REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05/04/2016	Master's of Military Studies	SEP 2015 - APR 2016

4. TITLE AND SUBTITLE

Today's Recruitment and Retention of the DoD Cyber Workforce Through the Lens of World War II and Bletchley Park

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Thomas, Danielle, E, Major, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
Dr. Matthew Flynn

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Similar to the codebreaking efforts at Bletchley Park, cyber warfare is an intellectual battle; one that will be driven by a cadre of primarily civilian expertise complemented with military leadership. With the deadline of the Cyber Mission Force to reach initial operating capability looming, USCYBERCOM should consider looking beyond military personnel to the civilian sector for their full integration within USCYBERCOM in conjunction with developing part-time civilian tech partnerships. To do so would mean that USCYBERCOM recognizes that the success of their organization will come at the hands of civilians led by military leaders, solidifying that the success of military operations far exceeds the capacity of the standing military.

15. SUBJECT TERMS
USCYBERCOM; Bletchley Park; cyber workforce recruitment and retention; Ultra

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	35	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:

TODAY'S RECRUITMENT AND RETENTION OF THE DOD CYBER WORKFORCE THROUGH THE LENS OF WORLD WAR II AND BLETCHLEY PARK

AUTHOR:

Major Danielle E. Thomas

AY 15-16

Mentor and Oral Defense Committee Member: MATTHEW FLYNN

Approved: _____

Date: 4/1/16

Oral Defense Committee Member: J.W. Gordon

Approved: _____

Date: 4/1/16

Executive Summary

Title: Today's Recruitment and Retention of the DoD Cyber Workforce Through the Lens of World War II and Bletchley Park

Author: Major Danielle E. Thomas, United States Marine Corps

Thesis: The United States' ability to successfully control the cyberspace environment today and in the future will come largely through the coordination and cooperation of a proficient military-civilian team closely resembling that of the highly effective World War II British-led decryption effort based in Bletchley Park, England.

Discussion: Cyber warfare is the most rapidly growing threat to the national security of the United States. As a result, each military service within the DoD is quickly working to establish doctrine that articulates the use of offensive and defensive cyber operations in support of its operational campaigns and/or schemes of maneuver. In doing so, the services have realized that to conduct effective cyber operations, they need to recruit and retain a highly technically educated workforce comprised of members who are more often lured by the comforts of a corporate office over the rigors of military training. While the military recruits and employs many intelligent service members with the capacity to learn the required skills and information, the size, scope, and duration of the training process is not supportable in the long term so the services will be forced to look to integrate a larger civilian workforce if they intend maintain readiness. An analysis of codebreaking efforts conducted at Britain's Bletchley Park during World War II allows the reader to see the parallel between Bletchley Park and those challenges that the United States Cyber Command (USCYBERCOM) faces today.

Conclusion: Similar to the codebreaking efforts at Bletchley Park, cyber warfare is an intellectual battle; one that will be driven by a cadre of primarily civilian expertise complemented with military leadership. With the deadline of the Cyber Mission Force to reach initial operating capability looming, USCYBERCOM should consider looking beyond military personnel to the civilian sector for their full integration within USCYBERCOM in conjunction with developing part-time civilian tech partnerships. To do so would mean that USCYBERCOM recognizes that the success of their organization will come at the hands of civilians led by military leaders, solidifying that the success of military operations far exceeds the capacity of the standing military.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Contents

Acknowledgements

I would like thank my husband, Adam, first and foremost for taking care of everything on the home front to allow me the time to research and write this paper. Second, I would like to sincerely thank Dr. Flynn, my mentor, for his critiques, thought provoking questions, and overall guidance. Last, I would like to thank Dr. Warner for his willingness to provide feedback and direction to a student he has never met. Without all three of you, this paper would not be possible.

Introduction

In today's tech-dominated environment, Google, Microsoft, Apple, and other technology-based corporations have become household names. Technological innovation is synonymous with these private sector monoliths and not with the U.S. military. The introduction of the personal computer in the 1980s delineates the private sector's emergence as the primary driving force of technological innovation in the modern U.S. economy. While the military has made significant technological advancements since its use of electromechanical analog computers in Navy submarines, true innovation resulting in a significant change in the way wars are fought and won has been relatively rare since World War II. With few exceptions beyond the aerospace industry, the military's operational needs no longer drive the tech industry to surpass the limits of human knowledge to derive new solutions, though some may argue that the military is attempting to do just that as it militarizes cyberspace. With the goal of taming this new frontier, the Department of Defense (DoD) needs the best tech minds the United States has to offer as it fights America's battles in the distinctly new dimension of cyber warfare.

Cyber warfare is the most rapidly growing threat to the national security of the United States. As a result, each military service is quickly working to establish doctrine that articulates the use of offensive and defensive cyber operations in support of its operational campaigns and/or schemes of maneuver. In doing so, the services have realized that to conduct effective cyber operations, they need to recruit and retain a highly technically educated workforce comprised of members who are more often lured by the comforts of a corporate office over the rigors of military training. While the military recruits and employs many intelligent service members with the capacity to learn the required skills and information, the size, scope, and

duration of the training process is not supportable in the long term so the services will be forced to look to integrate a larger civilian workforce if they intend to maintain readiness.

Analogously, the military services were confronted with the need to recruit a workforce that was equally as technical as the workforce required for today's cyber fight as it prepared to fight the world's top industrialized nations, Nazi Germany and Imperial Japan, during World War II. The United States' ability to successfully control the cyberspace environment today and in the future will come largely through the coordination and cooperation of a proficient military-civilian team closely resembling that of the highly effective World War II British-led decryption effort based in Bletchley Park, England. This proposed amalgamation of civilian and military personnel is a key change from past DoD efforts to address cyberspace in a military context and demonstrates clear evidence that cyberspace has put warfare on a new trajectory of nonviolence when settling inter-state conflict. By analyzing the recruitment, retention, and work of the personnel at Bletchley Park and applying the key outcomes, the DoD can gain both perspective and clarity as it faces continuing challenges in recruiting and retaining an equally proficient cyber workforce. In so doing, the U.S. Military may also lead the way in reshaping warfare from a military effort to a whole of government approach that all but supplants it as the means of waging war. This change is incredible to contemplate and proves demonstrative only when the historical context is presented as done in this analysis.

Literature Review

Prior to the 1970s, no historical account of World War II included any solid account of British code-breaking or the admission of a place known as Bletchley Park. That would quickly change in the 1970s when the history of Bletchley Park began to be declassified by both the United Kingdom and the United States. Since that time, much has been written about the

activities that took place at Bletchley Park. However, only a handful of valuable books recount the beginnings of Bletchley Park, the people who worked there, their activities, and their methods. These books include Fredrick William Winterbotham's, *The Ultra Secret;* Wladyslaw Kozaczuk's, *Enigma: How the German Cipher was Broken, and How it was read by the Allies in World War Two;* Gordon Welchman's, *The Hut 6 Story*; Hinsley's, *Codebreakers: The Inside Story of Bletchley Park;* Hervie Haufler's, *Codebreakers' Victory How the Allied Cryptographers Won World War II;* and Andrew Hodges' *Alan Turing: The Enigma*. F.W. Winterbotham, a British Royal Air Force officer who worked at Bletchley Park and was responsible for the dissemination of Ultra, wrote the first English book, *The Ultra Secret*, that details the activities of Bletchley Park and his role within Bletchley Park. For that very reason, every other account of Bletchley Park listed within the bibliography references Winterbotham's account. Wladyslaw Kozaczuk's, *Enigma: How the German Machine Cipher was Broken, and How it was Read by the Allies in World War Two*, also published in 1974, but by a Polish Army colonel and intelligence historian, recounts Poland's contributions to the development of the "Bombe." In 1982, Gordon Welchman, a mathematician recruited to work at Bletchley Park prior to World War II, recounts his memoir of Bletchley Park in *The Hut 6 Story*. Eleven years later, F.H. Hinsley, an analyst at Bletchley Park, provides a compilation of profiles of a number of key personnel in *Codebreakers: The Inside Story of Bletchley Park.*

From these detailed accounts of personal memories, one can begin to piece together the recruitment, culture, and retention of those who worked at Bletchley Park. Both Welchman's memoir and Hinsley's account are recognized as accurate records of Bletchley Park as both served within Bletchley Park, and both accounts are referenced numerous times in additional reference material that was considered for use. Ten years later, Haufler's account proves the

crucial contributions made by the civilians at Bletchley Park. Hodges' *Alan Turing: The Enigma* is an account of the life of Alan Turing. Though Turing does not stand alone amongst the civilians who made significant contributions at Bletchley Park, Hodges' account is a valuable biography of a maligned figure that finally gets the recognition he deserves for his contributions to modern computing.

