COMINT --- HARD FACTS IN THE COLD WAR

by J.A.Meyer

Rapid communications are the nervous system of the modern super-state, connecting a strong central control with widespread agencies and outposts. Traditionally these communications are sent in code or cipher to protect the information they carry. In the politics of competing nations, the timely analysis and exploitation of weaknesses in these vital communications is an important facet of statecraft.

"Gentlemen do not read other people's mail", said Henry L. Stimson, then Secretary of State, as he closed down the secret cryptanalytic section of the State Department. The time was 1928, and Stimson, as the new Secretary, was being gently introduced to the inner workings of the Department, however, the existence of the cryptanalytic section which had been decoding secret foreign diplomatic messages from World War I onwards, had been so carefully concealed that each new Secretary of State usually learned of it only after he was in office.[1]

A political euphoria and revulsion toward war and intrigue following World War I made the position of the cryptanalytic section somewhat insecure. Successive Secretaries of State regarded this espionage function with varied reactions ranging

from shock and disapproval, or feelings of moral conflict at trying to pry into the state secrets of brother nations while publicly espousing good will --- to businesslike rationalization of this as a neccessary diplomatic function.[2]

Stimson did not rationalize. He took direct action, disolved the section, and fired the people, a purge intended to restore honor to international politics. As a result, the head cryptanalyst H.O.Yardley, seeing the work of more than a decade suddenly terminated, wrote a book, "The Black Chamber", in which he revealed many incidents of the World War I code breaking in which he had taken part, and in the later part of the book, described in clinical detail the action of the section during the Naval Disarmenent Conference of 1922, in which the U.S. and Japansse governments had negotiated Japanese naval tonnage. To authenticate his narrative, Yardley included verbatim decipherments of the messages passed between Tokyo and the Embassey in Washington, with a running commentary on the way the American statesmen, knowing the instructions and terms of reference of the Japanese delegation --- bargained sharply to reduce the Japanese fleet to the smallest size Tokyo would stand for. This Naval Conference was hailed as a great diplomatic success for the U.S.

Yardley's book, published in 1929, was so convincing that the Japanese government , in an enraged protest, expanded their naval power, justifying this as a moral right after the way the unscrupulous American government had tricked them. Cryptanalysis,

the art of code breaking, suddenly grew in the public and political mind from a distasteful and somewhat sneaky habit, not mentioned in the best circles, to a dangerous political weapon--- which might boomerang.†

The ethical and political repercussions of reading other people's mail had occurred earlier, in England, during World War I, when Capt. R. Hall, Director of Naval Intelligence for the Admiralty, intercepted correspondence from German agents in Britain which was being sent to contacts in neutral countries through His Majesty's mails. Interfering with the mail was illegal, so Hall, acting largely on his own authority, set up a mail reading section, and insulated this activity from other branches of the government.

When his unofficial tampering was discovered, Hall was threatened with trial and prison, but he argued the practical urgency of the action, and the function was legalized.[3] *

Even earlier, in 18__, a secret British organization known as the Office of the Decypherer, a code breaking section of , was subjected to publicity, and abandonned as the scapegoat in an era of publicized political idealism.[4]

---

† Cryptanalysis went underground in the U.S. after the Stimson incident. The U.S.Army Signal Corps had a small section which kept the torch burning during the 1930's, but the existence of this group was not made known through all branches of the government. Signal Corps cryptanalysis produced the vital "Magic" intelligence of 1941.[5] In 1940 Stimson, as Secretary of War, had to authorize the expansion of the Signal Corps effort, which he did with mixed feelings.[6]

* Wiretapping is another method of intercepting messages, publicized but not approved.

Stimson's action, then, was just a repeat of an earlier pattern; the secret function begun to meet an emergency and continued to assist the state in its policies, was condemned as a gesture of good faith. The political repercussions of Yardley's book were eye opening, but the ideal persisted---- world peace must be sought in mutual trust and respect between nations, not cynical and ruthless opportunism.[7] Politics or not, there are some things that gentlemen do not do.[†]

The Ethics of Informal Espionage

This curious distaste for reality illustrated above derives from the supposition that foreign affairs are carried out by businessmen and gentlemen, and that the gentlemanly code, which forbids cheating, can be applied.[‡] In practical terms this means that espionage and aggressive methods of getting intelligence are bad form, whereas many activities quite like espionage are legal and approved, and the information they supply may be used with clear conscience. In fact, there is no dichotomous seperation between diplomacy and intelligence, the rules for both are inexact and blurred by outlook.

