

TŘETÍ ŘÍŠE POSLOUCHÁ

Prolamování spojeneckých šifer 1939–1945



CHRISTIAN JENNINGS

 PRESS

Třetí říše poslouchá

Vyšlo také v tištěné verzi

Objednat můžete na
www.cpress.cz
www.albatrosmedia.cz



Christian Jennings
Třetí říše poslouchá – e-kniha
Copyright © Albatros Media a. s., 2020

Všechna práva vyhrazena.
Žádná část této publikace nesmí být rozšiřována
bez písemného souhlasu majitelů práv.

ALBATROS  **MEDIA**



TŘETÍ ŘÍŠE POSLOUCHÁ

Pět lidí se zasloužilo více než kdokoliv jiný o to, že jsem mohl napsat tuto knihu: můj literární agent Andrew Lownie v Londýně, redaktorka Kate Moore v Madridu a Oxfordu, moji bratři Anthony v Římě a James v Rangúnu a nezdolná Kat Sacco v Turíně. Mé díky patří také Itálii. Jen málo míst se může hodit lépe pro pohodové psaní, než je Finale Ligure u Středozemního moře nebo Bardonecchia v italských Alpách.

TŘETÍ ŘÍŠE POSLOUCHÁ
PROLAMOVÁNÍ SPOJENECKÝCH
ŠIFER V LETECH 1939–45

CHRISTIAN JENNINGS

OBSAH

<i>Poděkování</i>	9
<i>Předmluva</i>	11
ČÁST PRVNÍ: NĚMECKO NA VZESTUPU	23
1. Prohra NA POLI SIGNÁLOVÉHO ZPRAVODAJSTVÍ v první světové válce	24
2. Obchodník s Enigmou	44
3. Noví němečtí luštitelé šifer	60
4. Příprava na válku	69
5. Válečné loďstvo začíná odposlouchávat	85
ČÁST DRUHÁ: NĚMECKO ÚTOČÍ	99
6. Dvě loďstva v době vypuknutí války	100
7. Rumunské kódy a rumunská ropa	115
8. Zprávy a dezinformace během invaze do Evropy	122
9. Válka ve vzduchu	132
10. Bitva o Atlantik	141
11. Starodávni nepřátelé, moderní luštění šifer	152
ČÁST TŘETÍ: NĚMECKO VE VÁLCE	159
12. Německé bitvy ve Středomoří	160
13. Prolomení Enigmy	169

14.	Hodný plukovník	179
15.	Signálové zpravodajství a kryptoanalýza na ruské frontě	190
16.	Tajemný Švýcar	216
17.	Rhubarb a Rodeo	223
18.	U-91 a bitva o Atlantik	228
ČÁST ČTVRTÁ: NĚMECKO SE BRÁNÍ		245
19.	Bitva v Egejském moři	246
20.	Nespolehlivá Enigma	259
21.	Bouře přichází	269
22.	Dopadení a poprava	282
23.	Zhroucení třetí říše	291
24.	My nic nevíme	299
<i>Doslov</i>		309
<i>Závěr</i>		313
<i>Chronologie</i>		321
<i>Bibliografie a zdroje</i>		328
<i>Glosář</i>		331
<i>Poznámky na konec</i>		334



PODĚKOVÁNÍ

Za pomoc všeho druhu, za rady a zdravý rozum během tohoto psaní si zasluhují poděkování: Cordula Kraemer v Berlíně, Giulia Avataneo, Daniele Calafiore, Otilia Cheslerean a Amor Ben v Turíně a můj bratr Martin v Oxfordu. Dále mi s touto knihou i se dvěma dalšími nesmírně pomohly Laura Callaghan a Gemma Gardner v Osprey Publishing.



PŘEDMLUVA

Dokumenty

Jaro roku 1945, Berlín a Bavorsko

Koncem března roku 1945 vtrhla Rudá armáda do Gdaňska v Polsku a překročila i rakouské hranice. Na západě dobyli Spojenci Kolín a překročili řeku Rýn. V době, kdy Německo čelilo útokům ze všech stran, Britové a Američané svůj postup zpomalili, aby umožnili Rusům dobýt Berlín. O měsíc dříve, v únoru, zaútočilo téměř tisíc amerických Létajících pevností B-17 na berlínskou železniční síť v mylném domnění, že německá 6. tanková armáda projíždí městem a směřuje po železnici k východní frontě. Zpravodajské informace Spojenců se ukázaly jako chybné, ale intenzivní bombardování způsobilo ohnivou bouři, která trvala čtyři dny a spálila na popel vše, co jí stálo v cestě. Protože k útoku došlo za denního světla a letectvo amerického generála Carla Spaatzeho nepoužilo příliš mnoho zápalných bomb, byl počet obětí na tak velký útok nízký. Zemřelo celkem 3 000 lidí, 20 000 lidí bylo zraněno a 120 000 jich přišlo o střechu nad hlavou. Ale díky tomu se německé hlavní město stalo místem, kde pracovat bylo stále obtížnější a nebezpečnější.

Šifrovací oddělení Vrchního velení wehrmachtu, tzv. OKW-Chiffrierabteilung (zkráceně OKW-Chi), Berlín již dávno opustilo. Zimní bombardování v letech 1943–44 již další pobyt v hlavním městě znemožnilo. V době, kdy někteří kryptoanalytici již byli pryč, několik z nich zde zůstalo, aby pracovali v hlubokých sklepech v rezidenční části města. Neměli žádné ústřední topení, dveře byly v některých případech použity jako palivo a v místnostech, kde pracovali, bylo vše pokryto vrstvou bílého prachu z omítky, který se zde usazoval

po neustálých otřesech způsobených leteckými útoky na budovy nad nimi. Během této chladné zimy pracovali někteří muži i ženy s rukavicemi nebo palčáky, jimiž se chránili před chladem. Tím obtížněji se jim tužkou a v mihotavém světle elektrických žárovek či svíček sepisovaly dešifrované zprávy signálového zpravodajství. Ve válečných dobách na přelomu let 1943–44 byly britské a americké depeše dešifrované kryptoanalytiky OKW-Chi plně podrobností o stálém postupu Spojenců Itálií směrem na sever, o jejich plánech na vytvoření druhé fronty a o obklíčení Němců Rudou armádou během Korsuň-ševčenkovské operace (také Korsuň-čerkaská kapsa). Rovněž byly dešifrovány zprávy o vzdušných náletech Spojenců na Německo, jež byly stále častější, stejně jako o naprosté porážce ponorek admirála Dönitze, které měly bránit v plavbě přes Atlantik spojeneckým zásobovacím konvojům, skládajícím se často z mnoha stovek lodí. Ačkoliv to nebylo patrné na první pohled, konec třetí říše již byl cítit ve vzduchu. Přesto němečtí dešifranti pokračovali v usilovné práci a monitorovali, zachycovali, dešifrovali a četli depeše od agentů, armád, letectva a lodí z nejrůznějších zemí.

Oddělení OKW-Chi bylo jen jednou z deseti agentur německého signálového zpravodajství, ale v červenci roku 1944, těsně po invazi do Evropy, pracovalo toto oddělení na luštění šifrovaných zpráv mnoha nepřátelských sil, neutrálních vlád i zahraničních agentů z jednačtyřiceti různých evropských i mimoevropských zemí. V březnu roku 1945, když americké bombardéry neustávaly ve svých útocích na Berlín, pracovala tato agentura v prostorách Školy spojovacích vojsk wehrmachtu v Halle v centrální části východního Německa. Velitelem a šifrantem oddělení OKW-Chi byl Wilhelm Fenner. Koncem března se rozhodl, že se všichni musí evakuovat a vydat se směrem na jih do Bavorska. Naložili stovky kilogramů tajných dokumentů do dřevěných beden, v nichž byly původně přístroje pro zachycování rádiových depeší. Rota vojáků obstarala nákladní vozy a benzín. Personál oddělení se vynořil z podzemí do šedého pochmurného počasí, zahalujícího město. Někteří z pracovníků dostali rozkaz vydat se směrem k železniční trati. Ostatní nastoupili na nákladní vozy. Obloha se začala vyjasňovat, až když opustili jižní předměstí Halle. Žádný z kryptoanalytiků či zpravodajců, kteří seděli na nákladácích, neměl ponětí o tom, kam jedou nebo co s nimi bude dál. Seděli nekonečné hodiny na korbách drkotajících nákladáků, vezoucích velké dřevěné bedny, jež vyplňovaly prostor mezi nimi. Ty obsahovaly jedny z nejdůležitějších zachycených depeší, dekodovaných zpráv a dokumentů, jež OKW-Chi zpracovalo

od roku 1938. Jejich nadřazení byli pevně rozhodnuti, že žádný materiál nesmí padnout do rukou postupujících Britů, Američanů nebo Rusů. A mezi muži či ženami, kteří ten den putovali na nákladních vozech, ať už šlo o vojáky či civilisty, panovalo tiché, neodbytné a vzájemné povědomí, že nikdo, ale opravdu nikdo nesmí padnout do rukou vojáků Rudé armády.

