Why Defeat Enigma?

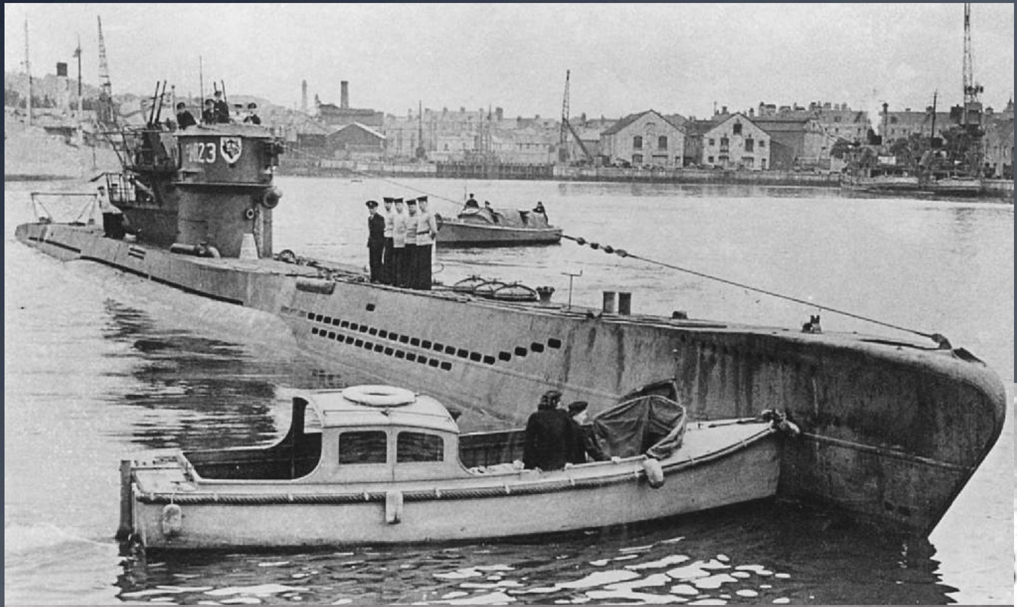
Military context of Turing's work at Bletchley Park

Dr Carlo Kopp, Associate Fellow AIAA, Senior Member IEEE, PEng
Monash University

Britain Under Siege

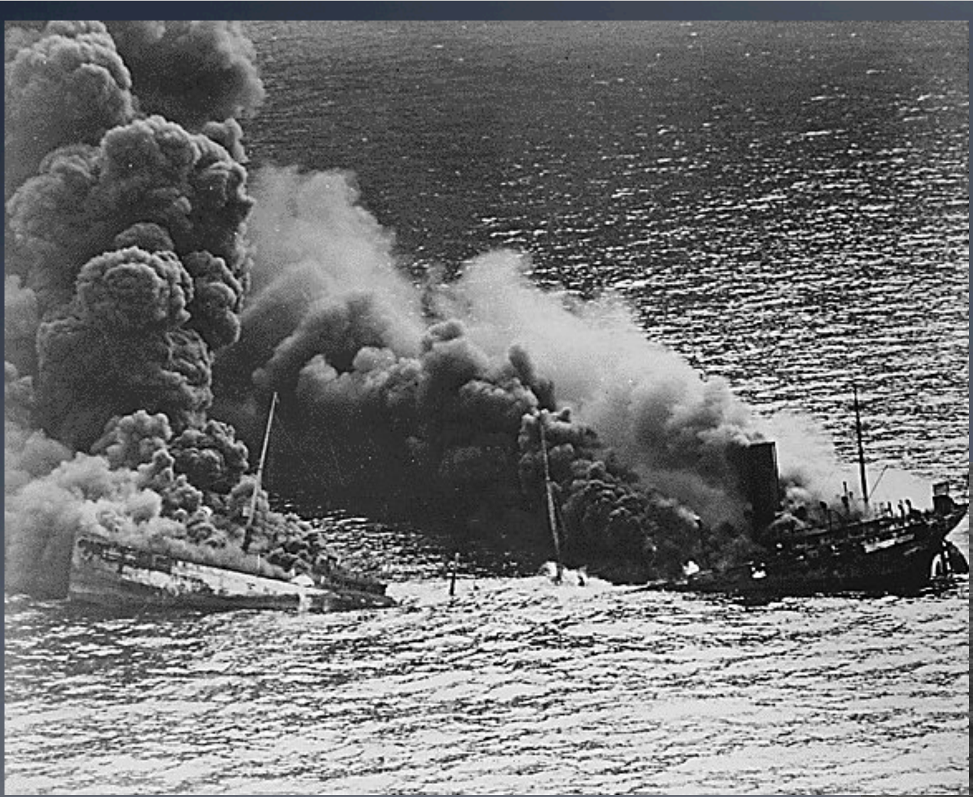
- With the outbreak of conflict between Germany and the Allies in 1939, Britain was for all intents and purposes under prolonged siege;
- British cities, industry and military installations were being systematically attacked by Germany's Luftwaffe;
- British shipping lanes were being systematically interdicted by the Kriegsmarine, especially by U-boat, and by the Luftwaffe's long range FW-200 Condors based in France;
- *Britain's ability to survive depended on the flow of supplies and personnel from the Commonwealth and military materiel from the United States, both of which were under threat.*

