THE PORT HENRY FACT FINDER

Reporting the News and Needs of Port Henry and Surrounding Area

vol. 5, issue 8 December 27, 2014

This issue has been made possible by the generous support of the following:
Louise and Skip Belden, Penelope the Clown and the Tim Bryants

May the New Year bring many wonderful surprises to one and all!

A FAREWELL

Farewells are always difficult but are particularly so when the person and her business has been such an integral part of Port Henry village for twenty-nine years. Natalie Clark and her always beautiful Fashion Corner were such a positive part of Port Henry, drawing people from over a hundred miles away so she could supply the necessities for a wedding or other special event. Moriah Central School students were so lucky to live right "next-door" to all her special prom dresses and prom wear for guys. Her shop windows were unusually special, not only for the beauty they offered, but that the offering changed every week! If you lived in the village or were here often, you automatically checked the Fashion Corner windows to see what was new. The windows are still being changed every week and we hope this will continue, but I personally already miss and will continue to miss being able to just drop in and talk with Natalie surrounded by the beauty she had created in her corner of fashion in Port Henry.

A WELCOME

A welcome to the lights shining in the upper windows of the old Sagan building, recently acquired by Mountain Lake Services; these second floor rooms have been empty for years and now have come to life as offices for Mountain Lake Services. The rumor is that the lower floor will house a business needing a store front. It is sincerely hoped this becomes a reality soon. Then Port Henry will have only one empty store front on the main portion of Main Street. Also, the new awning over the entry into the store is a real boon to the appearance of our Main Street.

A THANK YOU

The Fact Finder is grateful to The Press Republican for allowing the following, first appearing in its December 22nd issue's TO THE EDITOR section, to be reprinted below.

"On behalf of the Village of Port Henry Board of Trustees, we extend our sincere appreciation to Congressman Bill Owens for his help, cooperation and tireless efforts in helping the village obtain the FEMA reimbursement funds for our campground and beach restoration projects, as a result of the damages incurred from Tropical Storm Irene in August 2011.

We would also like to extend our appreciation to his former assistant, Chance St. Germaine, who was also instrumental in helping us with regard to this matter.

Again, we thank Congressman Owen very much. We have been very fortunate to have a congressional representative such as he representing the people of the North Country and we wish him continued success in his future endeavors.

ERNEST GUERIN
Mayor
Village of Port Henry"

The Fact Finder would like to end 2014 and begin 2015 in one of the best ways possible, print an article by a Moriah Central School student.

SOLVING the UNSOLVABLE

by Nicholas Manfred

The escalated demand for invulnerable radio communications succeeding World War I pushed German forces to espouse the Enigma machine (below) as an enciphering device. At the commencement of World War II, when the Allied forces cracked the Enigma machine's code, they obtained an unprecedented strategic advantage, assuring a democratic triumph. The immense awareness into German actions given by Enigma decryptions permitted the Allied forces to acknowledge a current importance in cryptology, serving as a catalyst for the advancement of communications intelligence. The intelligence gained an integral state in domestic and foreign affairs, basically modifying the idea of modern security.

Cryptology Through the Ages

For an extensive period of time in history, cryptology exhibited major potential for military tactics, but it suffered from negligible investigation and limited assets in the field even though humans have thought of communicating in a secure fashion since antiquity. The origins of cryptology, the study of codes, date back to 50 BC when Julius Caesar's cipher shifted the alphabet to encode military message. This shift was relatively simple to decode due to its dearth of complexity. Simplicity diminished when Leon Battista Alberti, "the father of western cryptology," invented the very first poly-alphabetic cipher in 1466 AD. The Alberti Cipher was the main method of coding for over a century but eventually was considered too simplistic, causing au courant coders of the day to establish an even more complicated cipher the Vigenere Cipher, which was a series of Caesar Ciphers.

Albeit there were preexisting ciphers, the Confederate Army decided to minimally use the Confederate Cipher Disk during the Civil War (1861-1865). However, the all-time high for decoding was in WWI when the Zimmerman Telegram was undergoing decryption. This is where coding showed severe salience militarily.

Learning from WWI

"More than anything else, [the Zimmerman Telegram) hardened the peace-loving American people to the conviction that war with Germany was an absolutely necessary step." states Charles F. Horne, an American author, in 1921. On February 24m 1917, a message sent from two German transmissions intended for Jose Venustiano Carranza Garza was intercepted by British Naval intelligence. This message, known as the Zimmerman Telegram, was supposed to be an incognito way for the Germans to attempt at involving Mexico in WWI in an alliance against the United States, but

ended up in the hands of the US government and became an expose for its citizens. Although the Zimmerman Telegram's significance lies within the first World War, it further proved to the Germans that there was indeed a need for communications innovation. Therefore it is mostly because of the failures of the Zimmerman Telegram that the invention of the Enigma machine happened and, once created, it was onerous to solve.

Intelligence

When World War I concluded with a victory for the allies, tension was still ubiquitous between the opposing powers. Germany still felt it a necessity to expand its empire under the leadership of Adolf Hitler, which was also the reason WWI occurred, causing a myriad of problems for surrounding countries and the beginning of the second World War. The biggest problem for the Allies, however, arguably could have been that there was a lack of preparation in terms of intelligence agencies [i.e. the British Security Intelligence Service (SIS, commonly known as M16) British Government Code and Cipher School (GC&CS), etc.) They were all too unorganized, informal, fragmented, small and un-influential with insufficient budgets. Meanwhile, the United States did not even have an adequate intelligence activity, in that it was thought to be unnecessary – comical almost in comparison to other forms of utilities. So at the start of WWII, the Axis Powers, possessing the Enigma machine, had an enormous advantage.