Lidé z OKW-Chi spálili vše, co nebylo zásadní. Ale to, co považovali za tak důležité, že to nebylo možné zničit, naložili na centrále v Halle a odvezli směrem k jednomu jezeru v jižním Bavorsku. Cesta byla plná zákrut a týmu z OKW-Chi zabrala téměř deset dnů. Během cesty na jih se pomalu oteplovalo, a když dorazili do Bavorska, bylo jaro v plném proudu. Auty i vlakem cestovali směrem na Norimberk, Mnichov a Berchtesgaden, kde měl Hitler své „Orlí hnízdo“. U Rosenheimu, patnáct mil jihovýchodně od Mnichova, sjel konvoj z cesty a vydal se k horám tyčícím se na bavorsko-rakouské hranici. Počátkem druhého dubnového týdne se vojáci i civilisté ubytovali v různých opuštěných školách, hotelích a železničních budovách v malém alpském městě s názvem Schliersee. Leželo u krásného modrého jezera. Jednoho rána uviděli příslušníky SS z jedné dělostřelecké jednotky, jak vyhazují celé vagony minometných a dělostřeleckých nábojnic do vody a jak na břehu pálí dokumenty. Následujícího dne naložilo pár příslušníků OKW-Chi a několik vojáků bedny s tajnými dokumenty na dva železniční vagóny: Ty byly přistaveny na břeh bokem k jezeru. Odtud pak naházeli do bahnité vody spoustu beden. Další skupina naložila bedny a všelijaké technické vybavení na vor, se kterým veslovali doprostřed jezera, kde celý náklad vyklopili do vody. Poté vyrazili němečtí vojáci i civilisté opět směrem k Mnichovu: Dostali rozkaz, aby se připojili ke smíšené jednotce armády a letectva, jež vznikala v rámci celého Bavorska a skládala se z opozdílů všech hodností a ze všech možných jednotek. Ta se pak měla organizovaně vzdát Spojencům, rychle se přibližujícím ze západu. Tou dobou již ležely bedýnky se záznamy oddělení OKW-Chi devět metrů v měkkém tmavém bahně jednoho bavorského jezera, kde zlehka dosedly na rozházené nábojnice dělostřelectva SS.

V červenci roku 1944 se Britové a Američané rozhodli, že se pokusí získat vědecká tajemství třetí říše. Spojenci byli velmi zvědaví, v čem nad nimi měli Němci technologickou převahu. Jak daleko se dostali v oboru řízených raket,

přesných bomb, tryskových letadel a bitevních tanků? A které šifry, ať už spojenecké nebo z neutrálních zemí, prolomili? Jak? Kdy? Za použití jakého zařízení nebo kterých interních informací? Krátce řečeno, co měli Němci z oblasti technologie nebo zpravodajství, co Spojencům scházelo?

Na podzim roku 1944 již bylo jasné, že Spojenci brzy zvítězí. Vytvořili tedy čtyři týmy zpravodajských „lovců“, kteří hodlali pročesat Německo, Rakousko a země Benluxu, když se válka chýlila ke svému nevyhnutelnému konci. Příslušníci CIOS (Combined Intelligence Objectives Subcommittee – Sdružený podvýbor pro zpravodajské úkoly) přidělili kódová označení pro tyto operace: ALSOS – pátrání po informacích týkajících se nukleárního výzkumu, OVERCAST – úkolem je zmocnit se čehokoliv, co by se týkalo raket V1 a V2, SURGEON – pátrání po technologiích týkajících se tryskových pohonů a avioniky. Ze všech čtyř zpravodajských operací to byla operace TICOM, jež podléhala nejpřísnějšímu utajení. V jejím zorném poli bylo vše, co se týkalo agentur pro signálové zpravodajství třetí říše.

TICOM (Target Intelligence Committee – Výbor pro cílovou zpravodajskou činnost) měl tři cíle: Zjistit, čeho a jak Němci dosáhli v případě prolamování námořních, vojenských a diplomatických šifer; pokusit se o získání cenných zpravodajských odborníků, záznamů a zařízení dříve, než se to podaří Rusům; a konečně zjistit úroveň kooperace německých zpravodajců s Japonci, na jejichž území se Spojenci chystali vpadnout. Příslušníci skupin TICOM byli vybíráni z řad britských a amerických námořních, vojenských a leteckých důstojníků. Prošli výcvikem v Bletchley Park a hodlali vstoupit na půdu třetí říše bok po boku frontových jednotek nebo těsně za nimi. Jeden z prvních plánů v rámci jejich nasazení obsahoval seskok parašutistů na území Berlína se 101. výsadkovou divizí, aby ve zničeném hlavním městě třetí říše pátrali po zpravodajských informacích, aby v případě nutnosti bojovali proti fanatickým skupinám SS, na něž by narazili, a pak čekali na vysvobození z rukou amerických či ruských obrněných jednotek, které by se probily do města. Důstojníci TICOM si oblékli své uniformy s plným vědomím, že by mohli být snadno posláni do bojové akce proti německým, japonským nebo italským nepřátelům. Ale byli rádi, když byl plán parašutistického seskoku do válečného kotle bojujícího Berlína zrušen.

Místo toho hodlali jet do okupovaného Německa auty. I tak to bylo velmi riskantní. Přes formální kapitulaci byly německé jednotky stále ozbrojené a některé z nich by se mohly pokusit o poslední odpor. Důstojníci skupiny

TICOM měli prověření typu „Ultra“ a znali veškerá tajemství prolamování šifry Enigma, takže ani v tomto pozdním stadiu války nesměli padnout do zajetí. V důsledku toho jim byla na ochranu přidělena jednotka Britského královského námořnictva, jednotka téměř tak charakteristická a osobitá jako oni sami.

30 Assault Unit (AU – 30. útočná jednotka) Královské námořní pěchoty byla duchovním dítětem podivínského a okázalého důstojníka námořní zpravodajské služby, korvetního kapitána Iana Fleminga. Ještě před katastrofálním britským a kanadským útokem na francouzský přístav Dieppe, který se odehrál v srpnu roku 1942, si Fleming uvědomil, že je docela možné, že by nějaké komando, jdoucí do akce společně s konvenčními silami, získalo ve zmatku bitevní vřavy zpravodajské dokumenty, zařízení či uneslo nějaké lidi. 30 AU, jak byla tato jednotka nazývána, měla svoji základnu v západním Sussexu ve městě Littlehampton a z důvodu utajení byla součástí většího komanda Královské námořní pěchoty. V Dieppe měli za úkol si probojovat cestu do německého velitelství v centru města a ukořistit tam přístroj námořní Enigmy. Avšak operace *Jubilee* (jubileum), což byl útok na Dieppe, byla do očí bijícím fiaskem a mariňáci z jednotky 30 AU – v jejichž řadách byl i jeden kasař – nedokázali ani opustit své vylodovací plavidlo. Tak silná byla německá palba na pláži, kde se měli vylodit. Avšak o tři roky později byla tato jednotka spolu s ostatními týmy TICOM již připravena vtrhnout do Německa.

Prvního května byl Hitler mrtev a Rudá armáda dobyla Berlín. Důstojníci TICOM, rozdělení do šesti samostatných týmů, se rázem ocitli v chaosem zmítaném Německu, kde šest let trvající válka skončila sotva před několika hodinami. Jejich zprávy a dokumentace, pocházející z několika prvních dnů, byly směsí výbušného napětí na ostří nože, okamžiků okázalého bláznovství i výbušného lidského ducha, k čemuž za války často dochází. Polovina německých civilistů k nim cítila nenávist a druhá polovina je vítala s otevřenou náručí. Cesty, po nichž se pohybovali, byly občas zaplněny tisíci vyhnanců z Ruska, Francie a Německa, právě propuštěnými válečnými zajatci, vojáky a utečenci. Byli v zemi, kde násilí, zoufalství a smrt visely ve vzduchu jako jablka, která mají každou chvíli spadnout ze stromu. Jindy, uprostřed dění, jemuž jeden z důstojníků TICOM říkal „naše soukromá válka“, zavládly chvíle míru a pokoje.