In comparison to the number of historical books that detail the events of World War II, relatively a limited number of historical accounts about Ultra (or intelligence for that matter) impacted World War II, specifically in the North Atlantic and in North Africa. David Kahn's, *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943*, was the most thorough account of how the Allies used cryptography to their advantage during the North Atlantic campaign, providing detailed explanations of when and how the campaign was fought. John Gordon's treatment of the British Special Forces in the desert, *The Other Desert War,* shows the impact of this "civilian war" on Rommel as significant, but measured. However, no one, specific book details the campaign in North Africa, rather, the details of Ultra's impact on the North Africa campaign are scattered in various chapters throughout numerous books within the bibliography. Presumably, this scattered information is due to the fact that Ultra was not as decisive in the North African campaign as compared to other campaigns within the Atlantic Theater. Therefore, the best source of information on the Desert Campaign came from histories of Rommel's actions, such as Martin Kitchen's, *Rommel's Desert War Waging World War II in North Africa 1941-1943*, which did not include the specific contributions from Bletchley Park's efforts.

In comparison, the available cyber literature is even further limited because recruitment and retention of personnel within the cyber field have recently emerged as significant challenges

and the DoD has rarely published unclassified versions of its plans for cyberspace. The newly published *Department of Defense Cyber Strategy* was the key reference used to understand United States Cyber Command's (USCYBERCOM) strategic goals and objectives to build and maintain cyber personnel. Admiral Roger's statements before Congress make it clear that manning within USCYBERCOM continues to be a challenge and that USCYBERCOM has not yet completely resolved how it plans to move forward. Beyond the sources that provide a researcher with the historical context of Bletchley Park and those that describe the current status of USCYBERCOM, no sources use the historical backdrop of World War II to consider the solution of a civilian lead workforce within USCYBERCOM. This fact makes the analysis below unique.

Bletchley Park

As war fell upon Europe in 1939, British Allied supporters from various walks of life converged on a place known as Bletchley, located fifty miles to the northwest of London in the Buckinghamshire countryside. The work performed at Bletchley, also known as "BP" or "Station X", played a pivotal role in the outcome of World War II as it helped Britain to escape early defeat and hastened the Allied victory.[1]

In 1938, Admiral Sir Hugh Sinclair, then head of the Secret Intelligence Service (SIS or otherwise known as MI6), purchased primary Bletchley property for use by the Government Code and Cypher School (GC&CS) and the SIS in case the tenuous situation with Germany should ever devolve into warfare.[2] Key leaders masqueraded as "Captain Ridley's Shooting Party:" during their month-long initial visit to Bletchley to ensure their true intentions to use the facility as the hub for British decryption efforts remained unknown.[3] Bletchley was specifically chosen for its location far outside of the hustle and bustle of London, allowing the intelligence

professionals from MI6 and GC&CS to work diligently toward breaking the ciphers and codes used by Nazi Germany.[4] At the peak of World War II, Bletchley and its outstations employed an estimated 10,000 military and civilian personnel.[5]

In 1939, Bletchley became operational as veteran cryptographers from World War I converged to form the core of GC&CS. Some of the notable veterans were Dilly Knox, Frank Birch, and John Tiltman.[6] When war broke in August 1914, the Admiralty's newly appointed Director of Intelligence, Rear Admiral Henry Oliver, was given copies of intercepted enciphered German wireless transmissions that he could not read.[7] Soon after, Winston Churchill and Admiral John Fisher tasked Oliver to establish a wireless intercept service that became known as "Room 40".[8] The former Director of Naval Education, Sir Alfred Ewing, had a proven track record for educating naval personnel and a personal interest in codes and ciphers, making him the obvious choice to lead Room 40. Upon accepting the position, Ewing concluded that he needed a multi-talented team of cryptographers to decipher the messages, linguists to translate the messages, and naval officers to put the messages in naval terms and practice.[9] Ewing needed personnel quickly so he looked to the Royal Navy, which had staff members at the colleges of Dartmouth and Osborne. Ewing recruited, "a disparate team of characters who came from many walks of life, creating a mixed bag of extraordinarily cerebral linguists and naval experts in his team."[10] One of the candidates he interviewed was Commander Alastair Denniston, who later served his signals intelligence apprenticeship in Room 40 with many of the other veterans who went on to serve as the leadership within Bletchley Park.[11] Ewing's team served as the foundation for what would become Bletchley Park during World War II.

As the success of Room 40 established the beginnings of Bletchley Park, the core group was joined by civilians from industry and academia, most notably Alan Turing and Gordon

Welchman.[12] Though Bletchley was run and operated by the British military service, it employed a significant number of specially trained civilians to aid the military in its mission to break the German Nazi ciphers. Daily operations were initially accomplished by only thirty people, but as Bletchley's mission to break the Enigma expanded, the British government had to recruit individuals with the specific expertise needed to solve the technologically advanced German ciphers.[13] GC&CS recruited many of the highly trained civilians from Cambridge and Oxford by forming annual drafts after asking the schools for recommendations.[14] Many other civilians were recruited by associates and friends from school. In the end, the military services did not have the intellectual capital immediately available to break enemy ciphers, so GC&CS sought for it where it was immediately available: academia.

The head of Bletchley, Commander Alastair Denniston and John Tiltman, chief cryptanalyst, conducted most of these interviews in a brief, informal style and then notified prospective candidates of their selection within a few days.[15] The entire interview process was completed with minimal formality and maximum efficiency. Denniston and Tiltman hired people from all walks of life, including mathematicians, chess players, teachers, and language experts.[16] Aside from the technical experts, Bletchley recruited businessmen who served as military administrators and others who simply volunteered for military service via the typical process of the Joint Recruiting Board and who were subsequently assigned to Bletchley following service selection. [17,18] Bletchley was a meritocracy where rank did not matter; rather, one earned respect by performance and nothing more. Typical military customs and courtesies were forbidden, and everyone was on either a first name basis or went by a nickname.[19]

Aside from breaking the codes and ciphers of Nazi Germany, the work performed at Bletchley played a significant role in the development of signals intelligence and modern

computing. For example, the algorithms developed by Alan Turing and Gordon Welchman to build the highly advanced electromechanical decryption machines are accepted as the beginning of the programmable computer, in addition to the fact that Bletchley became the Government Communications Headquarters the home of Britain's signals intelligence efforts. These accomplishments proved significant, except when set alongside the crowning achievement of the program.