The Complexity of Coding

The Enigma machine was an electro mechanical rotor machine, built in 1930, that replaced the letters of a message randomly before sending it, verifying that the message could only be read by its intended recipient. Due to the special procedures performed by the Enigma machine, the solvability is so far removed from practical possibility that the cipher system must be regarded as virtually incapable of solution. This astounding jump of complication in cryptology inevitably made the Enigma machine "the most fearsome system of encryption in history." and the "backbone" for military communicating, seeing as it can potentially create any of 3,283,883,513,796,974,198,700,882,069,882,752,878,379,955,261,095,623,685,444,055,315,226,066,433,615,627,409,666,933,182,371,154,802,769,920,000,000,000 combinations.

Planning Ultra

"It was thanks to Ultra that we won the war," Winston Churchill said. Despite these impressive statistics, Poles began decrypting the Enigma machine from 1932-1939 and became the precursor to the British decryption efforts at Bletchley Park know as "Ultra." While the messages simply cannot be decoded, the specialists at Bletchley Park (like Polish cryptanalyst Marian Rejewski who worked out the mathematical solution in four months) figured out how to work through this enigma. Then in 1939, facing a German invasion, Waclaw Stachiewicz, Polish Chief-of-Staff, authorized the Cipher Bureau to send their knowledge of the Enigma machine to the Allies. From there, Ultra had officially obtained the information it needed to get, "off the ground."

The Double-Cross System

"If one were forced to select a single form of activity in which Ultra was unceasingly and completely essential, it would have to be that of deception." Dr. Harold C. Deutsch, expert on the German military, explains. Decrypted Enigma messages provided forethought to Allied leaders and equipped them to make au fait, calculated decisions, which was crucial to securing many Allied victories throughout the war. With the help of the Double-Cross System, the Enigma machine played a major role in making long-term warfare plans and providing insight into the enemy's plans, by and large assuring more victories or the Allies. The main force behind the Double-Cross System was a process in which decrypted Enigma messages were rewritten by captured German agents under the supervision of Allied dedicatees and sent again to confuse, hinder, or redirect the Axis. By means of the Double-Cross System, we actively ran and controlled the German espionage system in Britain,"

says J.C. Masterman, chairman of the Double-Cross System.

British Intelligence Reformation

There are a variety of lasting impacts established by the Enigma machine, including British intelligence. Cryptology gained support after WWII, leading to rapid expansion of intelligence agencies, exemplified by the presence of communications intelligence in British policy. The sheer amount of incoming messages during WWII forced Bletchley Park to transform the process of intelligence gathering from small scale hand decryption to an industrialized process. During the Cold War, GC&CS was renamed Government Communications Headquarters, signifying the expansion into a powerful and active intelligence organization. "It is all but impossible to draw a distinction between GCHQ's work in Germany and her growing work in the Soviet Union in the 1940's," Richard Aldrich, professor of international security, states.

Military Cooperation

Another lasting impact of the development and analysis of the Enigma machine includes its effect on the military cooperation of the United States and Britain both during and after the second World War. The necessity of sharing highly sensitive decrypted information between the Allies led to an alliance that has extended into the twenty-first century and hopefully will stay intact indefinitely longer. Born out of cooperation achieved by international code breakers working together during WWII, particularly the Americans stationed at Bletchley Park. The 1943 British-United States Communication Intelligence Agreement (BRUSA) continued the special relationship between Britain and the United States. This alliance was strengthened by the United Kingdom-United States of America Agreement (UKUSA) of 1946, a document so based on secrecy it was not officially acknowledged until 2005. During the Cold War, the NSA (National Security Agency) and GCHQ shared intelligence regarding the USSR and its satellite nations. It is estimated that these agencies received billions of dollars and have been acknowledged by world leaders as being extremely significant. Lastly, the relationship established during WWII and the Cold War has contributed to broader political ties between the US and Britain.

The Information Age

Perhaps the long-lasting impact of the Enigma machine having the most importance is its role in giving birth to the Information Age. Research started with Enigma and conducted at GCHQ created public key encryption in 1973, providing security for the international business world in the Information Age. After Enigma was broken, the need for seccure cryptology was recognized, but further advancements were nearly impossible with the then current technology. Simon Singh, author *The Code Book*, explains, "The cost to key distribution was already enormous, and would become the limiting factor to any expansion in encryption." Without a new method of security, cryptology had reached its limit, until Enigma showed up. This need, and the research prompted by Enigma and conducted at GCHQ, led to the development of public key encryption. Public key encryption is the security standard for organizations ranging from the United States government to Facebook. It secures digital transaction such as electronic voting, bank transfers, and online payments.

Aftermath of Enigma

The breaking of the Enigma codes was a turning point in the war effort that resulted in direct military information that enabled the Allies to take strategic measures on the Atlantic, Eastern and North African fronts, which aided in victories across the board. The deciphered messages also gave the Allies information on German plans for advancement and confirmed that the double agents were free of suspicion. Simultaneously, the opportunities provided by the decryption of the code demonstrated the immense potential of military intelligence, revolutionizing Britain's strategy for the war and marking a decisive change in the focus of the Allied governments on information technology. This led to

significant growth in the British signals intelligence agency, or GCHQ. The work done at Bletchley revolutionized encryption techniques and led to further research that strengthened international alliances which continue to this day. The Allied nations' success with Ultra forever changed how intelligence is viewed.

Look for the next issue on **Saturday, January 10, 2015** at Macs, Moriah Pharmacy, Sherman Free Library, George's Restaurant, John Eisenberg's Service Center, Ken and Paula LaDeau's Champlain's Best Wash, Don Foote's "Miss Port Henry" Diner, and TFCU. NOTE: The Fact Finder may also be found on-line at porthenrymoriah.com. Go to "Living Here" and you will see "Fact Finder" to the far right, one line down.