Learning Cryptanalysis the Hard Way: A Study on German Culture of Cryptology in World War I

Dr. Ingo Niebel
Historian and journalist
Kasparstr. 10
50670 Köln, FR Germany
ingo.niebel@berriak-news.de

Abstract

The history of World War I is well documented, but a comprehensive study of German cryptology during that epoch is yet to be undertaken. Owing to the silence of German cryptologists and intelligence officers, this topic remains almost untouched to date. Hence, a perspective on the role of German cryptology in World War I comes mainly from British and US authors, but generally not from German sources. This paper provides an overview of an ongoing research, focused on the German culture of cryptology between 1871 and 1918. It is based on the assumption that a fixation on cryptography is the essential part of that cryptology culture of those times. From 1914 on, Germans had to learn cryptanalysis the hard way. Questions regarding who started this learning process, how it developed, the failures and successes it produced, and the structures that were involved in the process, are yet to be answered. This investigation links the current state of the art with data obtained from the archives. Connecting cryptology with intelligence and technology, it also evaluates its impact on decision-making. Finally, understanding the antecedent German culture of cryptology enables us to investigate that of its descendants – spanning the decades from World War II to the Cold War, as well as today's "information security culture".

1 Introduction

This article resumes the research to a still unwritten monograph on the German culture of cryptology (1870/71-1918/19), whose investigation intended to reconstruct the historical context of the intercepted and encrypted German telegrams collected after World War I by the US cryptanalyst, James R. Child. This collection was successfully decrypted by George Lasry, Nils Kopal, and Arno Wacker (Lasry et al. 2017). An outcome of that investigation was a realization that we lack a comprehensive study of German cryptology during the second German Empire (1871-1918).

Our investigation starts from David Kahn's statement on this subject: "German cryptology goose-stepped toward war with a top-heavy cryptography and no cryptanalysis." (Kahn 1996:pos. 5347). His conclusion underscores a specific aspect, namely: talking about German cryptology between 1870 and 1914 is clearly an oxymoron.

Today, we understand cryptology as a science with well-defined theories, methods, and results, consisting of cryptography and cryptanalysis as its two main pillars. As a third, we can add steganography. This, however, is a very modern (20th century) Anglo-Saxon definition, which does not match the German understanding of secret writing and deciphering prior to and at the beginning of World War I. In fact, the German term "Kryptologie" was neither introduced in German encyclopedias nor in the Duden dictionary until the end of the 20th century. The German "Geheimwissenschaft" (secret science) is the literal translation of the cryptology, which in general referred to occultism, and is therefore unsuitable for use in the modern context.

The research becomes even more complicated because prominent German cryptanalysts during both World Wars remained silent and their line of work was never publicly discussed. All what we know about the German cryptanalytic efforts, successes, and failures originate mainly from

Proceedings of the 1st Conference on Historical Cryptology, pages 65– 75,
Uppsala, Sweden, 18-20 June, 2018

Anglo-Saxon publications and sources. Kahn's books and articles are only a tip of that iceberg, and the German perspective awaits exploration. Uncovering this perspective will provide a better description of the German culture of cryptology.

Focusing on the cultural aspect is of importance because – though the science of cryptology itself can be applied irrespective of the language in use or the nationality of those using it – the national circumstances define the characteristics of its development and use; for instance, whether or not civilians are permitted to use this science.

"Culture is the art ('ars', 'téchne'), through which societies secure their survival and their evolution in an overwhelming nature", states Hartmut Böhme. (1996:53). In our case, the culture of cryptology can be understood as the art of utilizing this science in a hostile environment comprising of alien interests to convey information and intentions in secret. This definition can be applied to all countries involved in a given war during this time period and used cryptology to gather intelligence and plan their military and diplomatic operations.

However, we have to "nationalize" every culture of cryptology because it is defined by the cultural, social, political, and military characteristics of each country. All these factors may explain why the German culture of cryptology in 1914 was defined exclusively by a presence of cryptography and a near absolute absence of cryptanalysis. German decision-makers therefore came to learn of this imbalance the hard way.

During the Russian offensive against Prussia in August 1914, German reserve army officers – at great personal risk after ignoring several orders – discovered the advantages of signal intelligence (SIGINT) in combination with cryptanalysis. This new kind of intelligence enabled their commander to win the battle of Tannenberg. Therefore, this victoryalso shows that the culture of cryptology entails a learning process. In the aftermath of this military success, German commanders initiated a large, complicated, and inconsistent learning process to improve their interception and cryptanalytical skills.