---

‡ Von Papen: "What do you think the British would do if one of our people made them a comparable offer?"
Moyzisch: "I think they'd undoubtedly accept it, sir. In time of war no nation could afford to turn down such a proposition. In peacetime it would probably be better diplomatic business to do the gentlemanly thing and inform the British Ambassador rather than get involved with stolen documents. But in time of war, sir..." [8]

† Even the use of codes and ciphers for normal diplomatic communications has been regarded with disfavor.[9] One of the important advantages of diplomatic recognition of the USSR by the U.S. and Canada, was the authorization of coded messages.[10]

Intelligence is an institution as old as politics and war. It consists of knowing as much as possible about the opponent, his habits, resources and intentions, a reasonable aim in war, politics, business or personal affairs. The conventional forms are agent intelligence, information gathered by and from people, which in earliest times took the form of scouting parties, interrogation of prisoners, and planting spies in the enemy camp---- and communications intelligence (shortened by usage to comint) , which, after the invention of signalling and writing, involved interception and reading of messages.

The gentlemanly view of such activities is that they violate the rules of the game, and while a military organization might, as a wartime neccessity , hastily indulge in some of these practices, no statesman would condone and support them during peacetime. Gathering information on foreign countries is all right as long as the the methods are above board, simply a matter of being well informed, but espionage, pilfering secret information, and most especially peeking at other people's correspondence are definitely cheating.

Actually, there is an element of self deception in this. In the business world the use of agent intelligence is a time honored custom which has provoked the concept "Company Confidential" to shield new developments, and made company loyalty an important item of reputation. Marketing and technical information, rather than military and political details are the target, but the analogy persists.

An executive in a highly competitive industry would consider it of paramount importance to be well informed about the activities

and plans of his competitors, not only from published sources, but also from carefully sifted gossip and anecdotes gathered in neutral situations like the golf course, cocktail bar, and national conferences.

While the executive might not actually send spies to work for the opponents, corporation wives are useful links, and professional friendships can often be used for discreet trading of information. The rewards for the agents are indirect gifts, invitations and political favor, all skillfully disguised. For really important information, the executive may attempt the master coup of bribing a key man to defect from a rival organization to his own, and he might rationalize this polite subversion by the argument that the competition was trying at least as hard.

This type of espionage is "safe", it is done informally and face to face, it is hard to trace and easy to deny, and the competitor, even if he knows what is going on, can never make a case of it, or force the issue." However, a deliberate act of aggression, such a raiding the competitor's locked files, or tapping his phone, or slitting open his mail is rather a different story, and besides the illegality and risk of discovery, the executive, no matter how ruthless and singleminded he is in trying to advance his organization and his own position, might, aside from the risk, consider this a contemptible way of doing business.+

+ In 1933 Jacob Sterngluss, former GB chief in Afghanistan, came to the U.S. as an official of the Russian Red Cross. His specific job consisted of organizing the theft of mail from the mailboxes of certain individuals. He arranged contacts with minor employees of Western Union, Commercial Cables, and RCA, with a view to intercepting telegrams, cables, and radiograms in which he was interested.[12]

So the folkway is established, the ethics of business and personal life, which accept informal espionage and apparently recoil at formal espionage as an invasion of privacy, are projected into the aims and practices of foreign politics.+

Honor Among Nations

The statesman may prefer to avoid formal espionage for practical as well as moral reasons. Politics and the behavior of competing nations is infinitely more complicated than business or games, there is more at stake, and it is harder to determine whether a country is winning or losing since there is no simple scorecard or account ledger to consult. The most important ingredient for analysis of a political situation is information, plentiful, timely , and correct. Ignorance on any point is a dangerous weakness,