Bydleli v privátních domech, pod stany ve vojenských táborech jednotek americké armády, v opuštěných turistických hotelích, jejichž personál utekl

sotva před pár hodinami a jejichž knihy hostů byly plné jmen vysokých nacistických funkcionářů. Stanovali pod německým jarním nebem posetým hvězdami a v Bavorsku pročesávali sklepy a kasárna, která jen nedávno opustili prchající němečtí vojáci. Zabývali se podrobně veškerými informacemi obíhajícími mezi lidmi i šuškanou od kohokoliv, kdo mohl něco vědět o tom, kam mohli němečtí šifranti a dešifranti uprchnout. Jejich pátrání je vedlo přes chvějící se srdce země, co právě kapitulovala a byla sužovaná skomírající válkou tak kontrastující s velkolepostí prvních jarních mírových dnů. V jednom domě nedaleko Mnichova našli dvě tuny map a skryše s ručními násadkovými granáty s pojistkami. V útulku pro choromyslné pátrali po vyhozených zpravodajských depeších a podél cest nacházeli polospálené uniformy SS. Prohledali prázdné letní sídlo patřící von Ribbentropovi a vyslyšali nějakého kolemjdoucího esesáka, který jim sdělil, že by mohl něco vědět o neviditelných inkoustech. Z jiného soudku se jim doneslo, že vysoko v horách poblíž horského jezera byla tajná výzkumná stanice, kde nacisté dešifrovali zprávy. Když se pokusili na tuto horu vylézt, narazili na oddíl amerických vojáků, kteří se uvelebili v Himmlerově lovecké chatě. V jedné alpské boudě předstíralo šest francouzských nacistů, že jsou silničními dělníky, a o kousek výše byla horská bouda, v níž čtyři bývalí příslušníci Luftwaffe prožívali příjemné chvíle společně se třemi dalšími ženami. Ale žádnou tajnou výzkumnou stanici nenašli.

Mezitím ve vestibulu hotelu Astoria v Bad Gasteinu poblíž Berchtesgadenů tiše čekalo 126 japonských diplomatů, vedených japonským velvyslancem v Berlíně baronem Ošimou. Japonský velvyslanec byl blízkým Hitlerovým důvěrníkem a Američané četli jeho korespondenci s Tokiem, když prolomili japonskou diplomatickou šifru, jíž dali krycí název „Purple“. Tento materiál byl velmi věrohodný – mezi téměř 1 500 depešemi byla jedna z 6. června 1941, ve které Ošima sdělil svým nadřízeným v Tokiu, že se Německo chystá napadnout 22. června Sovětský svaz. V polovině dubna roku 1945 se setkal s německým ministrem zahraničí Joachimem von Ribbentropem a prohlásil, že zůstane v Berlíně až do konce bok po boku Hitlerovi i jeho poradcům. Ale osobní rozkaz Vůdce zněl, že on i ostatní diplomaté musí Berlín opustit. Odcestoval tedy do Bad Gasteinu, aby se zde setkal se svojí ženou. Američané je vzápětí zatkli a převezli lodí do Spojených států.

Mezitím doprovázel důstojník TICOM příslušníky jednotky Královské námořní pěchoty 30 AU na malý ostrov Mainau, nacházející se nedaleko

od břehu Bodamského jezera na švýcarsko-německé hranici. Byl zde na základě upozornění, že Němci evakuovali nějaké experimentální výzkumné pracoviště a přivezli sem vědce, kteří předtím pracovali na technologii raket V2 v Peenemünde na baltském pobřeží. Mainau je velké arboretum. Ostrov je dlouhý tisíc metrů a v nejširším místě měří jen 600 metrů. Roste tam 500 druhů stromů spolu s dalšími stovkami různých druhů růží, jirčin, azalek a rododendronů. Na začátku mostu spojujícího ostrov s pevninou sdělila hlídka příslušníkům týmu TICOM, že dále již nemohou pokračovat, protože ostrov je v soukromém vlastnictví a zároveň neutrálním teritoriem, které patří švédskému princovi Bernadottovi. Avšak bylo zřejmé, že jej Francouzi již používali jako tábor pro vyhnance. Francouzský důstojník-lékař sdělil britským mariňákům i důstojníkovi TICOM, že inspekce ostrova nemá smysl, protože dva jejich kolegové z britských vojenských zpravodajských služeb ji už provedli. Ale, pokračoval, pokud se chtějí podívat sami, potřebují propustku od místních úřadů v Kostnici. Mariňáci tedy otočili své džípy a vrátili se do města, jen aby zjistili, že všechny úřady byly celý den zavřené na počest státní návštěvy marockého sultána. Byla to další frustrující slepá ulička. Skutečně, po celý minulý květnový týden nedošlo k žádnému opravdovému průlomů v pátrání a zdálo se, že celé týdny šli jen po zvěstech a dezinformacích. Třeba 31. května, kdy celý den jen přšelo a přšelo, napsal někdo z týmu TICOM, že prostě zůstali pod střechou v opuštěném bavorském domě, který obývali, a popíjeli víno ze sklepa, ježž objevili ve městě Kaufbeuren.

Ale pak se na ně najednou usmálo štěstí. Skupina vysokých důstojníků wehrmachtu a vojenského námořnictva byla na cestě do Remeše, kde se hodlali vzdát Spojencům, když potkali jeden z týmů TICOM, operující dále na severu. Jedním z důstojníků německé armády v této skupině byl podplukovník Mettig, předchozího roku druhý vrchní velitel oddělení OKW-Chi. Bylo po válce, řekl si, a nikdo již neměl dále co skrývat. Američané byli nyní spojenci Němců, a obě strany by tedy měly spolupracovat proti Rusům. „Běžte do Bavorska,“ řekl, „a najdete jezero Schliersee.“

Byl konec června. Když o dva dny později dorazili britští a američtí důstojníci do města, první, kdo jim nabídl pomoc, byl malý uhlažený muž, který dříve pracoval jako policista ve Vídni. Měl na sobě civilní šaty a pásku na rukávu signalizující příslušnost k Freiheitsaktion Bayern, což byla protinacistická domobrana, jež podporovala Spojeneckou vojenskou vládu (Allied Military Government), sídlící v Mnichově. „Pojďte se mnou,“ řekl. „Ukážu vám,

kde byli lidé z SS a z wehrmachtu“. Členové týmů prohledali tři nemocnice, plné zraněných vojáků, a místní školu. V budově pošty nebo v místním hotelu nenašli nic, v převlékacích kabinkách na pobřeží nebylo téměř nic, kromě prázdných krabic s razítkem orla wehrmachtu. Na jednom odstavném kolejišti stály ve městě dva železniční vagóny patřící Luftwaffe, plné zařízení pro fotografickou rekognoskaci. Také zde byly dva nákladáky poškozené a vydrancované ruskými utečenci, kteří vnikli dovnitř, aby zde našli útočiště před zimou. V doprovodu svého průvodce z řad domobrany našly týmy Spojenců několik civilistů, o nichž se dověděli, že dva dny před tím, než Němci utekli, naložili dva železniční vagóny krabicemi s papíry a naházeli je do jezera – tato informace se zdála být věrohodná, protože v drobném bahnitém šterkopisku na kraji našli důstojníci TICOM několik polospálených osobních dokumentů SS a součástky dálnopisů. Poté si jeden britský a jeden americký důstojník vzali loďku a pokusili se poprvé prohledat dno jezera blízko břehu. Jejich lana se několikrát zadrhla o něco tak těžkého, že to nemohli ani vytáhnout na povrch.

Pak došlo k dalšímu průlomů. V druhé polovině července pročesávali vojáci Třetí americké armády jezero, když hledali tělo vojáka, který se utopil během plavání. Nalezli velkou bednu a tu vyzvedli na hladinu. Byla plná dokumentů popisujících operace OKW-Chi. Vojáci americké armády pak zavolali jak TICOM, tak i jednotky záchranných specialistů a techniků, kteří měli svoji základnu v Le Havre na francouzském pobřeží Atlantiku. Tam udržovali pontony umělých přístavů, jež Spojenci stále ještě používali pro vyloďování vojenských jednotek a zásob. Na konci srpna jeli Američané napříč Francií a pak dolů Německem se čtyřmi potápěči. Vybudovali velký vor s motorem a jeřábem a ten použili k prohledávání dna jezera. Netrvalo příliš dlouho, když našli dvacet osm velkých beden ležících devět až patnáct metrů pod hladinou vedle minometných a dělostřeleckých granátů jednotek SS. Byla to velmi důležitá část archivů OKW-Chi.

Příslušníci TICOM, kteří právě pracovali v severním Německu, zaznamenali nakonec podobný úspěch: obsadili odposlouchávací stanici v Neumünsteru, což bylo město, ležící na dánsko-německé hranici, a spojovací školu ve Flensburgu-Mürwiku, kde měli Němci na konci války své velitelství. Dostali se k detailům šifry „*Flusslauf*“ (Tekoucí řeka), což byla nová námořní šifra, která měla být zavedena 5. května. Znamenalo to, že v posledních osudových dnech války by Spojenci nebyli schopni číst depeše Ultra. Koncem září

příslušníci TICOM vystopovali a zajali německý personál kryptoanalytických jednotek námořnictva, armády, letectva a ministerstva zahraničí a začali je vyslýchat. Výsledky se uskutečnily v Bavorsku, Rakousku, Británii a ve středním či severním Německu. Výsledkem byly desítky tisíc stran dokumentů, k nimž bylo nutné přidat veškeré knihy kódů, dálnopisné stroje, mapy a nej-různější dokumenty, které spojenecké pátrací týmy nacházely do konce léta roku 1946. Tomuto obrovskému množství materiálu se v kruzích britských a amerických zpravodajců začalo říkat „archivy TICOM“.

