DOCID: 3978516

~~Top Secret Codeword HVCCO~~

Do Not Circulate
Do not Copy

The Room 40 Compromise (U)

(U) Abstract

In 1925 a file of over 10,000 sensitive highly secret decrypts from World War I Room 40 cryptanalysis was compromised in London to an American lawyer. He took several hundred of the decrypts out of Britain and in 1927 turned them over to the German government, in a lawsuit. Within weeks the German Army and German Foreign Office embarked on intensive and urgent programs to improve their cryptography. The steckered Enigma, and greatly increased production and use of one time pad were the direct results of these programs. The decrypts contained extremely derogatory information about German biowar and covert operations in neutral countries during World War I. The decrypts and associated lawsuit were widely publicized, and occupied the highest levels of the German government including Hitler and Goering, and the affair was cause celebre for over 12 years --- all because their cipher failures were exposed. This had a sinister effect on German cryptography before and during World War II.

Footnotes not included

DOCUMENT CONTROLLED
BY STATUTE 18USC798

NO COPY NO DISSEM

Declassified and approved for release by NSA on 06-13-2012 pursuant to E.O. 13526

DOCID: 3978516

~~TSC~~

NO COPY NO DISSEM

The Room 40 Compromise (U)

~~TSC~~ The consequences of compromising or declassifying decrypted messages are often difficult to identify. Part of the tragic background to World War II was the compromise of hundreds of political decrypts produced by Room 40 during the interwar period. What is unique about this compromise is that captured German documents show a sudden and urgent intensification in German military and diplomatic cryptography, which began a few weeks after the compromised decrypts were put in their hands in March 1927. The steckered Enigma was one of the developments. A considerable intensification of one time pad production and use was another. Nothing showed up in German traffic at the time --- the changes were much more fundamental, and were manifested years later in the non-exploitability of many crucial German nets.

~~(TSC)~~* Soon after the highly secret decrypts escaped control, the "inviolable secret" of Room 40 got into the newspapers, with a fanout of disclosures by people who had pledged to keep the secret. Admiralty tried to stifle this outpouring of cryptologic secrets, and suppressed books by several prominent people, but too late. In the detente of the period the preservation of wartime secrets was treated as no longer necessary. The Germans however, after they got the decrypts, clamped the tightest secrecy on their cryptographic innovations, backed up by the 1914 wartime secrecy law.* The political climate of the time, and the ideological motives of several of the key figures were important factors in how the compromise occurred, and the consequences that came from it. Years later the compromise was described as an authorized declassification of the decrypts, but the available evidence contradicts this.

S The cost to Britain and the U.S. of the cryptographic developments the Germans embarked on after the Room 40 decrypts reached them was profound, irrevocable, and long lasting.

(U) At the time the compromise occurred, no one in Britain or the U..S. grasped what the consequences would be. Even if they forecast the effects correctly, they could prove nothing because the Germans had adopted a friendly outward appearance. Gradually documents and records accrued , some classified and some unclassified, which could allow a reconstruction of what had happened. The central point of the story is simple but unpleasant, viz: disclosing decrypts or other cryptologic secrets is immensely damaging to future intelligence and warfighting capability.

(U) Background

At the end of World War I Room 40 O.B., ...

DOCID: 3978516

(TSC)*

At the end of World War I Room 40 OB, the British Naval codebreaking center was closed down, and the results sealed up in extreme secrecy.[1] There was no Naval threat from Germany, but the German diplomatic party at the Paris Peace Conference showed up with unbreakable new ciphers — which was attributed to the publicity given to the Zimmermann telegram in 1917[2] — and a policy of continued secrecy was firmly followed by the British Government, in order to avoid stimulating a cryptographic ~~race~~ race by disclosing what kinds of codes and ciphers could be solved.[3]*

(U) The Peaslee Connection

(U) Despite this policy of secrecy, word gradually spread in some circles about the Room 40 successes.[4] In 1924 the American companies who had suffered losses from the ~~"Black Tone"~~ "Black Tom" explosion of 24 July 1916 retained an American lawyer Amos Peaslee to try to track down the saboteurs responsible for ~~Black Tone~~ Black Tom and other sabotage, ~~as~~ so they could sue the German Government for damages.[5] The trail was cold after 8 years, and the FBI and private detectives had given up the case.[6] In the ensuing year Peaslee learned from some source of the existence of thousands of decrypts of German agent traffic and other secret messages in the possession of the British Government, which were thought to be related to the ~~Black Tone~~ Black Tom case.[7]

(U) Peaslee was a well-connected New York lawyer. Educated in the U.S. and in England, in World War I he was commissioned as a Major in the U.S. Army and put in charge of the "Silver Greyhounds", an elite high level AEF courier service which carried sensitive dispatches between Washington and the General Pershing's HQ in France.[8] After the Armistice this courier service was attached to the Paris Peace Conference, and reestablished

communications with U.S. Embassies and Legations and Field Commissions abroad.[9] They were the U.S. counterpart to the British "King's Messengers".[10] At Paris, Peaslee met Lansing, the U.S. Secretary of State.[11] One of Peaslee's subordinates in the Silver Greyhounds was Joseph Sims, cousin to Admiral W.S.Sims, commander of U.S. Naval Forces in European waters.[12] Joseph Sims later edited a book about Peaslee and Hall, lauding them.[13]

(U) When Peaslee learned of the Room 40 decrypts, he sought a way to meet Admiral Hall.[14] To this end he wrote Lansing on 29 July 1925 and arranged a conference.[15] At the meeting Peaslee learned that Admiral Sims, a noted anglophile, was the best friend of Admiral Hall in the U.S., and Peaslee wrote Sims on 5 August 1925 asking for a conference, reminding Sims that they had met during the war, and referring to his cousin Joseph Sims.[16] From Sims, Peaslee got a letter of introduction to Hall on 14 August 1925, and on 18 August 1925 wrote Hall, c/o Admiralty, asking for a "brief conference", and claiming U.S. Government sanction for his mission.[17] Peaslee signed the letter as "Major Peaslee, U.S.A".[18]

(U) The Peaslee-Hall Meeting

Peaslee met Hall at the latter's London residence on 27 August 1925 at noon.[19] He presented his credentials, including the letter from Adm. Sims, and described what he wanted -- which was to get access to the Room 40 decrypts to establish proof that the German government had ordered the sabotage at Black Tom and other episodes.

Incredibly, Hall said, "well, I will do it" and he thereupon led Peaslee to a place full of filing cabinets containing over 10,000 decoded German cables and radio grams.[20] These documents were dated 1919 and marked "not to be opened until 20 years after this date."[21] Hall left the same day on a shooting trip to Scotland, but put his house and servants at Peaslee's disposal so that Peaslee could live there while he was working.[22] By 30 August 1925, Peaslee had read through the 10,000

(U) The Peaslee-Hall Meeting

(U) Peaslee met Hall at the latter's London residence on Thursday 27 August 1925 at noon.[19] He presented his credentials, including the letter from Admiral Sims and described what he wanted --- which was to get access to the Room 40 decrypts to establish proof that the German Government had ordered the sabotage at Black Tom and other explosions.