---

+ Formal espionage is within the rules in competitive sports, particularly football, where the rules were altered pragmatically to legalize existing systems of espionage. Scouting games is recognized as a fair method of gathering information, but taking movies of the games, except on the home field, is disallowed. Pumping squad members for information about injuries is not de rigeur, although it is done. Remarkably, the style of play in football has changed as a result of communications intelligence. Thirty years ago the offensive team normally lined up at scrimmage, and the quarterback called off a string of numbers which defined the play, and the starting signal. Shrewd defensive players were able, however, to "break" the system, and toward the end of the game the defense could recognize the play, and shift to meet the attack. Surprise was eliminated and the offense bogged down. Systems of encipherment were too cumbersome to use on the field, so the "huddle", originally derided as "ring around the rosy", was developed to simplify and protect the communications.

Diagnosing the play from the signals was not "cheating", it was "heads up football", because victory was highly prized. 13

since national policy depends upon what the government believes, and naive scruples about methods of getting information may prove costly fetishes.

However, quite a lot of information can be gotten through informal channels, without the exertion and anxiety of extralegal activities. Formal espionage, buying information, setting up spy rings, bribing defectors, intercepting mail and reading secret communications---- these activities are outside the rules, outside the law, and distasteful to a good statesman, besides which they are expensive and hazardous.

Information which is for sale may be highly priced, and it must be verified before it can be believed.[14] A spy ring is exceedingly difficult to organize.[15] Years may be required to screen and select people who have the rare qualities that might enable them to function in an espionage system.[16] A. Foote, in his "Handbook for Spies", discusses in detail the elaborate and thorough work required to set up and operate a single ring in one country. The administration of the system is difficult once it is in operation, the financing is exceedingly tricky since individual agents may have to dispose of large amounts of cash without detailed accounting, and it is difficult to check the loyalties of all agents since they must blend into the system they are trying to penetrate.[17] Security is a constant threat, and a few leaks, or some bad luck may disable a network that has taken years to construct.[18] When a spy ring is unravelled, a diplomatic rift is certain, no matter how many reassuring lies are told----

thus even if the espionage system fails completely, the statesman cannot wash his hands of it.[19] Aside from the disgrace of being caught, the project will be regarded as a flop at home.

On the other hand, the information gotten through approved channels may be incomplete. One nation may cheat energetically while the other acts "by the rules". Then comes a day of reckoning when a shocked nation is presented with some convincing evidence which it must act on, diplomatic rift or no.[20]

Igor Gouzenko, the Russian code clerk who chose the West in 1945, provided just such a bitter lesson by his revelations about Russian espionage in Canada. From 1941 onwards, the Soviet had been considered and treated as an ally and "friendly" power, and altercations in eastern Europe were played down on the premise that wartime cooperation still existed and must be preserved. Belatedly , the Russian intentions and organization exposed and documented, we began our new role in the uninterrupted ideological war.

Gouzenko's defection and the chill that followed it did not alienate Russia from the West. Their policy was already formed and in operation, the West was simply blind to it, partly by deliberate optimism, and partly through lack of information. The facts about the Red spy network were not available through normal channels for obvious reasons. Except for Gouzenko's defection, the net might have spread and functioned, unrecognized, while the West forced themselves to recurring declarations of sincerity, friendship, and high principle. The rules of peace

had changed, the stakes were different, not coexistence but conquest, therefore both sides had to play differently.†

A post mortem implication of the episode is that, while Gouzenko's defection was a phenomenal stroke of luck, if the West had been interested in Russian comint, and had continuously, through the war and afterwards, hammered at the Russian codes and read some of the messages that Gouzenko was sending, we might have known about the espionage ring before his defection---- or even better, might, from comint, have been able to see the Russian plan in its formative period, and done something to disable the net and thwart the Red design before it had matured.

