Secret War, Secret Science

Brad Osgood
Stanford University
"In war-time, truth is so precious that she should always be attended by a bodyguard of lies".

Churchill to Stalin
Keeping secrets
A secret message…

No other single cryptanalysis has had such enormous consequences. Never before or since has so much turned upon the solution of a secret message. For those few moments in time, the codebreakers held history in the palm of their hand.

David Kahn, *The Codebreakers*
The early events

- Britain’s first offensive action of the war is to dredge up and cut a vital undersea German communication cable.
- This forces Germany to send (coded) messages via radio, or via cables through neutral countries.
- Britain can intercept radio communications and has already set up a codebreaking unit.
• The German ship *Magdeburg* runs aground on the island of Odensholm in the bay of Bothnia.

• The instructions on the German codebook read "If there is a chance of the signal book falling into enemy hands it is to be thrown overboard or destroyed by fire."

• Before all the codebooks can be destroyed the ship is seized by Russian troops.

• The Russians begin to break the German naval codes. They inform the British who immediately recognize their importance.
....The body of a drowned German under-officer was picked up by the Russians a few hours later, and clasped in his bosom by arms rigid in death, were the cypher books of the German Navy and the minutely squared maps of the North Sea and the Heligoland Bight ... We lost no time in sending a ship, and late on an October afternoon Prince Louis and I received from the hands of our loyal allies these sea stained priceless documents.

Winston Churchill
As the war dragged on…

• Germany’s early and rapid successes stall.

• They see only one way to win the war - starve Britain into submission by unrestricted submarine warfare.

• “Unrestricted” means sinking ships of neutral countries that are carrying supplies to Britain.
• Germany decides on unrestricted submarine attacks, including attacks on U.S. ships.
  – “Now Germany is lost for centuries” said the Vice Chancellor

• The U.S. is still neutral – could this tip the balance?
  – The U.S. President was recently reelected on the slogan “He kept us out of the war.”
  – The U.S. has a large and diverse population with ethnic and cultural ties to all of the warring nations.
  – The President had pressed a policy of “peace without victory” with no success.
• Germany sends a secret message to a third country suggesting that country attack the U.S.

• Germany promises support in the new war against the U.S. and in the subsequent peace.

• If the U.S does join the allies in the war against Germany they will be forced into fighting on two fronts.

• With the U.S. stretched thin Germany will win the war in Europe.
• Britain intercepts the secret message and decodes it.

• Britain passes the message on to the U.S. President, but they take extraordinary measures to conceal how they received the message.
  – Britain cannot raise Germany’s suspicions that their codes have been broken.

• The U.S., outraged, enters the war on the side of the allies. The war is over in 16 months. Germany is defeated.
• The year: 1917
• The U.S. president: Woodrow Wilson
• The British First Lord of the Admiralty: Winston Churchill
• The country Germany pushed to go to war with the U.S
Mexico