Válka skončila. Dešifrovací operace v Bletchley Park postupně ustaly, když Britové a Američané čelili najednou novému nepříteli: Rusku. Začala studená válka a několik německých kryptoanalytiků, co během války veleli signálovým zpravodajským službám, začalo pracovat pro Američany nebo pro novou německou vládu. Obrovské archivy TICOM byly uloženy ve skladištích v Británii nebo ve Spojených státech. A tam zůstaly i v době, když čtyřicátá léta končila a začínala léta padesátá. Britové i Američané do nich občas nahlédli, jako třeba v roce 1952, když se Americké námořnictvo rozhodlo provést konečnou analýzu bitvy o Atlantik, dále role, kterou zde sehrálo německé luštění šifer Spojeneckého námořnictva i úsilí Britů o prolomení šifer v Bletchley Park. V roce 1968 do nich Britové nahlédli znovu, když Němci „objevili“ téměř 100 stran důvěrných londýnských diplomatických telegramů z válečného období v archivu ministerstva zahraničí v Bonnu. Jak se tam dostaly? Britské vládní úřady to chtěly vědět. Němci přece neluštili šifry Britského ministerstva zahraničí ani šifry námořnictva, ne? A nejen to. Co třeba dělaly stovky dešifrovaných britských námořních depeší z oblasti Středozemního moře z let 1940 až 1943 v policích archivu námořnictva v Římě? Dokázali britské šifry prolomit také Italové?

A to vše ustoupilo do pozadí počátkem sedmdesátých let, kdy Britové a Američané odtajnilo materiály ohledně dešifrovacích operací Spojenců v době války, které se nacházely ve Vládní škole kódování a šifrování. Enigma, Ultra a Bletchley Park se staly historií. Následovalo čtyřicet let, kdy se toto téma stalo námětem pro psaní knih a točení filmů.

Archivy TICOM byly uloženy ad acta, stejně jako nesčetné množství jiných dokumentů, map, deníků, přístrojů a knih kódů, jež po sobě Němci zanechali na zpravodajských základnách svého válečného impéria, od Chorvatska po Itálii, od Ruska, Rumunska a Ukrajiny až po Estonsko, od Prahy až po Paříž. S růstem dosahu internetu v roce 2000 začaly Británie i Amerika

s odtajňováním archivu TICOM. Daný materiál buď vraceli do Německa nebo si ponechali vybrané položky ve svých vlastních muzeích nebo ve veřejných archivech. Například válečný operační deník Velitelství německého ponorkového loďstva zůstal uložen v námořním muzeu v Marylandu. Nepočtená hrstka nadšených bloggerů a autorů umístila toto malé množství tohoto nového materiálu o německém prolamování šifer během války do veřejné domény, ale jak se dalo očekávat, nic z toho nemělo ani zdaleka takový dopad jako zveřejnění tajemství Enigmy a Ultra.*

Podzim 2017

První sníh začal padat na alpský rezort Bardonecchia, nejzápadnější město v Itálii, pozdě. Od konce dubna až do prvního víkendu v listopadu převládalo permanentně modré nebe a jasné zářící slunce. Listy na kašanech lemujících městské ulice začaly opadávat. Osvěžující vítr zřetelně oznamoval, že zima je za humny, a když 5. listopadu nastala ve Spojeném království Neděle vzpomínek, vrcholky hor nad městem byly pokryté bílým sněhem. Na šedém kamenném památníku v Zahradě Vittoria Veneta je čtyřicet bronzových plaket obyvatel města, kteří zemřeli během druhé světové války. Reprezentují typický vzorek všech míst, kde se italsí vojáci účastnili bojů a kde za války zemřeli, ať už na straně Němců nebo jako partyzáni, co bojovali na druhé straně. Jsou také vzpomínkou na obrovský geografický a politický rozsah těchto bojů – Bardonecchia je jen malé alpské město a těchto jmen je zde pouze čtyřicet. Ale jsou zde, aby podala svědectví o zlomku rozsahu války a její ceny. Je tam voják Luigino Bompard, který v jednatřiceti padl v Sarajevu, a voják Attilio Garnier, jenž se stal nezvěstným v Chorvatsku. Rotný Sergio Tarraboire se v roce 1942 potopil na lodi nedaleko Malty. Italský horský myslivec (Alpino) Alberto Vallory padl na ruské frontě v roce 1942. Partyzán Giuseppe dalla Vecchia zemřel v roce 1944 ve věku pouhých šestnácti let v samotné Bardonecchii a Alberto Mallen byl deportován do koncentračního tábora Mauthausen. Nyní je po něm pojmenované dětské hřiště, jež se rozprostírá pod piniemi u lyžařských sjezdovek.

Chvilí po poledni v Neděli vzpomínek někdo přijel a měl s sebou plynovou láhev připevněnou ke kovovému mechanismu pro věčný oheň a zapálil jej.

* Chronologii událostí z let 1914 až 1945 naleznete na stranách 321–327

Jeho malý modrý plamen se třepotal a hučel ve studeném větru, zatímco zahrada s památníkem byla připravena na příchod místních funkcionářů. Po třiceti minutách bylo po všem a jediným strážcem zahrady zůstal velký věnec vavřínových listů, vysoký do půli pasu, opřený o kamenný památník. Sněhové mraky se honily po bocích hory, která stála naproti. Ale zima nebyla tím jediným, kdo se onoho studeného odpoledne dostavil. Pod střechou, v bezpečí před větrem a sněhem čeká jeden e-mail. Byl odeslán ze státních archivů německého Ministerstva zahraničí v Berlíně. S charakteristickou efektivitou poslali svůj nový excelovský tabulkový kalkulátor. Bylo v něm 3 917 položek. Námořní šifrovací knihy z Francie dvacátých let, mapy Bulharska, seznam španělských vojenských šifer, čínské, jugoslávské a italské diplomatické šifry, dokumenty s ruskými bigramovými šiframi, rumunská vojenská kniha kódů z roku 1941, etiopské diplomatické šifry z roku 1944, japonské a belgické šifry ministerstva zahraničí. Seznam obsahuje další a další položky. Všechny tyto položky našli příslušníci týmů TICOM v letech 1945 až 1946 v Německu a odvezli je do Anglie. Tam spočívaly v britských národních archivech celých padesát pět let a do Německa byly vráceny teprve v roce 2000. A za předpokladu, že i jiná muzea a archivy po celé Evropě a Americe obsahují také značnou část archivu TICOM, si můžeme představit rozsah a ambice třetí říše a jejího úspěchu či neúspěchu v oblasti vytváření šifer a jejich prolamování. Otázkou je, čeho Němci byli či nebyli schopni dosáhnout se vším nebo jen s částí toho, co v oblasti kryptoanalýzy získali. Tato kniha pojednává jen o špičce obrovského ledovce a pokouší se dát jen některé odpovědi.



ČÁST PRVNÍ

NĚMECKO NA VZESTUPU



Kapitola první

PROHRA NA POLI SIGNÁLOVÉHO ZPRAVODAJSTVÍ V PRVNÍ SVĚTOVÉ VÁLCE

V neděli 2. srpna roku 1914 se ve Finském zálivu plavil německý lehký křižník SMS *Magdeburg*. Jeho cílem byl přístav Libau (dnes Liepāja) na lotyšském pobřeží. S ním se plavil další křižník jménem *Augsburg* s jedním torpédoborcem a minonoskou. Den předtím vyhlásilo Německo válku ruskému impériu a tyto čtyři lodě dostaly rozkaz položit miny kolem přístavu Libau, aby jej pak ostřelovaly v rámci příprav na útok německé pěchoty. A tak první výstřely, které vypálilo císařské Německo na síly cara Mikuláše II., vyšly z křižníku *Magdeburg*, jenž ostřeloval Libau z děl ráže čtyři a půl palce. Ruská městská posádka utekla. *Magdeburg* zůstal na své pozici nedaleko pobřeží a pálil na další cíle. Posádka křižníku *Augsburg* položila minové pole, nicméně bylo tak špatně označené, že se ukázalo být spíše problémem pro Němce než pro jejich nepřátele. Během následujících tří týdnů hlídkovala tato dvě plavidla ve Finském zálivu v doprovodu několika dalších torpédoborců.