Gouzenko's defection spelled the end of a boom period of Soviet espionage, unfortunately too late to prevent the transfer of much of the vital atomic information and material that enabled the USSR to build its own A-bombs, and the true nature of Sovietn alliance was exposed too late to enable interference in the annexation of eastern Europe.* The history and effect of Red espionage and politics could be different today----for the sake of a successful cryptanalytic effort.*

---

† It was symptomatic of the political climate of the time that Mr. King (Canadian Prime Minister) not only refused to deal with Gouzenko and his papers but recommended that the young cipher clerk return to his embassy. "I thought he should be told," Mr. King reported later to the House of Commons, "to go back to the embassy with the papers he had in his possession...What I felt most important was to see that nothing should be done which would cause the Russian Embassy to believe that Canada had the least suspicion of anything which was taking place there..." Gouzenko did not follow the advice of the prime minister.[22]

* It was not considered gentlemanly to spy on allies while there were Germans and Japanese to be spied on.

The American Tourist

The U.S. , in considering a policy of formal espionage, is immediately confronted with a serious fundamental problem. The Soviet is walled off from the rest of the world by its security system. Much agent intelligence must take place in bordering satellite or neutral countries in the orient, near east, and Europe. For a diverse problem like this, the backbone of a good agent system is a supply of people who can blend into a target country, and, like a pickpocket, work undetected and without drawing attention. This implies suitable physical appearance, perfect command of the language and dialect, experience and savoir faire in adapting to the country, knowledge of minutae of local politics and history, the ability to play a role, and a rare quality of mind that makes an "agent" ~~----~~ plus unquestionable loyalty.+ Unfortunately, native born americans who fill this bill are rather rare. Many americans with suitable foreign backgrounds, travel and education, are barred from secret work by security policies which exclude people with foreign backgrounds. Foreign nationals can be hired for this work, but the security problem is very sensitive. The average educated american, with proper intellectual and loyalty qualifications, has an unmistakeable stamp to his speech and personality which permanently disqualifies him for this kind of work.+

+ Spy rings seldom succeed for long, principally because they must operate in the opponent's territory. Arrests, defections, and disintegration of painfully constructed nets are the norm, and once the counter espionage agents identify a spy, surveillance and interrogations can be used ~~km~~ not only to unravel the chain of people, but also to establish what kind of information, and how

much, has been passed over to the enemy.[23] By way of contrast, comint activities may be persued for decades without the target country ever being certain of how far its communications channels have been penetrated.[24]

‡ During World War II, American spies, after completing their training in the U.S., were frequently rejected by the British SAB at Pemberly, as unsuitable.[25]

In addition, merely in coordinating the information gathered from <u>any</u> sources, an intimate knowledge of European, mideastern and eastern history and politics and personalities is required to make intelligence out of a complex of uncertain and incomplete details.[26] However, sophisticated and thorough understanding of history and international politics is not in fashion in our technological society. A predominant number of good minds go into the exact sciences, and business, and other marketable channels, and considering our recent emergence as a major factor in international affairs, and the long experience of our allies and opponents, it may be some time before we develop a Weltanschaung which will enable us to meet the competition in these political fields.[27]

By comparison, we are much better equipped for communications intelligence, because of our technology. Comint begins with intercepting signals and messages. Radio signals can be intercepted by putting a receiving station in the right place, and having an operator copy down the messages. Sending stations, ships, planes and submarines can be located by coordinating information from several receiving stations. A thorough intercept system requires a vast outlay of equipment, and a large organization of people to

operate, maintain and administrate the function, but many of the equipments and skills needed are available in our electronics industry.

The signals and messages, after they are intercepted and copied down, are sent to central organizations for analysis, where they are sorted into appropriate classes, according to sender, receiver, and other characteristics. Where possible, individual messages are read and translated.[28]

The work of "reading" the messages often involves "breaking" a code or cipher system, and this is the most difficult and uncertain part of the entire comint effort, and the most crucial.[29] However, the task of gathering the information, the intercept phase, is much simpler and safer than the corresponding process in agent intelligence.† The intercept operator need know nothing about the language or habits of the country he is monitoring, his job is specialized and can be quickly learned. The analyst who tries to "break" the message need not play the role of a foreign national, cryptanalysis is an exact science, all be it an uncertain one, and scientific methods and brainpower can be used to expedite it.[30]