Bletchley is most known for its work to break the Enigma; an electromagnetic cipher machine adopted for use by the German Armed Forces including the Army, Navy, and Air Force, as well the Japanese and Italians.[20] The Enigma used rotors to scramble the text of each message into a cipher text that was decrypted by the receiving station. The cipher changed each night at midnight, pitting the Bletchley cryptographers against the daunting task of breaking a new code each day to ensure that the messages received could be properly decrypted and analyzed so as to provide added value to the war effort.[21] Though the mission at Bletchley began with breaking the German's use of the Enigma, its mission expanded and changed to breaking each new upgraded encryption machine and more advanced communications links between each of the Axis powers.

However, the personnel at Bletchley were not the first to break the Enigma. The Polish Cipher Bureau had done so in 1932 with the help of the French.[22] Similar to Denniston's recruitment of civilians to GC&CS and subsequently Bletchley, in 1929 the Cipher Bureau enrolled twenty or so young mathematicians in a cryptology course at the University of Poznan as they understood breaking the Enigma required advanced mathematical skills.[23] One of the great minds to graduate from the University of Poznan, Marian Rejewski, who first reconstructed the Enigma machine, faced the daunting task of deciphering the daily keys to read ongoing traffic.[24] During this time, German code clerks were told to connect only six of the cables of the

Enigma, creating only twelve-letter substitutions. Though it was a laborious task, Rejewski first broke the Enigma code by hand.[25] Rejewski knew that it was only a matter of time before his efforts would no longer suffice; he knew he needed to create a machine that could help find the Enigma keys quicker. England made this ambition real.

Developed at some point between 1934 and 1935, Rejewski's first device, the cyclometer, sped up the Cipher Bureau's cryptanalysis efforts until 1937.[26] In 1937, the Germans changed the Enigma's reversing reflector, which voided the Poles' decryption process. After months of effort, the Cipher Bureau was back to decoding German communications, though this came to a halt again in 1938 when the Germans made their first major change in procedures. Code clerks no longer used a uniform daily key setting; rather they were told to choose a new basic setting for each transmission.[27] Rejewski responded by building a new machine called a "bombe." The first Polish bombe machine consisted of six Enigma machines connected together that systematically ran through all of the possible permutations looking for the rare place where the plaintext letter would match the cipher letter. As the bombe identified all of the letters on all three rotor positions, analysts reconstructed the daily keys.[28] The results of the bombes did not, however, disclose the order in which the three Enigma rotors were placed into the machine (an order that changed daily). A fellow Cipher Bureau mathematician, Henryk Zygalski, prepared one-hundred and twenty-six sheets of two square feet cardboard known as Zygalski sheets that when layered over one another allowed the Poles' to determine the order of the rotors.[29]

In December of 1938, the Germans made their second major change to their Enigma operations, which proved to be beyond the capacity of the Polish Cipher Bureau. The Germans began using five rotors on their Enigma versus the original three. The two additional rotors required the Poles to connect sixty bombe machines and 1,560 Zygalski Sheets.[30] The Polish

Cipher Bureau did not have the resources to keep up so it, in turn, decided to share its work with their Allies, who at this time included both the French and the British. In July 1939, French and British delegates, including Dilly Knox and Alastair Denniston, visited Warsaw where the Cipher Bureau explained all of the details of its work. The Cipher Bureau informed Knox and Denniston of their plan to send the Enigmas via diplomatic pouch to Paris where they could be forwarded to England. The Cipher Bureau also agreed to provide the technical drawings of the bombes and samples of the Zygalski Sheets.[31] The cryptanalysts at Bletchley were astonished as they had a significant head start with the help of the Poles.

As additional personnel arrived at Bletchley, pre-fabricated wooden huts were constructed on the lawns to accommodate the growing workforce. Each hut was known by a number so as to mitigate any potential operational security concerns that a specific name could create.[32] The huts worked in pairs: Hut 3 worked with Hut 6 and Hut 4 worked with Hut 8. Hut 6 was built in January 1940 to aid in the breaking of both the German Air Force and the German Army Enigma messages. As messages were decrypted in Hut 6, they were sent to Hut 3 for follow on translation, analysis, and dissemination to the end user, whether that was the Ministries or Commands.[33] Similarly, Hut 8 was built in January 1940 to aid in the breaking of the German Navy's codes, and their decryptions were sent to Hut 4 for follow on translation and analysis. Hut 11 housed the "Bombe Machines" and the WRNS (Women's Royal Naval Service).

As the personnel from Hut 6 and Hut 8 realized the complexity and the timeliness of breaking the daily codes, they agreed with the Poles that they could only defeat machines with machines. Taking little other than the name of the machine from the Poles, Hut 6 built the British "Bombe Machines" that helped them rule out all of the incorrect daily cipher possibilities, greatly speeding up the decryption process.[34] The Bombe Machines helped to deduce the daily

settings of the Enigma machines by determining the settings on the rotor and plug board. The Bombe Machines were operated by WRNS members, known as “Wrens,” who were recruited in a similar fashion to the civilians working at Bletchley. After assignment to “Special Duties X,” Wrens were quickly indoctrinated in naval customs and courtesies, drill, and domestic duties, after which they made the trek to Bletchley and were briefed about the work that they had been chosen to perform.[35] Even though many of the Wrens had not expected to spend their time in the Navy hidden in a loud, dark, buildings that lacked temperature control, setting up machines about which they only ever knew the key, most agreed to accept this mission because they were young, patriotic, and opposed to Nazi Germany.[36] The financial compensation they received was so modest that it demonstrated the Wrens dedication and determination to beat Nazi Germany.

After deciding to stay, the Wrens were given in-depth training in how to set up and run the Machines. They were provided with menus, produced by the cryptanalysts in the various huts, of complicated letters and numbers that helped them set up the Bombe Machines. When the Machine suddenly stopped and the readings from the drum appeared to match the menus provided to the Wrens, they knew the daily settings for that particular key were found, and it was quickly phoned to the controller at Bletchley for deciphering, translation, and analysis.[37] At Bletchley’s peak, approximately 2,000 Wrens quietly toiled in less than ideal conditions to make the work of those in the huts at Bletchley possible.[38] The poor conditions at Bletchley were a product of the rapidly expanding mission and the equally rapidly dwindling space. None of Bletchley’s original leadership including Alastair Denniston understood how rapidly their mission would grow, hence the fabrication of huts on the lawn of Bletchley and the poor conditions in which the Wrens worked.

Hut 8's role at Bletchley is famous because it is the hut in which Alan Turing worked. Alan Turing's life's work and study, which developed significantly while he worked within Hut 8, was focused on a principle known as the universal machine or the Turing machine. The Turing machine could execute any mathematical computation that could be written as an algorithm and stored on tape, essentially making it programmable. The concept of the Turing machine is accepted as the basis for the modern computer. Turing believed that, "all algorithms or all mechanical processes could be implemented on a universal machine."[39] He developed, "particular algorithms, using sophisticated logic, statistics and parallel processing" that helped to break the Enigma.

As brilliant as Turing's theories and algorithms were, he still needed help from a colleague, Gordon Welchman, a fellow mathematician and Cambridge alumnus, to make his version of the Bombe work. Turing's first Bombe was designed to automatically test for specific "cribs" or "probable words" within a message.[40] Locating the cribs or loops of letters within the message allowed Turing's Bombe to solve the correct settings for the Enigma that sent the message. Though Turing's theories were correct, the machine did not work well because it stopped too many times and proved unreliable.[41] Welchman knew how to improve Turing's machine, "by interconnecting the scramblers in a completely new way one could increase the effectiveness of the automatic test by a very large number," he wrote in his memoir.[42] Welchman called the interconnecting scramblers a "diagonal board" that can be described as, "a matrix of terminals in a square in which twenty-six letters of the alphabet were arranged horizontally, with another twenty-six vertically."[43] The introduction of the diagonal board greatly reduced the number of false positives in Turing's Bombe, therefore increasing the speed at which the Enigma

keys could be broken. Though Turing's accomplishments at Bletchley are famous, they are not alone—many others made similar contributions.