Kriegsmarine U-Boat Fleet



Armed initially with deck guns and torpedoes, later with homing guided torpedoes; Operating from German, French and Norwegian ports, up to twelve *Unterseebootsflottille* were active at any time: 1154 U-boats built.

Kriegsmarine U-Boat Interdiction



1939: 0.6 million tons sunk

1940: 2.3 million tons sunk

1941: 2.2 million tons sunk

1942: 5.8 million tons sunk

1943: 2.3 million tons sunk

1944: 0.6 million tons sunk

1945: 0.2 million tons sunk

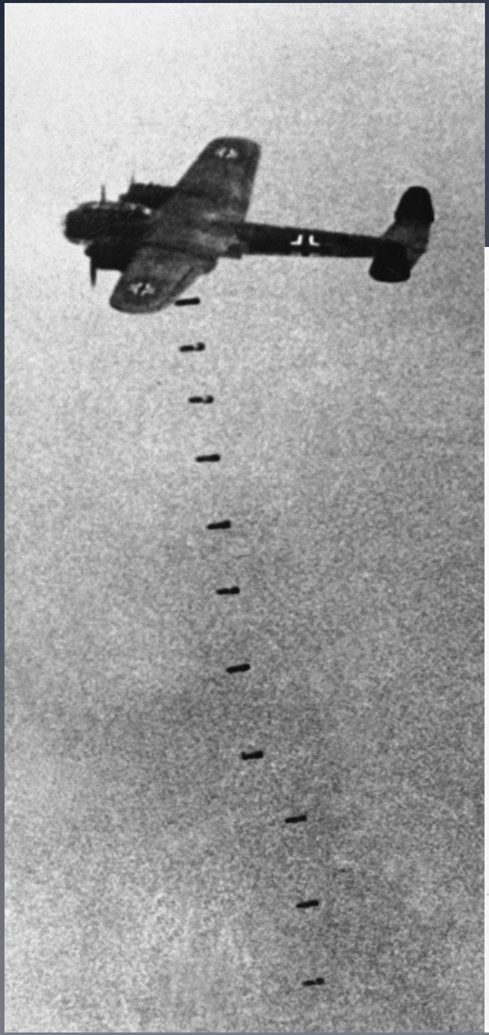
Total 1939-45: 14 million tons sunk

Above: allied tanker burns and breaks up following a U-boat torpedo attack; Right: allied freighter capsizes after U-boat attack.

Luftwaffe Sea Lane Interdiction

Focke-Wulf FW-200 Condor maritime interdictor; Kampfgruppe 40 and 100 operated from French airfields; In 1943 Hs-293 radio controlled smart bombs were introduced to attack Allied shipping.