Hall may have believed that Peaslee was a U. S. Army Major on some official mission.[20] Incredibly, he agreed and led him to a file of over 10,000 decoded German cables and radiograms.[21] By Sunday 30 August 1925, Peaslee had read through the 10,000 decrypts and selected 264 which dealt with German sabotage and covert war (including biological war operations) in America.[22] He wrote to Hall in Scotland from his London hotel about the German biowar operations.[23]

(U) From London, Peaslee went onto Berlin and from there back to the USA with copies of 264 of the decrypts.[24] These messages, with explicit dates and addresses clearly showed which German Attaché links had been read, and the text showed that the code books had been recovered.[25] In due course Peaslee turned these decrypted messages over to the German Government, as Hall knew he would.[26]

(U) Analysis of the Disclosure

(U) At the end of World War I it was "generally believed" that Hall had destroyed the files he had amassed as DNI from 1914 to 1919, but he kept them somewhere.[27] These were probably the filing cabinets that Peaslee saw on 27 August 1925.[28] The 10,000 decrypts that Peaslee saw were English translations of important political messages, which had been sent directly to Hall.[29] The total volume of military and political messages of Axis and neutral countries intercepted and decrypted by Naval Intelligence was very great[30] --- German traffic alone was more than 1000 messages a day[31] --- so Peaslee could not have seen all the wartime decrypts.[32] Hall had no contact with Room 40 or its successor G.C.&C.S. after he left the Navy in January 1919,[33] and would not have had access to their files in 1925.

(U) Although published accounts by James and Sims say Hall got authorization for Peaslee to use the decrypts, the details vary.[34] James in 1955 claimed Hall got prior authorization for Peaslee to see the decrypts.[35] Sims in 1944 gave a different version, viz:[36]

(U) PEASLEE AND HALL MEET

(U)

Peaslee met Hall at the latter's London residence, 63 Cadogan Gardens, on Thursday, August 27, 1925. He presented his credentials and told his mission.

After what seemed hours to Peaslee, during which Hall's famous eyes pierced Peaslee's "immortal soul," Hall snapped out, "Well, I will do it."

He led Peaslee to a place full of filing cabinets containing over 10,000 decoded German cables and radiograms. Hall had read and decoded every one which the Germans had sent or received during the war!

What Peaslee then saw quite took his breath away. They were the records—the documents which had been locked up in 1919 "not to be opened until 20 years after this date"—which Ambassador Page had wished to live to see.

Before the cables were finally released for use of the American government Hall took the matter up with the appropriate British authorities, and the way was cleared. He told Peaslee:

"I am going on a shooting trip to Scotland, but my house and servants are yours and you may live here while you are working."

(U) Hall made a decision on the spot, and "led" Peaslee to an archive, which apparently was in his own house. Hall certainly had the decrypts in his own house in Hampshire in 1930, and referred to the archives as "my files".[37] If the decrypts had been in Admiralty or in GCCS, they would have had to travel more than mile, which would not fit "led".[38]

(U) Sims' account is Peaslee's version of what happened, tailored for the public record 17 years after the event. James' account, which claims prior authorization before Peaslee saw the decrypts, was written over 30 years after the event in an admiring biography of Hall. A distinctly different account was given in 1937, some 12 years after the event, by Landau --- in which Hall explicitly did not get authorization. In Landau's narrative, Hall told Peaslee the decrypts were stored "in several tin boxes in my basement".[38A] Hall decided on the spot to disregard the 20 year secrecy caveat, and told Peaslee he could copy any cables he wanted to. Hall then left for grouse shooting in Scotland that afternoon, putting his house at Peaslee's disposal. In Landau's account:

(U)

> "His rapid and sweeping decision was typical of the man. Fortunately he was retired from the Navy and was, therefore, his own master". [38B]

(U) Landau of course was not an eyewitness, but neither were Sims of James. Landau's book The Enemy Within is a detailed account of the whole World War I sabotage operation and the legal case that followed it. Landau, a former wartime British Secret Service officer, had assisted the investigation, knew many of the principal characters well, and had gotten "the" personal stories".[38C]. In particular, Landau had no axe to grind.

(U) There are a number of implications of the Sims' account which support Landau's version of the incident. Peaslee went through the 10,000 decrypts between Thursday afternoon and Sunday afternoon, and it is unlikely that a government archive

containing such sensitive political materials would have been kept open over a weekend for an uncleared American private citizen. Landau says Peaslee worked in Hall's house. [38D]. Sims states that Hall made his house available for Peaslee to work in, so the file of decrypts could hardly have been anywhere else.

(U)?

Sims says that before the cables were "finally released" for the use of the "American government" Hall took the matter up with the appropriate British authorities, but that could have been long afterwards. Sims never says <u>when</u> Hall went to the "appropriate authorities" or <u>who</u> they were. James is equally uninformative. Since Hall left directly for Scotland there was really no time to get an official release, and neither G.C.&C.S. nor Admiralty would have let an unknown American cart such files off to Hall's house, or browse through them over a weekend. Some Room 40 records were gathering dust in an attic in Admiralty in 1937 [39], but in 1925 G.C.&C.S. was administratively under the Foreign Office. [40] Very high level Foreign Office authorization would have been needed to release these sensitive political decrypts because they were covered by the Official Secrets Act. [41] Since the Foreign Office disliked Hall, they had little motivation to

ISC

let Peaslee read and copy files which even senior British officials could not have seen without high level clearance.[42] Authority to release such sensitive political materials to a foreign national, or to the American government, would lie outside Admiralty authority.[43] Further, British policy in 1925 was sympathetic to the Germans, and the 1924 Dawes Plan had been encouraged by Britain[44] --- so releasing decrypts that would injure the German government would conflict with that policy.[45] Peaslee soon after wrote that Hall "arranged to place the British records at my disposal.[46] He also permitted me to take copies of certain cablegrams ..." Peaslee does not say that the British Government gave him access or permission to take away copies. Once Peaslee got the decrypts out of England, the situation was out of the control of the British government, and they may have decided to do nothing further to oppose the use of the decrypts because they didn't want publicity about GCCS, and had no real choice. The fact that neither Sims, nor James nor Hall nor Peaslee ever identifies who authorized the release lends an air of mystery. If Hall did release or expose the decrypts to Peaslee before getting a valid authorization, he could have been subject to legal action, but such proceedings are very rare --- especially since Hall was an Member of Parliament, and had the title "Admiral Sir Reginald W. Hall, K.C.M.G., C.B., D.C.L.,LL.D."[47]

(v) One very interesting point is that no one else disclosed anything about Room 40 publicly until November 1925, months after the decrypts had been given to Peaslee [48].

(U) "Blinker" Hall's Decision

(U) Hall gave Peaslee access to Room 40 decrypts pertaining to German sabotage and biowar and other covert operations under circumstances in which he knew

[redacted] publicity would inevitably follow. Even acknowledging the Room 40 decrypts gave away an official secret which had been tightly held.[49] Hall's archive contained a great deal more extremely sensitive political information that Hall had acquired during his tenure as DNI.[50] Hall could not release the information about the German covert war operations directly because no British publisher could touch it, but Peaslee could disclose the information --- if he chose to.[51]

(U) Although Peaslee described himself as "Major Peaslee, U.S. Army", he was not a U.S. official, and he did not approach Hall through official channels.[52] He was a private lawyer with good contacts and entree.[53] Hall continued to address him as "Major Peaslee" in correspondence for several years in correspondence which gave an official coloration to the arrangement.[54] Peaslee wanted the decrypts to build a case for his clients, but if they had leaked into public circulation or into the American press in the Fall of 1925 they could have had a significant effect on major British diplomatic and budgetary matters that interested Hall. British policy at that point --- particularly in defense matters --- hung on the question of trusting Germany.