It would take time, however, for these new machines to be manufactured and to arrive at Bletchley. During that time, the analysts relied on the genius of another mathematician recruited by Welchman, John Herivel, and what became known as "Herivel's tip." Herivel's thought was that Bletchley should collect the first messages sent each day by the German code operators as they were bound to take shortcuts when setting the new rotors, potentially using the same letters as the rotor settings. If this pattern was repeated, it was likely that the settings of the Enigma could be solved.[44] It was ingenious thoughts such as Herivel's tip and many others, compliments of the German code operators who chose not to follow the operating manual for the Enigma or who simply sent the same message repeatedly, that allowed Bletchley to break the keys to the Enigma by hand until the Bombe's arrived.

In the fall of 1940, Bletchley was met with a new cryptologic challenge. The Germans began encrypting radio traffic being used by higher-level communications, such as those between commands or from the headquarters to commanders in the field with the international code, Baudot-Murray.[45] Bletchley referred to these communications as "Fish" because the Germans referred to one of the systems as "Sägefisch" or "Sawfish."[46] The leadership of British intelligence understood that trying to solve three different types of Fish encoding machines (one used by each of Germany's military services—army, navy, and air force) would be resource intensive so in turn, it decided to focus on the cipher machine used by the army known as "the Lorenz." [47]

The Lorenz was used by Hitler, the German High Command and Hitler's Field Marshalls to communicate.[48] Tunny was the cover term used at Bletchley to describe both the network

traffic that came from the German High Command to its various Army Commands and the equipment that was used to decipher the messages.[49] The "Colossus," which was developed as a response to the development of the Lorenz, was developed out of necessity as the Germans had introduced a level of complexity within the Lorenz that made it nearly impossible to break it by hand.[50,51] The Colossus could read 5,000 characters per second which, in turn allowed, Bletchley to break the Lorenz within a matter of hours, not weeks.[52] Similar to the development of Turing and Welchman's Bombe, the first Fish messages to be decrypted were done so by the hand of John Tiltman, an Oxford graduate and chief cryptanalyst, with the unknowing compliance of German code operators who took forbidden shortcuts when sending messages.[53] The team of Tiltman, William Tutte, another Cambridge graduate, and Max Newman, a peer of Alan Turing's at Cambridge developed the technical design of the first Colossus.[54] The first Colossus, like the first Bombe, did not work as intended because it was driven by paper tape driven and high speeds over extended periods of time.[55] Seeing this, Alan Turing recommended that the Fish team seek the help of Tom Flowers, from Britain's Post Office Research Station, who used vacuum tubes in his development of postal equipment.[56] Within ten months, Flowers and his team, outside of the support of the leadership at Bletchley (due to the cost), developed a fully functioning Colossus that took the Fish decryption time from weeks to hours.[57] The Colossi were originally operated by the Wrens, just like the Bombe, though in the case of the Colossus, the analyst sat with the Wrens providing input to the process.[58] As the work on the Colossus developed, the analyst's presence was no longer needed as the analyst was replaced by written decision trees that allowed the Wrens to adjust the machine appropriately.[59]

The development of the Bombe and Colossus demonstrates the team effort used by the most talented minds in Britain to successfully break the Enigma and Lorenz, which proved to

have a significant influence on the outcome of World War II. Overall, civilians led this effort and proved their value from start to finish. Military officers were involved, given the context of fighting a war, but these few professionals quickly learned to abide by civilian mandates and needs. In doing so, military leadership proved to be necessary in the overall execution of the mission and proper dissemination of intelligence to commanders in the field, though it was at the hands of the civilian cadre inside Bletchley that the war was truly won.

Ultra's Impact on the Outcome of World War II

Ultra, as it was known, was the code name used during World War II to describe the decryption products of important enemy ciphers.[60] Historical accounts of World War II produced prior to 1970 do not directly account for the use of Ultra on the war effort as the codebreaking efforts were not yet declassified. Historians believe that Ultra did not contribute to the war effort until the spring of 1941, eighteen months after the war began.[61] Though decrypts were obtained earlier starting in the spring of 1940, they provided no impact on the war due to limitations in communications, security, and expertise.[62] Bletchley was simply unprepared for what it did not understand in pushing intelligence to the right people at the right time to have a direct impact on the battlefield. It took them those eighteen months to develop an effective system of passing intelligence that gained the trust of the military's leadership. Bletchley first strengthened its reputation among field commanders in the spring of 1940 during the Battle of France. Bletchley's German air force decrypts were delayed due to a change in German encryption procedures, and the intelligence eventually passed to the British Expeditionary Force (BEF) in France convinced BEF commander, Field Marshall John Gort, to leave France as quickly as possible instead of launching a counterattack at the request of the French.[63]

It is believed that the first Ultra decrypt that had the potential to have a tangible impact on the war was collected in January 1941, confirming the scale and timing of the German build up for the attack on Greece though this decryption was never used by Allied commanders.[64] Therefore, the first decisive impact that Ultra had on the war was in February and March 1941, when Ultra played a part in the defeat of the Italian army in North Africa and the Italian navy in the Battle of Matapan.[65] Two significant decryptions pushed Rommel back to El Agheila by the end of 1941—the breaking of the Italian machine cipher that was used for Axis Mediterranean shipping, in combination with the breaking of the German Army Enigma keys in use within the Panzer Army between North Africa, Rome, and Berlin.[66]

British interest in North Africa stemmed back to 1935 when the Italians attacked and then subsequently conquered Abyssinia, Ethiopia in 1936. As a result, the English built up their forces in Egypt.[67] In June 1940, Italy declared war on Britain, and as a result, the British forces in Egypt prepared for the offensive. The following December, the British (7th Armored Division, 4th Indian Division, and Selby Force) went on the offensive annihilating two Italian corps.[68] The British delivered the final blow in January 1941, exploiting the twenty-mile wide gap that separated the northern and southern strong points of the Italian forces defeating them at Bardia, Tobruk, and Benghazi.[69] As a result of the deteriorating situation in North Africa, the Italians requested help from the Germans. In response, the Germans dispatched a German blocking force reinforced by a Panzer regiment, an artillery battalion, and a Corps Headquarters under Lieutenant General Erwin Rommel.[70]Rommel entered Tripoli in early 1941 as Hitler looked to prevent the defeat of the entire Italian presence in North Africa. The British had successfully stopped an Italian advance toward Cairo and then threw back a large Italian army into Libya. Within forty-eight hours of his arrival in Tripoli, Rommel was on the offensive, driving the

British forces back to Tobruk.[71] The Allied forces were relieved during Operation Crusader (relief by the British Eighth Army), who then pushed Rommel's forces back to Tripoli.[72]

Rommel "suffered crippling losses, and unlike the British they had virtually no reserves."[73] The British ability to secure Italian decrypts allowed Allied forces to sink Rommel's supply ships which, in turn, prevented him from having the necessary equipment to effectively advance. In a report published by Panzergruppe Afrika dated September 1 1941 they, "found it noteworthy that the British always executed the air attacks at the time of day for which the Italian signals announced the arrival of cargo-carrying submarines."[74] Though Rommel was seemingly aware of his communications vulnerability, he did nothing to diminish this vulnerability. When England launched Operation Crusader, one expert commented: "The British commanders had the complete order of battle of Rommel's forces and an estimate of his desperate situation with fuel and other supplies, virtually all based on Enigma (Ultra) intercepts," which allowed the Eighth Army to push Rommel back.[75]