Luftwaffe Air Raids



Luftflotte 2, 3, and 5 bombers based in France, Belgium and Norway attacked targets across Britain initially in daylight raids, and later in night raids; Intent: *"Bomb Britain into Submission"*

Luftwaffe Air Raids

Bombardment of Britain's major cities to intimidate the community, but also to disrupt the wartime economy, and military operations.

Luftflotte 2, 3, and 5 based in Belgium, France, and Norway conducted most of these raids, respectively; In 1944, Germany shifted to V-1 cruise missile and V-2 ballistic missile bombardments.

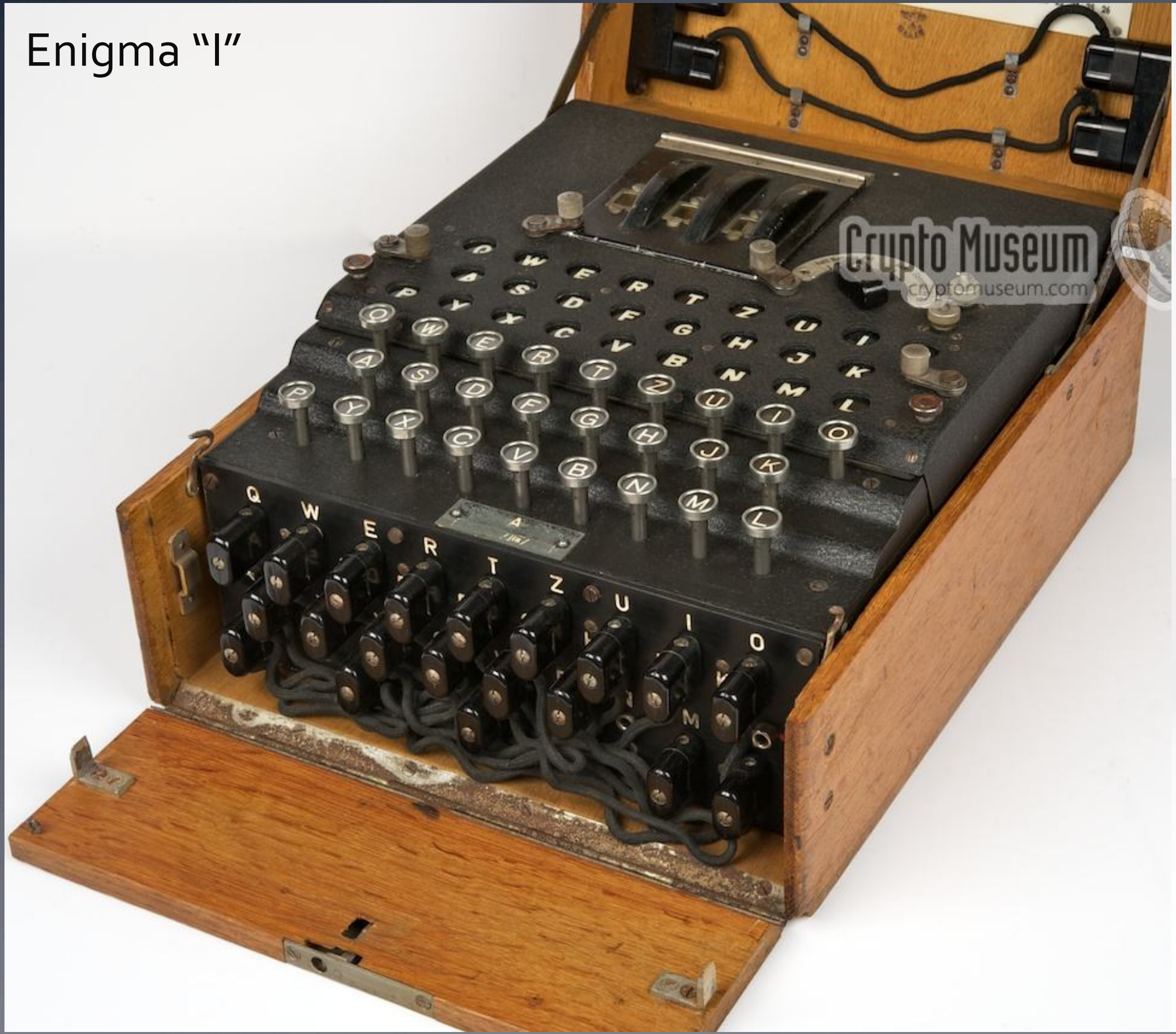
“Enigma Machine”