26. srpna se německé lodě plavily v husté mlze a ztratily v ní vzájemný vizuální kontakt. Mlha byla tak hustá, že jí žádné světlo signálních lamp nedokázalo proniknout. Prvním znamením, kdy posádka *Magdeburgu* pochopila, že jsou mimo kurs, byl burácející skřípot, jak třesoucí se loď najela na mělčinu. Byli pevně zaklínění na skaliscích malého ostrova Odensholm jen kousek od pobřeží ruské provincie Estonska.

Na jednom z doprovodných torpédoborců uslyšeli zvuk, jak *Magdeburg* narazil na podmořský útes. Mlha se začala zvedat. Posádka torpédoborce připevnila ke křižníku lano a snažila se jej odvléci, jenže *Magdeburg* byl zaklíněn příliš pevně. Jeho kapitán vydal rozkazy ke zničení lodi a k jejímu opuštění. Pak se udály současně a velmi rychle tři věci. Vítr začal zvedat mlhu, ve které se objevily dva ruské křižníky. Zahájily palbu. Pak předčasně vybuchly demoliční nálože, umístěné v přední části *Magdeburgu*. Patnáct členů posádky přišlo o život. Většinu zbývajících námořníků se podařilo dostat na palubu torpédoborce, jenž jim byl vyslán na pomoc. Zatímco na přední části křižníku zuřil požár, kapitán neměl čas na to, aby hodil všechny tajné lodní dokumenty přes palubu. Nebo aby zajistil, aby byly přemístěny na palubu torpédoborce.

Jako u mnoha lodí německého Císařského námořnictva, i *Magdeburg* vezl na palubě malou lodní okovanou truhlu, určenou pro podobné nouzové situace. Kapitán do ní vložil lodní deník, námořní mapy a dva výtisky tajné knihy kódů a hodil ji přes palubu do mělkých čistých vod Baltského moře. Ruské křižníky se rychle přibližovaly. Přední část *Magdeburgu* hořela. Kapitán zapálil třetí exemplář knihy kódů. Mlha se i nadále zvedala. Německý torpédoborec vyrazil pryč, jak nejrychleji mohl, a zanechal kapitána a padesát sedm členů posádky na palubě spolu se čtvrtým výtiskem knihy kódů Císařského námořnictva (*Signalbuch der Kaiserlichen Marine* – SKM), která se stále nacházela v trezoru v kapitánově kabině.

Byla tam i v okamžiku, kdy Rusové vstoupili na palubu a vzali kapitána a ostatní námořníky do zajetí. Rozhodli se *Magdeburg* nechat tam, kde byl, a pak jej dát do šrotu. Vyslali svého potápěče, aby se ponořil podél boku lodi. Objevil truhlu obsahující nějaké lodní dokumenty a dvě šifrovací knihy. Prohledali kapitánovu kajutu a našli další, čtvrtou kopii. Okamžitě je přenesli na palubu jednoho z ruských křižníků. Rusové pak kontaktovali britského námořního ataše v Petrohradu, teprve nedávno přejmenovaném z původního názvu St. Petersburg. Jednání bylo jednoduché. Spojencům z Britského královského námořnictva nabídli kopii této ceněné šifrovací knihy SKM za podmínky, že si ji převezme britská loď. Výsledkem bylo, že Admiralita vydala rozkaz křižníku HMS *Theseus*, aby vyplul ze Scapa Flow. Dne 7. září dorazil křižník do Murmanska. Zdárně pak doplul zpět do Skotska, kde 10. října zajel do doků se dvěma vysokými ruskými námořními důstojníky na palubě a s kopií č. 151 šifrovací knihy SKM. 13. října byla kniha v Londýně. Tehdy byl prvním lordem Admirality Winston Churchill. Samou radostí byl celý bez

sebe. Podal o této události zprávu, ve které hýřil nadšením, když popisoval, jak získal tyto „mořskou vodou potřísněné dokumenty nevyčísitelné hodnoty“ od ruských spojenců Británie.*

Počátkem září roku 1914 ztroskotal lehký německý křižník SMS *Magdeburg* v Baltském moři. O několik hodin později bylo vyzvednuto tělo jednoho utopeného německého poddůstojníka, který v posmrtné ztuhlosti svíral na své hrudi šifrovací a kódové knihy německého námořnictva a námořní mapy Severního moře a Helgolandské zátoky, detailně rozdělené na čtverce. 6. září mě navštívil ruský námořní atašé. Obdržel zprávu z Petrohradu, jež ho informovala o tom, co se stalo a že Ruská admirálita s pomocí šifrovacích a kódových knih byla schopna dešifrovat alespoň část zpráv německého námořnictva. Rusové se cítí jako vedoucí námořní mocnost a Britská admirálita by tyto knihy a mapy měla mít.¹

První světová válka trvala sotva dva měsíce a na bojišti zvaném signálové zpravodajství již bylo německé námořnictvo v defenzívě. Během několika následujících dnů po zajetí křižníku *Magdeburg* došlo k něčemu podobnému. Na druhé straně zeměkoule ztratili Němci další ze svých životně důležitých knih kódů. Dne 11. srpna navázali kontakt námořníci z Královského australského námořnictva, určení pro abordáž, s nákladní lodí plující nedaleko Port Phillip Heads severně od Melbourne. SS *Hobart* byla loď, ve společném vlastnictví německé a australské společnosti provozující parní lodě a měla německou posádku. Zprávy o vypuknutí války se na loď nedostaly. Takže australští námořníci prostě jen předstírali, že jsou karanténním inspekčním týmem. Důstojníci z *Hobartu* jim umožnili volný pohyb po lodi a domnívali se, že hledají mezi členy posádky jakýkoliv náznak žluté zimnice. Po půlnoci si jeden z australských námořníků všiml, jak se německý kapitán pokoušel hodit něco přes palubu. Byly to lodní dokumenty a velká šifrovací kniha: *Handelsverkehrsboek* neboli HVB, která byla na palubě každé německé obchodní lodi. Kniha obsahovala šifry signálů používaných německým obchodním loďstvem

* Kopie šifrovací knihy SKM, která byla uložena v Národním archivu (č. 151), nebyla znečištěna od mořské vody – Christopher Andrew píše ve své knize *Secret Service: The Making of the British Intelligence Community* (Heinemann, Londýn, 1985), že Rusové prostě předali Britům suchou šifrovací knihu z kapitánova trezoru. Na fotografiích této šifrovací knihy SKM nejsou vidět žádná poškození od slané vody.

pro komunikaci se svým válečným loďstvem a s pobřežními základnami. Ne každá německá obchodní loď měla tuto kopii – jejich vlastnictví bylo omezené na osmnáct největších německých rejdařských společností, jejichž lodě byly vybaveny rádiem. Získání této šifrovací knihy HVB znamenalo, že kdokoli, kdo dokázal rozluštit šifry obchodního loďstva, mohl teoreticky číst zprávy i signální depeše Císařského námořnictva. První vydání bylo v roce 1913 dodané všem válečným lodím s rádiem, námořním velitelstvím a pobřežním stanicím. Šifra používala tisíce skupin skládajících se ze čtyř písmen a každá skupina reprezentovala nějaké slovo. Kniha byla zkopírována a odeslána do Londýna, kam dorazila ve druhé polovině října roku 1914. Že šifrovací kniha HVB padla do rukou nepříteli, to se německá zpravodajská služba dozvěděla až v listopadu roku 1914. Vyplývá to z rádiových depeší, které obsahovaly varování, že je tato kniha vyzrazena. Ale náhrada přišla až v roce 1916.

Znenadání pak potkalo Němce neštěstí potřetí. Druhý týden v říjnu probíhaly mezi Britským královským námořnictvem a německým loďstvem v severní části Lamanšského průlivu šarvátky. Bitva na Yseru se vedla za účelem kontroly pobřežních měst Dixmude a Dunkerque. Britské loďstvo ostřelovalo německé pozice z moře. Poté na ně zaútočily německé torpédoborce. 17. října kapitán Cecil Fox velel úkolovému uskupení, které tvořil lehký křižník HMS *Undaunted* a čtyři další torpédoborce: HMS *Lance*, *Legin*, *Lennox* a *Loyal*. Plul vstříc německému útoku a vjel přímo mezi čtyři německé torpédoborce: *S115*, *S117*, *S118* a *S119*. Ty se plavily kanálem s rozkazem, aby zde kladly miny. Lodím Britského královského námořnictva to trvalo méně než hodinu, než německá plavidla potopily. Poté kapitán lodi *S119* hodil přes palubu v okované truhle všechny tajné dokumenty. 30. listopadu vytáhla tuto truhlu jedna rybářská loď ve své síti. Obsahovala kopii šifrovací knihy VB, tzv. *Verkehrsbuch*, kterou obvykle používali vlajkoví důstojníci německého námořnictva.