German military and diplomats learned the benefits of cryptanalysis the hard way, because – around the same time – they had already lost their first battle at the Marne river in France, as a consequence of French cryptanalysts breaking their codes. Despite all the efforts towards improvement, Germany would ultimately lose the war because her vulnerable codes would provide critical information to her enemies at crucial junctures. So, the history of the German culture of cryptology during that epoch is about how Germany's leadership learnt from a defeat it unknowingly suffered even before the imperial troops crossed the borders to Belgium, Luxembourg, and France.

Although British, French, and US went through their own learning processes, whose outcomes are known, it is worth describing how the Germans managed to transform their cryptography into cryptology by incorporating cryptanalysis. Therefore, we have to look for the various structures and personnel that intervened in this process.

On the one hand, we have the governmental structures and agents concerned above all with cryptographic matters. On the other hand, it is surprising how freely civilian "amateurs" wrote about cryptology and even criticized the government. That raises further questions, namely: Who were they, how could they acquire knowledge of cryptology, and how did the governmental institutions react to this kind of non-governmental cryptology? Looking for these answers, we have also to take into consideration the impact of their work on intelligence, as well as military and political decision-making.

Nearly a 100 years after the end of World War I, an investigation focused on the German culture of cryptology matches actual studies on what we call now the "information security culture". Maria Bada und Angela Sasse (2014) used this term when they analyzed how to improve Cyber Security Awareness Campaigns. The information security culture requires, according to the authors, on the one side, knowledge and awareness, on the other, positive information security behaviors. Though since 1914 our technology has improved a lot, the user remains to be the weakest link, not so much his hard- and software.

All these aspects should be taken into consideration if the goal is not to write a purely technical history of German cryptology concentrated only on its theories, methods, and

results, but also to link it with other fields and disciplines. That approach will be explained in the following three parts.

In the following section, I will present the assumptions on which I have based this investigation. In two subsections, my aim is to define my understanding of intelligence and why it is still a "missing dimension" in historiography. This in turn leads to the second subsection, which encroaches upon the German "culture of cryptology". The third section focuses on telecommunication and its impact on cryptology as in the earlier 20th century, the field of telecommunication was a relatively new with unknown advantages and disadvantages. Finally, I shall refer to the sources, with a focus on the the problems that historians encounter when using records obtained from the intelligence services.

Following which, I shall present some of my first results in chronological order. The four subsections describe different aspects of the German cryptology culture. It begins with specific terms Germans referred to in cryptology encyclopedias. The second subsection resumes the case when a German citizen publicly accused the Foreign Office of having plagiarized his code-system. The quarrel reveals that the Foreign Office showed no concern for security. The Crypto-Crisis of 1917 served two purposes, on the one hand, it discussed the problems a historian deals with when he or she has to rely on intelligence records; on the other, it indicated also how such a source can push the investigation forward. The last subsection provides a firsthand explanation as to why there is still no comprehensive study on German cryptology.

The fourth and last section brings us back from the past to the presence. It provides some hints as to why the German cryptology culture of 1914/1918 is linked in some way to the today's "information security culture". This would also provide some proposals for further investigations.

Due to time and space restrictions, and to the fact that this article resumes the status of a current investigation, it raises no claim to completeness.

2 Methods

Since the first decade of the 21st century, we count with declassified records and information recovered from encrypted radiograms. The US foreign secret service, the Central Intelligence Agency (CIA), and its technological partner, the National Security Agency (NSA), published historical documents related to cryptology including the names of persons, on their webpages. In parallel, the community of non-governmental researchers, who dedicate themselves to historical cryptology, were seeking unsolved messages from both World Wars. So, on the one hand, historians and cryptologists have access to new sources, on the other, cryptanalysts provide "new" records and insights by recovering and solving forgotten cryptograms. (Lasry et al. 2017, Sullivan and Weierud 2005) All these new sources need to be put in a greater academic context.

The ongoing investigation is based on two suppositions: Firstly, every state creates the intelligence community it considers necessary. Therefore, the organizational charts of its ministries and armed forces can reveal the importance given to the secret and cryptologic services. Investigating these structures, also sheds light on how the government allowed privateers to handle cryptology.

Secondly, the saying “once an agent, always an agent” defines the other mainline of research. It focusses on the persons who worked for one or various secret and/or cryptologic institutions. Both research fields are connected by seeking the interactions between institutions and their personnel. That implies that one must follow the organizational change in the departments. It would be interesting to know the social, professional, and cryptologic background of the personnel.