The decisive impact of the Italian shipping decrypts forced the Germans to strengthen their air power in the Mediterranean and to dispatch U-boats in an effort to counter all of their shipping losses.[76] The German counteractions essentially mitigated any of the positive effects of the decryption of the Italian machine cipher. As Rommel moved closer to his supply bases in Tripoli, the Axis powers continued to struggle to protect their convoys to North Africa as a result of Ultra decryptions, though on January 5 1942, one of the convoys successfully arrived, encouraging Rommel to launch a second offensive.[77] Rommel pushed the British back to Tobruk, though once again failing to obtain a decisive victory.[78]

To complicate matters, the Army Enigma was lost in December, during which time Rommel's field intelligence broke the cipher used by the U.S. Military Attaché in Cairo.[79] The

Germans were able to read this cipher from January to June 1942, during which time Rommel won the Battle of Gazala in May 1942, even though the Army Enigma keys were recovered and the Air Force Ultra decrypts provided a month's notice of Rommel's attack.[80] Despite Rommel's victory at Gazala, continued Ultra decrypts ensured Rommel could not exploit his victory because intelligence left his supply routes vulnerable thereby, proving that the use of timely intelligence was the key to allowing the British to slow Rommel's resupply. Consecutively, the British built their defense in depth, forcing Rommel to quit and withdraw his forces due to lack of supplies.[81]

In June 1942, the tides were again about to change as Bletchley began to read both of the German Army's keys with only a twenty-four-hour delay.[82] Simultaneously to breaking both Army keys, Bletchley broke a new German Army-Air Force liaison key.[83] Then in July, Bletchley broke a key that was associated with German transport of army supplies and reinforcements to North Africa.[84] With these last keys, the British had access to every enemy cipher used on the African front.[85] As a result, Middle East commands received more timely intelligence regarding the enemy's activities than any other force in any campaign in the entire war, which helped to prevent Rommel from reaching Cairo.[86]

Ultra was never again as crucial to the North African campaign, but by 17 August 1942, Ultra uncovered the approximate date and operational plans for the next German offensive in North Africa. Though the British were armed with this specific knowledge, they did not defeat Rommel at Alam Halfa; rather, Rommel was forced to retreat after two days as his supply shipping was once again suffering significant casualties due to a renewed offensive on his shipping made possible by Ultra.[87] The anti-shipping offensive significantly reduced Rommel's freedom of movement by the time the British launched their offensive in October 1942

contributing to Rommel's defeat, though it failed to help the British cut off Rommel's retreat to Tunisia.[88] Ultra's influence in the British Tunisia campaign was not nearly as complete or decisive.[89]

As previously discussed, when Bletchley finally broke the naval Enigma the Allies were very successful in reducing Axis shipping in the Mediterranean, which forced the Germans to shift U-boats and one-third of their operational fleet from the Atlantic to the Mediterranean.[90] The German Navy did not make it easy for Bletchley to break the Navy's Enigma as they followed strict radio protocols including monitoring their own traffic, setting up an internal investigative process within the navy, and using water soluble ink.[91] They even went so far as not to carry an Enigma machine at all if they believed there was an increased chance that the Enigma machine could fall into the hands of the Allies.[92] Bletchley's successful decryption of the naval Enigma began in June 1941 when British intelligence captured the *München* and the U-110, a German U-boat, and continued until the end of January 1942 when the Germans released the new Enigma model, M4, a four-rotor Enigma.[93,94] The *München*, a weather ship armed with only one machine gun, was considered an auxiliary ship by the German navy, and therefore, it maintained its original civilian crew, which was augmented by German radio operators to transmit the results of the ship's surveys to Germany.[95] Harry Hinsley, who worked in Hut 4 reading non-tactical reporting looking for trends in information, thought that if the British Navy could capture a weather ship, it might recover the settings for the Enigma rotors.[96] After detailed analysis and discussions with the British Navy, the Navy carried out the attack successfully, providing the Enigma rotor settings to Bletchley. Another decryption blackout began in January 1942 and ended in October 1942 as a result of the sinking of another U-boat, U-559, by the *Petard* and the valiant efforts of her crew to recover the Enigma onboard.[97]

These decryptions were crucial because they allowed the British to route their convoys around the U-boats, diminishing their effectiveness especially as the British anti-submarine force was fragile.[98] Historians estimate that Ultra's decryption of the U-boats from July through November 1942 saved approximately 1.5 million tons of shipping, allowing the British increase their level of supplies, ship building, and the development of anti-submarine capabilities.[99] As a result, the U-boats withdrew from the North Atlantic and instead focused on the coast of the United States.[100]

When the U-boats returned to the North Atlantic in the autumn, they were using a new key, which resulted in huge increase in the loss of Allied shipping.[101] Bletchley once again broke the new key, which slowed down the U-boat attacks until the end of February 1943, but in March 1943 the absolute size of the U-boat fleet made maneuvering around it impossible, and Allied losses rose to an unsustainable level.[102] Throughout this time, the continued U-boat impact on Allied shipping put, "extreme pressure on system (logistics), the shortage of which, the Chief of Imperial General Staff said put, 'a stranglehold on all offensive operations.' "[103] Significant losses pushed the Allied forces to go on the offensive against the U-boats; the success of the offensive can be accredited to Ultra as it allowed the Allies to pinpoint the exact locations where they could have the best effects in such a large theater of operations.[104] The U-boats suffered such heavy losses that Germany withdrew them from the north Atlantic in May 1943.[105]

Beyond providing day-to-day intelligence in support of both the land campaign and the naval campaign, Ultra proved to be an invaluable planning tool specifically in the planning of Operation Overlord (Battle of Normandy). In preparation for the landing, Ultra confirmed the identification and location of the German divisions, revealing that the Germans were sending reinforcements to Normandy and the Cherbourg which in turn allowed the Allies to modify their

plans for the landings on Utah beach.[106] Additionally, the decrypts in conjunction with the elaborate deception plan (which was driven by Ultra decrypts) allowed the Allies to understand that the Germans were still uncertain about the place and timing of the landing.[107]

Considering all of the impacts that Ultra had on the land campaign, the naval campaign, and the Allies ability to plan, one could argue that the Allies would still have won World War II, but it would have taken much longer and cost much more in blood and treasure.[108] Ultra decrypts were a key source in ensuring that Allied logistics continued to be reliable while simultaneously stretching the logistics of the Axis powers. Historical accounts estimate that the war would have taken two additional years, although the only way to provide a quantitative number as to the length of the delay would require an analyst to recreate history as different decisions and plans were made as a result of Ultra decrypts throughout the war. Therefore, it is only safe to estimate that the war would have been longer. [109]

As one considers the impact of Bletchley Park on the outcome of World War II, it is by no means the only place where intelligence was being processed, produced, and disseminated within the Allied command. The history of Bletchley Park is, however, one of the best documented and most publicly available histories as to how the Allied command exploited the weaknesses of Nazi Germany. The United States was significantly involved in the operations at Bletchley Park to the extent that many of the personnel at Bletchley felt as though the superior manpower and resources of the United States would quickly dwarf British efforts.[110]

Current Challenges to Cyber Recruitment

USCYBERCOM is a sub-unified command of United States Strategic Command based in Fort Meade, Maryland. It includes key service components cyber components: Fleet Cyber Command/Tenth Fleet, Air Force Cyber/24th Air Force, Army Cyber Command/Second Army,

and Marine Forces Cyberspace Command. Per Admiral Michael Rogers, Commander USCYBERCOM, the collective mission of USCYBERCOM is to, "direct the operation and defense of the Department of Defense's information networks (DODIN) while denying adversaries (when authorized) the freedom to maneuver against the United States and its allies in and through cyberspace."[111] Under this mission, USCYBERCOM is responsible for roughly 7 million networked devices and 15,000 network enclaves.[112] Outside of protecting the DODIN, USCYBERCOM prepares to, and, when directed, conducts, full-spectrum military cyberspace operations or offensive electronic intervention throughout the range of the electromagnetic spectrum at each level of war.