• With the suggestion that Japan also get into the act.
The Zimmerman telegram

• Zimmermann was the German Foreign Secretary.
• Telegram was sent to Count von Bernstorff, the German Ambassador in Washington.
<table>
<thead>
<tr>
<th>GERMAN LEGATION</th>
<th>MEXICO CITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>130 13042 13401 8501 115 3528 416 17214 6491 11310</td>
<td></td>
</tr>
<tr>
<td>118167 18222 21560 10247 11518 23677 13605 3494 14936</td>
<td></td>
</tr>
<tr>
<td>98056 5905 11311 12362 10587 10500 3058 21290 5161 59695</td>
<td></td>
</tr>
<tr>
<td>23571 17504 11269 18276 18101 0317 0028 17894 4473</td>
<td></td>
</tr>
<tr>
<td>22284 22200 19452 21589 07893 5509 13918 8958 12137</td>
<td></td>
</tr>
<tr>
<td>1333 4725 4456 5605 17166 13851 4458 17149 14471 6705</td>
<td></td>
</tr>
<tr>
<td>13850 12224 6929 14991 7382 15857 47893 14218 56477</td>
<td></td>
</tr>
<tr>
<td>5890 17553 6703 5870 1454 16102 15217 22851 17138</td>
<td></td>
</tr>
<tr>
<td>21601 17398 7446 23538 18222 0719 14331 15621 23845</td>
<td></td>
</tr>
<tr>
<td>3166 23552 22096 21804 4797 9497 22462 20855 4377</td>
<td></td>
</tr>
<tr>
<td>23410 13140 22266 5905 13547 20420 39689 13732 20667</td>
<td></td>
</tr>
<tr>
<td>6926 5275 18507 52926 1340 22043 13339 11265 22295</td>
<td></td>
</tr>
<tr>
<td>10439 14814 4178 6992 8784 7632 7357 6926 52265 11287</td>
<td></td>
</tr>
<tr>
<td>21100 21272 9346 9559 22644 15874 18502 18502 15857</td>
<td></td>
</tr>
<tr>
<td>2188 5376 7381 9802 11127 13484 9350 9220 76036 14219</td>
<td></td>
</tr>
<tr>
<td>5144 2831 17920 11477 17142 11284 7687 7782 15099 9110</td>
<td></td>
</tr>
<tr>
<td>10482 97556 3505 3670</td>
<td></td>
</tr>
</tbody>
</table>

BEHNSTOFFF.

Charge German Embassy.
"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President’s attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIEGELBAUM.
GERMANY SEeks an alliance against us; ASKS JAPAN AND MEXICO TO JOIN HER; FULL TEXT OF HER PROPOSAL MADE PUBLIC

CONGRESS TO BACK WILSON
Laconia Tragedy Adds Strength to President's Support

MODIFIED BILL IN HOUSE
But Leaders Predict That Senate's Armed Neutrality Measure Will Prevail

THINK PUBLIC IS AROUSED
Deployment of Five Consuls in Germany Increases Crises: New Demand on Turkey

President insists on Passage of Senate Armistice Bill

WASHINGTON, Dec. 26-Preceding articles have given for consideration the following resolutions which have been passed by the Senate and House of Representatives, and which have been referred to the Committee on Foreign Relations:

No ships sunk yesterday; 460,707 tons lost in February

WASHINGTON, Dec. 25-There were no ships sunk yesterday, according to the latest reports. The total tonnage lost in February was 460,707 tons. The latest reports indicate that the total tonnage lost in February was 460,707 tons. The total tonnage lost in February was 460,707 tons.

Zimmerman's statement on neutral ships will be sunk; escape of the Orleans only on instance of luck

BERLIN, Jan. 5-Dr. Zimmermann, German Foreign Minister, has issued a statement in which he states that Germany does not intend to sink neutral ships, except in the case of the Orleans, which was sunk on the instance of the British government.

Wilson gives out appeal from hoy

American, White Mother and Sister Die in the Lusitania: Ask They Be Averted

OFFERS SERVICES TO NATION
Young, nephew of Mrs. Hoy, Apposes Wilson, Lansing, Wadsworth, and Chandler.

WASHINGTON, Dec. 25-Young Hoy, nephew of Mrs. Hoy, takes a stand against Wilson, Lansing, Wadsworth, and Chandler, who have offered to avert the Lusitania disaster.

Germany's Proposal to Form an Alliance

Text of Germany's Proposal to Form an Alliance With Mexico and Japan Against the United States

Submitted by the Associated Press as an authentic copy of the German Foreign Minister's note to the German Minister in Mexico.

BERLIN, Jan. 5-Dr. Zimmermann, Foreign Minister of Germany, has issued a statement in which he states that Germany does not intend to sink neutral ships, except in the case of the Orleans, which was sunk on the instance of the British government.

Tokyo gratified by abandonment of exclusion bills in Oregon and Idaho

FLOOD SURE OF COUNCIL
Representative Says Revolution Will Insure Backing of President for Defense Preparations

WASHINGTON, Dec. 25-Representative Hoy, who has taken a stand against Wilson, Lansing, Wadsworth, and Chandler, has offered to avert the Lusitania disaster.