Today it is common to talk about the intelligence community by referring to all governmental, military, and police institutions dealing with intelligence. In parallel, we have the cryptology community, composed also of officials, privateers, and their departments or firms. In contrast to their British and US counterparts, the German cryptologists remain relatively unknown. This fact makes both cryptology and intelligence a part of a "missing dimension" in historiography.

2.1 Intelligence, a "Missing Dimension"

Spies were additional pawns on the great chessboard where the European powers played the tragedy of World War I. As previously mentioned, some crucial moves performed by the decision-makers of one or the other sides, were based on the intelligence gathered by their radio stations and cryptanalysts. The question lies in understanding to what extent this kind of intelligence influenced military and political decision-making.

In the 1980s some German and British authors had already mentioned intelligence as being the "missing dimension" in political and military historiography. (Höhne 1993:7) After analyzing several dozen international publications on the topic, Larsen (2014:282) concludes that this military conflict "remains in many ways underexplored by intelligence scholars." In fact, he found less than a handful of German works on that subject.

This problem is caused partly by the intelligence agencies themselves, because it is part of their nature to act secretly, without always acting in a legal or morally correct manner. So, for the sake of security, the intelligence services have good reason not to share their records with historians who, on the other, without these documents could not evaluate how large the "missing dimension" really is.

Although intelligence services release their records from time to time, historians cannot expect to receive complete files. Due to the fact that deception and cover-ups belong to the working tools of secret services and their assets, scholars are forced to crosscheck every disclosed information. Moreover, this makes their investigations more complicated. On the other hand, just Paul Gannon (2010) proved, referring to the British interception log books, that His Majesty's codebreakers could read enciphered German Naval messages already months before the war broke out and the Room 40 was installed. In consequence, his finding contradicts the official version and requires reviewing of the prewar history of British cryptological efforts.

Another complication derives from the necessity to define what intelligence really means. "I define intelligence in the broadest sense as information" concluded Kahn (2001).In my mind, information becomes intelligence according to the importance that is given to e.g., things, individuals, organizations, data, messages at a concrete time and for a specific aim.[1]

For delimiting intelligence as a "missing dimension", I consider its three principles very helfpful, which according to Kahn (2001), describe its function. First, it helps to optimize one's resources. Second, intelligence "is an auxiliary, not a primary, element in war". Thirdly, it is "essential to the defense but not the offense". The yet mentioned battles of the Marne and Tannenberg seem to confirm Kahn's theory. At this point we have the intersection between intelligence and cryptology, but it is not necessarily the only one.

In 2016 the German Historical Institute London (GHIL) held a conference on "Cultures of Intelligence". In that context, the GHIL stated that "Culture was understood to include the role of intelligence services in society and/or the state, the representation of intelligence in the public sphere and among the members of the military/intelligence community itself, as well as the interests, assumptions, and operating procedures of intelligence." (Sassmann, Schmidt 2016:135) This definition can be used to define the German culture of cryptology.

2.2 About a German Culture of Cryptology

It is difficult to answer whether it is "a" or "the" German culture of cryptology because it depends on the epoch. When we refer to a time before 1870/71, we should preferably use "a", because the culture in question may be linked to a specific kingdom on German soil. For example, Rous (2011) analyzed the Saxon culture of cryptology in the 17th and 18th century. But we unfortunately lack a similar investigation on the Prussian culture prior to 1870.

When the Germans created their second empire, the Prussian king got also their emperor. As a result all key areas such as the military, foreign, economic and home policy, for instance, became centralized to the Prussian capital,

[1] This is another very Anglo-Saxon definition of "intelligence", it differs to how German secret service officers used to interpret "Information" which, according to them, becomes "Nachricht" (intelligence) when it is confirmed by other sources.

Berlin. In the light of lacking documents, we have to assume that the overwhelming presence of cryptography and the absence of cryptology reflects the Prussian culture of cryptology.

A characteristic of the new Reich was that the ruling aristocracy managed to integrate the bourgeoisie in the new project. Instead of democratizing the state, by getting rid of the aristocrats, the bourgeois supported the monarchy. So entrepreneurs and bankers pushed Germany's industrialization and implementation of new technologies. Their crème de la crème were further ennobled. "Nonetheless the Wilhelminian Germany was still an authoritarian society with a static social order of considerable stickiness", states the historian Wolfgang Mommsen (1995:71).

This and further investigations on the social order should be taken into consideration, as they might explain the absence of an intelligence and cryptologic community, and also the incompetence of the armed services and the Foreign Office to develop intercepting and codebreaking capabilities, as it had occurred in the United Kingdom. The known facts indicate that listening to foreign conversations and reading confidential messages could have put the above mentioned rigid order and separation of powers at risk.

From this point of view, the use of cryptography seemed have come into place as a measure to guarantee the established order. In fact, only officers and high ranking civil servants were allowed to cipher and decipher encoded messages. Following that logic, another measure was to avoid the promotion of cryptanalytic skills.

Germany's oldest cryptographic institution was Chiffrierbureau of the Foreign Office. It was built in 1814 and belonged to the ministry's Zentraldepartement. (PAAA 1936), thereby putting the Chiffrierbureau and its personnel in the focus of the current investigation. During that time, the head of the government, the chancellor, was responsible for foreign policy. But his role was limited, as he was only a counselor to the monarch.

The Kaiser acted also as the commander-in-chief of the armed services. It is known that he used cryptography, but the extent to which it was used remains unknown. He supposedly got the codes and keys from the cipher-bureau. The Foreign Office provided the naval attachés with codes, too.

One research line focuses on the indivuuals within the the Army and the Navy structures who dealt with cryptography. The other research line concentrates on the "Abteilung für Nachrichtenmittel" (department of communication means)[2] of the Royal Prussian War Ministry, another on the "Reichsmarineamt" (Empire's Navy Office). Both produced codes and ciphers, and delivered them to the troops and the civil authorities. They primarily had administrative functions, not operative. Therefore, another research line looks for the importance the armed services gave to cryptography in the education of their officers.

The common denominator of these three governmental institutions was that they favored cryptography, reducing cryptanalysis to a "guessing" or buying codes and keys on the black market. This German credo of cryptography expressed itself by the main code books such as the Handelsschiffsverkehrsbuch (HVB), the Signalbuch der Kaiserlichen Marine (SKM) and the Verkehrsbuch (VB). These became one of the essential parts of the very specific German culture of cryptology

Opposite to the governmental cryptographic structures we find a considerable number of non-governmental cryptologists, who along the 19th and at the beginning of the 20th century, published a certain number of articles and books on secret scripts and their decipherment. This allowed people interested in the specific field access information without major problems.

2.3 Telecommunication and cryptology

Telecommunication is in many ways essential for understanding the development of the German culture of cryptology. On the one hand, the new technology changed how people handled communication. Telegraph, radio and telephone replaced the traditional royal messenger services, as the depeches were delivered faster by wire,

[2] The German "Nachrichten" can mean "news", "intelligence", "signals" or "communications". That makes is complicate to decide whether a "Nachrichtenoffizier" is an "intelligence" or a "signals/communications officer".

wave and cable. This mode of communication seemed to secure to everyone who believed that his or her codes were unbreakable.

At the very beginning of World War I, the British destroyed the German transatlantic telegraph cables. So they forced the Germans to communicate via radio with their colonies and embassies or by telegraph connections. These connections could be monitored by British telecommunication companies. In both cases, London could intercept the communication and try to read the encoded messages.

For this project it is necessary to take into account this fact because there are several German thesis in which lawyers addressed the legal and strategic issues of such a violation of the postal secrecy long before the Royal Navy made their worries real in 1914.

Another important aspect is that the importance of SIGINT can only be understood if we know the technical equipment of the signals troops and its limitation. Because of the technology, climate and geography, messages had to very often be repeated. This increased the possibility of a radiogram being intercepted. In this way, experienced cryptologists and analysts could complete crippled messages.

In this context it is also necessary to refer to the technical efforts to mechanize the encoding and decoding process. Although the German Army would purchase the Enigma only in the 1920s, some documents indicate that, at least, its theoretical development might have already started before World War I.

2.4 "Ad fontes" - To the Sources

As I mentioned above, Kahn's publications on cryptology are essential because they frame the investigation. Articles such as those written by Stützel (1969), Brückner (2005), and Samuels (2016) give further information on facts and sources regarding the German cryptology. In contrast, selected monographies on the French, British, US cryptology and SIGINT describe the "hostile environment" in which the German culture of cryptology started to grow in the summer of 1914.

The investigation takes into account, how the military commanders integrated cryptology SIGINT and this kind of intelligence gathering into their decision-making. This in itself constituted another learning process because in 1914 they had still not changed their plan of attack that had been drawn up in 1905 under very different circumstances. Nine years later, they still believed they could win the war in the west by the same manner as in 1870/71. They thought that once again infantry, artillery, and cavalry plus modern weapons would bring victory, but not the less regarded signals troops.

The information that is not included in the publications has to be found in the archives. This makes the project difficult because the principal Prussian-German military archives vanished during World War II. The records of the different cryptologic departments were either destroyed or captured by the victors who delivered them to their cryptologic or intelligence services. As mentioned before, the CIA and NSA declassified such documents, as also did the British services. In consequence, the respective holdings could aid in recovering such information that is lacking in the German archives.

A first look into the Political Archive of the German Foreign Ministry (PAAA) showed that the entire holdings of the Chiffrierbüro have disappeared. The existence of the cipher-bureau is only confirmed because its name appears in the organizational charts of the ministry, and on several documents which can be found in other holdings. If there has once been a correspondence, for example, between the cipher-bureau, the Army and the Navy on codes, it not longer exists, at least not in this archive. The unpublished memories of cryptologists such as those of Adolf Paschke somewhat enlightened the gloomy situation.

The situation in the German Federal Archive, the Bundesarchiv, is slightly different. On the one hand, there are only a few sources related to the cryptography in the Army, on the other hand there is much more information on the cryptological work done by the Navy before and during World War I. The first impression after a stay in the Military Archive of the Bundesarchiv at Freiburg is that there is more information than I expected.

Due to the fact, that the archives of the Prussian Army and the War Ministry were destroyed, there is some hope that the correspondent holdings of the Bavarian State Archive could close this gap in some way. The

research in the regional archive of North Rhine-Westfalia provided some information on how the Prussian Interior Ministry introduced cryptography in its communication with the regional military institutions.[3]

In this context, the "William F. Friedman Collection of Official Papers", as called by the NSA, is of particular interest. It contains more than 7,600 documents spanning over 52,000 pages. The collection can be searched and downloaded as a PDF via Internet.[4] Due to the close relationship between the cryptologic and intelligences communities of the US and the UK, the NSA collection must be seen in connection to the respective holdings in the British National Archives at Kew, as some German related documents of supposed US origin were gathered in fact by their English "cousins".

In this context, and from a purely academic point of view, the decrypts of intercepted German radiograms published by Lasry et al. (2017) present a special kind of document. To some extent, they are "retranslations" from an original text which was encoded and sent by radio. Albeit the cryptanalysts broke the code and got a plaintext again, the latter should be compared with the original message, if possible.

In any case, researchers need an organizational chart of the institution in question. This is essential for two reasons. First, an organizational chart helps to identify the departments concerned with cryptology inside a ministry, which can be helpful if the search using keywords was not successful. Second, an organizational chart uncovers the position of a cryptologic section in the respective structure. It makes a difference if it is attached directly to the minister's bureau or if it is a department or if it positioned on a lower level being only a section or a subsection. So, the archives and their holdings themselves generate valuable "intelligence" on the German culture of cryptology.

3 How Germans learnt cryptology

3.1 Ignoring cryptanalysis and SIGINT

In search of reasons to explain the German fixation on cryptography, I consulted several editions of the popular encyclopedias such as Meyer's Konversations-Lexikon and the Brockhaus. Between the 19th and 20th centuries, both publications not only ignored the existence of the word "Kryptologie", but also indicated that the term should be replaced by "Geheimschrift" or "Chiffre". Since the beginning of the 19th century, the cryptologic horizon seemed to be limited to cryptography.

This limitation is curious because just a retired officer published a classic on cryptology in 1863. Major Friedrich Wilhelm Kasiski titled his book "Die Geheimschriften und die Dechiffrir-Kunst" (Secret scripts and the art of decipherment). As the title indicates, it reflects upon our modern understanding of cryptology and is based on cryptography and cryptanalysis.

The facts collected on Kasiski indicate that he had nothing to do with the cryptology while in the military. Though he dedicated his book to the acting war minister Albrecht von Roon, the author addresses him only as his former commander. It seems that the military hierarchy decided to ignore both Kasiski's cryptological efforts and SIGINT as well.

"In Germany to be sure, the General Staff thought of such possibilities, but down to the outbreak of World War I had undertaken practically nothing. Even in the Foreign Office nothing had been done in this direction which was worthy of mention" states the signals officer Wilhelm Flicke.[5] Only during the battle of Tannenberg in 1914, the high command would discover the advantages of SIGINT and cryptanalysis. It took several months until the new possibilities were included into its military organization.

3.2 The Chiffrierbureau Accused of Plagiarism

Due to the lack of documentation, it is assumed that the Foreign Office and its

[3] LAV NRW, Abteilung Rheinland, BR 0021 Nr. 107, 108

[4] https://www.nsa.gov/news-features/declassified-documents/friedman-documents/, last seen 15.01.2018

[5] https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/beginnings_radio_intercept.pdf, p.21.