The DoD Cyber Strategy published in April 2015 sets out five strategic goals, the first of which is to, "build and maintain ready forces and capabilities to conduct cyberspace operations."[113] With that goal in mind, the DoD began to invest heavily in its personnel through the creation of its Cyber Mission Force (CMF). The development of the CMF began in 2013 and was scheduled to be executed over the course of the subsequent five years. When the CMF meets final operational capacity, it will include approximately 6,200 personnel in 133 teams. According to Admiral Rogers' testimony in March 2016 to the House Armed Services Committee (HASC), twenty-seven teams are complete and sixty-eight have reached initial operating capability.[114] Of the 133 teams that will complete the CMF development, Admiral Rogers stated that 93% will be delivered on time in 2018. In his 2015 statement before the HASC Admiral Rogers stated:

> "I have been working with the Services to accelerate the work we are doing to keep on schedule, but I can promise you that will not be easy. We are hard pressed to find qualified personnel to man our CMF rosters, to get them cleared, and to get them trained and supported across all one hundred thirty-three teams. To address these gaps, I am working with our Service components, Chief, National Guard Bureau, and Reserve Chiefs to ensure we have considered a total force solution."

More recently in March 2016, Admiral Rogers once again alluded to the difficulties USCYBERCOM faces in finalizing the CMF, admitting that the solution needs more collective work proposing a, "DoD-generated capacity outside the government in the private sector."[115]

To achieve the strategic goal of building and maintaining ready forces, the DoD has developed specific objectives with which the office of primary responsibility is tasked, including developing a project plan that is tracked by the Principal Cyber Advisor to ensure the objective is achieved and ultimately the strategic goal is met.[116] The six specific objectives are as follows: "1) maintain a persistent training environment, 2) build viable career paths, 3) draw on national guard and reserve, 4) improve civilian recruitment and retention, 5) develop and implement exchange programs with the private sector, and 6) support the national initiative for cyberspace education."[117]

Objectives four and five tie directly to the case study of Bletchley: improve civilian recruitment and retention and develop and implement exchange programs with the private sector. While it recruited heavily from academic institutions, Bletchley did also recruit from within the services if a person showed an aptitude for the technical work necessary to solve the Enigma. As prospective candidates, military personnel were given specific exams and interviewed to ensure they could meet the necessary requirements, but still civilians conducted the majority of cryptanalysis. Military members recruited to Bletchley received the rudimentary training necessary for the task they would complete (i.e., the Wrens who operated the Bombes or the intelligence officers that ran the huts). Any new skill the service members learned was as a result of on-the-job training working alongside other military members or civilians. Cryptography was not seen as a purely military skill (nor is cyber today); rather, it was understood to be an academic endeavor long before World War II, which is perhaps why Bletchley recruited from

academia almost immediately as opposed to exhausting all of its options within the military services.[118] Of course, one cannot ignore the immediacy Bletchley felt in needing to form the cadre inside of Bletchley quickly, pushing recruitment to the civilian sector where there was a proven record of academic success in various disciplines. One could make a similar argument in the cyber arena as previously quoted, Admiral Rogers, stated that USCYBERCOM is still challenged to build out the CMF with qualified military personnel. With the deadline for reaching initial operating capability by the end of FY16 looming, USCYBERCOM should consider looking beyond military personnel to the civilian sector for their full integration within CYBERCOM in conjunction with developing part-time civilian tech partnerships. To do so would mean that CYBERCOM recognizes that the success of their organization will come at the hands of civilians led by military leaders, solidifying that the success of military operations far exceeds the capacity of the standing military.

Similar to the situation within the military at Bletchley, today's military is not an exhaustive pool of tech-minded people, which is why the recruitment of civilians is of the utmost importance. The leaders of Bletchley developed habitual relationships with institutes of higher education, specifically focusing on mathematicians and language experts. These relationships forged significant growth in the civilian expertise at Bletchley. In his March 2016 testimony before the HASC, Admiral Rogers did state that CYBERCOM needs to continue to broaden its relationship with academia, pointing out the relationships that USCYBERCOM has begun to develop with Carnegie Mellon, Harvard, Stanford, and Berkley.[119] What is the focus of these relationships and have they, in fact, leveraged them in the form of recruitment?

At Bletchley, civilians with specific expertise were used in a very specific technical capacity within each of the huts; likewise, the civilians that the DoD recruits to work within

USCYBERCOM should be utilized in the very technical jobs that require education and experience beyond what the military typically can recruit within its ranks. Within the tech sector, there is significant competition for graduates with "STEM" degrees (science, technology, engineering, and mathematics) with a specific focus on computer science, information security, information technology, computer engineering, and electrical engineering.[120] In comparison to the military, where enlisted members are not required to have advanced degrees, it may be necessary to use those civilians with very specific technical degrees in jobs that require advanced skills that few possess such as software reverse engineering, advanced malware analysis, and identifying advanced stealthy attacks.[121] Additionally, specialization within the use of both civilian and military personnel will ensure that each person is required to maintain expertise in a limited number of technology trends, facilitating greater depth of knowledge.[122] The military services can only make so much by headway by using civilians inside tech companies as part-time help; a healthy balance must exist between a full-time civilian cadre that supports the military from within the services and part-time expertise that is available in today's tech industry.

Based on Admiral Rogers March 2016 testimony to the HASC, USCYBERCOM appears to recognize that it needs to forge the relationships with academia and the tech sector in order to ensure the success of the organization. Admiral Rogers referenced on numerous occasions that the next big areas of development for USCYBERCOM is its relationship with both the private sector and academia as he discussed what he called the "USCYBERCOM Point of Partnership" or "Point of Presence" (an identified team of prior military individuals currently working in Silicon Valley in conjunction with one active duty member permanently stationed in California).[123] USCYBERCOM intends to look to the "Point of Presence" as an incubator for a

model they can apply elsewhere. Arguably, this model falls short when one cannot directly task or control the actions of the personnel within the “Point of Presence”. This solution may serve in the short term, but in the long term, USCYBERCOM should consider greater civilian recruitment within its ranks. Similar to the codebreaking efforts at Bletchley, cyber warfare is an intellectual battle, one that will be driven by a cadre of primarily civilian expertise complemented with military leadership.

If the military services choose not to heavily integrate civilians into the cyber workforce, significant changes to the military (specifically the Marine Corps’) manpower structure are needed to ensure the services are recruiting and placing their members in the most optimal career fields. Unlike in today’s recruitment of cyber personnel, British military services during World War II did not require prospective military candidates to take a standard exam to identify the strengths and weaknesses of each recruit thus allowing the services to quickly identify the potential aptitude of all new accessions. Today, prospective candidates from the military take the Armed Services Vocational Aptitude Battery, which helps each of the services identify the strengths and weaknesses of the prospective candidates. Aside from the minimum scores needed to enlist in any of the Armed Services, the specific scores in each of the categories within the exam help the services identify which military occupational specialty (MOS) may best suit a candidate. Unlike the Army, Navy, and Air Force, within the Marine Corps, the cyber expertise is built from the intelligence and communications MOSs and is therefore not its own specialty. It begs the question, why is the Marine Corps not interested in making a cyber MOS? The personnel structure exists, but the Marine Corps is not interested in making it a separate specialty. Rather, does the Marine Corps see the evolution of cyber like the leaders of Bletchley

Park in that the evolution and development of cyber capabilities will come at the hands of a largely civilian workforce and they are instead focused on civilian integration?