(U) Prosperity through Pacifism

(U) After World War I there was considerable public interest in disarmament, even though the governments were fearful of Russian expansion.[55] The U.S. had a naval building program to give parity with the wartime British Navy.[56] The British did not get the German warships because they were scuttled at Scapa Flow.[57] As a result the British Coalition Government under LLoyd George had to face the question of a Naval building program at a time when they had big debts, a large Army in Germany, and the world economy was still devastated by the war.[58] Pay cuts and discharges were initiated.[59] Hall had a keen interest in Naval and Merchant Service matters, and made his maiden speech the day he joined Parliament 13 March 1919 on the Navy's service in the war, and on pay and pensions for the Navy.[60] The Washington Naval Conference of 1921-22 resulted in commitments to reduce the Royal Navy and to stop building major warships.[61] Sir Eric Geddes, former First Lord of the Admiralty, made severe cuts in the Navy budget in 1922 and many long service officers were summarily discharged.[62] A crisis between Greece and Turkey at Chanak in 1922 brought a threat of war to Britain and the Empire, and public rejection of this --- the British people wanted disarmament and no commitments --- led to a breakup of the Coalition Government and the resignation of LLoyd George.[63] Bonar Law became Conservative Prime Minister, while Lord Curzon the Foreign Secretary began to reassert the authority of the Foreign Office, which had lost power to the War Cabinet after 1914.[64] The Germans had become allied with the Russians at Rapallo in April 1922, and secret military

projects developed between them.[65] At the same time the Germans cultivated the British and Americans to offset the pressure from the French.[66] It was possible to see, in the combination of German industrial capability and Russian resources, a potential threat. The British Government feared Bolshevism,[67] and Hall on the day he left the Navy in 1919 had warned his Admiralty staff that Russia was a greater enemy than Germany.[68] In 1922 Lord Curzon had G.C.&C.S. and the cryptanalytic mission transferred totally from Admiralty to the Foreign Office --- ending Admiralty control of that critical intelligence.[69] Even the DF mission was transferred at a time when radio interception and DF were still extremely secret.[70] Austen Chamberlain in 1921-22 had caused considerable stress within the Conservative Party by taking a leading part in negotiating with the Sinn Fein (whom Hall had fought bitterly during the war) for the establishment of the Irish Free State.[71] In late 1923 the Conservative Party under Baldwin was badly defeated in a General Election[72] --- even Churchill lost his seat[72A] --- and the Socialist government of Ramsay MacDonald embarked on Anglo-Russian talks in 1924 which, after publication of a Zinoviev letter advocating violent revolt, became an election issue that defeated MacDonald in October 1924.[73] Baldwin became Prime Minister again , but made Austen Chamberlain the Foreign Secretary and Churchill the Chancellor of the Exchequer.[74] Churchill undertook drastic reductions in the Navy budget[75] while Chamberlain --- long a Lloyd George affiliate --- pursued a pro-German policy based on a repudiation

of war and militarism, resulting in the Locarno compact in 1925,[74] and the admission of Germany (still an ally of Bolshevik Russia) to the League of nations in 1926.[77] There were severe battles between Churchill and Beatty the First Sea Lord, over the Naval budget.[78] Despite the treaty of 1922 Britain continued to build cruisers to keep the shipyards active, but the Fleet Air Arm was taken away.[79] Navies were regarded as "offensive" systems and the major arms cuts concerned them.[80] Hall was obviously well thought of by the Admiralty for they promoted him in 1922 from Rear Admiral (Retired) to Vice Admiral (Retired), and to Admiral (retired) in 1926 [81].
When he rejoined the Parliament in 1925 after an absence, he continued to champion Navy causes.[82] However, in the climate of detente --- which was based on trusting Germany and discounting Russia --- Navy prospects were not encouraging. The negotiations in mid 1925 were very uncertain and required all of Chamberlain's energy.[83] He got the Nobel Peace Prize in 1925 for his efforts (shared with Dawes).[84] While the victors of World War I were commited to a pacifist policy, and Europe basked in a feeling of peace and hope,[85] the Germans were already secretly rearming.[86]

(U) Hall on the Outside

(U) This moralistic anti-war foreign policy, the budget cuts, and the politics surrounding Chamberlain himself, all had considerable significance in mid 1925 for "Blinker" Hall. Hall, during his reign as DNI, had shown himself to be a ruthless, ambitious opportunist, extending his tentacles into Scotland Yard, M.I.6 and foreign policy.[87] His exploitation of the Roger Casement diary was disapproved by many people at high levels,[88] as was his extreme secretiveness and tight

personal control over the diplomatic decrypts of Room 40.[89] When the war ended he was summarily released from active Navy service.[90] He had expected to go to the Paris Peace Conference as the Head of the Intelligence Bureau, but Sir Rosslyn Wemyss, first Sea Lord, rejected him.[91] He had received KCMG in October 1917, but was not included in any post-war Honours List, although the other Directors of Military Intelligence all received the Order of the Bath.[92] He had, at the end of the war, been spoken of as a future Foreign Secretary, but he had made too many enemies, and once he was out of the Navy he was never again taken into the Government.[93] He accepted a Directorship with a large British company and, his financial position assured, was elected to Parliament representing a constituency in Liverpool.[94] Honored in 1919 by Cambridge University and Oxford University,[95] he became involved in the Unionist Coalition Party organization at the request of Prime Minister Bonar Law in 1923, against the strong advice of his friends.[96] When the coalition was defeated he lost his seat in Parliament and was subjected to an unscrupulous vendetta of character assasination by his former political cohorts.[97] His health broke down and he resigned from the Party organization in March 1924.[98] He ran again for Parliament for Eastbourne and returned to London as an M.P. in 1925, at about the same time Peaslee's letter arrived.[99] After these excoriating experiences, Hall may have hesitated to trust the judgement of people in authority concerning the handling of the Peaslee visit. Hall was never reluctant to rely on his own unaided judgement, no matter what the outcome.[100]

(U) Whatever benefit Hall expected in letting Peaslee at the decrypts, e.g. punishing Germany financially, or exposing German perfidy, he knew he was communicating and exposing secrets of the greatest sensitivity.[101] Peaslee did not publicize the decrypts until they were filed in formal claims in 1927,[101A] by which time the British Army and Allied Control Commission had left Germany, and detente was in place.

~~(S)~~* Hall had caused sensational propaganda and become a force in wartime policy by manipulating and releasing secret information,[102] but he was not a cryptanalyst and was not at all qualified to judge the strategic effect of releasing verbatim decrypts to the Germans.[103] James claimed in 1955 that cryptanalysis had ended in 1919 because of widespread cipher changes,[104] but that was neither true nor a defense* --- since the content of the decrypts was still sensitive. Hall was always more of an opportunist and adventurer than a strategist --- as his personal career and several downfalls showed --- and even his "great coup" of public exploitation of the Zimmermann telegram did not actually cause the USA to enter World War I, although Hall may have thought so.[105]

(U) What is evident is that the decrypts released to Peaslee, if they had become public in 1925 instead of 1930, would have been very upsetting to British negotiations and policies at a critical stage in 1925. Official release seems improbable, and the decrypts were not published by the British Government.[106]

~~TSC~~

(U)? The Peaslee case and other unofficial releases that followed made Hall's contribution to World War I victory widely known after 1925 [107] --- when British peacetime cryptanalysis was still extremely secret. [108] Hall was a gambler but not a good judge of consequences. [109] Peaslee was a channel through which the Room 40 secrets were disseminated, with far-reaching effects --- but probably not those Hall had in mind.