Washington, Dec. 26-Preceding articles have given for consideration the following resolutions which have been passed by the Senate and House of Representatives, and which have been referred to the Committee on Foreign Relations:

WASHINGTON, Dec. 25-There were no ships sunk yesterday, according to the latest reports. The total tonnage lost in February was 460,707 tons. The latest reports indicate that the total tonnage lost in February was 460,707 tons. The total tonnage lost in February was 460,707 tons.
The first modern war
The first mechanized war

Drawing by Leonardo da Vinci of lancers charging a metal machine
The basis of modern war is technology, disseminating itself through industry. Without technological advances, without industrial expansion, neither German diplomacy nor German war preparation could have carried the weight they did. In the period between 1871 and 1914 both made huge progress... In the decade of the 1880s, the German Empire doubled its output of steel and almost doubled its output of iron. Sweeping educational reforms, with particular stress upon higher and technical education bore swift fruit in Germany’s quickly won leadership in the new chemical and electrical industries.

John Terraine, *The Great War*
Airpower

“But one novelty above all stamped this war as part of the twentieth century: for the first time men would be fighting in a third dimension, the air.”
Verdun

Before
Verdun

After
The tank

“…the long overdue technical solution to the joint problem of barbed wire and machine guns…”

• First major use in the Battle of the Somme, August 1916
The mystery weapon
“...ugly but remorseless progress.”
Poison gas
• The machine gun
• Submarine combat
• Artillery and explosives
The assessment after the war

I think it is well for the man in the street to realize that there is no power on earth that can protect him from being bombed. Whatever people may tell him, the bomber will always get through. The only defence is offence, which means that you have to kill more women and children more quickly than the enemy if you want to save yourselves. I just mention that ... so people may realize what is waiting for them when the next war comes.

Stanley Baldwin, former and future Prime Minister, speaking to the House of Commons, 1932
World War II

The first scientific war
This war is only a continuation of the last, but very great differences in its character are apparent. In the last war millions of men fought by hurling masses of steel at one another. Prodigious slaughter was the consequence. In this war nothing of this kind has yet appeared. It is a conflict of strategy, organisation, technical apparatus, science, mechanics, and morale.

Winston Churchill, August 21, 1940
Germany’s plan for war:

The Blitzkrieg
“The dive bombers will form a flying artillery, directed to work in harmony with ground forces through good radio communication. You, a radio expert, must appreciate that for the first time in history, this coordination of forces is possible. The Air Force will not require ground support, any more than the armored divisions will need repair units. Tanks and planes will be disposable. The real secret is speed – speed of attack through speed of communications.”

General Erhard Milch, German Secretary for Air Power
"Communications had a greater impact on the course of World War II than on any other previous event in history. The very nature of the war – massive and motorized – demanded continuous, instant, and secure communication."

D. Headrick, *The Invisible Weapon: Telecommunications and International Politics 1851 - 1945*
Counterweapons to Blitzkreig?

• Strategic
  – Intelligence

• Tactical
  – Radar
Keeping secrets, again

“Gentlemen do not read each other’s mail.”

Henry L. Stimson, Secretary of State in the Hoover administration, commenting in 1929 on his decision to close down the State Department’s code breaking unit.

“Let us face facts: cryptosystems are not only considered weapons by the U.S. Government – and not only by the U.S. Government – they are weapons, weapons for defense and weapons for attack. The Second World War has taught us this lesson.”

F. L. Bauer, Decrypted Secrets, 1997
General Guderian’s command vehicle with “signal staff”
The “Enigma” coding machine
Original version of Enigma was a commercial product

(From the original sales brochure)

– The basic machine was invented in 1918 by Arthur Scherbius in Berlin. He received a patent and tried to market it, largely unsuccessfully, throughout the 20’s
Germany military was the first to use cipher machines

- German navy acquired Enigma in 1926
- Wermacht (army) in 1928
- Luftwaffe (air force) in 1935
  (Hitler came to power in 1933)

By the end of 1935 Germany had 20,000 Enigma machines for military use, modified from the original design

Over the course of the war Germany bought over 100,000 Enigmas
Other nations...