If the Marine Corps did choose to make cyber expertise a separate MOS, it would be able to recruit from within the service and with new accessions to the service. As a separate MOS, the Marine Corps would not only be able to incentivize cyber billets with pay and additional opportunities for higher education (beyond what is offered to a typical new accession), but it would also be able to recruit against specific prerequisites instead of mixing and matching those individuals who meet undefined requirements from within the current populations. Having a separate cyber MOS would also help recruit new accessions; a perspective candidate knows the "cyber" MOS exists and that he/she can specifically request a cyber billet similar to how new accessions can specifically request special operations billets as opposed to rolling the dice with the typical assignment process. Additionally, making cyber a separate MOS would allow the Marine Corps to treat the MOS differently (similar to the President's Own, the United States Marine Band) than other MOSs in ways such as length of tour, incentive pay, prerequisites, etc. Aside from integrating civilians in cyber, a new MOS will allow the Marine Corps to make better use of the talent that already exists within the Marine Corps and to attract new cyber talent from among new accessions. A new MOS, however, does not completely negate the Marine Corps need for an expert civilian cadre upon which to build the military cyber workforce. In addition to the integration of civilians, the creation of a new MOS will help ensure that those military members who will work alongside the civilian cadre are appropriately identified upon accession to the Marine Corps and then subsequently tracked and given the opportunity for promotion.

While the integration of civilians at Bletchley Park is a parallel to the efforts of the DoD today to integrate civilians within military cyber operations, the similarities are not absolute. Today, the DoD faces more competition than in the past from the private sector for the recruitment of qualified civilians. World War II was an existential threat to the people. Private industry shifted to support the war effort, so there was limited to no competition for talent; British citizens felt it was their duty to support the war effort. In stark contrast, the "War on Terror" has not assumed control over the daily life of the average citizen, so those individuals with the technical acumen are going to work for tech companies where they can receive high pay and great benefits without the risks of military service or being forced to assimilate into a demanding culture. This risk and concern of rigorous standards would be circumvented with the integration of civilians within USCYBERCOM.

However, even considering that the societal circumstances surrounding today's War on Terror are fundamentally different than those that existed in World War II, the case study of Bletchley Park is useful because it demonstrates that civilians and both the private sector are a resource of specific talent that can be tapped to fill in the knowledge gaps that exist in a standing military force. As it becomes more and more difficult for the military to recruit the same level of expertise that private industry is capable of recruiting and retaining, it makes sense to share information and specific technical expertise instead of the military trying to own it all. Indeed, the DoD has already identified in its fifth objective to its strategic goal to "develop and implement exchange programs with the private sector." Sharing relationships will benefit from the exchange programs for both officers and enlisted. The one challenge to developing these exchange programs and sharing relationships is the perceived control that any sharing/exchange

relationship with the government may allude to (such as the fallout from the Edward Snowden leaks).

Endnotes

[1] F.H. Hinsley, ed. and Alan Stripp, ed., *Codebreakers: The Inside Story of Bletchley Park (*New York: Oxford University Press, 1993), v.
[2] Hervie Haufler, *Codebreakers' Victory How the Allied Cryptographers Won World War II* (New York: New American Library, 2003), 35.
[3] "Bletchley Park: Home of the Codebreakers," Bletchley Park Trust, accessed December 28, 2015, https://www.google.com/culturalinstitute/u/0/exhibit/bletchley-park-home-of-the-codebreakers/wRANFg9s?position=4%2C0.
[4] "Bletchley Park: Home of the Codebreakers," Bletchley Park Trust, accessed December 28, 2015, https://www.bletchleypark.org.uk/content/hist/worldwartwo/captridley.rhtm.
[5] "Bletchley Park: Home of the Codebreakers," Bletchley Park Trust, accessed December 28, 2015, https://www.google.com/culturalinstitute/u/0/exhibit/bletchley-park-home-of-the-codebreakers/wRANFg9s?position=2%2C0.
[6] "Bletchley Park: Home of the Codebreakers," Bletchley Park Trust, accessed December 28, 2015, https://www.google.com/culturalinstitute/u/0/exhibit/bletchley-park-home-of-the-codebreakers/wRANFg9s?position=4%2C0.
[7] Peter Matthews, *SIGINT The Secret History of Signals Intelligence 1914-45* (Stroud, Gloucestershire: The History Press, 2013), 88.
[8] Ibid, 88.
[9] Ibid, 89.
[10] Ibid, 91.
[11] Ibid, 91.
[12] Hinsley and Stripp, *Codebreakers*, 90.
[13] Ibid.
[14] Ibid, 77.
[15] Ibid, 77.
[16] Haufler, *Codebreakers' Victory*, 35.
[17] Hinsley and Stripp, *Codebreakers*, 96.
[18] Ibid, 100.
[19] Haufler, *Codebreakers' Victory*, 36.
[20] "Bletchley Park: Home of the Codebreakers," Bletchley Park Trust, accessed December 28, 2015, https://www.google.com/culturalinstitute/u/0/exhibit/bletchley-park-home-of-the-codebreakers/wRANFg9s?position=4%2C0.
[21] "Bletchley Park: Home of the Codebreakers," Bletchley Park Trust, accessed December 28, 2015, https://www.google.com/culturalinstitute/u/0/exhibit/bletchley-park-home-of-the-codebreakers/wRANFg9s?position=7%2C36.
[22] Haufler, *Codebreakers' Victory*, 28.
[23] Ibid, 23.
[24] Ibid, 28.
[25] Haufler, *Codebreakers' Victory*, 30.
[26] Ibid.
[27] Ibid, 31.
[28] Ibid, 32.
[29] Ibid.
[30] Haufler, *Codebreakers' Victory*, 33.
[31] Ibid, 34.
[32] "Bletchley Park: Home of the Codebreakers," Bletchley Park Trust, accessed December 28, 2015, http://www.bletchleypark.org.uk/content/hist/worldwartwo/enigma.rhtm.
[33] Hinsley and Stripp, *Codebreakers*, 19.
[34] "Bletchley Park: Home of the Codebreakers," Bletchley Park Trust, accessed December 28, 2015, https://www.google.com/culturalinstitute/u/0/exhibit/bletchley-park-home-of-the-codebreakers/wRANFg9s?position=24%2C0.
[35] Hinsley and Stripp, *Codebreakers*, 132.