(U) Peaslee's Brief

~~(TSC)~~* From 1925 to 1927 Peaslee sorted out the decrypts, and tracked down and interrogated various elusive witnesses, and then he filed a lengthy brief with the Mixed Claims Commission in Washington in two parts on 14 March 1927 and 25 March 1927, including the decrypts in the brief. [110] This produced an immediate cipher crisis in the German Army and Foreign Office, who took steps to improve their cipher security.* The details are interesting.

~~(S)~~ The German Army's Reaction

~~(TSC)~~ On 28 March 1927 ---just two weeks after the first formal filing of the decrypts came into the hands of the German Agent to the Mixed Claims Commission [111] --- there was a hastily called meeting between Cipher Machine A. G. (CMAG) and the Cryptologic Agency of the War Ministry to improvise changes to the lamp-panel Enigma by the introduction of a variable plugging between the endplate and the fast wheel [112]. The Army had already adopted the unsteckered Enigma, which was used in other German government departments, and was in fact technically well ahead of all other armies in cipher security [113]. But they changed the Enigma abruptly, and imposed severe wartime secrecy laws on every aspect of the design and manufacture [114]. Up to that point Enigma design had not been secret [114A]. (The Germans also intensified their secret rearmament program in 1927 [115]).

~~(TSC)~~ At that March meeting CMAG suggested a pluggable reflector as well [116]. The Army insisted that the idea for the pluggable endplate was its property, and therefore subject to the secrecy law [117]. On 2 May 1927 a contract was let to CMAG, specifying the changes to the "small" Enigma (26 letter battery model) and imposing total secrecy [118]. A long trail of changes and revisions over the next several years underscore the haste of the stecker introduction [119]. Originally the plugboard was to have 52 holes and 26 wires. On 17 February 1928 the Cryptologic Agency proposed the use of double-pole

contacts, with 13 plugwires [120]. A CMAG memorandum about the meeting noted that CMAG had filed a patent application on 9 August 1926 for the concept of a variable plugging in front of or within the machine [121]. The Army had altered machine Number A.336 to demonstrate the double-prong plugboard [122]. The 52-hole plugboard had been rejected as a source of error [123]. The Army expected to use only 6 pairs of plugs at a time, the other points being automatically self-steckered [124]. By this time 400 Enigma machines had been delivered with a 13 x 2 plugboard [125]. CMAG considered the new plugboard more complicated [126]. On 1 March 1928 Siefert, Fenner and Schroeder for the Army met Rinke, Scherbius and Korn of CMAG and there was a squabble over the Patent application of 9 Aug 1926 [127]. The Army insisted that <u>any</u> plugging feature of the Enigma be kept totally secret, and assumed the costs of the Patent Office [128]. On 30 March 1928 another CMAG/Army conference discussed suppressing any mention of plugging from the CMAG Patent claims, and keeping <u>all</u> pluggable Enigma variations and designs secret [129]. The Army was insistent [130]. On 20 August 1928 CMAG suggested a switch matrix to replace the double-pole plugs and cables [131]. On 6 August 1929 there was an Army/CMAG conference to replace the previous plugboard arrangement of the "small Enigma" with a better one [132]. The Army wanted two-prong plugs, but because of limited space in the radio trucks any changes had to be very compact [133]. CMAG proposed commercial exploitation of the pluggable reflector, which they considered their own property and had already offered to

Hungary [134]. The Army Cryptologic Agency refused the pluggable reflector because it was not covered by the 1914 wartime secrets and treason law --- cited in the contract of May 1927 [135]. Later, on 18 Februaryy 1930 Siefert of the Army Cryptologic Agency told CMAG that public use of the pluggable reflector would violate the secret contract of 1927 [136].

On the evidence in the TICOM documents, it appears that the Army forced a sudden change in the Enigma, already in production, which gave a step-function improvement in its security. They also clamped the wartime secrecy law on every aspect of the Enigma that concerned variable plugging. They then "froze" the design (but not the embodiment) at that point and refused to make any further improvement in Enigma security --- even though CMAG patented improvements in motion and plugging --- because the secrecy law only covered the 1927 keyboard-to-fast-wheel plugging. No other improvements in Enigma security were adopted until late in World War II when they knew the machine was being read. The 28 March 1927 meeting was adecisive[illegible]

TSC

(U) Other Services

(TSC) There is no evidence of a cipher crisis in the Navy or the Luftwaffe in 1927.[137] The Luftwaffe was coverts and had no existence outside the Army.[138] The Navy was very small, after the reductions of the Versailles Treaty, and was trying to keep its identity separate from the land forces.[139] The War Ministry did not particularly trust the Navy after the mutiny of 29 Oct 1918 and ensuing revolt --- subsequently called "the stab in the back" --- that made the Armistice inevitable.[140] In addition, the Navy was middle class in its Officer corps, while the Army Officer corps was drawn from the aristocracy --- and had more political power.[141] The War Ministry kept its cryptologic developments secret from the Navy, even in World War II.[142] The decrypts Peaslee provided concerned wartime Army agents, who had used Army and Foreign Office ciphers, and the Army and the Foreign Office may have decided not to share them with the Navy in 1927. The Enigma itself had been watched over by the Army since 1918,[143] and the 26 letter battery Enigma was developed and manufactured to meet Army specifications for a compact machine.[144] The Navy used commercial Enigmas (with great confidence in their security), beginning about 1920 with the big table model Enigma which was later displayed by Scherbius in 1923.[145] In 1925 they ordered 50 of the lamp Enigmas[146] --- a 29 letter machine without a variable plugging [147]
In 1926 the 26 letter unsteckered three wheel commercial Enigma became available,[148] but was apparently not adopted by the Navy until 1931.[149] In the late 1920's the Navy only had about two dozen ships larger than a patrol boat.[150] The Poles were able to break into the 29 letter machine during the 1920's and get the continuity and cribs to attack the steckered Enigma when the Navy adopted it.[151] In the 1920's the German Navy had complete confidence in the security of their cipher machines, and they were the only Navy using modern cipher machines operationally.[152] They only obtained the steckered

Enigma --- with War Ministry approval --- in 1934, when Hitler was in power and the steckered Enigma was adopted uniformly by all three Services.[154] In 1927 the 26 letter Enigma was just going into serial production to meet Army needs, and the War Ministry was the department concerned with its security for military purposes.[155] [153]

The Foreign Office Reaction

The German Foreign Office (Auswaertiges Amt) was very sensitive to COMSEC threats after the painful lesson of World War I. During the 1914-1918 war they had used comparatively simple codes and enciphered code systems which they considered secure.[156] Then the publicity given to the Zimmermann telegram by Admiral Hall showed the German nation that their diplomatic ciphers were catastrophically vulnerable. This produced a major cipher crisis in 1917, resulting in the Army breaking the main Foreign Office cipher (see Appendix).[157] As soon as the war ended the Foreign Office abruptly changed to one-time pad encipherment, and their messages from the Paris Peace Conference were completely unreadable.[158] Within a few years the British cryptanalysts abandonned all work on the German diplomatic systems, and did not even collect the traffic.[159]