Encipherment and ~~xxxxxx~~ systems of secret writing were used by the ancient Greeks in their political and military affairs, and since that time have recurred frequently in European history.[31]

---

† The German Abwehr used comint methods to penetrate and unravel the famous Rote Kapelle (Red Orchestra) spy ring in Germany during World War II.[32] Direction finding techniques were used to isolate the houses from which coded messages were being sent. A raid captured the radio operator and cryptographic materials. With the Russian keys known, other Rote Kapelle messages, which up to then

had been insoluble, were deciphered, and the information contained in them was used to locate Rote Kapelle agents, and to verify their confessions after interrogation.[33]

After the invention of the telegraph and wireless, great volumes of official communications could be quickly sent to all parts of the world. Remote activities could be controlled from a central point, and the modern state and military system is profoundly dependent upon a continuous flow of communications.[34]

When secrecy in communications became important, new methods of encipherment which could provide security for large numbers of messages, were sought. Most codes and ciphers are "broken" by arranging and combining evidence from a large number of messages. Poe, in "The Gold Bug", and Yardley, in "The Black Chamber" show examples of how a cipher system displays characteristics after it has been used enough. For decades a long battle has been waged between cryptographers, to develop secure ciphers, and cryptanalysts, to find better methods and tools for breaking messages.[35]

Modern cryptanalysis is characterized by a large amount of work done on a large amount of data, counting, searching, sorting, calculation, in general, information processing. Some parts of cryptanalysis require human insight and imagination. Other phases can be reduced to exact logical proceedures.[36]

The advancing electronic technology in the U.S. has evolved equipment and skills which could be applied to this mechanistic part of cryptanalytic work, and because of the speed of communications between the intercept point and the analytic center, much of the analysis and processing can be done within the

continental U.S. with great advantages in security and staffing.[37]

The U.S. resources in industry, technology and scientific manpower are greater and more accessible than our resources in trained intelligence agents, so any policy of formal espionage would have to consider not only our history of political inexperience, but also our future position in the changing technological race.

Needle in the Haystack

Immediately before the Pearl Harbor attack in 1941, Signal Corps cryptanalysts were searching for a particular Japanese message, "East wind---rain", which was a battle signal.[38] Although they had sufficient "Magic" intelligence to know a war was immenent, this message was (allegedly) never found in time. This illustrates an important aspect of cryptanalysis and comint, the element of luck.

Even where a cipher system has been broken, and messages can be read, a great volume of traffic may have to be laboriously processed before a few significant items are found.[39] In other cases, critical messages can be isolated before they are solved. The famous Zimmerman telegram of World War I is an example of this. Because British Intelligence thought the transmission of German coded messages within Swedish diplomatic telegrams was especially important, certain of Ewing's Room 40 colleagues gave this traffic their full attention, and this single message, when solved, was the catalyst which brought the U.S. into World War I.[40]

Customarily, because of traditional differences between military and political groups, a target country may have a number of different cipher systems.[41] The opposing cryptanalyst must review all these systems and decide which ones appear "breakable", and what kind of information can be derived from the messages. Some cipher systems are completely unsolveable, many are very stubborn and may be solved only by luck or brilliant insight, others give up easily but yield poor returns. Searching for a "break" into a system is analogous to prospecting, i.e. looking in the right places, and recognizing clues. Once a system is broken, individual messages can usually be read by sufficient straightforward hard work.[42] This phase is called exploitation, and is analogous to mining operations once a rich lode has been discovered.

Countries change their cipher systems from time to time just as they change and improve their aircraft and other military instruments. Because complete overhaul is expensive, gradual modification is conventional.[43] The cryptanalyst, reading a system, suddenly finds it unreadable. He must quickly determine if it is radically new or just slightly different, and in this reanalysis, one of the most important factors is continuity, a knowledge of the history of the crypt system. A cryptanalyst follows changes in a cipher system like a broker follows fluctuating stocks, or a designer follows fashions, and this repetoire (frequently) enables him to evaluate a change much more quickly than the system was originally solved.