Šifra obsahovala na sto tisíc pětimístných číselných skupin, z nichž každá měla svůj specifický význam. Byla určena po telegramy posílané do zahraničí válečným lodím, námořním atašé, velvyslanectvím a konzulátům. Používali ji vyšší námořní důstojníci s alternativním klíčem *Lambda*, ale co dělala tato kniha na palubě malého torpédoborce na začátku války, zůstalo tajemstvím. Během války spočíval její největší význam v tom, že umožňovala sledování komunikace mezi německými námořními atašé v Berlíně, Madridu, Washingtonu, Buenos Aires, Pekingu a Konstantinopoli. Tato šifrovací kniha byla ještě

důležitější než předchozí dvě, které byly ukořistěny v Austrálii a v Baltském moři.

Britská námořní zpravodajská služba prolamuje německé námořní šifry

Britské dešifrovací a signálové odposlouchávací operace byly v roce 1914 teprve v plenkách. To nemohlo být žádným překvapením, protože elektronická media, do nichž chtěli proniknout, byla také nová. Guglielmo Marconi dotáhl svůj vynález do konce až v roce 1907. V roce 1912 byl na *Titaniku* nainstalován vysokovýkonný radiotelegrafický vysílač, aby sloužil operačnímu provozu a vysílal „marconigramy“ cestujících. Byl to tehdy vrchol technické inovace.

Ve Staré budově Admirality v Londýně byla jedna velká místnost označená číslem „40“. Bylo to ústředí rodící se dešifrovací jednotky. Až do konce války ji nazývali prostě „Místnost 40“. A nikdy netrpěla nedostatkem rádiových depeší, které dostala ke zpracování. O tři roky dříve v roce 1911 udělal Britský výbor pro obranu Impéria prozíravé rozhodnutí. Německé podmořské komunikační kabely měly být přerušeny ihned po vypuknutí války. Členové výboru předpokládali, že to přinutí Němce, aby posílali své zprávy buď po komunikačních sítích jiných států nebo aby je zašifrovali a použili rádiové sítě, a nebyli tak závislí na kabelech. V obou případech platilo, že kdyby se Britům podařilo ukořistit šifrovací knihy nebo prolomit jejich šifry, mohli by tyto informace číst. To se ukázalo jako správné. Tři dny poté, co byla dne 4. srpna vyhlášena válka Německu, přerušili Britové pět německých transatlantických kabelů, které ležely na dně Lamanšského průlivu. Provoz rádiových šifrovaných zpráv se ihned navýšil. A protože každá zpráva byla zašifrovaná pomocí šifrovacích knih SKM, VB nebo HVB, měli důstojníci britských zpravodajských služeb a jejich civilní zaměstnanci obrovské množství materiálu ke zpracování. V Místnosti 40 údajně pojmenovali událost, při níž došlo k ukořistění tří německých šifrovacích knih, jako „zázračný záťah sítí“. Na počátku sloužilo k odposlechu rádiové zařízení, které používala Pošta, dále technika od Marconioho a od soukromých rádiových nadšenců. Ale když se ve Zpravodajském oddělení Admirality v Místnosti 40 poprvé objevily ukořistěné německé šifrovací knihy, nikdo z námořních důstojníků je nebyl schopen rozšifrovat.

Jednoduše řečeno, nikdo se dostatečně nevyznal v technikách luštění šifer. V této situaci začal první šéf tohoto oddělení, admirál Henry Oliver, tvrdě pracovat na náboru nových členů. Dříve velel navigační škole na starším křižníku britského královského námořnictva a také měl neortodoxní a akční přístup. Na začátku války byl v září roku 1914 odeslán do Antverp, aby zde pracoval se spojenci z oddělení belgických námořních zpravodajských služeb a s civilním personálem Antverpského přístavního úřadu. V přístavu uvízlo třicet osm německých obchodních lodí, zkonfiskovaných na základě válečných omezení. Oliver vstoupil spolu s Belgičany na paluby těchto lodí a u všech z nich prostě vyhodili do povětří jejich strojovny.

Na prvním místě si uvědomoval nutnost přísného utajení. Pro své nové oddělení dešifrování a signálového zpravodajství se rozhodl zaměřit se na dvě skupiny potenciálních nových členů. Obě považoval za důvěryhodné. První skupinu tvořili námořní důstojníci a kadeti z Royal Navy Colledge v Dartmouthu a v Osbornu. Druhou tvořili muži z Oxbridge, kteří studovali němčinu, matematiku a klasické předměty (starověkou řečtinu, latinu, antickou historii a filozofii). Zanedlouho vystřídal Olivera na pozici ředitele admirál sir William Reginald Hall, přezdívaný „Blinker“ kvůli cukání v obličeji, díky němuž se údajně občas rozzářil jako námořní signální lampa. Mezi novými lidmi, co měli vést Místnost 40 nebo se měli stát jejími příslušníky, byl ředitel námořního výcviku Alfred Ewing, který uvedl kryptografii jako svého koníčka, Nigel de Grey, jenž hovořil plynule francouzsky a německy a pracoval ve vydavatelství Heinemann, a William Montgomery, presbyteriánský duchovní překládající teologické knihy z němčiny.

Když dorazila šifrovací kniha SKM, byla předaná intendantovi Britského královského námořnictva kapitánu Charlesi Rotterovi, kterého právě získali pro práci v oddělení námořních zpravodajských služeb a který hovořil německy. Byl jedním z mála mužů, co pracovali pro Admiraltu a o šifrách a jejich prolamování něco věděli: Jako nadšený luštitel křížovek a matematik rychle rozpoznal, že se šifrování dle SKM provádělo za použití substituční tabulky. Každé písmeno abecedy bylo nahrazeno nějakým jiným. „Klíč“ uživateli sdělil, které písmeno abecedy se má nahradit kterým. Pokud mělo písmeno N nahradit H, vyplývalo z toho, že I bude nahrazeno písmenem O, J písmenem P a tak to pokračovalo v abecedním pořadí. Mazaný námořní intendant aplikoval to, čemu se v kryptologii říká Kerckhoffsův princip: Předpoklad, že

o daném kódu či systému šifrování víme vše, kromě klíče. Tento princip byl pojmenován po holandském kryptoografovi Augustu Kerckhoffsovi.*

Rotter věděl, že pokud by se používala stejná substituční tabulka dostatečně dlouho, byla by snadno prolomitelná metodou frekvenční analýzy. V angličtině je nejfrekventovanější písmeno E, po něm následuje T, pak A, I, N a tak dále. Pokud například obsahuje zašifrovaná zpráva, používající metodu jednoduché substituce, nejčastěji písmeno K, je velmi pravděpodobné, že K odpovídá písmenu E. Tři nejčastěji používaná písmena v němčině jsou E, N a I. Takže pokud se ve zprávách často opakují tři písmena G, W a C, je vysoce pravděpodobné, že odpovídají písmenům E, N a I. Pokud bychom chtěli klíč chránit, nesmíme používat stejnou substituční tabulku příliš dlouho, aby ji nebylo možné prolomit pomocí frekvenční analýzy.

Šifrovací kniha SKM ukořistěná z křižníku *Magdeburg* byla na stejném principu jako šifrovací knihy používané v jiných velkých loďstvech. Obsahovala 34 300 různých instrukcí, z nichž téměř všechny byly předem definované a na lodích se běžně používaly – „*Zahajuji palbu, Vytvářím kouřovou clonu, Vplouvám do přístavu po levoboku, Moje pozice je následující*“. Každou z tisícovek těchto instrukcí reprezentovala zvláštní skupina tří písmen. Zprávy rovněž používaly čtyři dodatečná písmena, alfa, beta, gama a ró, převzatá z řecké abecedy. To by znamenalo, že pro přenos zpráv nelze použít Morseovu abecedu, protože její základní verze o šestadvaceti písmenech tato písmena neobsahuje. Šifrovací kniha SKM byla doplněna o samostatnou substituční tabulku pro identifikaci a dekodování zvláštních písmen, jako je alfa nebo gama. S pomocí dostupných zachycených zpráv, ukořistěných německých šifrovacích knih a znalostí o substitučních tabulkách se Rotter dal do práce. Britské radiové odposlouchávací stanice na břehu Severního moře nyní začaly odposlouchávat německé námořní zprávy každý den. S pomocí šifrovací knihy SKM mu netrvalo dlouho, a mohl začít přepisovat některé z nich do prostého německého textu. Došlo mu, že tyto zprávy nebyly tak jednoduché, jak se zdálo na první pohled: Byly také před odesláním zašifrované. Rotter potřeboval číselný nebo abecední klíč, aby toto dodatečné zašifrování prolomil.