In order to reduce their diplomatic telegraph bills the F.O. used condensing codes (Kurzungssatzbuch) for different languages, which they reedited and improved during the 1920's.[160] They also purchased a machine in 1925 for generating and printing pages of key, for 5000 Reichsmarks.[161] The machine was supplied by a British engineering firm Loranco Ltd. of London, through a business agent Otto Krebs.[162] This system was later known to the Allied cryptanalysts in World War II as the GEE system.[163]

~~(TSC)~~ After Versailles the German rearmament program depended on secrecy.[164] By 1927 they had a number of secret foreign operations in progress which required secure communications. The secret naval supply service, Etappdienst, was being reconstituted to supply German Naval operations abroad in case of war, or to run critical materials through a blockade.[165] Secret war training for the Army and Air Force was being conducted in Russia.[166] "Mole" operations were being set up in many countries.[167] German military and naval attachés were engaged in secret activities, and depended on diplomatic channels for their communications.[168] Part of the secret rearmament program was being conducted abroad, and Krupp carried out experimental arms construction outside Germany in neutral countries.[169] Financial and business operations across German borders were limited by the Versailles Treaty and were conducted secretly.[170] In peacetime most of these activities would communicate over Foreign Office channels.[171] In the cipher crisis of 1917 the Navy and Army had been severely critical of Foreign Office attaché ciphers,[172] and the War Ministry was very interested in the security of their attaché traffic.[173]

~~(S)~~ When the Room 40 decrypts, many of which came from diplomatic and attaché messages, arrived from Peaslee in March 1927, they produced a double crisis. First, there was the legal and propaganda matter of the sabotage[174] and germ warfare[175] operations at a time when the U.S. Government and private investors were helping the German nation, through the Dawes Plan, to recover from the economic collapse of the

mid-1920's.[176] Second, there was the irrefutable evidence --- soon to be made public at the Hague in litigation[177] --- that the most secret agent ciphers had been read extensively.[178] The clear evidence of the Room 40 decrypts could not be disregarded, even though the messages were ten years old and the war long over --- it gave unarguable proof of the need for permanent secrecy for diplomatic communications.*

The Foreign Office had been offered the Enigma machine[179] in 1924 and 1926,[180] and each time the head cryptologist Selchow rejected it as insecure and unsuitable for diplomatic traffic.[181] A later offer in 1928 was also refused.[182] Because telegraph rates to foreign embassies were very high, and the rate was double for cipher text (which the ENIGMA produced), the Foreign Office used code books to condense the stereotyped diplomatic language, and then used conversion tables to translate the five digit enciphered code into "pronounceable" five letter groups.[183] This cut cable costs by at least a factor of four, and in 1926 these economies were standard practice for F. O. cipher clerks.[184] However, Selchow's principal objection in 1924 and 1926 was that cipher machines did not give more than temporary secrecy.[185] The steckered Enigma did not exist in 1926 and the unsteckered machine was known to the F. O. to be vulnerable to attack.[186] In 1927 the development of the steckered Enigma was secret from the F. O.[187] In 1928 the War Ministry tried to get the Foreign Office to support an outright purchase of the Enigma rights and patents for 1.8 million

Reichsmarks to protect future cryptanalysis and German COMSEC at the same time.[188] The F. O. , which had refused to adopt the ENIGMA in 1928 also refused to support the purchase of the Patent rights, pointing out that the ENIGMA was vulnerable to machine aided cryptanalysis.[189] Their preference for pad systems continued even after Hitler came to power and the Enigma or steckered ENIGMA were adopted by all other departments.[190] In 1942 problems in pad distribution made the F. O. look for a cipher machine, but even then they refused the four wheel naval Enigma as insecure and proposed a very secure version of the ENIGMA themselves, but Heimsoeth und Rinke refused to build it for them.[191]

By 1927 the German F. O. was quite sure that the one-time pad was what they wanted, but so far they had only bought one "Numierwerk" in 1925 to generate the key pages, and two presses to do the printing.[192] After the Peaslee materials arrived --- hundreds of the most humiliating decrypts, backed up by a multimillion dollar damage suit, and the guarantee of publicity at the Hague during the trial ---- they set about acquiring more COMSEC materials, even though their ciphers at that time were as secure as any in the world.[193]

Captured documents show a number of significant COMSEC expenditures in the period 1927-1933, totalling over 200,000 Reichsmarks, and considerable wear and tear on the pad generating equipment.[194] They bought at least two more pad

generating machines, and apparently an additional two machines. They had at least three different "frames" and four different sets of 240 or 250 key generating wheels.[196] They obtained three Numierwerk pad generators from the British firm Loranco Ltd. in 1925, 1928 and 1932,[197] but also apparently purchased comparable equipment from German suppliers in 1927 and 1933.[198] Despite the shortage of money and the low volume of diplomatic traffic, the Foreign Office bought a substantial ensemble of pad generating equipment and used it heavily.[199]

The first Numierwerk was delivered 16 Oct 1925 at a cost of 5000 RM.[200] They were then offered a 240 wheel Numierwerk for 5000 RM on 14 Nov 1925, which was apparently declined.[201] A new "speed press" was obtained in December 1926.[202] On 19 May 1927, after the Room 40 decrypts had arrived, they received three different proposals for Numierwerk with 250 wheels from Clemens Mueller.[203] On 22 Oct 1927 they paid 17800 RM for the equipment they selected.[204] In 1928 Loranco Ltd. supplied a Numierwerk through their agent Otto Krebs.[205] On 19 Jan 1929 the F. O. got an estimate on 240 new wheels.[206] In September 1929 they received 500 copies of a new code book.[207] On 24 Sep 1931 they paid 13595 RM for new codebooks.[208] In 1931 they paid over 6700 RM for repairs to the equipment.[209] There was a 1 June 1931 bill for the amazing amount of 136,331 RM for some undisclosed COMSEC purchase[209A] --- during a world depression when contemporary repair bills ran about 400 to 500 RM.[210] Over 19000 RM were spent in 1931 for new codebooks.[211] By 20 Jan 1932 they needed

repairs to Numierwerk No. 1 after printing more than one million sheets of pad on it, and this repair was done by Mueller for 500 RM.[212] In 1932 or 1931 Loranco Ltd. supplied a new Numierwerk, the third from that source.[213] On 10 Nov 1932 Krebs offered a tender for a frame and 240 wheels for 11400 RM.[214] Three different proposals were made (as in 1927).[215] On 27 Mar 1933 Selchow wrote a justification for the Krebs proposal, noting that there had been a great increase in secret traffic and Military Attaché material.[216] Hitler had come into power in January 1933 and immediately pressed the secret rearmament program,[217] but Selchow had estimated on 3 Dec 1932 that a new Numierwerk would be needed on the basis of the pre-Hitler secret traffic.[218] On 3 April 1933 the Krebs machine was ordered.[219] The 1927 Numierwerk was repaired in 1936 for 36 RM.[220] In 1934 the War Ministry proposed a cooperation with the Foreign Office on clandestine radio nets and cipher security because it was dependent on the facilities and cipher links of the F. O. for its Attaché traffic.[221]

~~(tsc)~~ In 1927 the German Foreign Office had better codes and ciphers than almost any other country,[222] and a pad printing and generating system that was in advance of any other country and capable of producing a million pages of key at high speed.[223] They also had a capable cryptanalytic staff that knew how to break and also to evaluate ciphers.[224] The captured documents clearly show that after ordering a single Numierwerk in 1925 for 5000 RM, by May 1927 --- about two months after

