1953*, p.80, COMNAVSECGRU FOIA; Confidential interview.
77. Marshall L. Michel III, *Clashes: Air Combat Over North Vietnam, 1965–1972* (Annapolis, MD: Naval Institute Press 1997) pp.114–15.
78. 'Good Times With Bad-Eye: The Adventures of John 'Bad-Eye' Martin, undated, located at www.vietvet.org/badeye.htm.
79. Joan Edwards, 'Reagan's Charges "Total Untruths", ex-CIA Man Says', *Toronto Globe and Mail*, 29 June 1984, p.12.
80. Victor Sheymov, *Tower of Secrets* (Annapolis, MD: Naval Institute Press 199?) p.15.
81. Aldrich contribution, p.88.
82. Marian Wilkinson, 'Our Spies Knew Balibo Five at Risk', *Sydney Morning Herald*, 13 July 2000, located at www.smh.com.au/news/0007/13/pageone/pageone13.html
83. Horgan (note 42) p.85.
84. See for example Memo, Tarkenton to Assistant Chief of Staff, G2, I Corps *et al.*, *Classified Information for Limited Use*, 30 Dec. 1950, RG-500 Records of Eighth US Army 1946–1956, AcofS, G-2, Box 53, File: Classified Information for Limited Use, NA, CP.
85. The NSA COMINT report language is taken from NSA, 3/0/__/R26-63, *COMINT Report*, 23 Nov. 1963 2103Z, JFK Assassination Files.
86. Memo, Belmont to Boardman, 1 Feb. 1956, pp.1, 9, FBI Venona Files; SRH-123, *Brownell Committee Report*, pp.103–4, 108, RG-457, NA, CP; Dr Ray S. Cline, *The CIA Under Reagan, Bush and Casey* (Washington DC: Acropolis Books 1981) p.130; Woodrow J. Kuhns (ed.) *Assessing the Soviet Threat: The Early Cold War Years* (Washington DC: