# CRYPTOGRAPHY

# IN THE FIRST WORLD WAR

Cadet Lucy R. Lee

Massachusetts Institute of Technology

Army ROTC Paul Revere Battalion

1 April 2018

The onset of World War I opened the door to a flood of technological innovations, many of which made lasting impacts on the way war is fought, some even remaining relevant to this day. Advancements in weaponry such as machine guns, tanks and artillery caused massive losses of life on both sides, which had never been seen before at such a large-scale. However, it wasn't just the advancements that caused the immense number of deaths, it was the misuse of these new weapons now capable of mass destruction which made war "more horrible and more complex than ever before".[1] Many leaders refused to believe that the old military doctrine they had learned would lead them astray. They "were slow to adapt" and refused to consider new possibilities ultimately led to their downfall and crushing defeats for their forces.[2] Those new weapons also resulted in the introduction of a new warfare tactic that would completely define the course of the war: trench warfare. Trench warfare meant that an extreme amount of lives were being lost in exchange for just "a few hundred yards of shell-torn earth".[3] Chemical warfare, most commonly used by the Germans, became very commonplace as a result of the trenches and also resulted in a large increase of "misery and death".[4] Besides these bloody physical innovations, information technology also evolved to become a vital part of military strategy and tactics.

As World War I began, ancient communication technologies were still being employed alongside newly invented ones. "Ancient systems of communication such as carrier pigeons"[5] were still commonplace throughout the first strides of the war, only getting fazed out when faster and more efficient technologies "such as the telephone and wireless telegraphy" replaced them, and when people lamented the exponential increase of pigeon deaths.[6] While telephone calls and telegrams through cables were a much quicker way to communicate, they were "easily broken"[7] and "easily intercepted".[8] Towards the end of the war, wireless communications such as radio

became more commonplace. These continued to be used after the war and into today's wars, where almost all communication is done wirelessly. This boom in information technology on the battlefield resulted in a similar urgency for people or technology capable of intercepting and deciphering enemy communications. A new type of technology that had never been seen before on the battlefront was invented: cryptography, defined by Merriam Webster as "the enciphering and deciphering of messages in secret code or cipher." During ancient times, communication broke down on the battlefield and miscommunications were often the reason for defeat. However, with the increasing growth of communication technology came the increasing need for cryptology. The use of cryptography during World War I influenced the tactics of the United States Army by pushing the country to develop its own working codes, expand its cryptology forces to better conduct counterintelligence, and decode enemy communications to conduct counter-offensives.

Before World War I, cryptography was "mostly used for diplomatic purposes", and rarely, if ever, for military operations.[9] By the time countries realized its importance to the war effort, they rushed to form official organizations that were solely dedicated towards intercepting enemy communications and decoding them in a reasonable amount of time to gain an upper hand in the war. Although spying had proven to be essential since ancient times, this was a completely new and untested form of spying. Two powers, the Austro-Hungary Empire and France, "foresaw the opportunities [cryptography] would create" and had trained cryptographers and a department ready even before the war began.[10] By the time the United States entered the war, other powers had already developed their cryptology forces over the course of several years, while the US had "no organized cryptologic effort" in any of its military services.[11] Top generals quickly realized that encoding and decoding communications would be vital to success in the

war, especially after seeing other countries benefit from it. For the next year, the United States struggled to frantically catch up in all aspects of the war, including in cryptology. Therefore, during those days, the US had a minimal impact on the war, and was in a general state of disarray. However, as the war progressed, our country's cryptography programs matured as well, to match and combat those of enemy forces.

Did cryptography lengthen or shorten the war? On one hand, it seems intuitive that the new technology would shorten the war. Cryptography allowed the military of one country to understand the thoughts within its enemy's head, which conferred a major advantage to that country's leaders. They knew with certainty where and when their enemy would strike, and with exactly how much force. Armed with this knowledge, they were able to launch counter-offensives or surprise attacks that led to definitive victories, since they knew exactly how to react to each step of the enemy's plan. However, the power with the strongest and "most successful" cryptography program was actually the Austro-Hungary empire.[12] Their department, called the "Dechiffrierdienst,"[13] was already established as a "branch of the respected Army Intelligence Service."[14] It was split functionally into "geographic teams" around areas such as Russia and Italy.[15] The "breathtaking ethnic diversity" population within the empire, normally a weakness because of its resulting divisiveness, became a strength since the empire had subjects who already spoke the enemy's native tongue to help them decipher codes.[16] Because the side that had the greatest advantage in this technological advancement also happened to be the weakest power militarily, the cryptography strength created a force multiplier for the empire and leveled the playing fields. The cryptology department definitely prolonged the life of the dying empire through years of total war, and often "prevented a bad situation from becoming a life-threatening

one."[17] Although one would expect that cryptography shortened the length of the war, it actually ended up lengthening it due to the relatively equal footing it put everyone on.

The innovation of cryptology began in other countries, but the United States military quickly followed suit by changing their tactics to incorporate experimenting with producing their own codes, especially prevalent within the Army. Because of the mass scale of warfare employed during World War I due to advancements in machine guns and artillery, trenches became vital for survival at the front lines. Long and deep lines of men dug into the ground was extremely commonplace, especially on the western front. Trench lines were quite immobile, usually only moving a few hundred yards over long periods of time in exchange for a massive amount of lives lost. This resulted in the development of a new type of technology to communicate with: trench codes. Trench codes were used to pass orders between trenches and to soldiers themselves. They had to be simple enough to quickly translate back into English, yet indecipherable by enemy forces. Both the Allies and Germans "decided that ciphers were too difficult to use" [18] at the front lines, so they had developed trench codes already. The US followed suit, believing it to be the best form of communication between the dug trenches.

The United States's first foray into cryptography was a major disaster. Inspired by the efficiency of other countries' trench codes, the US sought to create a code that was as simple as possible, but still unable to be deciphered by the enemy. The first trench code produced by America was the "American Trench code of 1,600 codewords."[19] It used a mono alphabetic substitution cipher as its "one-part code", and was intended for distribution down to the company level.[20] However, when Major Parker Hitt, the American Expeditionary Forces' assistant chief signal officer, tested the newly written code by asking an Army cipher amateur, Lieutenant J. Rives Childs, to try to break the code, Lieutenant Childs was able to crack the code "within five

hours,"[21] solved all 44 of the messages that had been given to him, and "recovered the entire cipher alphabet".[22] This was disastrous for the country, as surely a code used along miles of trench lines should not be able to be solved within a day by a single person. Imagine the easy time the enemy would have intercepting and deciphering that first trench code the United States Army made.

The United States started with nothing relating to cryptography, but ended with one of the most well-encrypted trench codes seen at the time. After the humiliating experience with the first trench code they made, Americans began looking into a "two-part code", which would actually be both easier to encode and decode in the field than the one-part code used previously.[23] It also did away with the "need for the superencipherment," another hindrance of the first code.[24] There were different methods the Germans used to try to decode the new American trench codes. They intercepted them and tried to decode them, and also always had a chance of stealing a copy of the codebook, a book containing the entire trench code, during a trench raid or an offensive. To prevent any possibility of the code being cracked, the Americans began the policy of distributing a new set of codes "on the average of every two weeks" which had never been done before.[25] This revolutionary idea helped protect American trench codes from the enemy exceptionally well, and resulted in the wildly successful "River Series trench codes - all were named after American rivers."[26] The first delivery of this type of code, the "Potomac" code, happened a year and two months after the United States entered the war on "24 June 1918",[27] displaying the long stretch of time it took for the country to catch up to others in terms of innovations, but also demonstrating the massive improvement that led to this success. The innovation of cryptology in other countries caused the US to reform its tactics and quickly

develop its own cryptology, which eventually led to afore mentioned series of successful trench codes.

Besides building their own codes, the United States Army also changed their tactics by using cryptography to better conduct counterintelligence. The abundance of German spies that had infiltrated into the United States was extremely disturbing to the general public. In fact, many newspaper articles and propaganda within the country implanted fear into the general public, leading them to believe that anyone around them could be spying for Germany. One of Wilson's reasons to declare war even included the German spies. They set off terrorist attacks within the country, bombing infrastructure and killing people on American soil. These explosions "carried out by German agents operating in the United States"[28] combined with the anti-German hysteria building up during that time caused a strong surge in the need for counterintelligence measures, and code breakers would "ramp up efforts to intercept and crack enemy messages".[29] When capturing these spies, the US Army often decoded any documents the spies had on themselves, gaining vital insight into German plans and information about any other spies inside the country.

The work put into decrypting German ciphers was extremely useful in identifying German spies and sentencing them with evidence. Some spies "planted in Mexico began slipping across the border" to infiltrate into the United States.[30] However, the Treasury Department's Bureau of Investigation was able to anticipate these deceptions, and caught Lothar Witzke, a German naval lieutenant turned spy. After searching him, they found that "a cryptogram was…sewed into his jacket".[31] This major opportunity for deciphering was immediately sent off to the Army military intelligence headquarters where Captain John Manly immediately devoted his full attention to cracking the code. After using a masterful blend of determining the language

of the message and frequency analysis, Manly took an educated guess that "he was looking at a columnar transposition cipher".[32] Armed with this estimate and his knowledge of the German language, Manly's hard work paid off and resulted in a brilliant solution. The "Waberski message"[33] ended up being used as evidence "to convict Witzke of espionage".[34] This example demonstrates how important cryptography became to counterintelligence, since they proved the accused's innocence or guilt.

A separate branch of cryptology was also used for counterintelligence - secret inks. Instead of cracking an encoded message, US officials had to find a chemical which revealed what the letter said without permanently damaging the letter. Luckily, on one occasion, Dr. Emmett K. Carver was both able to expose an intercepted message with "a new test using iodine vapor" and take a picture of it before it disappeared forever.[35] The letter, addressed to a notorious female German spy in America named Madame Marie de Victoria, resulted in the "subsequent arrest and confession"[36] of said spy, which in turn caused the "collapse of the largest German spy ring" in the United States at the time.[37] Both branches of cryptology demonstrate the shifting tactics of the US Army to incorporate cryptography into their counterintelligence operations.

Finally, the United States Army decoded enemy communications, which they used to launch counter-offensives and surprise attacks. Besides decoding the notes spies carried with themselves, the US actually used intercepted communications to their advantage outside of the country, in Europe. These interceptions gave the United States the ability to understand exactly what the German Army and population in general were thinking. They were then able to directly react to that information knowing exactly what the Germans would try to do. The US Army was also able to play upon the fears of the German commanders, and use soft power to chip away at their mental resolution to continue the war. In mission planning (METT-TC), gathering

information about the situation, and specifically the enemy, is extremely important. Cryptography opened an entirely unexplored world towards deciphering what the enemy was thinking and planning to do. Intelligence is one of the most important aspects of planning operations and cryptological advancements completely revolutionized this. Information gathering about the enemy was performed during World War I at an unprecedented level, greatly changing the tactics of all militaries fighting the war.

The United States Army used intercepted transmissions to launch counter-offensives that took the enemy by complete surprise. This impact of signals intelligence is demonstrated within a battle "in the early morning hours of Christmas Day 1917".[38] A German transmission that had been intercepted was successfully decoded within a short span of time, allowing the Allies to use the information they obtained to their advantage. With "20 minutes to spare"[39] before the attack was due to happen, American divisions were notified and told to "be alert for possible trench raids".[40] With their French allies, the Americans unleashed a counter-offensive "that kept the enemy in their trenches" and deterred the entire attack from happening.[41] This successful counter-offensive demonstrated to higher up that intelligence was becoming more and more crucial towards winning battles. If the intelligence staff could "timely exploit information in their possession", it would confer a great advantage upon given army and play an important role in the front lines.[42] Many commanders began noticing this correlation and started regarding intelligence sections, specifically cryptography ones, as integral to the success of the Army directly at the front lines.

Besides launching counter-offensives on the enemy, the United States Army was actually able to use soft power to play a mind game upon deeply ingrained enemy fears. Lieutenant J. Rives Childs, the same one that had tested the first failed version of the trench codes, once again

cracked a code that would lead to a major change in the United States Army's tactics. Childs was not a cryptanalyst by training, but he turned out to be incredibly observant and "often discovered mistakes in transmissions" which would end up being the key to unlocking and translating the ciphers.[43] Due to an oversight by the way the communication had been sent out, the German transmission that Childs ended up translating was only sent with "only a single transposition", making it much simpler to crack.[44] Within 48 hours of the receipt of the actual transmission in Berlin, the Allied Supreme War Council in Versailles had received it as well, attesting to the speed and efficiency in which Childs was able to decode the message and send it to Versailles. This one deciphering ended up changing the US Army's entire strategy. In fact, it "would alter the thinking of the Allied strategic planners at the highest levels".[45] After reading the transmission, the Allies began to see cracks in the Germans' system, specifically the fear that the public was turning against this total war. From then on, the US Army focused resources into spreading propaganda into Germany that "their army was on the verge of collapsing".[46] They focused on "recent German battlefield losses", and used word of mouth updates to inject more cracks into the population's will to continue to support the war.[47] This masterful use of soft power and communication efforts was only made possible because of our ability to break enemy codes. It gave the Allies the ability to understand the situation of the German population and figure out what they were thinking, which in turn helped us win the entire war! This use of cryptography completely revolutionized the US Army's tactics and ended up being a major factor in the Allied Powers' victory.

Besides being extremely useful for the United States, cryptography was also a tool of success for other powers. For the British, the campaign at Palestine perfectly demonstrates the advantage conferred upon the side with the most intelligence about their enemy. "Lord Allenby's

victory in Palestine had been certain," since he knew exactly what the other side would do one step at a time, giving him the opportunity to play his hand with complete certainty.[48] For the Austro-Hungary empire, they experienced immense "success against Serbian ciphers"[49] and were "exceptionally well informed about the Serbian order of battle and likely deployments".[50] They even had early successes against Russian cryptograms, and launched a wildly successful offensive with the Germans against Russia called the "Gorlice-Tarnow Operation".[51] The offensive fell exactly where the Russians were weakest due to exceptional cryptology done by the Austro-Hungary empire. When done well, cryptography turned out to be war-changing and could cause weaker armies to still inflict devastating damage if they knew exactly where to attack. However, cryptography only worked well paired with adequate fire power and leaders that believed in it. Due to the Austro-Hungary empire's ever-weakening military and their leaders' refusal to believe the information their cryptographers found, they ended up being defeated even with the strongest cryptography department. However, the Allied Powers, after recognizing the amazing successes information could get them, paired cryptology with strong firepower and believing leaders, resulting in a winning combination. Therefore, the Allied Powers ended up benefitting the most from cryptography innovation, even though they did not have the strongest cryptology forces.

Advancements in cryptography didn't only benefit the Army, it benefitted the other services as well. The United States Navy used a "code called A-1" during the war to communicate discretely.[52] Britain's famed "Room 40" was part of the Royal Navy, and extremely vital to the outcome of the war.[53] Germany also had their own code for their powerful U-subs to avoid detection and interception. After World War I, cryptography did not die out. In fact, it became increasingly influential throughout the next century and during wars such as

World War II and the Cold War. In the modern day, cryptography has manifested itself in our daily lives. With the recent formation of the Cyber branch in the US Army, the military is beginning to expand more and more into the realm of cryptology and information networks as a whole. Civilian infrastructure, such as banks and social media sites, must be constantly aware of cyber security and actively preventing outside forces from hacking and stealing personal information. Security breaches and foreign hackers stealing information from our databases have become common news headlines. This relevance to today's society all began in World War I, when the innovation of cryptology greatly changed the United States Army's tactics by forcing them to encode their own messages, develop stronger counterintelligence measures, and launch counter-offensives or soft attacks all based on information they learned from decoding intercepted messages. Modern cryptography has expanded outside the military to civilian life, becoming the cornerstone of computer and communications security, and an indispensable tool for our own protection.

Notes

[1] WWI: Technology and the weapons of war. (n.d.). Retrieved April 31, 2018, from https://www.ncpedia.org/wwi-technology-and-weapons-war, 1.

[2] Ibid. 1

[3] Ibid. 3

[4] Ibid. 3

[5] Communication Technology. (n.d.). Retrieved March 31, 2018, from https://encyclopedia.1914-1918-online.net/article/communication_technology, 1.

[6] Ibid. 1

[7] Ibid. 2

[8] Ibid. 2

[9] Kahn, D. (1984). Codebreaking in World Wars I and II: The Major Successes and Failures, Their Causes and Their Effects. The Missing Dimension, 138-158. DOI:10.1007/978-1-349-07234-7_8, 617.

[10] Ibid. 617

[11] Dooley J.F. (2013). Crypto and the War to End All Wars: 1914–1918. In: A Brief History of Cryptology and Cryptographic Algorithms. SpringerBriefs in Computer Science. Springer, Cham, 1.