Peaslee gave the Room 40 decrypts to them --- the F. O. began a systematic program of ordering new equipment and codebooks, and had gotten money and administrative support to invest in their expensive one-time pad system even though secret traffic was comparatively light until Hitler got into power.[225]

The intensification of the F. O. COMSEC occurred at the same time the Army was changing the ENIGMA to its steckered version.[226] With the plain evidence of the sensational decrypts in their hands, backed by a controversial and unwelcome suit for damages against the German Government to hold the interest of the high level people above them,[227] the F. O. cryptographers had justification to get permanent security for their cipher traffic. One of their cryptanalysts Schauffler had perceived a way to attack the ENIGMA in 1927,[228] and they knew it was theoretically solvable by "Enigma-like" mechanical devices as technology advanced.[229] Even when Hitler came to power and cryptography was centralized, Selchow still refused to adopt the Enigma[230] and he was backed up by the chief of the Foreign Office von Bülow[231]

Even though Hitler's personal staff, and the Sicherheitdienst and Gestapo used the ENIGMA,[232] the Foreign Office never yielded,[233] in their continued use of the cumbersome but secure one-time pad. This had a very marked effect on intelligence and diplomacy ~~for~~ during the entire Hitler [239]

(U) The German Counterploy

? (U)

The German Foreign Office in 1927 did not merely accept the windfall of the Room 40 decrypts, but cleverly intimated that they would contest the evidence on the grounds that the messages were forgeries.[235] Peaslee, alarmed, asked Hall on 30 May 1927 if the British cryptanalysts who had done the work could reproduce the decryption and justify the reconstruction of the codebooks.[236] Hall, who had kept in touch with some of the Room 40 people, including Nigel de Grey (who was then running a rare book store)[237] offered to produce the cipher books and cipher experts and have the decipherment repeated in Peaslee's presence from the original German cipher text.[238] He told Peaslee to get the cipher texts from the "Washington telegraph office".[239] When the Germans were sure that the decryption and the reconstruction of the codebooks could be proved, they reversed their position, declaring, "The statements of Admiral Sir Reginald Hall will not be disputed".[240] At the time the Zimmermann telegram was published, Hall had gone to a lot of trouble to create the impression that the plain text of the telegram had been obtained by the American secret service, to conceal the code breaking and pinching of German codebooks.[241] The readiness of Hall to repeat the decoding gave the German cryptologists proof positive, which their senior adminsirators had to accept, that the British had actually decrypted their traffic and had not simply gotten copies of the plaintexts somehow. The questions of inexact language gave further proof that the codebooks had been reconstructed, rather than merely stolen --- a further revelation of British capability. Apparently the purpose of the German ploy was over the heads of Peaslee and Hall.

(U) Peaslee's Case

(U) The Black Tom and other sabotage claim cases dragged on.[242] In 1930 the case was heard in the Palace of Justice at the Hague.[242A] The case attracted considerable publicity, and Admiral Sir Reginald Hall appeared as an expert witness for the American parties, but the Germans won the case.[243] The decrypts did not prove anything in court.[244] There were appeals, and a new law was passed which permitted new records to be subpoenaed.[245] A message in secret ink was introduced by the American side, and denounced as a forgery by the Germans.[246] Admiral Hall again appeared as an expert witness, this time on the subject of secret inks.[247] Both sides were paying witnesses for their testimony, and the witness changed sides.[248] In 1939 after negotiations involving Hess, Goering and Hitler and much additional investiggtion and litigation the Mixed Claims Commission reversed the Court of Justice on grounds that had nothing to do with the Room 40 decrypts, and awarded Peaslees clients 55 million dollars on 30 October 1939.[249] This was challenged by other American claimants, but upheld by the Supreme Court in 1941.[250] However there were many other war claims awarded against a $ 27 million settlement account, so Peaslee's clients after 25 years of litigation got a victory but not much money.[251]

(U) Detente and Security Policy

After Peaslec got copies of the decrypts out of England in 1925, the British government could --- if they actually knew of the compromise [252] --- have asked the U.S. and Peaslee to keep them out of the hands of third parties because their release was not consistent with U.S. or British policy towards Germany. They could even have pointed out the possible cryptographic benefit to Germany or other countries of knowing the extent of Room 40's success and the kinds of ciphers that were solvable. But even though both the U.S. and Britain were doing cryptanalysis in peacetime, and knew about each other's efforts, [252A] they couldn't admit it, and would have had to base their arguments on the impact of better cryptography in a future war. An argument of this kind would have conflicted with the detente of the era. [253] Peaslee, who believed that war should be outlawed, was pursuing his case to punish German aggression as a way of guaranteeing future peace --- so arguments about future wars would have had an uphill struggle.

Security policy, secrecy and cryptanalysis had all been subordinated to a belief in peace and the vicissitudes of domestic politics in Britain for a long time. The cryptanalytic activity which had run for three centuries in complete secrecy was shut down in 1844 as a result of a political struggle between Whigs, Radical and Tories at a time when naval and industrial supremacy made secrecy and communications intelligence seem unnecessary. [254] As a result Britain entered World War I without a cryptanalytic or radio intelligence service. [255] Under wartime conditions there was every motive for secrecy, to allow the good fortune of cryptanalytic exploitation to be continued. [256] In spite of this, there were errors in usage that, combined with German radio intelligence, caused the German Navy to change its codes and ciphers and the source dried up. [257] Jellicoe later said "the blank curtain descended" after which the previous

contribution of cryptanalysis was appreciated.[258] Political and agent decrypts from Axis and neutral traffic continued,[259] but then Hall caused the Zimmermann telegram to be published and this had further effect on German cryptographic security --- despite deception efforts.[260]* After the German Armistice there was still the Russian problem, and Room 40 cryptanalysis on Russian-German diplomatic messages in the last year of the war had a marked effect on British policy toward the new Russian government.[261] The Greeks and Turks were still fighting, and in the face of continued military uncertainties the British government ~~still~~ wanted the cryptanalytic activity continued and kept secret.[262]*

(5)* The operation in Room 40 was closed down in 1919,[263] but some staff and the files of that section and the War Ministry Cork Street section were consolidated in G.C.&C.S. and moved --- out of Admiralty -- to "Watergate House" on the Embankment below Charing Cross Station.[264]* Because of the wartime secrecy policy, neither the British, French or U.S. governments published anything about Room 40, even though other cipher stories crept out.[265] Most of the knowledgable officials kept silent, although the U.S. had no "official secrets" law for peacetime or for foreign government secrets.[266] However Lord Fisher, in his 1919 book Memories alluded to "elucidation of naval ciphers" in a tribute to the cryptanalysts.[267] Since the Germans had already changed their naval and diplomatic ciphers, and the war was over, this did not disclose any new information, but secrecy was generally still kept. In the 1921-22 Washington Naval Conference cryptanalysis played an important part in the U.S. negotiations,[268] and the U.S. government was very secretive, as was the British government, because they wanted the public and diplomats to use their profitable cable and radio networks.[269] In 1921 Churchill and Lord Hankey publicly praised Ewing's wartime work at Admiralty, but discretely did not say what it was.[270] Then in 1923 Churchill published his The World Crisis in which he disclosed for the first time the story of the recovery of the Magdeburg naval codebook in late 1914 which gave exploitation

of German naval signals on a current basis for several years.[271] It is not clear whether Churchill's disclosures were authorized by anyone else, although Churchill had been part of the Lloyd George Coalition government until late in 1922.[272] It was believed that the Russians, who were engaged in secrct military projects with the Germans , had told them of the Magdeburg incident.[273] Since the codebook was captured and the messages easy to exploit, the disclosure would have downplayed the British cryptanalytic capabilities.[274] Even though Admiralty had lost administrative control of G.C.&C.S., the head of the secret service was Admiral Sinclair, who was very security conscious and had Admiralty interests in mind.[275] Despite the defeat of Germany and its forced disarmament, the French were building a large Navy and submarine fleet --- which worried Admiralty --- and their Army had occupied the Ruhr in 1923 while they continued to build weapons at an intense pace.[276] The Communist movement was advocating revolution throughout Europe[276A] and the Russian Army was still considered a potential menace to peace,[276B] in spite of the efforts of the diplomats. Frank Birch, who had worked in Room 40, wrote a history of it and submitted it to Sinclair.[277]* Sinclair, who was then "C", immediately locked it in a safe and told Birch (who later directed and edited the massive World War II G.C.&C.S. history)* that it would stay locked up permanently.[278][279]* Cryptanalysis was still a secret to be kept![280]

(e)* The continued secrecy policy in the Admiralty, who had to think about the military developments and intentions of Russia, Japan, and other nations,[281] was not sustained at the higher levels of the British government. Detente was popular with the voters and gave the leading politicians a good press.[282] If war had been eliminated by various pieces of paper, then cryptology was expendable. In 1924 the British Foreign Secretary publicly disclosed decrypts of Russian diplomatic messages to prove a point, and this damaged G.C.&C.S. cryptanalysis on those links.[283]* The Admiralty had kept cryptanalysis and radio intelligence extremely secret,[284] but

they no longer had that responsibility.[285] The political exposure and leaking of intelligence results to affect domestic politics came into vogue. Later, in October 1924 just before a General Election, the Foreign Office and the press publicized a notorious "Zinoviev Letter" which was purported to be a secret communication from a noted Soviet head of the Comintern.[286] The "letter" was savagely critical of the current British Labour leaders, who were friendly to Russia, and it urged the British Communist Party to penetrate the British Army and to promote revolutionary action.[287] The British Foreign Office sent a sharp note to the Soviet Chargé d'Affairs in London, apparently without Prime Minister MacDonald's knowledge.[288] There was public indignation, Labor was overwhelmingly defeated and the Conservatives took power.[289] After his defeat the ex-Prime Minister MacDonald and the Soviet government denounced the letter as a forgery[290] --- although it was no different from what Zinoviev and other Soviet leaders had been saying publicly.[291] The letter had obviously been obtained from some secret source ---quite possibly a decrypt of a diplomatic message to the Russian mission in London.[292] These disclosure incidents, and the fact that cryptanalysis had been taken away from the Admiralty, would certainly have been known to Hall when he met Peaslee in mid 1925.[293] In 1927 the British Government under Baldwin ordered the famous "Arcos raid" in which the police entered and searched Arcos Ltd. a Soviet trading organization on 12 May 1927.[294] The government believed that some stolen secret War Office documents were on the premises.[295] The documents were not found, but the Baldwin government declared that they had found evidence of espionage and revolutionary activity.[296] The offices of the Soviet Trade Delegation in the same building were also searched.[297] On 26 May 1927 Britain severed diplomatic relations with Russia.[298] Questions were raised about the affair,[299] and the Government published a White Paper in 1927 containing the decrypts of Russian

diplomatic messages to justify the raid and the subsequent severance.[300] The Russians immediately put all their diplomatic messages into one-time pad, and cryptanalytic success on those vital links came to an end.[301]* In 1945 the German Pers Z cryptanalysts still recalled this incident with amazement.[302]* The U.S. was more secretive about its cryptanalysis than Britain,[303] and Yardley suppressed an attempt to use decrypts in a rum running prosecution in the 1920's,[304] but it too suffered from high policy and was shut down in 1929 in the name of international morality.[305]

(v) The leakage of the Room 40 story began quite soon after Peaslee got the decrypts, but without publication of the sabotage and biowar messages. Until November 1925 the subject of wartime cryptanalysis had been "an inviolable secret"[305A] A magazine article was then published containing a description by Mr. Walter Page, who had been American Ambassador to England during the war, of how the Zimmermann telegram had been solved by Admiralty.[306] Peaslee had already told Admiral Sims that he had gotten the decrypts,[307] and the news about his penetration of Room 40's secret presumably spread among the small number of key Americans who knew the story. Motivated by the Page disclosures, Lord Balfour, who had been First Lord of the Admiralty during the war, gave a talk at Edinburgh with Prime Minister Baldwin present, about the Room 40 work, lauding Alfred Ewing.[308] Ewing then began to talk about his work, and planned a book.[309]

After 1925 Lord Balfour urged Ewing to give a more complete account of Room 40, and "in view of the disclosures already made about Room 40 in various publications, both at home and abroad", Ewing agreed in late 1927.[310] On 13 December 1927 he gave a talk to the Edinburgh Philosophical Institution" and this was reported fully in the press.[311] Next day Admiralty enquired why he had not asked their permission before he gave the lecture.[312] For several months "echoes of this lecture disturbed the serenity of Admiralty circles" so that Ewing

agreed in writing not to publish anything further without prior Admiralty consent.[313] He also said that he had sent a precis to Lord Balfour, then President of the Council in the Baldwin government , and had discussed the matter with some Room 40 colleagues.[314] The objections that Admiralty raised to Ewing's lecture in late 1927 strongly suggest that they did not authorize the release of the decrypts to Peaslee in 1925. In 1932 Ewing wrote a history of Room 40 and sought official permission to publish, but was refused by Admiralty.[315] In 1931 the prospect of war was made visible by the Japanese invasion of Manchuria in September.[316] By mid 1932 the disarmament conference at Geneva stalled, then Germany withdrew, and Japan proposed increasings its power.[317] The British Navy was too weak to oppose Japan in the Far East, and Lord Hankey urged that the "Ten Year Rule" (that no war would occur) be abolished in the face of these developments.[318] Hall's proposed memoirs were suppressed in 1933, by which time Hitler was in power.[319] In all, security policy in the 1920's was quite different from one department to another, and high levels of government at the cabinet level were much readier to reveal "old" or "new" secrets than the service ministries. Balfour, the venerable politician, was willing to release the whole story in 1925 as soon as Ambassador Page published part of it, but the Admiralty and M.I.6 were still interested in security, detente and domestic politics notwithstanding.

(U) The Broken Dike

(U) After the German sabotage and covert war decrypts had been publicly transmitted to the German government in 1927 there was no way to keep the facts about Room 40 out of the public domain. The Ewing lecture of 13 December 1927 was given to an audience of 1500 at Edinburgh, and reported fully in the Times of 14 Dec 1927.[320] Ewing received a flood of mail afterwards asking for newspaper articles on how to defeat "enemy cryptographers" (sic) [324].

George Young, who had been in charge of the political section of Room 40 after Ewing left, co-authored a book on naval disarmement in 1928 in which he described more of the work of Room 40, including the interesting fact that the cryptanalysts in Room 40 solved cipher messages "by the technical methods and machines they had invented."[322] The use of machines in cryptanalysis was subsequently weighed by the German Foreign Office in rejecting the Enigma.[323]* Hall testified at the 1930 trial at the Hague about the Black Tom sabotage.[324] Yardley was the first real cryptanalyst to disclose the actual techniques used in war and peace, and he also disclosed facts about British wartime and peacetime cryptanalysis and delivery of peacetime cable traffic to the Admiralty (sic) in his 1931 book the American Black Chamber.[325] A law 48 Stat 122 (18 USC 952) was passed to suppress a second Yardley book in 1933.[326] Secretary of State Lansing published more decrypts in 1935 in an autobiography,[327] despite the new law and the furore over the 1931 Yardley book. One of the German agents von Rintelen published a book Dark Invader in 1933 recounting many conversations with Hall which disclosed details of Hall's wartime activities. A book by H.C.Hoy in 1934 told more about Room 40.[328] Ewing's son published a biography of Sir Alfred in 1939 recounting his work at Admiralty, and the reaction of Admiralty in 1927 to his Edinburgh lecture.[329] A biography of Dr.. Walter Page, wartime U..S. Ambassador to London, contained

Room 40 decrypts.[330] The French and the Germans apparently published and released nothing.[331] Hall himself had been directed by the British Government not to publish anything.[332] One of the interesting things about the Room 40 compromise is that the material that got out only concerned German traffic or German agents, although much of Room 40's work was directed at the traffic of neutrals.[333] The Nauen-Sayville link that yielded a number of messages that Peaslee got was actually run for U.S. diplomatic and commercial traffic between Germany and the U..S.[334] and the imbedded German cipher messages and diplomatic notes were sent in a code known to the U.S.[335] Presumably U.S. cable and radio traffic, like that of other neutrals, went to Room 40,[336] but whatever happened to it is still shielded by secrecy. Another point is that almost all the information about Room 40 was revealed by high ranking people, once Peaslee managed to get the decrypts out of England. Except for that starting crack, the wall of secrecy might have held as well for the German materials which did escape as it held for the other decrypts and intelligence which did not escape.

45C

(U) The Effect of the Room 40 Disclosures

~~(TSC~~ The German TICOM documents do not refer directly to the Room 40 decrypts, so the effects of the disclosures must be inferred.[337] The cipher crisis of 1917 is illuminating in showing German reaction to cipher insecurity (see Appendix). Inferences and suspicions of what the British had done in World War I had nothing like the weight of literal decrypts, backed up by public revelations in 1927 from Ewing and Hall.[338] The steckered Enigma and the increase in one-time pad resulted. By starting early the Germans had the most technically advanced cipher systems in the world in operational service before World War II.[339] This had a profound effect on German operational and cryptographic security and diplomatic and military sucesses at the outset of World War II.[340]

(U) Righteousness and Government Secrecy

(U) The available evidence indicates a compromise of the decrypts by Hall to Peaslee, followed up by some kind of after the fact authorization. What is very clear is that Peaslee did not go after the decrypts --- which he knew were sensitive and secret [341] --- through official channels, but deliberately circumvented the British security system by contriving a chain of referrals that got him access to Admiral Hall.[342] Peaslee had gone to school in England, and he knew the Official Secrets Act was a definite public policy. He went directly to Hall to elicit and gather classified information with the intent to transmit it to a foreign government --- despite the law.[343] Although he made his penetration under the veneer of good social contacts, it was still an unorthodox act.[344]

(U) Peaslee saw his "mission" --- to punish Germany --- as an overriding justification that dominated any other consideration.[345] He got what he wanted from Hall in 1925, and cultivated him while he pursued the case. Peaslee's career blossomed.[346] His clients, after 23 years, got a "victory" but there was almost no money to pay the claim.[347] Even Sims' editorial comment said that the importance of the case lay "in the prominence of the witnesses".[348]

(U) A Quaker,[349] Peaslee was both idealistic and vindictive. He wrote a number of books on disarmament, international law and world government.[350] He favored a strong world government

to suppress "international banditry and outlawry", especially by Germany.[351] Despite his abhorance of war --- which he wanted outlawed --- he volunteered for an Officer's commission in both wars. In World War I he directed the special courier service, and in World War II was a Commander in the Coast Guard.[352] He became National Commander of the U.S. Coast Guard League in 1947.[353] Ambitious and successful, he married at the age of 33.[354] He had many honors, among them, President of the American Branch of the International Law Association in 1928, and secretary general of the International Bar Association 1947-53.[355] In 1953-56 he was U.S. Ambassador to Australia.[356] During 1956-59 he was a deputy special assistant to the President, and deputy chairman of the U.S. delegation to the UN disarmament conference in London in 1957.[357] His biography in Who Was Who is extensive.[358]

(U) Peaslee's letters and briefs denounce the Germans for violating U.S. neutrality in 1915 and onwards.[359] In 1919 he predicted, in a letter, that the Germans would disavow and resist the Covenant of the League of Nations,[360] and this theme --- that the guilty must suffer --- is woven through his writings. One of his letters in 1940 contained the remark:

(U) "How can thuggery and thievery ever be stopped unless the guilty party is made to pay for the damages?"[361]

~~(S)~~ (Possibly, Peaslee would have been surprised to be presented with a bill for his damages to Allied SIGINT).

(U) Hall , on his part, clearly hated and disdained the Germans.[362] His wartime letters to Peaslee --- up to his death in 1943 --- were unsparing in denunciations of "the Hun" and everything German.[363] Yet he did not hesitate to give further top detailed evidence about still secret British codebreaking directly to the Germans during the 1927-30 period in efforts to punish Germany via Peaslee's case.[364] In 1934 he invited von Rintelen, one of the key German saboteurs in the case, to his daughter's wedding , a ceremony attended also by 14 British Admirals.[365] In 1939 Hall pleaded for his former enemy before an enemy aliens' tribunal, but Rintelen was interned.[366] The London Editor of the Manchester Guardian described Hall as "half Machiavelli and half school-boy" and his confidential shorthand typist agreed that "the Machiavelli in him could be cruel, and the 'means'he used often 'justified the end' in many a battle he fought in the murky world of Intelligence. But the school-boy was always round the corner, and his love of the dangerous game he, and all of us, were playing would bubble out, and the fun and hazard of it all would fill him with infectious delight. 'Adventures are for the adventurous' he would chant, rubbing his hands and grinning like a crafty little French Abbé' ".[367]

(S) The two men may have <u>thought</u> they were artfully furthering world peace and morality by pursuing the sabotage claims.[368] What they clearly <u>did</u> achieve was to expose Room 40's work, and make British cryptanalysis much less successful than it might otherwise have been. Britain alone lost 50000 sailors and 30000 merchant seamen during World War II, and suffered permanent economic damage[369] --- to say nothing of all the other consequences of Germany's improved cryptography.[370] With all their honors, Hall and Peaslee apparently never grasped what they had done --- the secret drama of cryptology and realpolitik was, perhaps mercifully, over their heads.

(U) No German agent could ever have penetrated the closely guarded secrets of Room 40 and relayed them to Germany in the 1920's better than Peaslee. No German "mole" penetrating the British government could have nullified British secrecy policy better than Hall. It was a remarkable tour de force --- an Intelligence catastrophe in which the protagonists never perceived the ironic consequences of their tragic zeal for retribution.

(U) If only we could learn from this. Decrypts do have consequences.

#