Chiffrierbureau underestimated cryptanalysis and the interception of foreign messages by technical means. Security did not seem to feature high on their list of priorities.

It seems strange, at first, that until the end of World War I the Auswärtiges Amt published in the "Handbook for the German Reich" the identities of all the officials who worked for its Chiffrierbureau. This extent of governmental transparency included the names of individuals who were civil servants and all the medals they had been awarded. Any foreign intelligence serviceman would have been grateful to get his hands on the list of potential targets, who had access to classified material.

Secondly, neither the Ministry nor the cipher-bureau seemed to be concerned when in 1872 the printer M. Niethe accused both to have stolen his code-system. The fact that several editions of his book can be found in various German public libraries proves his enthusiasm but also that neither the Reich government nor the Auswärtiges Amt tried to silence him using censorship, albeit at one point during the conflict Niethe was summoned by the police.

The background information on the cipher-bureau personnel mentioned in the Handbook, and the Niethe case are the basis for further investigation on the culture of cryptology followed by the Auswärtiges Amt.

3.3 The Crypto-Crisis of 1917

The publication of the Zimmermann-telegram in spring of 1917 not only brought the US into the war but also exposed the opinion of the Auswärtiges Amt about the security of its codes. The incident caused a major discussion reagarding cryptography between the Foreign Office, High Army Command, the Army and the Navy. The “crypto-crisis” can be considered also as the endstart of the German cryptology because from that point on, cryptanalysis was used as a means to test the strength or weakness of German codes.

On 23 March 1917, the secretary of State, Alfred Zimmermann, wrote to the representative of his Foreign Office at the General Headquarters, the baron Kurt von Lersner:

"Decipherment of these telegrams is simply impossible even for the most clever specialists. It can only result if the entire cipher is betrayed or essential parts and keys come to the knowledge of a foreign government. Of course, there is no absolute security against betrayal and the only aid is the frequent change of cipher and of keys, which is abundantly provided for here."[6]

This information on the Foreign Office's culture of cryptology is provided by a document kept in the above-mentioned Friedman Collection. The NSA labeled it "CRYPTOGRAPHIC SYSTEMS USED BY GERMAN FOREIGN OFFICE; THE ZIMMERMAN [sic] TELEGRAM.” A handwritten remark on the first page of the PDF indicates that it belonged to a folder where Friedman stored various information on the Zimmermann-telegram. This thereby leads to the beginning of the problem.

The NSA, as the CIA, does not scan entire folders but only documents. At this point, we see again the primacy of intelligence and information over the archival context of a document, as described in chapter 2.4. From the historical point of view we are not dealing with an original but with a copy, meaning, an English translation.

Though the translator seemed to be a professional -he or she even reproduces the layout of the German original- but we are unaware of how Friedman got possession of the document. Nor do we have further information on the remaining original German texts. Despite all these questions, Zimmermann's statement and other correspondences scanned into the PDF seem to be genuine because they are supported by the article Stützel (1969) mentionededited in a West German military publication.

In 1917, Stützel was a "lieutenant of the reserve", as we can read in one of the translated letters. He proved that in terms of the strength and security of its codes, the quoted assumption of the Foreign Office was inaccurate. Stützel intercepted and solved the encrypted messages sent between the Auswärtiges Amt and the German Embassy at Madrid. His discovery generated the mentioned discussion on insecure codes.

This incident is important because it uncovers different aspects of the German cryptology culture. First, it stresses the role of the

[6] The PDF’s filename is 41716799075610.pdf

Chiffrierbureau as the unique provider of diplomatic codes. Second, to believe that its codes are unbreakable can be considered as ignorance but it also expresses the inflexibility that was characteristic of imperial Germany. Third, itthis above mentioned stickiness made it impossible that the governmental structures reacted quickly regarding changes in its structures and codes. Finally, Stützel's cryptanalysis on the diplomatic codes questioned not only the expertise of the Chiffrierbureau but also theput at risk the trust competence of the entire division of the the armed services in the Foreign Office.

3.4 The imposed silence

In the 1920s, the former Austrian captain, Andreas Figl, planned to publish his memoires and experiences as the head of the cryptologic section of the Austro-Hungarian army intelligence service, Evidenzbüro. This publication reveals reasons as to why German cryptology of World War I never was treated by its protagonists as the British did.