SKM byla kniha kódů, jakou používala námořnictva po celém světě již stovky let. Nejslavnějším příkladem použití této knihy je možná Nelsonův

* Americký matematik Claude Shannon to shrnul do tzv. „Shannonova pravidla“, když řekl „předpokládejme, že nepřítel systém zná“.

signál z bitvy u Trafalgaru: „*Anglie očekává, že každý muž splní svou povinnost*“ („*England expects that every man will do his duty*“). Každá signální vlajka používaná na HMS *Victory* reprezentovala nějaké číslo, a pokud byly použity po třech, tvořily trojice čísel představující různá slova uvedená v šifrovací knize. Kniha kódů přiřazovala trojiciferným kódům určité slovo, takže např. 253 znamenalo „England“, 269 znamenalo „expects“, 863 znamenalo „that“ atd. Pokud některé ze slov v knize chybělo, jako třeba povinnost („duty“), bylo nutné je hláskovat za použití jednoduché abecední substituční tabulky: 4 znamenalo D, 21 znamenalo U, 19 znamenalo T a 24 znamenalo Y. (Nelson chtěl původně říci „Anglie spoléhá“ („England confides“) namísto „očekává“ („expects“), ale protože „confides“ nebylo v knize kódů, bylo použito slovo „expects“, aby se ušetřil čas.)

Šifrovací kniha SKM byla komplikovanější verzí tohoto systému a velkému počtu obecně používaných slov a frází přiřazovala čtyřmístné šifry. Také obsahovala substituční tabulku, a pokud v ní některý výraz chyběl, bylo možné jej hláskovat písmeno za písmenem. Problémem bylo, že k dešifrování zachycených zpráv, které lidé z Místnosti 40 zpracovávali, šifrovací kniha nestačila, protože zprávy byly ještě zašifrovány pomocí další monoalfabetické substituce.

Abecední substituční tabulky jsou dvojího druhu: monoalfabetické a polyalfabetické. Luštění té první je jednodušší, protože používá jen jednu množinu substitucí; jinými slovy jedno písmeno abecedy je nahrazeno jiným. V okamžiku, kdy je k dispozici dost zašifrovaných zpráv, lze monoalfabetickou šifru prolomit přímou frekvenční analýzou – ta určí, které zašifrované písmeno odpovídá písmenu „E“, které „N“, které „I“ atd. Aby se tomu předešlo, používají komplikovanější šifry více substitučních tabulek měnících se podle toho, která z daných částí dokumentu se právě zpracovává. To je principem polyalfabetické substituce. Když Rotter zjistil, že prostý (tj. nezašifrovaný) text byl zašifrován pomocí knihy kódů SKM a poté ještě pomocí monoalfabetické substituce, byl jeho úkol jednodušší. Protože základním textem nebyla běžná němčina, ale čtyřmístné skupiny písmen z knihy kódů, frekvenční analýza, založená na četnosti písmen v němčině, nebyla k ničemu. Přesto byl tento problém celkem jednoduchý. V zašifrovaných německých zprávách, jež Britové zachycovali, bylo možné určit často se vyskytující skupiny a uhádnout jejich význam. Bylo možné identifikovat stejné vzory souhláska-samohláska-souhláska jak v šifrovací knize, tak i v zašifrované zprávě, protože Němci požadovali, aby se jejich kódovací skupiny daly snadno vyslovit. Rotter začal

od nuly, ale za tři týdny měl hotovou monoalfabetickou substituční tabulku, která byla klíčem ke knize SKM.

Německá přenosová stanice v Norddeichu, měště na německém pobřeží Severního moře, poskytla definitivní důkaz správnosti tohoto „klíče“. Začátkem října roku 1914 odvisíla série zpráv s podrobnostmi o pohybu flotily torpédoborců blížících se k holandskému pobřeží. Zprávy tvořily numericovou posloupnost a na začátku každé z nich se opakovaly sekvence: „S116, S107, S139 mířící směrem k Zuiderzee, následující pozice...“ a lišily se jen svými souřadnicemi. Takže jakmile se podařilo dešifrovat první zprávu, následovaly i ostatní. Potvrdilo se to, co Rotter předpokládal, totiž že Němci používali pro šifrování substituční tabulku. To mělo obrovský význam, protože takto měl k dispozici spolehlivý postup, jak číst německé zprávy. Znamenalo to také lepší pracovní podmínky, protože ředitel Britských námořních zpravodajských služeb měl takové obavy o utajení, že kromě intendanta nesměl být v místnosti nikdo jiný. Teprve v listopadu, když byla šifrovací substituční tabulka prolomena, směl opět pracovat se svými kolegy. Ti začali v době jeho nepřítomnosti s pokusy přijít na to, jak pracuje německá šifrovací kniha HVB. A pokud Britové potřebovali další zpravodajský materiál nebo ukořistěné šifrovací knihy, pak jim rok 1915 přinesl další překvapení.

Britské jednotky ukořistily a vzápětí zkonfiskovaly zavazadla a vybavení německého cestovatele a tajného agenta v Persii Williama Wassmuse. Aniž by je kdo otevřel, byla zavazadla odeslána do Londýna, kde admirál „Blinker“ Hall zjistil, že obsahovala výtisk německé diplomatické knihy kódů. Dalším zdrojem ukořistěných knih kódů byly německé ponorky, jež Britové potopili. Potápěči Britského královského námořnictva ze Záchraného oddílu admirality se soustředili na nedávno potopené lodi. Často pracovali v nervydrásajícím prostředí, kde plavali utopení němečtí námořníci. Lodní konstruktér E. C. „Dusty“ Miller byl expertem na záchranné operace Britského královského námořnictva. Popsal, jak to vypadalo, když se potápěli do ponorky v Kanálu. Do jejího trupu vstoupil dírou po výbuchu, kde narážel na plovoucí těla, dokud nenašel námořní šifrovací knihy v kovové krabici v malém kupé v ubikacích pro důstojníky. Pracovní podmínky byly obtížné: „Plavou tu malí žraloci a sežrali by cokoliv.“ Napsal:

V období páření přirozeně nesnesou žádného vetřelce. Častokrát, když mě pronásledovali, jsem jim nabídl botu a oni po ní vždy chňapli...

v ponorkách byly někdy podivné výjevy... našel jsem spoustu mořských úhořů, sedm až osm stop dlouhých a pět palců tlustých, a všichni hořečně žrali... tihle dokázali pěkně vylekat.²

Britové získávají v signálové válce převahu

„Jejich (Němců) hloupost byla větší než naše stupidita,“ zhodnotil německý pracovní přístup ke svému signálovému zpravodajství a k technickým chybám Britů Alastair Denniston, jeden z vyšších příslušníků štábu Místnosti 40.^{3*} Námořní válka mezi Británií a Německem v roce 1914 až 1915 se soustředila na tři priority. Tou první byla taktika blokády, kdy se obě strany snažily uzavřít nepřátelské loďstvo v jejich domovských základnách, jako je Kiel, Brémy, Portsmouth nebo Scapa Flow. Britové uvalili na Němce blokádu a bránili jejich námořním lodím v plavbě do Atlantiku. Britové chtěli, aby se jejich námořnictvo mohlo bez jakýchkoliv omezení plavit po klíčových trasách, jako byl například Lamanšský průliv. Druhou prioritou bylo pobřežní hlídkování, aby bylo možné zabránit ostřelování přístavů. A za třetí šlo o občasná ambiciózní gesta, jako třeba nasazení britských vojsk v Dardanelách. Válka na západní frontě se na jaře roku 1915 zasekla v patové situaci. Válečná loďstva jak Britů, tak i Němců vězela převážně ve svých přístavech díky obavám na obou stranách z katastrofální porážky. Palebná síla velkých bitevních lodí již byla na takové úrovni, že při neexistenci výkonných bombardérů byly tyto lodě téměř nezranitelné. Ohrozit je mohly jen ponorky nebo jiné bitevní lodě. Takže výsledek stěžejního námořního střetnutí by mohl rozhodnout o výsledku války, což vysvětluje oboustrannou váhavost britského či německého námořnictva.

Císařské námořnictvo se několikrát vydalo do Severního moře, aby se pokusilo vylákat Velké britské loďstvo na širé moře. Pokaždé ale bezvýsledně. Bitvy u Helgolandské zátoky, u Dogger Banku a u Jutska byly tři otevřené konfrontace: Ve srovnání s nimi existovala řada dalších příležitostí, kdy britské a německé lodě prostě jen propluly kolem sebe. Na přelomu let 1914 a 1915 prolomili analytici z Místnosti 40 šifru SKM. Zpočátku se dešifrované zprávy týkaly počasí nebo šlo o oznámení pozic jednotlivých německých lodí. Poté zjistili, že Němci posílali přesnější a pracovně důležitější zprávy – například o pohybu loďstva – na krátkých vlnách, které britské námořní zpravodajské

* Denniston se později stal prvním ředitelem britské Vládní školy kódování a šifrování.

služby nebyly schopny zachytit. Vysvětlení nebylo nijak obtížné. Byla to otázka alokace zdrojů. Na jaře roku 1915 začali Britové experimentovat se zařízením pro rádiové zaměřování a rádiové stanice byly postaveny v Lerwicku, Aberdeenu, Yorku, Flamborough Head a Birchingtonu. Hlavní britská odposlouchávací stanice, schopná zachytit krátkovlnná rádiová vysílání z německých lodí nebo vojenských jednotek na západní frontě, byla v Hunstantonu na pobřeží Norfolk. Naladit se na klíčová německá námořní vysílání na krátkých vlnách nebylo jednoduché, protože nebyl dostatek přijímacích zařízení a antény nebyly dostatečně velké. Takže na jeden víkend zadala Místnost 40 odposlouchávací stanici v Hunstantonu test. Bylo jim řečeno, aby přestali odposlouchávat rutinní vojenské zprávy, třeba ty od německých dělostřeleckých jednotek ležících za Ypres, ze stanovišť Zeppelinů v Belgii nebo situační zprávy od německých pěších jednotek, spekulující o tom, která britská brigáda se přesunula do zákopů v prostoru před nimi. Bylo jim řečeno, aby se soustředili pouze na německé Širokomořské loďstvo.