[12] Schindler, John R. (2000). A Hopeless Struggle: Austro-Hungarian Cryptology During World War I*. Cryptologia, 24:4, 339-350. DOI:10.1080/01611190008984251, abstract.

[13] Ibid. 341

[14] Ibid. 341

[15] Ibid. 341

[16] Ibid. 342

[17] Ibid. 343

[18] Dooley, 8.

[19] Ibid. 9

[20] Ibid. 9

[21] Ibid. 9

[22] Ibid. 9

[23] Ibid. 10

[24] Ibid. 9

[25] Ibid. 10

[26] Ibid. 10

[27]Ibid. 10

[28] America's First Code-Breakers – How the U.S. Military Helped Win the WW1 Intelligence War. (2016, May 30). Retrieved March 31, 2018, from http://militaryhistorynow.com/2016/05/30/uncle-sams-first-code-breakers-how-the-u-s-military-helped-win-the-ww1-intelligence-war/, 5.

[29] Ibid. 5

[30] Ibid. 5

[31] Ibid. 5

[32] Ibid. 6

[33] Ibid. 6

[34] Ibid. 6

[35] Ibid. 7

[36] Ibid. 7

[37] Ibid. 7

[38] Gilbert, J. L. (2015). World War I and the Origins of U.S. Military Intelligence. Lanham, MD: Rowman & Littlefield, 64.

[39] Ibid. 64

[40] Ibid. 64

[41] Ibid. 65

[42] Ibid. 65

[43] Ibid. 197

[44] Ibid. 197

[45] Ibid. 197

[46] Ibid. 197

[47] Ibid. 197

[48] British Military Intelligence in the Palestine Campaign, 1914-1918. (1998). DOI:10.4324/9781315037646, 74.

[49] Schindler. 343

[50] Ibid. 343

[51] Ibid. 345

[52] Kahn. 619

[53] Ibid. 620

Bibliography

America's First Code-Breakers – How the U.S. Military Helped Win the WW1 Intelligence War. (2016, May 30). Retrieved March 31, 2018, from http://militaryhistorynow.com/2016/05/30/uncle-sams-first-code-breakers-how-the-u-s-military-helped-win-the-ww1- intelligence-war/

British Military Intelligence in the Palestine Campaign, 1914-1918. (1998). DOI: 10.4324/9781315037646

Bruce, James (2017). 'A shadowy entity': M.I.1(b) and British Communications Intelligence, 1914-1922, Intelligence and National Security, 32:3, 313-332, DOI: 10.1080/02684527.2016.1270992

Communication Technology. (n.d.). Retrieved March 31, 2018, from https://encyclopedia. 1914-1918-online.net/article/communication_technology

Dooley J.F. (2013). Crypto and the War to End All Wars: 1914–1918. In: A Brief History of Cryptology and Cryptographic Algorithms. SpringerBriefs in Computer Science. Springer, Cham

Gilbert, J. L. (2015). World War I and the Origins of U.S. Military Intelligence. Lanham, MD: Rowman & Littlefield.

Hammant, Thomas R. (2000). Russian and Soviet Cryptology I Some Communications Intelligence in Tsarist Russia, Crytologia, 24:3, 235-249, DOI: 10.1080/01611190008984244

Kahn, D. (1984). Codebreaking in World Wars I and II: The Major Successes and Failures, Their Causes and Their Effects. The Missing Dimension, 138-158. DOI: 10.1007/978-1-349-07234-7_8

Keylor, William R. (2015). The Zimmermann Telegram: Intelligence, Diplomacy, and America's Entry into World War I, by Thomas Boghardt, The International History Review, 37:2, 414-416, DOI:10.1080/07075332.2015.1021080

Leeuw, Karl de (2015). The Institution of Modern Cryptology in the Netherlands and in the Netherlands East Indies, 1914-1935, Intelligence and National Security, 30:1, 26-46, DOI:10.1080/02684527.2013.867223

Schindler, John R. (2000). A Hopeless Struggle: Austro-Hungarian Cryptology During World War I*. Cryptologia, 24:4, 339-350. DOI:10.1080/01611190008984251

WWI: Technology and the weapons of war. (n.d.). Retrieved April 31, 2018, from https://www.ncpedia.org/wwi-technology-and-weapons-war