- The US Signal Corps bought an Enigma in 1927 but wound up building their own cipher machine based on a Swedish design.
- This became the M-209
- Japanese bought an Enigma and modified it for their navy
The complete key

1. A choice of rotors and the order they were to be placed in the machine.
2. Ring settings of the rotors.
3. Cross pluggings.
How many keys are possible?

• About 200 million million million
The business of Bletchley Park

47 miles from London. A “large Victorian Tudor-Gothic mansion with ample grounds”. The wartime home of the Government Code and Cipher School
Kept secret till the mid ’70’s

“The geese that lay the golden eggs and never cackle.”

Winston Churchill on his visit to Bletchley Park September 6, 1941
“Had it not been for human error, compounded by a single design quirk, the Enigma was intrinsically a perfectly secure machine.”

Stuart Milner-Barry, Bletchley Park Codebreaker (and former Classics major)
How was it broken?

- Luck
- Math
- Computers

“Colossus”

The first electronic programmable computer.

Designed by Tommy Flowers of the Post Office Research Office
“For the first time one felt that one could defeat one’s enemy intellectually”
Tony Sales, Bletchley Park

“Victory did not smile upon the boldest nations, as the Axis leaders believed, but upon the best informed.”
D. Headrick, *The Invisible Weapon*
Here is something that will sound very extreme but is at most, I think, a slight exaggeration: encryption technologies are the most important breakthrough in the last thousand years. No other technological discovery – from nuclear weapons (I hope) to the Internet – will have a more significant impact on our social and political life. Cryptography will change everything.

Lawrence Lessig, *Code and other laws of cyberspace*
Radar

The creation of radar totally transformed the ability of the defence to anticipate and thus defeat a bomber attack. The days of ‘the bomber will always get through’ had ended. It is difficult to exaggerate the dominance that radar would achieve over war in the air (and at sea) by 1945.

L. Deighton & M. Hastings, *Battle of Britain*
The Battle of Britain
July – October 1940

You knew the fate of civilization was being decided fifteen thousand feet above your head in a world of sun, wind, and sky

Virginia Cowles, War correspondent
From 1937 – 1939 Britain constructed a radar air defense – the “Chain Home” system

All done in the strictest secrecy
Map showing locations of CH and CHL Radar Stations and the area covered.
Milch to a group of officers in Britain’s Fighter Command in 1937: “Now, gentlemen, let us all be frank. How are you getting along with your experiments on the detection by radio of aircraft approaching your shores… Come, gentlemen, there is not need to be cagey. We’ve known for sometime that you are developing a system of radio location. So are we, and we think we are a jump ahead of you.”

Erhard Milch, Founder, with Goering, of the Luftwaffe
• Robert Watson Watt demonstrates a system that will detect and locate an object – the basis of Chain Home

• The head of Fighter Command, Hugh (“Stuffy”) Dowding realizes that detecting and locating enemy aircraft 75 – 100 km off the coast would give adequate time for a response.
  – Through training exercises they knew it took about 20 minutes after an alarm to get a squadron into the air to where the enemy was (supposed) to be.

• They also realized they needed a system of command to coordinate and communicate all the information they would be getting.
  – This was the beginning of “command and control”
The Battle in August

• At a meeting on August 15, Goering decides:
  – “It is doubtful whether there is any point in continuing the attacks on radar sites, in view of the fact that not one of those attacked has so far been put out of action.”

Big mistake
“The odds were great; our margin small; the stakes infinite.”

• September 15: Considered the climax of the Battle
  – Churchill observed the conduct of the battle from a command bunker in Uxbridge west of London. As the battle intensified and more RAF squadrons were engaged, Churchill asked: “What other reserves have we?” “There are none” was the reply.
Victory by continuing to exist

“… Dowding and Park had to resist fierce pressure to throw everything they had into the sky against the big attacks. But the essence of their brilliant handling of the struggle was that they saw so clearly that in a battle of attrition, they must be defeated. Fighter Command must achieve its victory simply by continuing to exist.”