Unfortunately, this detailed knowledge of cryptographic

history can be gotten only by a thorough and continuing cryptanalytic effort.[44] Continuity once lost, is hard to regain, like losing momentum on an icy hill.

In peacetime, political intelligence may be more topical than military communications, and the military cipher systems may not be used enough to provide much material for solution or exploitation. At such times when greater effort is directed at political and diplomatic communication channels, the military links must be persistently studied, even if the yield is small, because the continuity is needed to detect and analyze the usual increasing difficulties of the system.

In time of war, the volume of military communications changes sharply, many more messages are sent, and under wartime urgency, mistakes may be made. If military action disables normal communications, the wireless may carry an additional burden, and sooner or later, a break may occur.+

Then the odds are more favorable to the cryptanalyst, providing he has the organization, special knowledge, material and trained personnel to react swiftly. In terms of modern warfare, much of the comint work can be done in the hinterlands, but a lapse of several years to develop and expand a comint organization may be too long.

+ One of the hazards of agent intelligence is that abrupt military or police action may cut their lines of communications.[45] Thus the agent system may be gathering information with no way of sending it.[46] Many Red spy rings were overrun by the German military successes in Europe.[47] The Rote Kapelle in Germany had trouble communicating its vital information to Moscow.[48] The Swiss network was also cut off by arrests of its radio operators.[49]

Even during a limited or expanded military action, the diplomatic channels cannot be ignored, or the political implications of the end of the war may be misjudged, at some cost. At a time of extreme tension or immenent war, the most urgent mission for comint might be to pick up a battle signal [redacted], like the "East wind---rain" of 1941. There is only a slim chance that such a message could be found and solved in time, even if the crypt systems had been opened up, however so much preparatory communication and direction is needed to get any large military project under way, even in these days of "push button" warfare, that scraps of evidence might emerge in time.† Furthermore, the position of the West would be stronger, even where atomic warfare agreements existed and were respected, if comint had, over a period of time, revealed weapon sites, numbers, and state of readiness inside the Soviet----and penetrated the Russian attitude toward their use.

The Hard Facts

Razvedka, Russian intelligence and espionage, dictates a pragmatic ethic for modern Western diplomacy. Containment and the cold war depends on accurate, reliable intelligence, i.e. peaceful coexistence will be much easier to expedite if we know what is really going on inside the Soviet. Agent intelligence

---

† During the campaign in Africa, Rommel learned of British deployments and logistics through signal intelligence before a crucial battle at

and comint must both be pursued, since they use complementary sources and methods, and a continuing intelligence effort must be carried out in spite of fluctuations in the political barometer.+ The Russians have a long lead in experience and organization, and confidence based on success. We must play our best cards, our wealth, technology and industry, organized in the right direction, to gain the initiative.

One critical advantage of comint over agent intelligence in this struggle is the validity of the product. Agent reports [redacted] under the best conditions may be untrue, half true, or disorganized.[51] It is difficult to take forceful action on vague information. A solved cryptogram carries the weight of exact legal evidence, it is an official communication which defines what the organization is <u>really</u> going to do. This is why a single message like the Zimmerman telegram, or [redacted],[52] occurring in a sea of conflicting and unproved rumors, testimony and opinions, can be treated as a hard fact, and the history of nations turned around it.

Finally, any intelligence effort is uncertain and difficult, years of effort and expense may be in vain, and success may dissappear overnight, but failure should carry no stigma, and the rewards for winning are high.

* * * * *

+ In contrast to the West, the flow of people and information from Russia is meagre and guarded. Soviet security measures are effective in preventing infiltration of agents into Russia. Defectors and deserters can provide some currect intelligence, but it is rarely high level. The importance of Russian cable and radio communications as a source of intelligence is thereby increased.