A během osmačtyřiceti hodin měli odpověď. Pohyby lodí v příštích dvou dnech se vysílaly na krátkých vlnách. Pro komunikaci mezi jednotlivými loděmi byla použita kombinace šifry SKM a mezi německou Admirálitou v Berlíně a vysokými důstojníky na moři byla použita šifra HVB. Pro Brity to znamenalo další průlom. S pokračující válkou se Němci k těmto praktikám uchýlovali stále častěji. V roce 1915 se jejich šifrovací klíč nezměnil po dobu tří měsíců, ale v roce 1916 se měnil o půlnoci každých 24 hodin. Přesto, díky obrovskému objemu zachyceného materiálu, několika ukořistěným šifrovacím knihám a znalosti, jak na to, byli lidé z Místnosti 40 obvykle schopni prolomit nový klíč do následujícího rána. Někdy to dokázali do dvou či tří hodin po půlnoci. Od října 1914 do února 1919 zachytili a vyluštili příslušníci Místnosti 40 odhadem 15 000 zpráv.

Námořníci německé flotily měli ve zvyku podávat zprávy o pozici každé ze svých lodí. Takto, díky více či méně přesným znalostem o počtu bitevních lodí, bitevních křižníků, křižníků a torpédoborců, které měla německá flotila, mohli Britové sestavit přehledný operační obraz o tom, co právě německé námořnictvo dělá: Jaké používá trasy, což naznačovalo, kde by mohly být položeny miny, jakou rychlostí se pohybovaly jejich lodě a kde

doplňovali palivo. Pak objevili ve strategii německého šifrování ještě jedno slabé místo. I když se ze zachycených zpráv dalo usoudit, že Císařské námořnictvo vědělo, že knihy kódů SKM byly zřejmě z křižníku *Magdeburg* ukořistěny, Němci byli se změnou kódů buď příliš pomalí nebo se jim to prostě nepodařilo. Kódy VB a HVB, jejichž knihy byly ukořistěny v říjnu roku 1914 v Lamanšském průlivu, byly změněny až v roce 1917.* Rozsah každé z těchto knih byl jedním z důvodů, proč jejich výměna nebyla jednoduchá a proč kódy zůstaly platné až do léta roku 1916. I poté posádky lodí zprvu odmítaly novou knihu kódů používat, protože její výměna byla příliš komplikovaná, takže *Flottenfunkspruchbuch* (kódová kniha flotily – FFB) nahradila v plném rozsahu kódy SKB až v květnu roku 1917. Němci si nebyli jisti, zda jsou knihy kódů SKM bezpečné – nebo zda vůbec byly z křižníku *Magdeburg* ukořistěny. Od roku 1914 bylo vedeno úřední vyšetřování ztráty knih kódů, na jehož základě se pak princ Jindřich Pruský, vrchní velitel baltických operací, písemně obrátil na vrchního velitele německého Širokomořského loďstva a sdělil mu, že považuje za jisté, že námořní mapy a knihy kódů ukořistili Rusové. Němci postupně odhalovali chyby v mapách a knihách kódů – pokud již padly do rukou nepřítele, bylo nutné je vyměnit a vybavit jimi všechny lodě i všechny námořní instituce na pevnině. Za druhé, někdy bylo obtížné nebo i nemožné zjistit, zda knihy kódů či mapy skutečně padly do rukou nepřítele, což pro Němce znamenalo dilema. Za předpokladu, že ukořistěny byly, mají se bez rozdílu změnit všechny knihy kódů? Nebo to risknout a nedělat nic? Samotný fakt, že kniha kódů HVB byla sama o sobě tak rozsáhlá a obsahovala více než 300 000 skupin písmen, byl jedním z důvodů, proč ji Němci prostě nezměnili. Dospěli k názoru, že logistická složitost této akce je obrovská. To, že se v první světové válce Němci spoléhali na knihy kódů, a dále to, že se po jejich vyzrazení dostalo do rukou Spojenců množství zpravodajských informací, mělo velký dopad na německé tvůrce i luštitelé šifer o deset let později, v době příprav na druhou světovou válku.

* O dvacet let později vypracovala Německá námořní monitorovací služba, tzv. B-Dienst, působící po první světové válce, zprávu ohledně ztráty knihy kódů z křižníku *Magdeburg*. Německá zpráva vypracovaná v roce 1934 korvetním kapitánem Kleinkampem zjistila, že ztráta knihy kódů SVB křižníku *Magdeburg* byla „katastrofální“. Hlavně proto, že německé námořnictvo neučinilo žádné kroky, aby staré šifry nahradilo novými, bezpečnějšími.

Operace německého námořnictva sloužící k prolamování šifer

Jedné noci roku 1914 na začátku války měl službu mladý německý námořní technik jménem Wilhelm Tranow. Byl na palubě ve vysílací místnosti bitevní lodi SMS *Pommern* třídy Deutschland, jedné z pěti největších válečných lodí první třídy německého námořnictva*. Radiostanice obdržela depeši z křižníku *Breslau*. Tranow ji předal veliteli flotily, ti ale odpověděli, že ji nedokážou přecíst. A Tranow, nadšenec do kryptoanalýzy**, šifer a jejich luštění, se rozhodl, že ji prolomí sám. Byl úspěšný. Předal dešifrovanou zprávu zpět svým velitelům a očekával, že mu poblahopřejí, nebo alespoň se ho zeptají, jak dokázal něco, co se nepodařilo rádiovým technikům flotily. Nestalo se ani jedno, ani druhé. Dostalo se mu přísného varování, aby se v budoucnu do těchto záležitostí nikdy nepletl.

Tato událost byla drobným, ale velmi ilustrativním příkladem přístupu Císařského námořnictva. Krátce po tomto incidentu Tranow požádal o svolení k rozhovoru s pracovníky zpravodajských služeb Císařského námořnictva. Jeho žádosti bylo vyhověno. *Nachrichtenabteilung* neboli „Oddělení zpráv“ bylo spíše známé pod zkratkou skládající se z jediného písmene – „N“. Admirál Tirpitz se od roku 1898 zuřivě bránil vzniku a financování takovéto zpravodajské instituce, takže v době vypuknutí první světové války měl její personál méně než deset zaměstnanců. Od roku 1914 se jejich počet značně zvýšil, ale nezlepšila se jeho operativní efektivita. Nejpresnější hodnocením činnosti tohoto oddělení během první světové války bylo, že na rozdíl od svého vojenského protějšku toho dosáhlo velmi málo.*** Částečně to bylo proto, že neměli k dispozici žádnou z ukořistěných knih kódů Britského královského námořnictva, a částečně proto, že britské námořnictvo vysílalo své zprávy nezašifrované. Věděli, kde se nachází německé loďstvo, ať už šlo o Lamanšský průliv, Severní moře či Atlantik, a v roce 1915 dávala Británie ráda najevo, že stále vládne všem mořím. Třetím důvodem, proč mělo oddělení „N“ tak hubené výsledky, bylo, že spoléhalo na dva hlavní zdroje zpravodajských informací.

* Všechny lodě v Císařském námořnictvu měly označení SMS, znamenající *Seiner Majestät Schiff* – loď Jeho Veličenstva

** Slovo kryptoanalýza pochází z řeckých slov *kryptós* – „skrytý“ a *analjein* – „uvolnit“ nebo „rozvázat“. Je to nauka o analýze informačních systémů za účelem studia skrytých aspektů systémů. Kryptoanalýza znamená tudíž prolamování kryptografických bezpečnostních systémů a získávání přístupu k obsahu zašifrovaných zpráv, když kryptografický klíč není známý.

*** Uvedené hodnocení získala tato sekce v roce 1916 po německém neúspěchu zachytit a dešifrovat jakoukoliv zprávu, která se týkala pohybu britského Velkého loďstva před bitvou u Jutska.