After the first of three volumes werewas published, Figl was pressurized to step back from his project. "The action against me came from the [Austrian] Federal Army and -as I ascertained later- from the German General Staff", Figl recognized in his unpublished memories.[7] He states that the intelligence and cryptologic communities held opposite opinions on weather he and his colleagues were still bound by the duty of secrecy or not. Figl thought he was no longer bound as the state he swore to - the Austro-Hungarian Monarchy- was no longer in existence since 1918, when it broke into several independent republics. The Austrian Emperor had to abdicate and go into exile, similar to his German incumbent.

Obviously, on the other side of the Alps, the German military saw that quite differently. From the legal perspective, one has to question whether the duty of secrecy sworn before 1918 persisted or not. The oath was considered legitimate if it was to the German Reich but not to the Kaiser and king. The latter, although converted from monarchy into republic, persisted as the official denomination of the new state.

[7] Bundesarchiv, MSG 2_18031

Though the political system changed, and the military had to downsize its structures according to the Treaty of Versailles, the Army and the Navy maintained their principal SIGINT and cryptology organizations, which also included part of the personnel.

Lasry et al. (2017) provide solved radiograms sent by the signals captain Walther Seifert. After the collapse and defeat of 1918, he switched over to the Chiffrierstelle (cipher-section) of the Reichswehrministerium (Ministry of the Armed Forces). In 1933, he was a part of the founders of the Forschungsamt (Research Office). The latter became the technical intelligence agency of the National-Socialist Germany, which was a part of Hermann Göring's Reich Air Ministry, and Seifert its head of cryptanalysis.

Albert Praun started his military career in the signals troops of the Bavarian Army. He later took over several military commands until 1944 and then became the Army's Chief Signals Officer. From 1956 to 1965 he headed the SIGINT department of the West German foreign intelligence service, the Bundesnachrichtendienst (BND). Although Praun published some articles on that subject, he kept his imposed silence.

4 The Presence of the Past

In spite of the mentioned publications and sources, the imposed silence on the German culture of cryptology persists. The research on this area has recently begun and some questions might never be answered. Investigating the German culture of cryptology prior to and during World War I is linked to our modern security culture because both are parts of the same chain.

There are at least two further links, those of cryptology and intelligence during World War II and the Cold War. For the latter it would be interesting to know whether the cultures of cryptology in the two German states were different because of their opposite politicalideological views due to their particular intelligence cultures. The next step would be to compare it at least with the French, English, US, and Russian cultures of cryptology, if possible.

But before we follow the chain up to the present time, we should look back from the German Reich of 1871 to the earlier epoch of the 18th-century-Black Chambers. Perhaps, on the one hand, this investigation can provide

information for closing the gap between the cryptologic and intelligence system of the late 19th century and that of Prussian king Frederick the Great in the 18th century. If, on the other, due to the lack of reliable sources, it could be helpful to compare at least the code-systems used in both periods. Maybe similarities could be found and shed some light on Prussian cryptology and its continuity.

Describing the learning process the German culture of cryptology, it underwent, between 1870 and 1918, several changes. The truereal activity of the Chiffrierbureau will never be discovered but at least the files on its personnel could provide information on how they entered the section and what kind of preparation they undertook for their work. In this context it would be interesting to analyze the path and networks of those cryptologists who started their career in the Army or in the Navy.

A part of a learning process is also how people handle their successes and above all their failures. As Figl mentioned, the German military and political elites avoided being held liable for their failures in matters of cryptology and intelligence. They covered up their first major defeat in France by calling the correspondent battle the "wonder of the Marne". In this and other cases, the history of German cryptology can correct the greater picture of World War I by demythologizing some of its narratives.

In this context, the fact that humans tend to copy behaviors, becomes a problem. To change certain cultures renders itself even more difficult if people are not used to questioning ideals. The official silence imposed on cryptology and its history was absolutely not helpful. This might explain the reason, amongst others, why in World War II German officials kept using the Enigma cipher machine even though they knew of its weaknesses. Referring to Zimmermann's statement on code security, one has to question human ignorance because till date some things were not meant to be. In this context matches the warning, the US-philosopher George Santayana gave us: "Those who cannot remember the past are condemned to repeat it."

Acknowledgements

I would like to express my appreciation to Prof. Christof Paar (Bochum) who brought me from history into the world of cryptology, to Prof. Arno Wacker, Dr. Nils Kopal, and Dr. George Lasry who invited me to reconstruct the historical context of the German messages they had solved. I also thank the three anonymous reviewers whose commentaries made me rethink some aspects of this article. Last but not least, I am deeply indebted to Dr. Roopika Menon who helped me to improve my English text.