- Variants of the Enigma built crypto machine were used by the Kriegsmarine, Luftwaffe, Wehrmacht, SS, German civilian government agencies, and export clientele;
- Short wave radio links carried Enigma encoded traffic to German military units and warships at sea, especially U-boats – any traffic of importance was encrypted using Enigma machines;
- Defeat of the Enigma was crucial to the defeat of Nazi Germany;
- Decoded Enigma traffic, codenamed *Ultra*, was the best protected secret the Allies had.

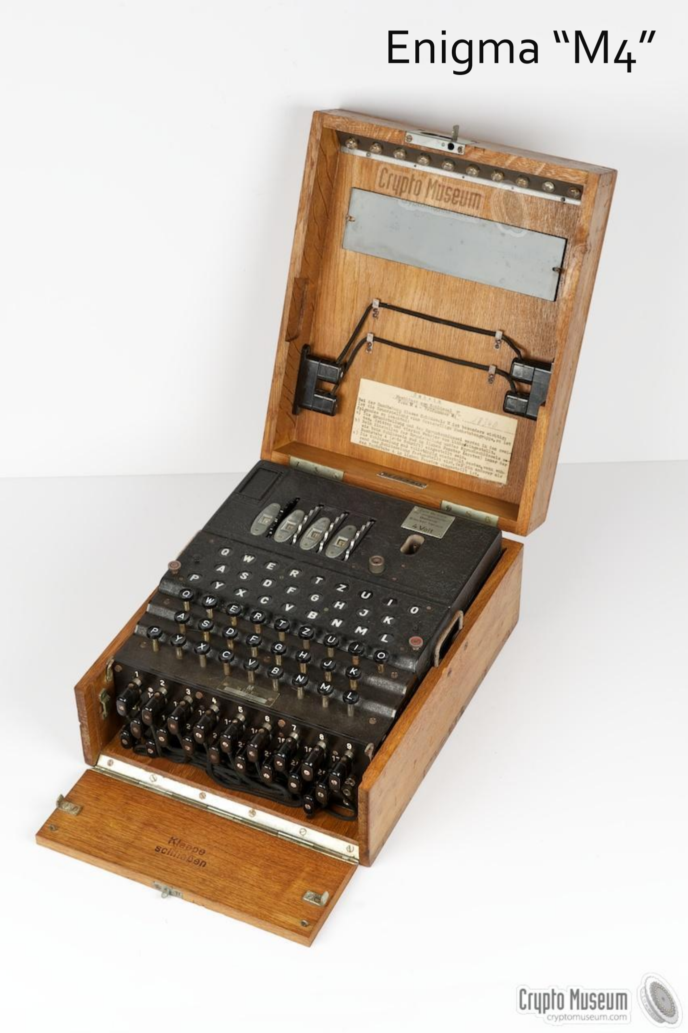
Enigma Variants

- Germany's Enigma company manufactured twelve basic variants of the "Enigma" cipher machine family;
- Most naval units operated the Enigma M1, M2 and M3 with three wheels, based on the "generic" Enigma "I" variant;
- U-boats were equipped in 1942 with the four wheel "M4" Enigma;
- Luftwaffe, Wehrmacht and other agencies used the Enigma "I" and "H" variants, with three wheels;
- Defeat of the M4 was much more difficult than defeat of the three wheel variants.