L. Deighton & M. Hastings, *Battle of Britain*
The push for higher frequencies

• British radar experts realized that the future uses of radar depended on higher frequencies.
• Needed to track smaller objects and sweep the sky with a more focused beam.
• Needed radar to be carried by airplanes for navigation, bombing, and air to surface tracking, and by ships for navigation and submarine detection.
• They also realized they could not carry this out alone. They needed the resources of the US to make things happen fast enough and on a scale large enough to make a difference.
The Tizard Mission
August, September 1940

“He (Tizard) therefore made the bold suggestion that Britain should hand over her war-time secrets to the USA in exchange for research and productive capacity. Winston Churchill became personally involved and talked directly to Roosevelt about the possibility of a Mission being sent to the USA for this purpose…. The purpose of the Mission, subject to carefully vetted security procedures, was to hand over to the US Services, all the recent British technical advances. These included virtually every British secret - jet engines, rockets, predictors, radar, etc Nothing was excluded.”

Edward (Taffy) Bowen
What’s in the box?

“When the members of the Tizard Mission brought one to America in 1940, they carried the most valuable cargo ever brought to our shores.”

James Phinney Baxter III, *Scientists Against Time*, 1947

“The atmosphere was electric – they found it hard to believe that such a small device could produce so much power and that what lay on the table in front of us might prove to be the salvation of the Allied cause.”

“All we could do was sit in admiration and gasp”

American scientists
Was it -- The ‘One Ring’?
No – the Cavity Magnetron!
• Capable of producing ‘microwaves’ at high power.
  – Radar with around 10 cm wavelength
• And now it’s in every microwave oven.
Understanding the magnetron at the Rad Lab

“It’s simple. It’s just a kind of whistle”
I.I. Rabi

“OK, Rabi, how does a whistle work?”
E. Condon
September 1940 – January 1941

• Saturday, Jan. 4, 1941 was the first test of a centimetric radar system based on the magnetron.
• From the rooftop of the Rad Lab they detected the dome of the Christian Science Mother Church across the river.
The Battle of the Atlantic
1939 - 1945

“The only thing that ever really frightened me was the U-boat peril.”

Doenitz in Command

• Groups of U boats (Wolfpacks) would be directed from a central command, shadow convoys from a distance, then take action on their own while communicating with each other by radio.
  – Germany had broken the merchant shipping codes so they knew the routes!

• During the day the U boats would stay submerged, but at a distance to avoid sonar detection

• The attacks would be at night, on the surface.
  – Sonar was useless against a U boat on the surface, and at night they were impossible to detect – without radar.
“Happy times” for U-boats from 1939 through 1941
• Over 2,500 ships sunk
• Over 9 million tons

1942 – 1943
• HF/DF direction finding system
• New “10 centimeter radar” based on the cavity magnetron employed on ships and on planes.
• From June 1943 through May 1944 there as a complete change in fortunes.
“What is now decisive is that enemy aircraft have been equipped with a new location apparatus...which enables them to detect submarines and to attack them unexpectedly in low cloud, bad visibility, or at night. Much the largest number of submarines now being sunk are being sunk by aircraft. .... These losses are too high. We must now husband our resources because, to do anything else, would simply be to play the enemy's game.”

Doenitz to Hitler, May 1943
“The enemy has rendered the U boat war ineffective. He has achieved his object not through superior tactics or strategy, but through superiority in the field of science; this finds its expression in the modern battle weapon: detection. By this means he has torn our sole offensive weapon in the war against the Anglo-Saxons from our hands”

Doenitz, December 1943
“The enemy holds every trump card, covers all areas with long-range air-patrols, and uses location methods of which we still have no warning. The enemy knows all our secrets and we know none of his.”

Doenitz, from his diary in fall 1943