References

Maria Bada and Angela Sasse. 2014. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? http://discovery.ucl.ac.uk/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf, last seen 15.01.2018.

Böhme, Hartmut: Vom Cultus zur Kultur(wissenschaft). Zur historischen Semantik des Kulturbegriffs. In: Renate Glaser/Matthias Luserke (Ed.). 1996. *Literaturwissenschaft – Kulturwissenschaft. Positionen, Themen, Perspektiven.* Westdeutscher Verlag, Opladen: 48-68.

Hilmar-Detlef Brückner. 2005. Germany's first Cryptanalysis on the Western Front: Decrypting British and French Naval Ciphers in World War I. *Cryptologia,* 29(1):1-22.

Paul Gannon. 2010. *Inside Room 40: The Codebreakers of World War 1.* Ian Allan Publishing, Hersham.

Heinz Höhne. 1993. *Der Krieg im Dunkeln. Macht und Einfluss der deutschen und russischen Geheimdienste.* [The war in the dark. Power and influence of the German and Russian secret services.] (Special printing). Gondrom Verlag, Bindlach.

David Kahn. 1996. *The Codebreakers. The Story of Secret Writing,* [Kindle, ipad mini version]. Downloaded from Amazon.com.

David Kahn. 2001. An Historical Theory of Intelligence. *Intelligence and National Security*, 16:79-92. http://david-kahn.com/articles-historical-theory-intelligence.htm, last seen 14.01.2012.

Friedrich Wilhelm Kasiski. 1863. *Die Geheimschriften und die Dechiffrir-Kunst.* [The Secret Scripts and the Art of Decipherment] E.S. Mittler, Berlin.

Daniel Larsen. 2014. Intelligence in the First World War: The State of the Field. *Intelligence and National Security*, 29(2):282-302.

George Lasry, Ingo Niebel, Nils Kopal, and Arno Wacker. 2017. Deciphering ADFGVX messages from the Eastern Front of World War I. *Cryptologia* 41(2): 101-136.

Wolfgang J. Mommsen. 1995. *Bürgerstolz und Weltmachtstreben. Deutschland unter Wilhelm II. 1890 bis 1918.* Propyläen Verlag, Berlin.

David Paull Nickles. 2003. *Under the Wire: How the Telegraph Changed Diplomacy.* Harvard Univ. Press, Cambridge, Mass.

M. Niethe. 1875. *Das "Suum cuique" in neuer Interpretation seitens des Auswärtigen Amts: nothwendig gewordener Anhang zu des Verfassers Werk: Das bei der Chiffrir-Abtheilung des Deutschen Reichskanzleramts eingeführte telegraphische Chiffrirsystem etc.* [The "Suum cuique" (to each his own) in a new Interpretation from the Foreign Office: An Annex, which had become necessary, to the Author"s Work: The Telegraphic Cipher-System introduced into the Cipher-Department of the German Reich Chancellory etc.] M. Niethe, Berlin.

Markus Pöhlmann. 2005. German Intelligence at War, 1914-1918. *Journal of Intelligence History,* 5(2):25-54.

Politisches Archiv des Auswärtigen Amtes (PAAA). 1936. Organisation des Auswärtigen Amtes bis 1936. [handwritten chart] Berlin.

Anne-Simone Rous. 2011. Geheimschriften in sächsischen Akten der Neuzeit [Secret Writing in Saxon Files of the Modern Age]. *Neues Archiv für sächsische Geschichte*, 82:243-254.

Anne-Simone Rous and Martin Mulsow (Ed.). 2015. *Geheime Post: Kryptologie und Steganographie der diplomatischen Korrespondenz europäischer Höfe während der Frühen Neuzeit* [Secret Mail: Cryptology and Steganography in the Correspondance of the European Courts during the Early Modern Age]. Duncker & Humblot, Berlin.

Martin Samuels. 2016. Ludwig Föppl: A Bavarian Cryptanalyst on the Western front. *Cryptologia,* 40(4):355-373.

Bernhard Sassmann and Tobias Schmitt. 2016. Cultures of Intelligence Conference Report. *German Historical Institute London Bulletin*, 38(2):135-140.

Hermann Stützel. 1969. Geheimschrift und Entzifferung im Ersten Weltkrieg [Code and Decipherment in World War I]. *Truppenpraxis* 7:541-545.

Geoff Sullivan and Frode Weierud. 2005. Breaking German Army Ciphers. *Cryptologia*, 29(3):193-232.