Enigma Variants



Enigma "I"



Enigma "M4"

References

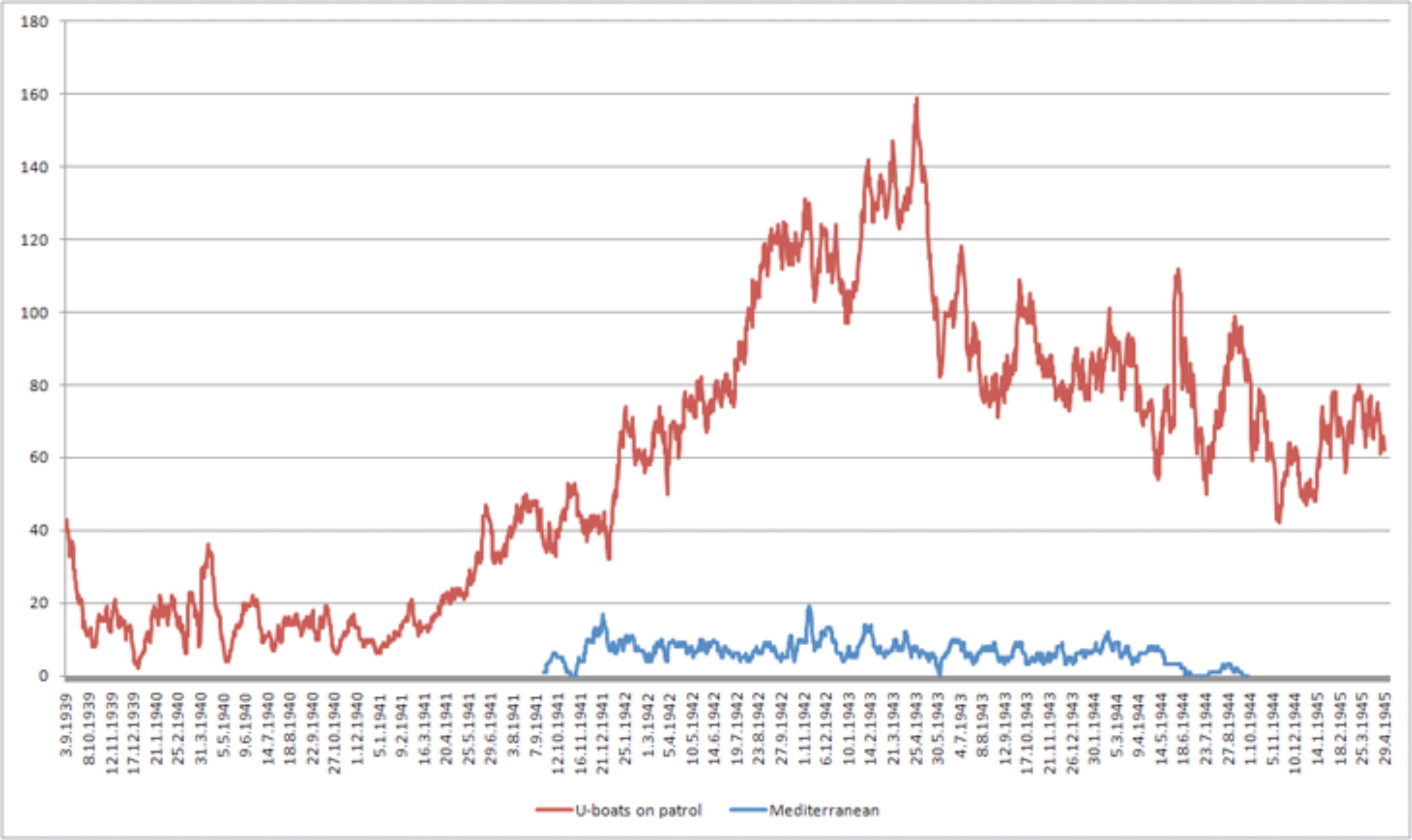
- Paul Reuvers and Marc Simons, **Enigma Cipher Machine, Crypto Museum, URI: http://www.cryptomuseum.com/crypto/enigma/**

- **Guðmundur Helgason, Uboat.net, URI: http://www.uboat.net/**

- **Images: mostly *Bundes Archiv*, Federal Republic of Germany and Crypto Museum, Enigma Logo by Crypto Museum.**

Backup Slides

Kriegsmarine U-Boat Activity



U-Boat.net: http://www.uboat.net/ops/combat_strength.html