Bibliography

Fletcher Pratt, Secret and Urgent(Blue Ribbon Books,1939)

W, James, The Eyes of the Navy (Methuen & Co, London, 1955)

D.J.Dallin, Soviet Espionage (Yale Univ. Press, 1955)

O.Heilbrun, The Soviet Secret Services (G.Allen & Unwin,1956)

W.J.Morgan, Spies and Saboteurs (Victor Gallanez,London,1955)

M.Bialoguski, The Petrov Story (W.Heinemann Ltd,London,1955)

L.C.Moyzisch, Operation Cicero (Readers Union.Wingate,London,52)

Von Mellenthin, Panzer Attack

Knute Rockne, Coaching Football

H.O.Yardley, The Black Chamber

H.L.Stimson, Memoirs

Congress , Pearl Harbor Report

The Secret Post Office

Please note that in some cases I do not have the books at hand, and therefore cannot properly complete the documentation.

Notes

1. Yardley, The Black Chamber, p.
2. Yardley, The Black Chamber, p.
2'. Pratt, Secret and Urgent, p. 249.
3. James, The Eyes of the Navy, p. 38-42.
4. The Secret Post Office, p.
5. Pearl Harbor Report, p.
6. Stimson, Memoirs, p.
7. James, The Eyes of the Navy, p.70
8. Moyzisch, Operation Cicero, p.40
9. Pratt, Secret and Urgent, p.191
10. Dallin, Soviet Espionage, p.273
11. ibid. p.110
12. ibid. p.406
13. Rockne, Coaching Football, p.
14. Moyzisch, Operation Cicero, p.39
    Dallin, Soviet Espionage, p.485, p.452, p.449
15. Heilbrun, The Soviet Secret Services, p.24
XXX Dallin, Soviet Espionage, p.5-14
16. Bialoguski, The Petrov Story, p.132-133
    Dallin, Soviet Espionage, p.450, p.19-21, p.198-200
17. Dallin, Soviet Espionage, p.229-231
    Morgan, Spies and Saboteurs, p.115
18. Dallin, Soviet Espionage, p.465
19. ibid. p.294-299, p.303
20. ibid. p.289
    Bialoguski, The Petrov Story, p.xiii-xvi

21. Dallin, Soviet Espionage, p.471
22. ibid. p.290
23. ibid. p.254
24. ibid. p.298

    Pratt, Secret and Urgent, p.233
25. Morgan, Spies and Saboteurs, p.14
26. Moyzisch, Operation Cicero, p.203-205

    Dallin, Soviet Espionage, p.494, p.499

    Pratt, Secret and Urgent, p.233

    James, The Eyes of the Navy, p.xii-xvi

    Heilbrun, ~~pz25x26~~ The Soviet Secret Services, p.35-36
27. Heilbrun, The Soviet Secret Services, p.154

~~28~~ Dallin, Soviet Espionage, p.vii-viii

28. James, The Eyes of the Navy, p.28-31
29. Pratt, Secret and Urgent, p.15-16
30. ibid. p.83
31. ibid. p.40
32. Dallin, Soviet Espionage, p.154
33. ibid. p.254
34 Pratt, Secret and Urgent, p.190, p.163
35. James, The Eyes of the Navy, p.136-154
36. Pratt, Secret and Urgent, p.12
37. special, see note.
38. Pearl Harbor Report
39. James, The Eyes of the Navy, p.30-31

    Pratt, Secret and Urgent, p.80-81

40. James, The Eyes of the Navy, p.136-154

41. Pratt, Secret and Urgent, p.13

42. ibid. p.239

43. ibid. p.180

44. ibid. p.184

45. Dallin, Soviet Espionage, p.143-145

46. ibid. p.245-247

47. ibid. p.216-217

48. Heilbrun, The Soviet Secret Services, p.24

49. ibid. p.28

50. Von Mellenthin, Panzer Attack, p.

51. Dallin, Soviet Espionage, p.452.

Moyzisch, Operation Cicero, p.54, p.86-99

52. special

Note that in some cases , where I do not have the books at hand, I cannot supply the page number of the reference.

Special:

37. I believe that in 1953, Fletcher Pratt wrote and article in Computers and Automation (Berkley Ent.) dealing with the application of computers to cryptanalysis. I have never seen this article, and I am not sure it exists, but a good cross reference on Pratt, or a direct inquiry, might give us a valuable source of public domain literature.

52. What I need here, for a filler, is a reference to a vital piece of comint, like the Yamamoto incident, which is p.d., and important. Do you know of any?