[36] Ibid, 133.
[37] Hinsley and Stripp, *Codebreakers*, 134.
[38] Ibid, 137.
[39] Andrew Hodges, *Alan Turing: The Enigma* (New Jersey: Princeton University Press, 2014), xvi.
[40] Haufler, *Codebreakers' Victory*, 38.
[41] Ibid, 39.
[42] Welchman, Gordon, *The Hut 6 Story* (New York: McGraw-Hill, 1982), 81.
[43] Haufler, *Codebreakers' Victory*, 39.
[44] Ibid, 40.
[45] Haufler, *Codebreakers' Victory*, 43.
[46] Ibid.
[47] Ibid, 44.
[48] "Bletchley Park: Home of the Codebreakers," Bletchley Park Trust, accessed December 28, 2015, https://www.google.com/culturalinstitute/u/0/exhibit/bletchley-park-home-of-the-codebreakers/wRANFg9s?position=28%2C14.
[49] Hinsley and Alan Stripp, *Codebreakers*, 167.
[50] Hodges, *Alan Turing*, 336.
[51] "Bletchley Park: Home of the Codebreakers," Bletchley Park Trust, accessed December 28, 2015, https://www.google.com/culturalinstitute/u/0/exhibit/bletchley-park-home-of-the-codebreakers/wRANFg9s?position=40%2C0.
[52] "Bletchley Park: Home of the Codebreakers," Bletchley Park Trust, accessed December 28, 2015, https://www.google.com/culturalinstitute/u/0/exhibit/bletchley-park-home-of-the-codebreakers/wRANFg9s?position=40%2C0.
[53] Haufler, *Codebreakers' Victory*, 44.
[54]Ibid, 45.
[55] Ibid, 46.
[56] Ibid, 45.
[57] Ibid, 46.
[58] Hodges, *Alan Turing*, 348.
[59] Ibid.
[60] Hinsley and Stripp, *Codebreakers*, 1.
[61] Ibid, 2.
[62] Ibid.
[63] Haufler, *Codebreakers' Victory*, 52.
[64] Hinsley and Stripp, *Codebreakers*, 3.
[65] Ibid.
[66] Ibid.
[67] Hans Otto Behrendt, *Rommel's Intelligence in the Desert Campaign 1941-1943* (London: William Kimber and Company Limited, 1985), 21.
[68] Ibid, 27.
[69] Ibid.
[70] Ibid, 33.
[71] Ibid, 34.
[72] Martin Kitchen, Rommel's Desert War Waging World War II in North Africa, 1941-1943 (New York: Cambridge University Press, 2009), 157.
[73] Ibid, 161.
[74] Ibid, 21.
[75] Wladyslaw Kozaczuk, *Enigma: How the German Machine Cipher was Broken, and How it was read by the Allies in World War Two*, ed. Christopher Kasparek and Christopher Kasparek, trans. (Frederick: University Publications of America, 1984), 169.
[76] Ibid, 4.
[77] Ibid, 180.
[78] Ibid, 191.
[79] Ibid.
[80] Ibid.

[81] Kozaczuk, *Enigma*, 169.
[82] Hinsley and Stripp, *Codebreakers*, 4.
[83] Ibid.
[84] Ibid.
[85] Ibid.
[86] Ibid.
[87] Ibid, 5.
[88] Ibid.
[89] Ibid.
[90] Ibid, 6.
[91] David Kahn, *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943* (London: Frontline Books, 2012), 230-231.
[92] Ibid, 232.
[93] Hinsley and Stripp, *Codebreakers*, 6.
[94] Kahn, *Seizing the Enigma*, 245.
[95] Ibid, 177.
[96] Ibid, 181.
[97] Ibid, 265.
[98] Hinsley and Stripp, *Codebreakers*, 6.
[99] Hinsley and Stripp, *Codebreakers*, 6.
[100] Ibid.
[101] Ibid, 7.
[102] Ibid, 7.
[103] Kahn, *Seizing the Enigma*, 289.
[104] Hinsley and Stripp, *Codebreakers*, 7.
[105] Ibid.
[106] Ibid, 9.
[107] Ibid, 10.
[108] Ibid, 11.
[109] "Bletchley Park: Home of the Codebreakers," Bletchley Park Trust, accessed December 28, 2015, https://www.google.com/culturalinstitute/u/0/exhibit/bletchley-park-home-of-the-codebreakers/wRANFg9s?position=2%2C0.
[110] Hinsley and Stripp, *Codebreakers*, 98.
[111] *Statement of Admiral Michael S. Rogers Commander U.S. Cyber Command: Hearing Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities.* 114th Cong., 1 (2015) (Admiral Michael S. Rogers, Commander U.S. Cyber Command).
[112] Ibid.
[113] U.S. Department of Defense, *The DoD Cyber Strategy (*Washington, D.C., April 2015), 13.
[114] *Statement of Admiral Michael S. Rogers Commander U.S. Cyber Command: Hearing Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities.* 114th Cong., (2016) (Admiral S. Rogers, Commander U.S. Cyber Command).
[115] *Statement of Admiral Michael S. Rogers Commander U.S. Cyber Command: Hearing Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities.* 114th Cong., (2016) (Admiral S. Rogers, Commander U.S. Cyber Command).
[116] U.S. Department of Defense, *The DoD Cyber Strategy*, 17.
[117] Ibid, 17-18.
[118] Christopher M. Andew, *Her Majesty's Secret Service: The Making of the British Intelligence Community* (New York, Viking Penguin Inc., 1986), 87.
[119] *Statement of Admiral Michael S. Rogers Commander U.S. Cyber Command: Hearing Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities.* 114th Cong., (2016) (Admiral S. Rogers, Commander U.S. Cyber Command).
[120] *Perspective on 2015 DoD Cyber Strategy: Hearing Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities*, 114th Cong., 2 (2015) (Dr. Lara Schmidt Associate Director, RAND Project AIR FORCE; Senior Statistician, RAND Corporation).
[121] Ibid, 3.

[122] Ibid, 4.
[123] *Statement of Admiral Michael S. Rogers Commander U.S. Cyber Command: Hearing Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities.* 114th Cong., (2016) (Admiral S. Rogers, Commander U.S. Cyber Command).

Bibliography

Andrew, Christopher M. *Her Majesty's Secret Service: The Making of the British Intelligence Community*. New York, Viking Penguin Inc., 1986.

Behrendt, Hans Otto. *Rommel's Intelligence in the Desert Campaign 1941-1943*. London, William Kimber and Company Limited, 1985.

"Bletchley Park: Home of the Codebreakers," Bletchley Park Trust, https://www.google.com/culturalinstitute/u/0/exhibit/bletchley-park-home-of-the-codebreakers/wRANFg9s?position=4%2C0.

Gordon, John W. *The Other Desert War: British Special Forces in North Africa, 1940-1943.* Westport: Greenwood Press, 1987.

Haufler, Hervie. *Codebreakers' Victory How the Allied Cryptographers Won World War II.* New York: New American Library, 2003.

Hinsley, F.H., ed. and Alan Stripp, ed. *Codebreakers: The Inside Story of Bletchley Park.* New York: Oxford University Press, 1993.

Hodges, Andrew. *Alan Turing: The Enigma*. New Jersey: Princeton University Press, 2014.

Kahn, David. *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943*. London: Frontline Books, 2012.

Kitchen, Martin. *Rommel's Desert War Waging World War II in North Africa, 1941-1943.* New York: Cambridge University Press, 2009.

Kozaczuk, Wladyslaw. *Enigma: How the German Machine Cipher was Broken, and How it was read by the Allies in World War Two*. Edited by Christopher Kasparek. Translated by Christopher Kasparek. Frederick: University Publications of America, 1984.

Matthews, Peter. *SIGINT: The Secret History of Signals Intelligence 1914-45*. Stroud, Gloucestershire: The History Press, 2013.

U.S. Congress. House. *Statement of Admiral Michael S. Rogers Commander U.S. Cyber Command: Hearing Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities.* 114th Cong., 2015.

U.S. Congress. House. *Perspective on 2015 DoD Cyber Strategy: Hearing Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities,* 114th Cong., 2015.

U.S. Congress. House. *Statement of Admiral Michael S. Rogers Commander U.S. Cyber Command: Hearing Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities.* 114th Cong., 2016.

U.S. Department of Defense. *The DoD Cyber Strategy*. Washington, D.C., April 2015.

Warner, Michael. *The Rise and Fall of Intelligence an International Security History.* Washington D.C.: Georgetown University Press, 2014.

Welchman, Gordon. *The Hut 6 Story*. New York: McGraw-Hill, 1982.

Winterbotham, Fredrick William. *The Ultra Secret.* London: George Weindenfeld and Nicholson, 1974.